W&T

www.WuT.de

Anleitung

Inbetriebnahme und Anwendung

Microwall Gigabit

gültig für folgende Modelle:

#55210: Microwall Gigabit
(ab Firmware Version 1.52)

Release 1.02 11/2020

W&T

Irrtum und Änderung vorbehalten:

Da wir Fehler machen können, darf keine unserer Aussagen ungeprüft verwendet werden. Bitte melden Sie uns alle Ihnen bekannt gewordenen Irrtümer oder Missverständlichkeiten, damit wir diese so schnell wie möglich erkennen und beseitigen können.

Führen Sie Arbeiten an bzw. mit W&T Produkten nur aus, wenn sie hier beschrieben sind und Sie die Anleitung vollständig gelesen und verstanden haben. Eigenmächtiges Handeln kann Gefahren verursachen. Wir haften nicht für die Folgen eigenmächtigen Handelns. Fragen Sie im Zweifel lieber noch einmal bei uns bzw. Ihrem Händler nach!

Dieses Gerät enthält Softwarekomponenten, die unter einer oder mehreren Open-Source-Lizenzen stehen. Kopien dieser Lizenzen enthält der Anhang dieses Dokumentes sowie die folgende Webseite unter welcher auch der zugehörige Quelltext kostenlos heruntergeladen werden kann.

http://www.wut.de/e-5wwww-60-inde-000.php

Sie können den Quelltext auch für einen Zeitraum von drei Jahren nach letztmaliger Auslieferung von uns in Form eines Datenträgers zum Selbstkostenpreis beziehen. Bitte kontaktieren Sie uns hierzu unter info@wut.de.

Dieses Angebot gilt für jeden Empfänger dieser Information.

Einleitung

Die Microwall ist ein industrietauglicher IPv4-Router mit zwei 1000BaseT-Netzwerkanschlüssen und integrierter, whitelist-basierter Firewall. Sie bindet eine Netzwerkinsel z.B. mit Automatisierungskomponenten an ein übergeordnetes lokales Netzwerk an. Geeignete Filterregeln auf TCP/IP-Ebene schützen alle Netzwerke vor unberechtigter, unerwünschter und schädlicher Kommunikation.

Inhalt

1 Rechtliche Hinweise und Sicherheit

1.1 Rechtliche Hinweise

Warnhinweiskonzept

Diese Anleitung enthält Hinweise, die zu Ihrer persönlichen Sicherheit sowie zur Vermeidung von Sachschäden beachtet werden müssen. Die Hinweise sind durch ein Warndreieck hervorgehoben. Je nach Gefährdungsstufe werden die Warnhinweise in abnehmender Reihenfolge wie folgt dargestellt:

⚠GEFAHR
kennzeichnet eine Gefährdung, die Tod oder schwere Körperverletzung zur Folge hat, wenn keine entsprechenden Vorsichtsmaßnahmen getroffen werden.

⚠WARNUNG
kennzeichnet eine Gefährdung, die Tod oder schwere Körperverletzung zur Folge haben kann, wenn keine entsprechenden Vorsichtsmaßnahmen getroffen werden.

⚠VORSICHT
kennzeichnet eine Gefährdung, die eine leichte Körperverletzung zur Folge haben kann, wenn keine entsprechenden Vorsichtsmaßnahmen getroffen werden.

⚠ACHTUNG
kennzeichnet eine Gefährdung, die Sachschaden zur Folge haben kann, wenn keine entsprechenden Vorsichtsmaßnahmen getroffen werden.

Bei Vorliegen mehrerer Gefährdungsstufen wird immer der Warnhinweis der jeweils höchsten Stufe verwendet. Wenn in einem Warnhinweis mit dem Warndreieck vor Personenschäden gewarnt wird, dann kann im selben Warnhinweis zusätzlich eine Warnung vor Sachschäden angefügt sein.

Qualifiziertes Personal

Das in dieser Anleitung beschriebene Produkt darf nur von

Personal installiert und in Betrieb genommen werden, das für die jeweilige Aufgabenstellung qualifiziert ist.

Es muss die für die jeweilige Aufgabenstellung zugehörige Dokumentation beachtet werden, insbesondere die darin enthaltenen Sicherheits- und Warnhinweise.

Qualifiziertes Personal ist aufgrund seiner Ausbildung und Erfahrung befähigt, im Umgang mit den beschriebenen Produkten Risiken zu erkennen und mögliche Gefährdungen zu vermeiden.

Entsorgung

Elektronische Geräte dürfen nicht über den Hausmüll entsorgt werden, sondern müssen einer fachgerechten Elektroschrott-Entsorgung zugeführt werden.

Die vollständigen Konformitätserklärungen zu den in der Anleitung beschriebenen Geräten finden Sie über die jeweiligen Internet-Datenblattseite auf der W&T-Homepage unter http://www.wut.de.

Symbole auf dem Produkt

Symbol	Erklärung
	CE-Kennzeichnung Das Produkt entspricht den Anforderungen der zutreffenden EU-Richtlinien.
	WEEE-Kennzeichnung Das Produkt darf nicht über den Hausmüll, sondern muss gemäß den am Installationsort gültigen Entsorgungsvorschriften für Elektroschrott entsorgt werden.

1.2 Sicherheitshinweise

Allgemeine Hinweise

Diese Anleitung richtet sich an den Installateur der beschriebenen Microwall und muss vor Beginn der Arbeiten gelesen und verstanden werden. Die Geräte dürfen ausschließlich durch qualifiziertes Personal installiert und in Betrieb genommen werden.

Bestimmungsgemäßer Gebrauch

⚠GEFAHR

Die Microwall ist ein industrietauglicher IPv4-Router mit zwei 1000BaseT-Netzwerkanschlüssen und integrierter, whitelistbasierter Firewall. Sie bindet eine Netzwerkinsel an ein übergeordnetes lokales Netzwerk an. Geeignete Filterregeln auf TCP/IP-Ebene schützen alle Netzwerke vor unberechtigter, unerwünschter und schädlicher Kommunikation.

Nicht bestimmungsgemäß ist jegliche andere Verwendung oder eine Modifizierung der beschriebenen Geräte.

Elektrische Sicherheit

⚠WARNUNG

Vor Beginn jeglicher Arbeiten an der Microwall muss die Stromzufuhr durch geeignete Maßnahmen vollständig getrennt werden. Achten Sie darauf, dass das Gerät nicht versehentlich wieder eingeschaltet werden kann!

Die Microwall darf nur in geschlossenen und trockenen Räumen eingesetzt werden.

Das Gerät sollte keinen hohen Umgebungstemperaturen und einer direkten Sonnenbestrahlung ausgesetzt werden, sowie nicht in der Nähe von Wärmequellen betrieben werden. Bitte beachten Sie hierzu die Einschränkungen in Hinblick auf die maximale Umgebungstemperatur.

Lüftungsöffnungen müssen frei von jeglichen Hindernissen sein. Es sollte ein Abstand von 10-15 cm der Microwall zu benachbarten Wärmequellen eingehalten werden.

Eingangsspannung und Ausgangsströme dürfen die Nennwerte der Spezifikation nicht überschreiten.

Bei der Installation ist darauf zu achten, dass keine vagabundierenden Drähte durch die Lüftungsschlitze der Microwall ins Innere des Gehäuses ragen. Stellen Sie sicher, dass keine einzelnen Drähte von Litzen abstehen, sich die komplette Litze in der Klemme befindet und die Schrauben der Anschlussklemmen fest angeschraubt sind. Ziehen Sie die Schrauben von unbenutzten Anschlussklemmen fest.

Das zur Versorgung der Microwall verwendete Netzteil muss zwingend eine sichere Trennung der Niederspannungsseite gegen das Versorgungsnetz gemäß EN62368-1 gewährleisten und „LPS“-Eigenschaft besitzen.

EMV

⚠ACHTUNG

Zum Netzwerkanschluss der Microwall dürfen ausschließlich geschirmte Netzwerkkabel verwendet werden.

Die Microwall erfüllt in diesem Fall die industriellen Störfestigkeitsgrenzwerte und die strengeren Emissionsgrenzwerte für Haushalt und Kleingewerbe. Daher gibt es keine EMV-begründeten Einschränkungen in Hinblick auf die Verwendbarkeit der Geräte in diesen Umgebungen.

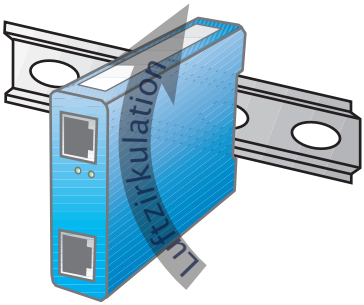
Die vollständigen Konformitätserklärungen zu den in der Anleitung beschriebenen Geräten finden Sie über die jeweiligen Internet-Datenblattseite auf der W&T-Homepage unter http://www.wut.de.

2 Hardware, Schnittstellen und Anzeigen

- Hardware-Installation
- Spannungsversorgung
- Netzwerkschnittstellen
- Service-Taster

2.1 Hardware-Installation

Die Microwall ist mechanisch für die Montage auf einer Standard Hutschiene konzipiert. Hierbei, sowie auch bei alternativen Montagearten, muss die skizzierte Luftzirkulation gewährleistet sein.



Der Montageort muss den Security-Anforderungen der jeweiligen System-Umgebung angepasst sein. Physikalischer Zugriff auf die Microwall ermöglicht einem potenziellen Angreifer das Gerät außer Betrieb zu nehmen oder auch über den Service-Taster das Passwort zu ersetzen.

2.2 Spannungsversorgung

Die Spannungsversorgung der Microwall erfolgt alternativ über PoE oder ein externes Netzteil. Gleichzeitiger Anschluss beider Versorgungen ist nicht zulässig. Die Stromaufnahme kann den technischen Daten entnommen werden.

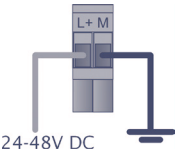
2.2.1 PoE-Versorgung

Die Microwall kann über die Schnittstelle *Network 1* (gelb) per PoE entsprechend IEEE802.3af versorgt werden. Sie ist ein Gerät der PoE-Leistungsklasse 2 (Leistungsaufnahme von 3,84W bis 6,49W).

2.2.2 Externe Spannungsversorgung

Alternativ zur PoE-Versorgung, kann die Microwall über die an der Gehäuseunterseite befindliche, steckbare Schraubklemme extern versorgt werden. Die verwendete Gleichspannung muss in folgendem Bereich liegen und die Polarität muss beachtet werden:

- Gleichspannung: 24V (-10%) - 48V (+10%)



⚠WARNUNG

Für die externe Versorgung der Microwall 55211 darf ausschließlich ein potenzialfreies Netzteil verwendet werden. Dessen Bezugsmasse für die Ausgangsspannung darf keine *direkte Anbindung an den Schutzleiter haben.*

*Das zur Versorgung der Microwall verwendete Netzteil muss zwingend eine sichere Trennung der Niederspannungsseite gegen das Versorgungsnetz gemäß EN*62368*-1 gewährleisten und „LPS“-Eigenschaft besitzen.*

2.3 Netzwerkschnittstellen

Die Microwall verfügt über zwei Netzwerkschnittstellen: *Network 1* (gelb) und *Network 2* (grün).

Network 1 (gelb) dient dem Anschluss an das übergeordnete Netzwerk, in welches das Inselnetzwerk am Anschluss *Network 2* (grün) integriert werden soll.

Die Inbetriebnahme mit den Werkseinstellungen sowie eine eventuelle Versorgung per PoE sind nur über *Network 1* (gelb) möglich.

2.3.1 Gigabit-Ethernet Eigenschaften

Beide Gigabit-Ethernet-Anschlüsse verfügen über folgende Eigenschaften:

RJ45-Buchse, geschirmt
Anschlüsse an die Netzwerk-Infrastruktur erfolgen über geschirmte Patchkabel mit maximal 100m Länge

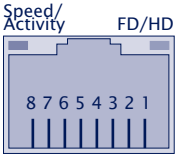
Autocrossing / Auto MDI-X
Die Sende-/Empfangsleitungen des angeschlossenen Gerätes werden automatisch erkannt. Es können sowohl 1:1 verdrahtete wie gekreuzte Patchkabel verwendet werden.

Galvanische Trennung
Gegenüber der Versorgungsspannung besteht eine galvanische Trennung mit mindestens $500V_{rms}$

Auto-Negotiation
Übertragungsgeschwindigkeit und Duplex-Verfahren werden mit dem angeschlossenen Gerät automatisch ausgehandelt. Zur Vermeidung von Problemen wie z.B. Duplex-Mismatch, empfehlen wir die angeschlossenen Geräte ebenfalls im Modus Auto-Negotiation zu betreiben.

2.3.2 Link-Status

Der Link-Status wird durch in die RJ45-Buchsen integrierte LEDs signalisiert.



Speed/Activity (grün/orange)
Grün = 1000MBit/s Link
Grün blinken = 1000MBit/s Link und Datenverkehr

Orange = 100MBit/s Link
Orange blinken = 100MBit/s Link und Datenverkehr

FD/HD (gelb)
ON = Full-Duplex
OFF = Half-Duplex

2.4 System- und Error-LED

2.4.1 System-LED (grün)

ON: Signalisiert normale Betriebsbereitschaft.

Blinken: Die Microwall führt einen Neustart durch oder erhält eine neue Firmware.

2.4.2 Service-LED (rot)

Die Service-LED dient zur Signalisierung der über den Service-Taster steuerbaren Funktionen *Notzugang* und *Factory-Default-Reset*.

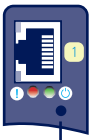
Langsames Blinken: Der Service-Taster wurde zwischen 3,5s und 10s betätigt. Der Notzugang der Microwall ist aktiviert.

Weitere Informationen zum Notzugang enthält das Kapitel *Notzugang*.

Der Notzugang öffnet einen nicht-passwortgeschützten HTTPS-Zugang (TCP-Port 446) mit der Möglichkeit, das aktuelle Passwort zu überschreiben. Starten Sie den Notzugang daher nur in einer entsprechend sicheren Umgebung (z.B. Direktverbindung zu einem Konfigurations-PC).

Schnelles Blinken: Der Service-Taster wurde länger als 10s betätigt und die Microwall bereitet einen Reset auf die Werkseinstellungen vor. Wird der Service-Taster weiterhin betätigt, erfolgt nach insgesamt 20s ein Reset auf die Werkseinstellungen.

2.5 Service-Taster



Der Service-Taster ist zur Vermeidung von Fehlbedienungen versenkt auf der Frontseite der Microwall zugänglich. Die Betätigung erfolgt mit einem geeigneten, spitzen Gegenstand (z.B. Büroklammer).

Über den Service-Taster werden die folgenden Aktionen ausgelöst:

Reset/Neustart
Kurze Betätigungen des Tasters zwischen 0,2 und 3,5s löst einen Neustart der Microwall aus.

Start des Notzugangs
Nach Betätigung des Tasters für mehr als 3,5s, beginnt die Error-LED mit langsamem Blinken. Wird der Taster in dieser Phase und vor Ablauf von 10s gelöst, ist der Notzugang der Microwall auf beiden Netzwerkanschlüssen über TCP-Port 446 aktiviert. Erneutes kurzes Betätigen führt einen Reset durch und beendet den Notzugang.

Weitere Informationen zum Notzugang enthält das Kapitel *Notzugang*.

Der Notzugang öffnet einen nicht-passwortgeschützten HTTPS-Zugang (TCP-Port 446) mit der Möglichkeit, das aktuelle Passwort zu überschreiben. Starten Sie den Notzugang daher nur in einer entsprechend sicheren Umgebung (z.B. Direktverbindung zu einem Konfigurations-PC).

Reset auf Werkseinstellung
Bei Betätigung des Service-Tasters für mehr als 10s startet die Service-LED mit schnellem Blinken und signalisiert die Vorbereitung zu einem Factory-Default-Reset. Bei weiterem Halten der Taste, wird die Microwall nach 20s auf die Werk-

seinstellung zurückgesetzt. Ein Lösen des Service-Tasters während die Service-LED schnell blinkt (Zeitfenster 10-20s) führt zu einem Abbruch des Factory-Default-Resets. Die Microwall fährt mit dem Standard-Betrieb der aktuellen Konfiguration fort.

Durch einen Reset auf die Werkeinstellung gehen alle *vorgenommenen Einstellungen (Filterregeln, IP-Parameter, Log-Dateien ...) verloren. Die Wiederinbetriebnahme muss wie im Kapitel* Inbetriebnahme *beschrieben erfolgen.*

3 Inbetriebnahme

Die Inbetriebnahme kann ausschließlich über die Schnittstelle *Network 1* (gelb) erfolgen. Im ersten Schritt wird die für den initialen Zugriff notwendige IP-Adresse zugewiesen. Der anschließende Browserzugriff führt auf die initiale Webseite zur Konfiguration der für den Betrieb benötigten Basis-Parameter inklusive dem Systempasswort.

- IP-Vergabe per DHCP
- Einstellung der IP-Adresse mit dem Management-Tool *WuTility*
- Ändern der IP-Parameter per Web-Based-Management
- Erstzugriff per Browser

3.1 IP-Vergabe per DHCP

In Netzwerkumgebungen mit DHCP-Unterstützung und einem dynamischen Adresspool, erhält die Microwall die folgenden IP-Basisparamter automatisch über den Anschluss *Network 1*.

- IP-Adresse
- Subnetmask
- Gateway-Adresse
- DNS-Server

Die für die Erstinbetriebnahme erforderlichen weiteren Parameter werden nach der IP-Vergabe über die initiale Webseite mit Hilfe eines Browsers vorgenommen. Informationen hierzu finden Sie im Kapitel *Initiale Webseite der Erstinbetriebnahme*.

Mit Anschluss des Interfaces Network 1 *an das Netzwerk ist die initiale Webseite zur Vergabe des Systempasswortes über die Default-IP oder der per WuTility bzw. DHCP vergebenen IP-Adresse erreichbar. Stellen Sie sicher, dass bis zur Passwortvergabe auf der initialen Webseite keine unberechtigten Zugriffe auf die Microwall erfolgen (z.B. durch eine Inbetriebnahme mit einer Direktverbindung zu dem jeweiligen PC).*

Für operativen Einsatz der Microwall empfehlen wir den Betrieb mit einer statischen IP-Adresse. Besonders im Modus Standard-Router erfordert ein Wechsel der IP-Adresse durch den DHCP-Server ansonsten eine Anpassung aller statischen Routen in den über die Microwall kommunizierenden Hosts. Weitere Informationen enthält das Kapitel Modus Standard-Router.

3.2 Erstvergabe der IP-Parameter mit WuTility

Das Windows-Tool *WuTility* unterstützt ab der Version 4.52 die Inventarisierung und das Management der Netzwerkbasis-parameter der Microwall

- IP-Adresse
- Subnetmask
- Gateway-Adresse
- DNS-Server

Es müssen WuTility-Versionen >= 4.52 verwendet werden.

Mit Anschluss des Interfaces Network 1 *an das Netzwerk ist die initiale Webseite zur Vergabe des Systempasswortes über die Default-IP oder die per WuTility vergebene IP-Adresse erreichbar. Stellen Sie sicher, dass bis zur Passwortvergabe auf der initialen Webseite keine unberechtigten Zugriffe auf die Microwall erfolgen (z.B. durch eine Inbetriebnahme mit einer Direktverbindung zu dem jeweiligen PC).*

Für die Vergabe der IP-Adresse müssen sich der PC und das Interface *Network 1* der Microwall im gleichen physikalischen Netzwerk befinden.

Installation von *WuTility*

Den Download-Link für das Windows-Installations-Paket der jeweils aktuellen Version von *WuTility* finden Sie auf unserer Webseite unter

https://www.wut.de/wutility

Der Start erfolgt nach der Installation über

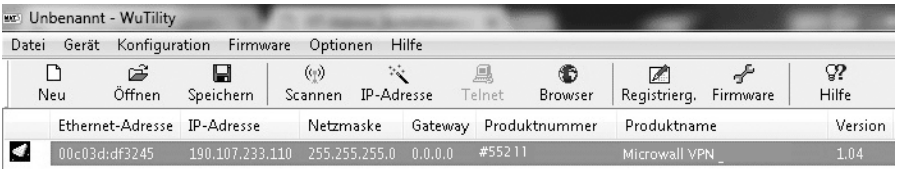
Start → Programme → Wutility Version 4 → WuTility

Start des Vergabe-Dialogs

Stellen Sie sicher, dass das Interface *Network 1* der Microwall und der verwendete Rechner an das gleiche physikalische Netzwerk angeschlossen sind. Beim Start durchsucht *WuTility* automatisch das lokale Netzwerk nach angeschlossenen W&T

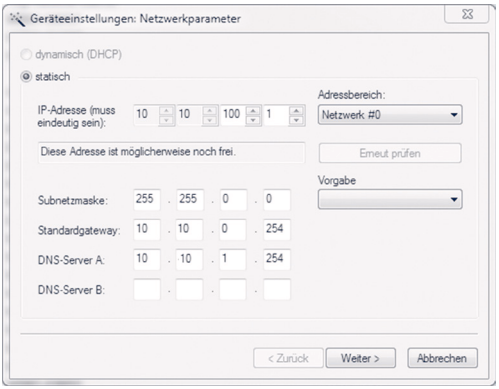
Netzwerkgeräten und erzeugt eine Inventarliste. Dieser Suchvorgang lässt sich beliebig oft durch Betätigen des Buttons *Scannen* wiederholen:

Innerhalb der Inventarliste ist die gewünschte Microwall über ihre MAC-Adresse identifizierbar. Ab Werk lautet die IP-Adresse 190.107.233.110.



Markieren Sie die gewünschte Microwall und betätigen dann den Button *IP-Adresse:*

Geben Sie die gewünschten Werte für IP-Adresse, Subnetmaske, Gateway und DNS-Server ein.



Mit Betätigung des Buttons *Weiter*, werden die Netzwerk-Parameter von der Microwall gespeichert.

Die IP-Vergabe mit WuTility kann so lange wiederholt werden, bis die Microwall über die initiale Webseite ein Systempasswort erhalten hat. Anschließend ist eine Änderung der IP-Pa-

rameter nur noch über das Standard Web-Based-Management möglich.

Die für die Erstinbetriebnahme erforderlichen weiteren Parameter werden über eine initiale Webseite mit Hilfe eines Browsers vorgenommen. Informationen hierzu finden Sie im Kapitel *Initiale Webseite der Erstinbetriebnahme*.

3.3 Inbetriebnahme über die Default-IP-Adresse

Im Auslieferungszustand sowie nach einem Reset auf die Werkseinstellungen lautet die Default-IP-Adresse des Interfaces *Network 1* 190.107.233.110.

Mit Anschluss des Interfaces Network 1 *an das Netzwerk ist die initiale Webseite zur Vergabe des Systempasswortes über die Default-IP oder die per WuTility vergebene IP-Adresse erreichbar. Stellen Sie sicher, dass bis zur Passwortvergabe auf der initialen Webseite keine unberechtigten Zugriffe auf die Microwall erfolgen (z.B. durch eine Inbetriebnahme mit einer Direktverbindung zu dem jeweiligen PC).*

Die Inbetriebnahme mehrerer Microwalls über deren Default-IP kann nur nacheinander *erfolgen. Erst nachdem eine Microwall eine neue IP-Adresse erhalten hat, darf die nächste Microwall an das Netzwerk angeschlossen werden.*

Rechnerseitig muss hierfür die folgende Voraussetzung erfüllt sein:

- Der Netzwerkanschluss des verwendeten Rechners muss eine IP-Adresse im Bereich 190.107.233.0/24 haben und sich im gleichen physikalischen Subnetz (Collision Domain) mit der Microwall befinden. Die Änderung der IP-Adresse des Rechners erfordert Administratorrechte. Klären Sie IP-Änderungen im Vorfeld mit dem zuständigen Netzwerkadministrator ab.

Alle weiteren für die Erstinbetriebnahme erforderlichen Parameter werden anschließend über die initiale Webseite mit Hilfe eines Browsers vergeben. Informationen hierzu finden Sie im Kapitel *Initiale Webseite der Erstinbetriebnahme*.

3.4 Initiale Webseite der Erstinbetriebnahme

Nach der IP-Vergabe ist im Zuge der Erstinbetriebnahme ist ausschließlich die initiale Webseite verfügbar. Hier muss das für alle weiteren Konfigurationszugriffe benötigte Passwort der Microwall vergeben werden. Gleichzeitig können die IP-Basisparameter der beiden Netzwerkschnittstellen und die Betriebsart bestimmt werden.

Das Speichern der initialen Webseite ist mit keinerlei Kommunikationsfreigaben verbunden. Diese müssen anschließend in Form von ausdrücklichen Whitelist-Regeln formuliert werden.

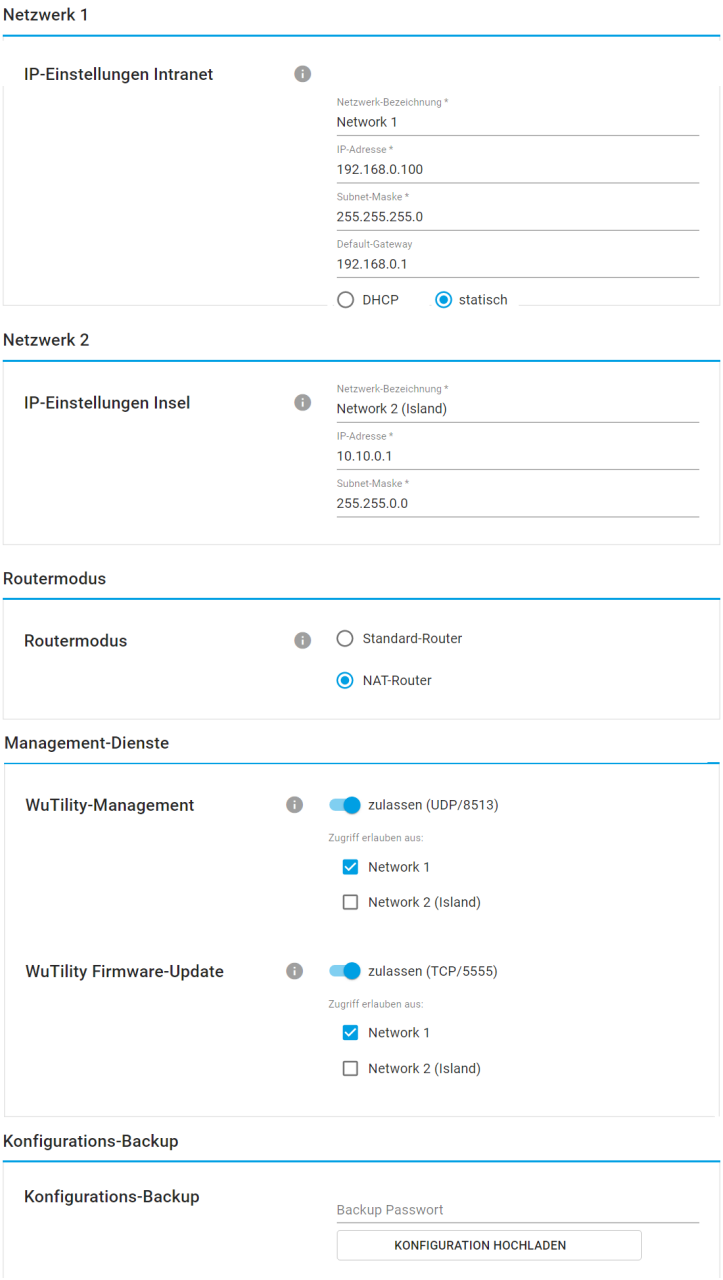
Mit Anschluss des Interfaces Network 1 *an das Netzwerk ist die initiale Webseite zur Vergabe des Systempasswortes über die Default-IP oder die per WuTility vergebene IP-Adresse erreichbar. Stellen Sie sicher, das bis zur Passwortvergabe auf der initialen Webseite keine unberechtigten Zugriffe auf die Microwall erfolgen (z.B. durch eine Inbetriebnahme mit einer Direktverbindung zu dem jeweiligen PC).*

Wurde die IP-Adresse über das Tool *WuTility* vergeben, markieren Sie dort die gewünschte Microwall und betätigen den Button *Browser*:

Soll der Zugriff über die Default-IP-Adresse der Microwall erfolgen, starten Sie auf dem aus IP-Sicht vorbereiteten PC einen Browser. In die Adressezeile geben Sie folgende URL ein:
https://190.107.233.110

Die Microwall ist ab Werk mit einem selbstsignierten Zertifikat ausgestattet. Entsprechende Warnungen des Browsers müssen bei Aufruf der initialen Webseite ignoriert und/oder quittiert werden. Nach der Inbetriebnahme kann das Default-Zertifikat durch ein individuelles Zertifikat ersetzt werden kann.

Alle Einstellungen der initialen Webseite sind später über das Standard Web-Based-Management änderbar.


Netzwerk 1
IP-Einstellungen Intranet
Netzwerk-Bezeichnung *
Network 1
IP-Adresse *
192.168.0.100
Subnet-Maske *
255.255.255.0
Default-Gateway
192.168.0.1
DHCP
statisch
Netzwerk 2
IP-Einstellungen Insel
Netzwerk-Bezeichnung *
Network 2 (Island)
IP-Adresse *
10.10.0.1
Subnet-Maske *
255.255.0.0
Routermodus
Routermodus
Standard-Router
NAT-Router
Management-Dienste
WuTility-Management
zulassen (UDP/8513)
Zugriff erlauben aus:
Network 1
Network 2 (Island)
WuTility Firmware-Update
zulassen (TCP/5555)
Zugriff erlauben aus:
Network 1
Network 2 (Island)
Konfigurations-Backup
Konfigurations-Backup
Backup Passwort
KONFIGURATION HOCHLADEN

Loginpasswort (Pflichtfeld)
Vergeben Sie das Passwort für alle Konfigurations-/Steuerzugänge der Microwall. Wir empfehlen Passwörter mit einer Mindestlänge von 15 Zeichen, bestehend aus Groß- und Kleinbuchstaben, Ziffern sowie Sonderzeichen. Die Maximallänge des Passwortes ist 51 Zeichen. Ein Betrieb ohne Passwort ist nicht möglich.

Es existiert kein Default- oder Master-Passwort. Ein verlorenes Passwort kann nur über den per Service-Taster aktivierbaren Notzugang oder einen Reset auf die Werkseinstellungen zurückgesetzt werden.

Network 1 (gelb)
Legen Sie fest, ob der Anschluss mit einer statischen IP-Adresse arbeitet oder die IP-Parameter per DHCP bezogen werden.

Im statischen Betrieb vergeben Sie die IP-Parameter für den Anschluss *Network 1* (gelb).

Für operativen Einsatz der Microwall empfehlen wir den Betrieb mit einer statischen IP-Adresse. Besonders im Modus Standard-Router erfordert ein Wechsel der IP-Adresse durch den DHCP-Server ansonsten eine Anpassung aller statischen Routen in den über die Microwall kommunizierenden Hosts. Weitere Informationen enthält das Kapitel Modus Standard-Router.

Network 2 (grün)
Vergeben Sie die IP-Parameter für den Anschluss *Network 2* (grün). Die Net-IDs von *Network 1* und *Network 2* müssen unterschiedlich sein.

Befinden sich im *Network 2* weitere Router in entfernte Netze, können diese später in den Netzwerkeinstellungen des Web-Based-Management über statische Routen konfiguriert werden.

Betriebsart (Pflichtfeld)
Wählen Sie die gewünschte Betriebsart der Microwall. Weitere Informationen hierzu finden Sie im Kapitel *Betriebsarten und Regelkonfiguration.*

Nach korrekter Eingabe aller Parameter wird der Button Speichern aktiviert und die Eingaben können gespeichert werden. Sie werden automatisch auf die Startseite der Microwall weitergeleitet.

Management-Dienste
Konfigurieren Sie, ob und aus welchen Netzwerken die Microwall über das Management-Tool WuTility erreichbar ist und ob hierüber Firmware-Updates durchgeführt werden können.

Für den operativen Betrieb werden beide Dienste nicht zwingend benötigt. Firmware-Updates können jederzeit auch über die die Weboberfläche im Menüzweig Wartung erfolgen.

Zur Verhinderung von angriffsvorbereitender Informationsbeschaffung und zur Verkleinerung der Angriffsfläche empfehlen wir deshalb, diese Option in kritischen Umgebungen zu deaktivieren.

Konfigurations-Backup
Erlaubt das Hochladen eines von einer anderen Microwall gesicherten Konfigurations-Backups. Sollte die Backup-Datei mit einem Passwort gesichert sein, muss dieses vor Betätigung des Upload-Buttons in das Feld Backup-Passwort eingegeben werden. Nach erfolgreicher Prüfung der Datei wird deren Inhalt übernommen und die Microwall arbeitet nach einem automatischen Neustart mit den neuen Parametern.

Backup-Dateien enthalten auch die neue IP-Adresse der Microwall. Um einen IP-Konflikt zu vermeiden, stellen Sie vor dem Upload sicher, dass die ursprüngliche oder eine zuvor programmierte Microwall nicht mehr an das Netzwerk angeschlossen sind.

Details zu Konfigurations-Backups enthält das Kapitel *Up-/Download von Konfigurations-Backups*

4 Web-Based-Management

Die Konfiguration der Microwall ist ausschließlich verschlüsselt per HTTPS möglich. Das WBM (Web-Based-Management) arbeitet sessionorientiert. Vorgenommene Änderungen auf den jeweiligen Seiten werden mit dem Speichern-Button sofort gespeichert und gültig.

- Navigation innerhalb des WBM

4.1 Start und Navigationskonzept des WBM

Um auf das WBM der Microwall zuzugreifen, benötigen Sie einen aktuellen Internet-Browser. Session-Cookies, Javascript und Websockets müssen unterstützt werden bzw.aktiviert sein.

Die Konfiguration ist ausschließlich verschlüsselt über HTTPS möglich. Ab Werk ist der Standardport 443 vorkonfiguriert.

Starten Sie Ihren Browser und geben die IP-Adresse der Microwall und gegebenenfalls die zu verwendende Portnummer ein.

https://[IP-Adresse]:[Portnummer]

4.1.1 Navigationskonzept der Microwall

Das WBM der Microwall arbeitet sessionorientiert über ein passwortgeschütztes Login. Ein Betrieb ohne Passwort ist nicht möglich.

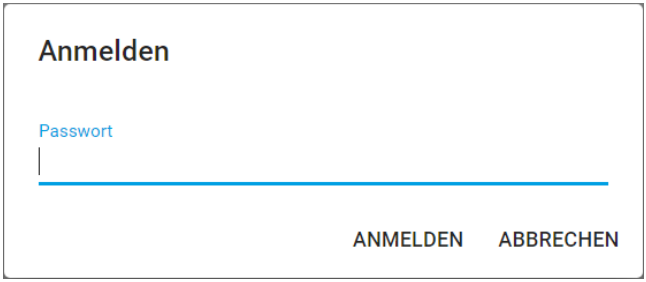
Nach dem Login werden vorgenommene Änderungen mit Betätigung des Buttons *Speichern* auf der jeweiligen Seite sofort übernommen. Sollte die Übernahme der Parameter einen Neustart der Microwall erfordern, erfolgt nach Betätigung von *Speichern* ein entsprechender Hinweis.

Das Beenden einer Konfigurations-Session erfolgt über den Button *Abmelden*.

4.2 Anmelden/Abmelden

Die Startseite der Microwall bietet nur die Möglichkeit der Passwort-Eingabe für das Login sowie die Umschaltung der Oberflächensprache über das Flaggensymbol.

4.2.1 Anmelden



Geben Sie das Passwort ein und betätigen den Button *Anmelden*. Nach erfolgreichem Login steht der erweiterte Navigationsbaum mit allen Konfigurationsmöglichkeiten zur Verfügung.

Zum Schutz vor Brute-Force-Attacken ist die Passwort-Eingabe mit einem eskalierenden Timeout geschützt. Nach jeder Fehleingabe des Passwortes ist die erneute Eingabe erst nach einem sich mit jedem Versuch verdoppelnden Timeout möglich.

4.2.2 Abmelden

Zum Beenden einer Konfigurations-Session betätigen Sie den Button *Abmelden*.

4.3 Hilfe und Beschreibungstexte

Sofern die einzelnen Konfigurationspunkte nicht selbsterklärend sind, enthalten die zugeordneten Infosymbole die nötigen Beschreibungen, Erklärungen und Hinweise.

Detailinformationen zu den Betriebsarten und den Freigaberegeln enthält diese Anleitung im Kapitel *Betriebsarten und Regel konfiguration*.

5 Betriebsarten und Regel Konfiguration

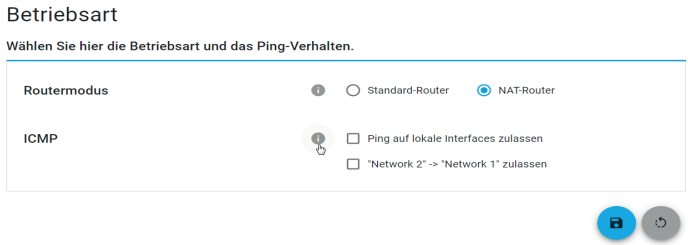
- Modus NAT-Router
- Modus Standard-Router
- Regel-Konfiguration und Labels
- IP-Inventare

5.1 Modus NAT-Router

Im Modus NAT-Router bindet die Microwall das Insel-Netzwerk am Anschluss *Network 2* (grün) über eine feste IP-Adresse des übergeordneten Netzwerks am Anschluss *Network 1* (gelb) an. Die Betriebsart ist vergleichbar zu vielen Standard DSL-Routern, welche das heimische Netzwerk über nur eine öffentliche IP-Adresse an das Internet anbinden.

Die IP-Adressen der Insel-Hosts werden im übergeordneten Netzwerk durch die dortige IP-Adresse der Microwall ersetzt und sind somit zu keinem Zeitpunkt im Intranet sichtbar. Der Insel-IP-Bereich kann im NAT-Modus völlig frei gewählt werden. Auch mehrere Inseln mit jeweils identischen IP-Bereichen können auf diese Weise gleichzeitig an das Unternehmens-Intranet angebunden werden. Ein Eingriff in dessen Routing-Konzept ist nicht erforderlich.

Aktivieren Sie die Betriebsart *NAT-Router* über den Menübaum unter *Firewalleinstellungen -> Betriebsart* und legen Sie die Behandlung von ICMP Echo Requests/Replies (ping) auf die lokalen Interfaces sowie die Weiterleitung anderer ICMP-Datagramme fest.



Über den Button *Speichern* wird der Modus *NAT-Router* aktiviert und der zugehörige Regel-Satz geladen.

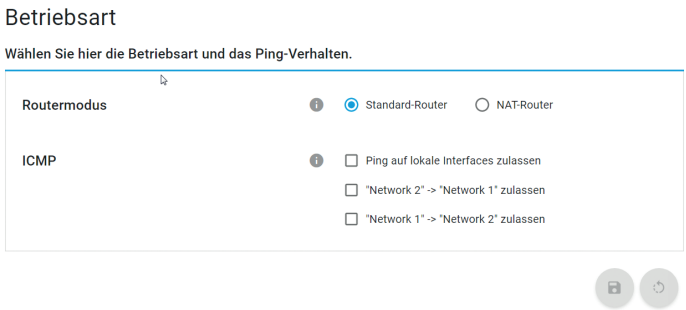
5.2 Modus Standard-Router

Im Modus Standard-Router trennt die Microwall das Inselnetzwerk am Anschluss *Network 2* (grün) vom Unternehmensintranet am Anschluss *Network 1* (gelb). Das Inselnetzwerk wird zu einem *offiziellen* Subnetz der intranetseitigen Infrastruktur.

Intranetseitig muss der Pfad in das Inselnetz den beteiligten Hosts in der Regel als statische Route bekannt gemacht werden.

Ist das Inselnetz ein Randnetz ohne Verbindung in weiterführende Netze, wird auf den Insel-Hosts die lokale IP-Adresse der Microwall als Standard-Gateway konfiguriert. Existieren im Inselnetz weitere Router in andere Netze, so müssen diese Pfade allen Insel-Hosts als statische Route bekannt gemacht werden.

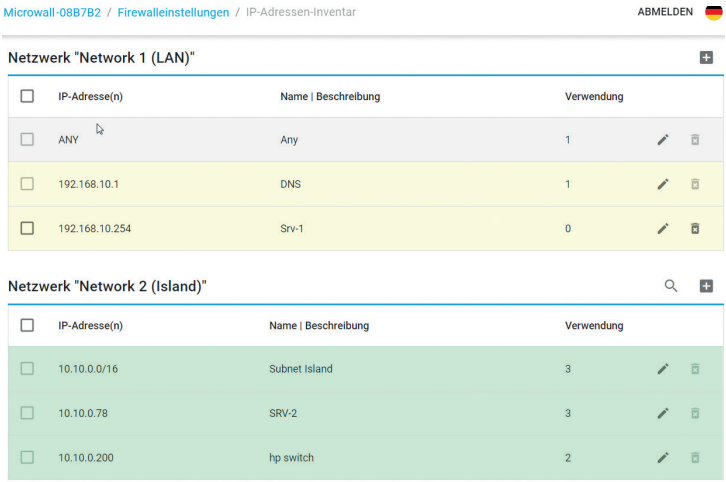
Aktivieren Sie die Betriebsart *Standard-Router* über den Menübaum unter *Firewalleinstellungen -> Betriebsart* und legen Sie die Behandlung von ICMP Echo Requests/Replies (ping) auf die lokalen Interfaces sowie die Weiterleitung anderer ICMP-Datagramme fest.



Über den Button *Speichern* wird der Modus *Standard-Router* aktiviert und der zugehörige Regel-Satz geladen.

5.3 IP-Iventare

Im Menüzweig *Firewalleinstellungen -> IP-Adressen-Inventar* stellt die Microwall für jedes Netzwerk ein separates Adressen-Inventar zur Verfügung. Die Konfiguration der Ziel-/Quell-Adresse(n) bei der Erstellung von Firewallregeln erfolgt immer aus diesen Adress-Inventaren.



Inventar-Einträge können sowohl aus einzelnen IP-Adressen, wie auch aus Bereichen oder Listen bestehen. Folgende Eingaben sind zulässig:

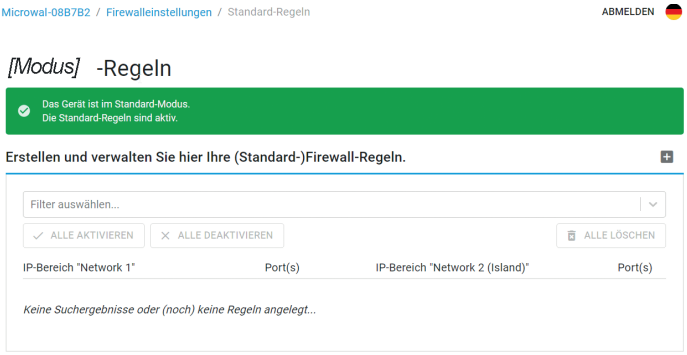
- *any*
  Schlüsselwort für beliebige IP-Adressen
- *einzelne IP-Adresse*
  IP-Adresse in Dot-Notation (z.B. 10.20.0.4)
- *Komma-getrennte IP-Adressliste*
  Liste von IP-Adressen in Dot-Notation (z.B. 10.10.10.1, 20.20.20.2)
- *IP-Bereich*
  Durchgängiger IP-Bereich in der Form „von-bis“ (z.B. 10.10.10.1 - 10.10.10.20)
- *IP-Bereich CIDR-Notation*
  CIDR-notierter IP-Bereich (z.B. 10.10.0.0/16)

5.3.1 Scannen von Network 2

Über die Lupe im Bereich von *Network 2* besteht die Möglichkeit, das Inselnetzwerk nach Teilnehmern durchsuchen zu lassen. Bei einem Scan neu gefundene Teilnehmer können dann automatisch in die Inventarliste von *Network 2* übernommen werden.

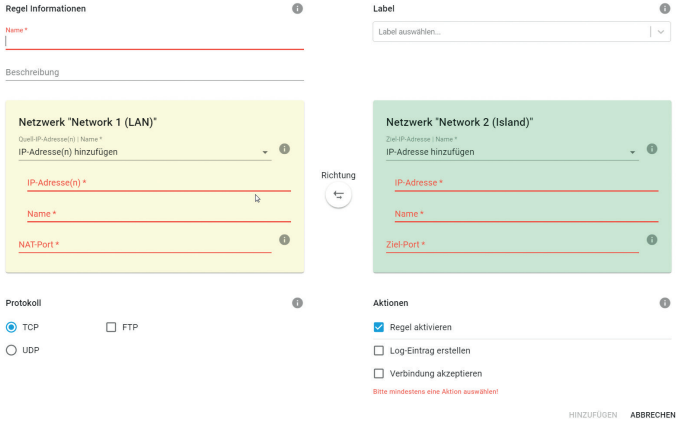
5.4 Erstellen von Firewall-Regeln

Das Erstellen von Firewall-Regeln für den jeweils aktuellen Modus erfolgt auf der Seite *Firewalleinstellungen -> Firewall-Regeln*. Die Übersicht enthält Informationen zu den bereits existierenden Regeln mit der Möglichkeit, diese über den jeweiligen Schiebeschalter zu aktivieren und deaktivieren.



Der Button *Plus* am oberen rechten Rand der Tabelle öffnet den Dialog für das Anlegen neuer Regeln.

Regelbeispiele für viele Standardanwendungen finden Sie auf unserer Webseite unter https://www.wut.de/rule-examples.



Name

Frei vergebbarer Name der Regel.

Beschreibung

Optionale zusätzliche Beschreibung der Regel.

Label

Zur übersichtlicheren Darstellung bzw. Anzeigefilterung in der Regelübersicht können der Regel ein oder mehrere Label zugewiesen werden. Ab Werk sind die Label *Normal mode* und *Service* angelegt. Über die Seite *Label-Inventar* können zusätzliche eigene Label angelegt werden.

Richtung

Mit einem Klick auf den Richtungspfeil erfolgt die Festlegung der Richtung für die Regel aus Sicht des Verbindungsaufbaus bei TCP. Bei UDP wird die Richtung durch das initiale UDP-Datagramm bestimmt.

Network 1 (gelb) & Network 2 (grün)

Konfiguration der Ziel-/Quell-IP-Adressen und Ziel-/Quell-Portnummern, die für die Regel verwendet werden. In welchem Netzwerk sich Quelle oder Ziel befinden, wird dynamisch über die gewählte Richtung der Regel bestimmt. Je nach aktueller Betriebsart sind entweder nur einzelne Adressen und/oder Ports konfigurierbar oder

auch ganze Bereiche und Listen. Details hierzu enthalten die jeweiligen über den Info-Button aufrufbaren Hilfetexte.

Die *Ziel-IP-Adresse(n)|Quell-IP-Adressen* können entweder über die Select-Box aus den Inventarlisten ausgewählt oder direkt numerisch angegeben werden. Bei numerischer Angabe, wird der neue Host bzw. der neue Adressbereich automatisch mit der unter *Name* angegebenen Bezeichnung in das jeweilige IP-Inventar für *Network1* oder *Network2* übernommen.

Zulässige Eingaben und Formate der Adressen und Adressbereiche:

- *any*
  Schlüsselwort für beliebige IP-Adressen
- *einzelne IP-Adresse*
  IP-Adresse in Dot-Notation (z.B. 10.20.0.4)
- *Komma-getrennte IP-Adressliste*
  Liste von IP-Adressen in Dot-Notation (z.B. 10.10.10.1, 20.20.20.2)
- *IP-Bereich*
  Durchgängiger IP-Bereich in der Form „von-bis“ (z.B. 10.10.10.1 - 10.10.10.20)
- *IP-Bereich CIDR-Notation*
  CIDR-notierter IP-Bereich (z.B. 10.10.0.0/16)

Unterschiedliche Eingabeformen und Verkettungen von IP-Bereichen innerhalb eines Eingabefeldes sind nicht möglich. Das heißt, „10.20.0.4, 10.20.0.10-10.20.0.20“ oder „10.20.0.0/16, 10.10.0.0/16“ sind ungültige Eingaben.

Zulässige Eingaben und Formate der Portnummern und und Portnummern-Bereiche:

- *any*
  Schlüsselwort für beliebige Portnummer
- *einzelne Portnummer*
  z.B. 8000
- *kommagetrennte Portnummern-Liste*
  z.B. 80,443,8000
- *Portnummern-Bereich*
  z.B. 100-1000

Unterschiedliche Eingabeformen lassen sich nicht kombinieren. Das heißt, „8000, 10-1000“ ist z.B. eine ungültige Eingabe.

Protokoll

Festlegung, ob die Regel für *TCP* oder *UDP* gilt.

Die TCP-Option *FTP* muss aktiviert werden, wenn die Regel für FTP-Verbindungen formuliert wird. Im Protokollverlauf ausgehandelte parallele TCP-Verbindungen werden automatisch erlaubt und gesperrt.

UDP ist ein verbindungsloses Protokoll welches allerdings häufig nach einem Request-Reply-Prinzip (z.B. DNS) arbeitet. In diesen Fällen muss die Option *Antwort in Rückrichtung zulassen* aktiviert werden. Die Microwall akzeptiert innerhalb eines Timeouts automatisch ein ggf. eingehendes Reply-Datagramm.

Aktionen

Regel aktivieren aktiviert die Regel sofort nach Betätigung des Buttons *Speichern*. Ist die Option nicht gesetzt, wird mit Betätigung von *Speichern* die Regel angelegt, aber nicht angewendet. Datenverkehr entsprechend der Regel ist nicht möglich. Eine Aktivierung der Regel kann auch nachträglich in der Regelübersicht erfolgen.

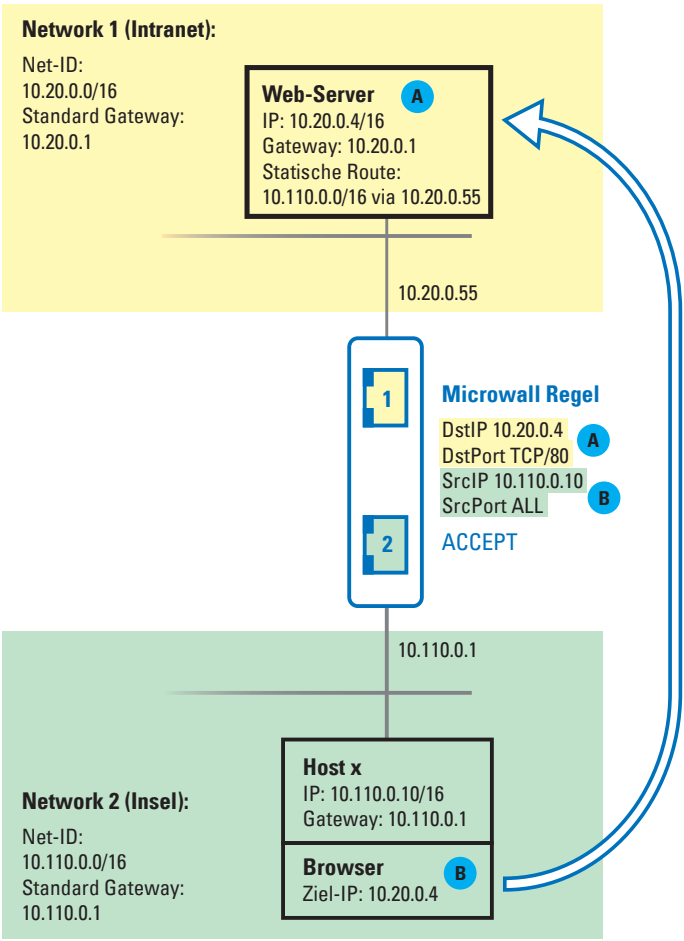
Log-Eintrag erstellen erzeugt für jeden Verbindungsaufbau entsprechend der Regel einen Eintrag im Logfile der Microwall.

Verbindung akzeptieren erlaubt den durch die Regel definierten Datenverkehr.

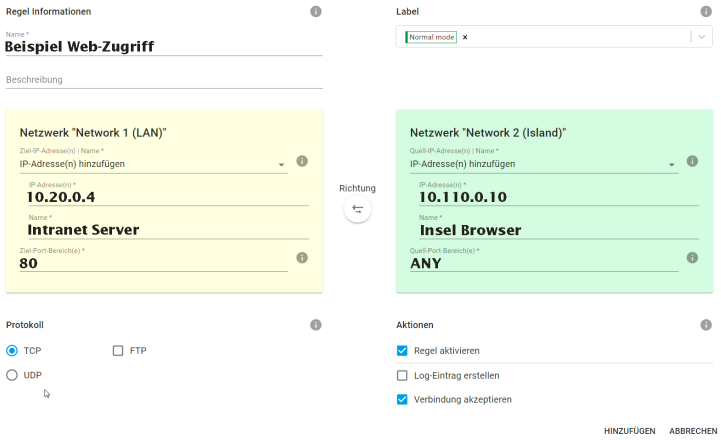
5.5 Beispiele Firewall-Regeln

5.5.1 Modus Standard-Router, Network 2 nach Network 1

Insel-Host B 10.110.0.10/16 am Anschluss *Network 2* soll per Browser auf den Intranet-Web-Server A 10.20.0.4/16, TCP/80 am Anschluss *Network 1* zugreifen. Die jeweils lokalen IP-Adressen der Microwall lauten 10.110.0.1 und 10.20.0.55. Für eine Ansichts-Filterung in der Regelübersicht wird die Regel mit dem Label *Normal mode* gekennzeichnet.

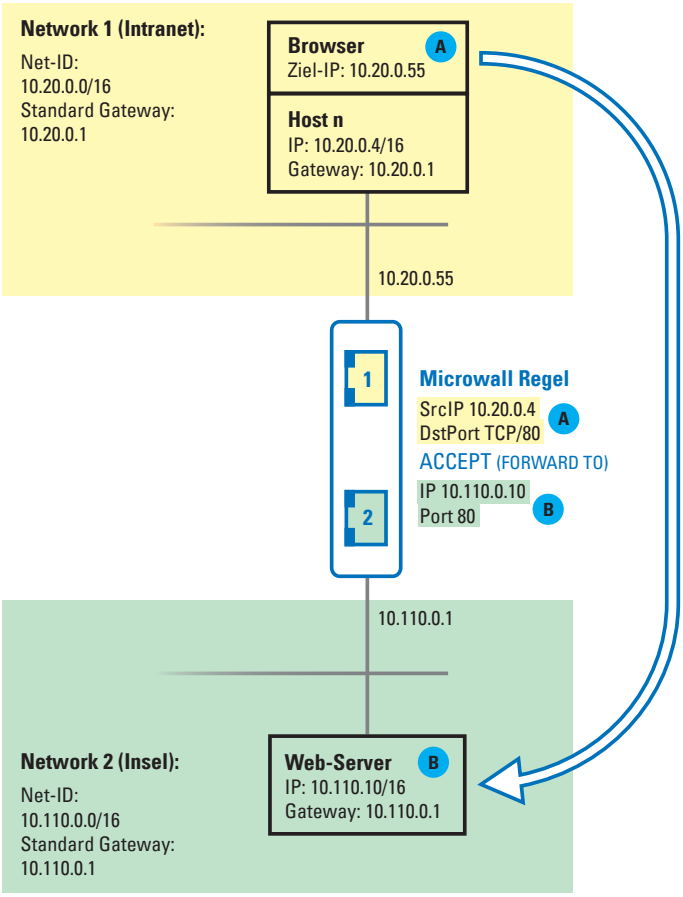


Der zu diesem Beispiel auszufüllende Regeldialog:

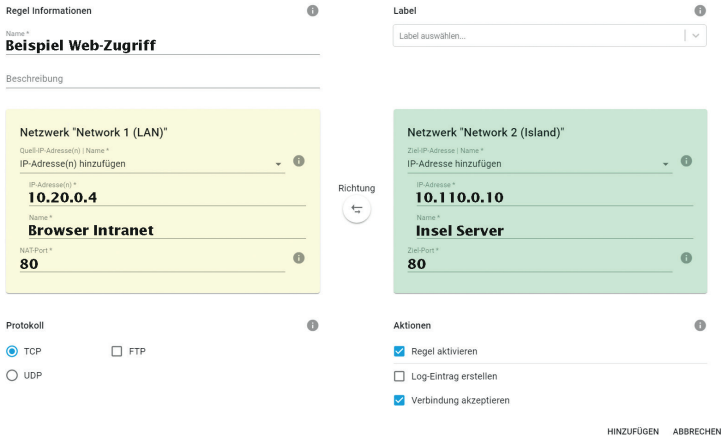


Modus NAT-Router, Network 1 nach Network 2

Intranet-Host A 10.20.0.4/16 soll per Browser auf den Insel-Web-Server B 10.110.0.10/16, TCP/80 zugreifen. Die Microwall selbst ist mit den IPs 10.110.0.1 und 10.20.0.55 in die Netze integriert. Als Ziel-Adresse im Browser wird die Intranet-IP der Microwall verwendet, wo sie dann per Regel durch die Insel-IP 10.110.0.10 ersetzt wird.



Der zu diesem Beispiel auszufüllende Regeldialog:



Weitere Regelbeispiele für viele Standardanwendungen finden Sie auf unserer Webseite unter https://www.wut.de/regelbeispiele.

6 Security & Wartung

- Security- und Betriebshinweise
- Firmware-Updates
- Eigene Zertifikate
- Notzugang per Service-Taster
- Reset auf Werkseinstellungen

6.1 Security-Hinweise

Die folgenden Abschnitte enthalten aus Sicht der IT-Sicherheit relevante Hinweise und Empfehlungen für Inbetriebnahme, Konfiguration, Betrieb und Wartung der Microwall.

6.1.1 Funktion

Die Microwall ist eine als Router konzipierte Kleinfirewall mit zwei Ethernet-Anschlüssen. Die typische Anwendung besteht darin, eine Netzwerkinsel von einem übergeordneten Intranet zu entkoppeln und nur über eine whitelistbasierte Firewall ausdrücklich erlaubte Verbindungen zu ermöglichen.

6.1.2 Installationsort

Der Installationsort der Microwall muss gewährleisten, dass keine unauthorisierten physikalischen Zugriffe erfolgen können (z.B. geeignet gesicherter Raum oder Netzwerkschrank). Ein physikalischer Zugriff auf die Microwall birgt z.B. folgende Risiken:

- Außerbetriebnahme des Gerätes (Entfernen Netzwerkkabel, Spannunsgversorgung ...) und Verlust aller Verbindungen zu den Teilnehmern des Inselnetzwerks.

- Start des Notzugangs der Microwall über den Service-Taster und somit Deaktivierung bzw. Änderung des Passwortes. Ein Angreifer erhält Vollzugriff auf die Managementoberfläche und ist z.B. in der Lage, Firewall-Regeln zu erstellen.

6.1.3 Inbetriebnahme

Die Inbetriebnahme einer Microwall unterteilt sich in die Vergabe einer IP-Adresse mit dem Tool *WuTility* und dem

anschließenden Aufruf der initialen Webseite mit der Konfiguration des Passwortes und den netzwerkseitigen Basisparametern. Erst nach diesem Schritt ist der Zugang zur Managementoberfläche der Microwall durch das Passwort geschützt.

IP-Vergabe und Vergabe des Passwortes
Stellen Sie bei einer Erstinbetriebnahme bis zur Vergabe des Passwortes auf der initialen Webseite sicher, dass keine unauthorisierten Zugriffe auf die Microwall erfolgen. Eine geeignete Maßnahme ist zum Beispiel die Inbetriebnahmeschritte über eine Punkt-zu-Punkt-Verbindung mit dem konfigurierenden Rechner durchzuführen. Erst anschließend wird die Microwall dann mit den Zielnetzwerken verbunden.

Passwort
Das Passwort der Microwall ist der zentrale Schutz vor unauthorisierten Zugriffen auf die Konfiguration und das Management der Microwall. Wir empfehlen die Verwendung eines sicheren Passwortes mit einer Länge von mindestens 15 Zeichen, bestehend aus Groß- und Kleinbuchstaben, Ziffern sowie Sonderzeichen.

Registrierung für sicherheitsrelevante Informationen
Über das Inventarisierungstool können Geräte bei W&T registriert werden. Im Fall von sicherheitsrelevanten Updates und/oder Informationen werden sie von uns sofort per Email benachrichtigt. Neben den angegebenen persönlichen Daten werden bei einer Registrierung auch die gerätespezifischen Daten gespeichert.

6.1.4 Betrieb und Konfiguration

Individuelles Geräte-Zertifikat
Der Zugriff auf das Web-Based-Management kann ausschließlich verschlüsselt per HTTPS erfolgen. Ab Werk wird hierfür ein selbstsigniertes Default-Zertifikat verwendet, für welches bei der Inbetriebnahme eine Ausnahme in dem verwendeten Browser eingerichtet werden muss. Für den Zugriff im operativen Betrieb, empfehlen wir das Default-Zertifikat durch ein individuelles eigenes Zertifikat zu ersetzen.

Deaktivierung nicht benötigter Dienste

Die Microwall stellt mit den Werkseinstellungen nach der Inbetriebnahme die folgenden eingehenden eigenen Dienste zur Verfügung:

Port-/Socket-nummer	Anwendung	System-passwort-Schutz?	Konfigurier-/ab schaltbar?
443 (TCP)	HTTPS-Management	ja	ja/ja
8513 (UDP)	Inventarisierung z.B. durch WuTility	nein	nein/ja
5555 (TCP)	Firmware-Update per WuTility	ja	nein/ja
446 (TCP)	HTTPS Notzugang (nur nach manueller Aktivierung über den Service-Taster)	nein	nein/ja

Konfiguration und Aktivierung/Deaktivierung dieser Dienste erfolgen im Menübaum unter *Einstellungen -> Netzwerk*. Für jeden Dienst kann bestimmt werden, auf welchem Anschluss er verfügbar ist. Für Web-Based-Management kann zusätzlich auch der verwendete TCP-Port umgestellt werden.

In Umgebungen mit erhöhten Sicherheitsanforderungen kann es sinnvoll sein, nach der Einrichtung der Kommunikationsregeln im operativen Betrieb diese Dienste teilweise oder auch alle zu deaktivieren. Für eventuelle später erforderliche Änderungen kann der HTTPS-Zugriff über den per Service-Taster zugänglichen Notzugang bedarfsgesteuert jederzeit wieder aktiviert werden (s. Kapitel Notzugang per Service-Taster).

Formulierung der Whitelist-Regeln

Die Microwall verfügt über keine Default-Regeln zur Kommunikation zwischen den beiden Netzwerkanschlüssen. Bei der Formulierung von Regeln empfehlen wir, diese nach dem Need-to-know-Prinzip so knapp wie möglich auszulegen. Zum Beispiel bietet die Verwendung einer Unicast-Adresse eine höhere Sicherheit als ein IP-Bereich.

Vertraulichkeit von Private Keys
Asymmetrische Verschlüsselung mit den zugehörigen Public-/Private-Key-Paaren werden in der Microwall für das TLS-Protokoll bei Web-Zugriffen verwendet. Der Private-Key der Microwall ist nicht auslesbar.

6.1.5 Service und Wartung

Trotz hoher Qualitätstandards kann Elektronik jederzeit z.B. durch externe Ereignisse ausfallen. Abhängig von den Anforderungen an die Verfügbarkeit der jeweiligen Anwendung empfehlen wir geeignete Vorkehrungen zu treffen.

- Sicherung/Speicherung der Gerätekonfiguration
- Ggf. Vorhaltung eines Ersatzgerätes
- Dokumentation der Vorgehensweise bei Gerätetausch

6.2 Up-/Download von Konfigurations-Backups

Auf Webseite *Wartung* besteht die Möglichkeit, die aktuelle Konfiguration der Microwall zu sichern oder eine zuvor heruntergeladene Backup-Datei zurückzuschreiben.

Konfigurations- bzw. Backup-Dateien enthalten neben den operativen Parametern (Firewall-Regeln,

Inventar-Listen etc.) auch die für den administrativen Zugriff auf die Microwall relevanten Daten (IP-Parameter, System-Passwort, Zertifikat etc.). Backup-Dateien sind aus diesem Grund verschlüsselt und nicht editierbar. Für einen erweiterten Schutz empfehlen wir die Datei zusätzlich mit einem individuellen Backup-Passwort zu versehen. Dieses muss dann bei einem späteren Upload in eine Microwall bekannt sein.

Konfiguration herunterladen
Der Button *Konfiguration herunterladen* startet den Download aller aktuellen Konfigurationsparameter der Microwall. Soll die Datei ein individuelles Backup-Passwort erhalten, muss dieses vor dem Download in das Feld Backup-Passwort eingegeben werden.

Der Upload einer mit Passwort versehenen Backup-Datei ist nur mit Kenntnis dieses Passwortes möglich. Sichern Sie daher das Passwort in geeigneter Form separat von der Backup-Datei.

Konfiguration hochladen
Der Upload einer Backup-Datei ist an zwei Stellen möglich:

- Standard-WBM -> Wartung
- Initiale Webseite im Zuge der Inbetriebnahme

Ist die Backup-Datei mit einem Passwort geschützt, muss dieses in das Feld *Backup-Passwort* eingegeben werden. Der Button *Konfiguration hochladen* startet den Dateiauswahl-Dialog und die Übertragung. Nach erfolgreicher Prüfung der Datei wird deren Inhalt übernommen und die Microwall arbeitet nach einem automatischen Neustart mit den neuen Parametern.

Backup-Dateien enthalten auch die neue IP-Adresse der Microwall. Um einen IP-Konflikt zu vermeiden, stellen Sie vor dem Upload sicher, dass die ursprüngliche oder eine zuvor programmierte Microwall nicht mehr an das Netzwerk angeschlossen sind.

6.3 Firmware-Updates

Ein Update der Firmware kann entweder mit Hilfe des Management-Tool WuTility oder über das Web-Based-Management der Microwall erfolgen.

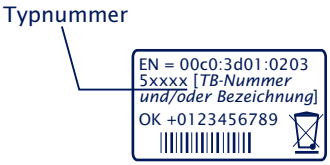
6.3.1 Wo ist die aktuelle Firmware erhältlich?

Die jeweils aktuellste Firmware inkl. der verfügbaren Update-Tools und einer Revisionsliste ist auf unseren Webseiten unter folgender Adresse veröffentlicht:

https://www.wut.de

Sie navigieren von dort aus am einfachsten mithilfe der auf der Seite befindlichen Suchfunktion. Geben Sie in das Eingabefeld zunächst die Typnummer Ihres Gerätes ein.

Sollten Sie die Typnummer nicht kennen, können Sie diese dem auf der Gehäuseschmalseite befindlichen Aufkleber entnehmen, auf dem sich auch die Ethernet-Adresse befindet.

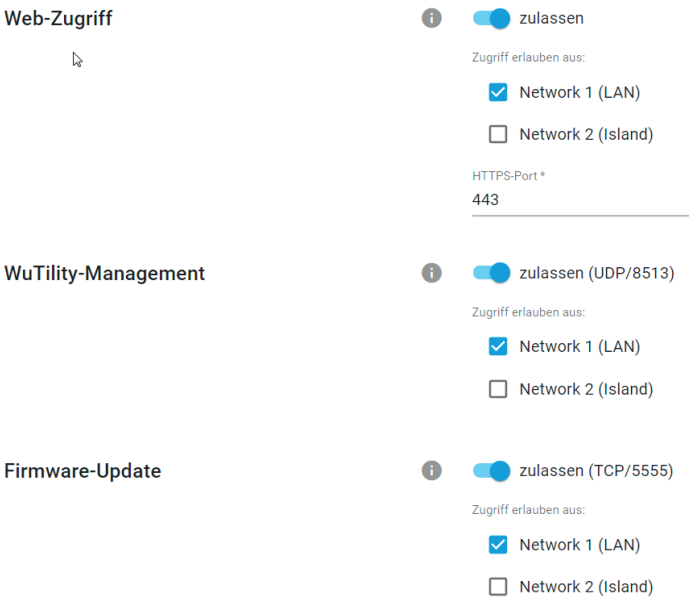


Auf dem Web-Datenblatt der Microwall folgen Sie dem Link *Firmware* und starten den Download der gewünschten Version. Vor dem Upload in die Microwall muss die eigentliche Firmware-Datei aus dem zip-Archiv entpackt werden.

6.3.2 Firmware-Update mit WuTility

Für das Firmware-Update mit WuTility muss dieses auf einem Windows-PC installiert sein. Dessen IP-Einstellungen müssen die Kommunikation mit der Microwall und deren aktuellen IP-Paramtern erlauben.

Voraussetzung für das Firmware-Update mit WuTility ist der aktivierte Update-Dienst auf TCP/5555 in der Microwall. Mit den Werkseinstellungen ist das Update mit WuTility nur über die Schnittstelle *Network 1* möglich.



Die Netzwerkkommunikation bei der Übermittlung des System-Passworts und auch der eigentliche Upload werden verschlüsselt durchgeführt und sind somit vertraulich.

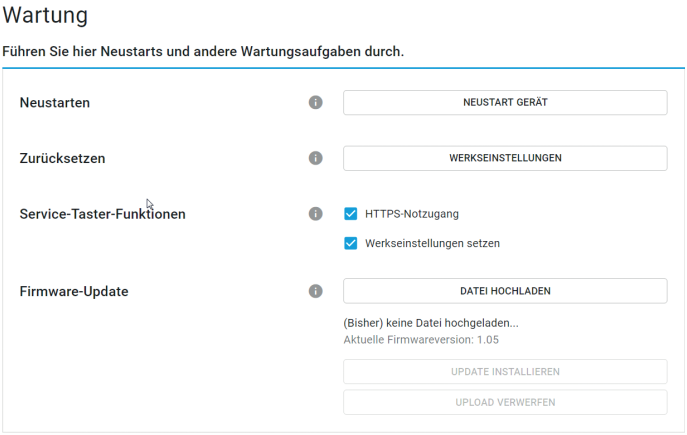
Für die Übertragung der neuen Firmware an die Microwall markieren Sie in der Inventarliste von WuTility die gewünschte Microwall und betätigen dann den Button *Firmware.*

In dem folgenden Dialog wählen Sie die zu übertragende Firmware-Datei (*.uhd) aus und betätigen dann den Button *Weiter*. Nach der erfolgreichen Übertragung entschlüsselt die Microwall die Firmware-Datei, überprüft die Signatur und schreibt die Firmware in ihr internes Flash. Abschließend wird automatisch ein Neustart durchgeführt und die Microwall ist wieder betriebsbreit.

6.3.3 Firmware Update per Web-Based-Management

In Netzwerkumgebungen, die den Einsatz von WuTility nicht zulassen oder in denen aus Sicherheitsgründen der Update-Service in der Microwall deaktivert wurde, kann das Firmware-Update aus dem Web-Based-Management heraus erfolgen.

Wechseln Sie im Menübaum der Microwall auf die Seite *Wartung*.



Der Button *Datei hochladen* startet den Auswahldialog für die Firmwaredatei. Wählen Sie hier die zuvor heruntergeladene und entpackte Firmware-Datei (*.uhd) aus. Nach dem Upload startet der Button *Update installieren* die eigentliche Installation der neuen Firmware.

6.4 Eigene Zertifikate

Der Zugriff auf das Web-Based-Management der Microwall ist aus Sicherheitsgründen ausschließlich verschlüsselt über das HTTPS-Protokoll möglich.

Das ab Werk vorinstallierte, selbstsignierte Zertifikat der Microwall erzeugt bei aktuellen Browsern entsprechende Sicherheitswarnungen. Diese müssen bei WBM-Zugriffen quittiert und/oder mit geeigneten Ausnahme-Regeln bestätigt werden.

In Netzwerkumgebungen mit erhöhten Sicherheitsanforderungen, in denen diese Ausnahmen nicht erwünscht/erlaubt sind, kann das Werkszertifikat durch ein individuelles Zertifikat ersetzt werden.

Erzeugung, Signatur und Installation eines eigenen Zertifikates unterteilen sich hierbei in folgende grobe Schritte:

- Erzeugung eines CSR (Certificate Signing Request) mit zugehörigem Private-Key in der Microwall
- Download des CSR und externe Signatur zu einem Zertifikat durch eine vertrauensvolle Zertifizierungsstelle.
- Upload und Installation des Zertifikates in die Microwall

Navigieren Sie im Menübaum auf die Seite *Grundeinstellungen -> Zertifikat*. Neben Informationen zu dem aktuell installierten Zertifikat sind hier alle Funktionen für das Handling individueller Zertifikate enthalten:

Erzeugen eines Certificate Signing Requests (CSR)
Tragen Sie alle benötigten Informationen in das CSR-Formular ein. Pflichtfeld ist lediglich der *Common Name,* unter welchem die Webseiten der Microwall später im Browser aufgerufen werden. Unter *Alternative Names* können zusätzliche Namen, IP-Adressen und auch Wildcard-Names eingegeben werden. Der in *Common Name* eingetragene Name wird automatisch auch in die Alternative Names übernommen.

Durch Klick auf *Erstellen* generiert die Microwall ein Schlüs-

sel-Paar und erstellt aus den getätigten Angaben einen CSR.

Installation eines selbstsignierten Zertifikates
Durch Klick auf *Installieren* unter *Selbstsigniertes Zertifikat*, kann der zuvor erzeugte *Signing Request* mit einer Selbstsignatur versehen werden. Browser werden bei Abruf der Webseiten eine entsprechende Sicherheitswarnung melden.

Extern signiertes Zertifikat
Der erzeugte Signing Request kann über den Button *Herunterladen* zur externen Signatur von der Microwall heruntergeladen werden. Der Download erfolgt im PEM-Format

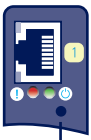
Nach der Signatur durch eine vertrauenswürdige Zertifizierungsstelle (CA) können das Zertifikat sowie eine eventuell benötigte Zertifikatskette über die entsprechenden Upload-Buttons in die Microwall geladen werden. Alle Dateien müssen im PEM-Format vorliegen.

Nach einer formalen Prüfung wird das Zertifikat durch Klick auf *Installieren* unter *Extern signiertes Zertifikat* in das System integriert und bei allen Web-Zugriffen verwendet.

Informationen und Ablauf von Zertifikaten
Unter *Aktuelle Information* finden Sie die Datei-Informationen des aktuellen Zertifikates und der Zertifikatskette sowie auch das Gültigkeitsdatum.

6.5 Notzugang der Microwall

Bei einem vergessenen Passwort oder wenn das Web-Based-Management aus Security-Gründen deaktiviert wurde, kann über den versenkt montierten Service-Taster auf der Frontseite der Notzugang aktiviert werden.



Start des Notzugangs
Betätigen Sie mit einem geeigneten spitzen Gegenstand (z.B. Büroklammer) den Taster und halten diesen gedrückt bis nach ca. 3,5s die Error-LED langsam blinkt. Wenn Sie den Taster jetzt lösen, ist der Notzugang aktiviert.

Die Router-/Firewall-Funktion bleibt in diesem Zustand vollständig erhalten.

Der Notzugang aktiviert auf der Microwall eine nicht-passwortgeschützte Web-Seite mit der Möglichkeit, das aktuelle Passwort zu überschreiben. Treffen Sie daher im Vorfeld geeignete Maßnahmen gegen unauthorisierte Zugriffe.

Aufruf und Funktion des Notzugangs
Der Notzugang erfolgt per Browser mit HTTPS über den TCP-Port 446:

https://[IP-Adresse|Hostname]:446

Ohne Passwortabfrage gelangen Sie auf die Webseite mit folgenden Möglichkeiten:

Überschreiben des aktuellen Passwortes
Durch Aktivieren der Option *Passwort ändern*, haben Sie die Möglichkeit, das aktuelle Passwort für den Zugriff auf das Web-Management zu ändern.

Wir empfehlen Passwörter mit einer Mindestlänge von 15

Zeichen, bestehend aus Groß- und Kleinbuchstaben, Ziffern sowie Sonderzeichen. Die Maximallänge des Passwortes ist 51 Zeichen.

Aktivierung des Standard Web-Based-Managements
Legen Sie unter Management fest, auf welchem Anschluss und unter welchem Port das Web-Management der Microwall anschließend erreichbar sein soll.

Beenden des Notzugangs
Änderungen werden mit einem Klick auf *Anwenden* übernommen und die Microwall führt einen Neustart der betroffenen Dienste durch. Anschließend ist der Zugriff auf das passwortgeschützte Standard Web-Interface über den zuvor konfigurierten TCP-Port möglich.

Ein Klick auf *Abbrechen* verwirft ggf. durchgeführte Änderungen und die Microwall führt einen Neustart der erforderlichen Dienste durch. Anschließend ist der Zugriff auf das passwortgeschützte Standard Web-Interface über den konfigurierten TCP-Port möglich.

6.6 Werkseinstellungen

Ein Reset auf die Werkseinstellungen der Microwall kann über den versenkt montierten Service-Taster auf der Frontseite erfolgen.

Betätigen Sie mit einem geeigneten spitzen Gegenstand (z.B. Büroklammer) den Service-Taster und halten diesen für mindestens 20s gedrückt. Nach 3,5 startet die Error-LED mit langsamem Blinken und nach ca. 10s mit schnellem Blinken. Nach insgesamt ca. 20s wird der Reset auf die Werkseinstellung durchgeführt. Ein Lösen des Service-Tasters bei schnell blinkender Service-LED im Zeitfenster von 10-20s, führt zu einem Abbruch des Factory-Default-Resets und die Microwall fährt mit dem Standardbetrieb entsprechend der aktuellem Konfiguration fort.

Der Reset ist abgeschlossen, sobald die System-LED wieder dauerhaft leuchtet. Die Microwall muss jetzt neu in Betrieb genommen werden. Informationen hierzu enthält das Kapitel *Inbetriebnahme*.

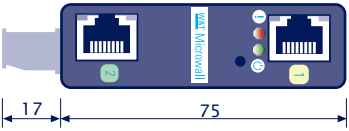
7 Anhang

- Technische Daten und Bauform
- Lizenzen

7.1 Technische Daten und Bauform

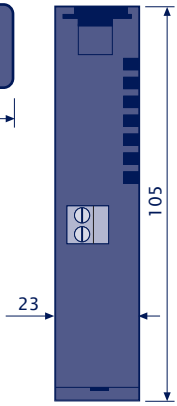
Spannungsversorgung ... Power-over-Ethernet: Externe Speisung, Schraubklemme	 37-57V DC aus PSE DC 24-48V (+/-10%)
Stromaufnahme ... Power-over-Ethernet: Ext. Speisung	 PoE Class 2 (3,84 W - 6,49W) typ. 150mA@24V DC max. 200mA@24V DC
Galvanische Trennung	Netzwerkanschlüsse: min 500V
LAN-Port *Network 1*	10/100/1000BaseT auf RJ45, autosensing, autocrossing, PoE
LAN-Port *Network 2*	10/100/1000BaseT auf RJ45, autosensing, autocrossing
Zulässige Umgebungstemperatur ... ... Lagerung ... Betrieb, nicht angereihte Montage	 -40 ... +85°C 0 ... +50°C
Zulässige rel. Luftfeuchtigkeit	0 - 95% (nicht kondensierend)
Abmessungen	105 x 75 x 22mm
Gewicht	ca. 120g

Frontansicht 55210



Maße in mm, +/-1mm

Unterseite 55210



7.2 Lizenzen

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and

(2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you

conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the

entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the

operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you

may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions

either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Index