

W&T

www.WuT.de

Anleitung

Inbetriebnahme und Anwendung

Microwall Gigabit

gültig für folgende Modelle:

#55210: Microwall Gigabit

Release 1.00 10/2018

© 10/2018 by Wiesemann und Theis GmbH
Microsoft, MS-DOS, Windows, Winsock und Visual Basic
sind eingetragene Warenzeichen der Microsoft Corporation.

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-5www-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 Gigabit ist ein Industrie-tauglicher IPv4-Router mit zwei 1000BaseT-Netzwerkanschlüssen und integrierter, Whitelist-basierter Firewall. Sie bindet eine Netzwerkinself z.B. mit Automatisierungskomponenten an ein übergeordnetes Netzwerk an. Geeignete Filterregeln auf TCP/IP-Ebene schützen beide Netzwerke vor unberechtigter, unerwünschter und schädlicher Kommunikation.

1 Rechtliche-Hinweise und Sicherheit	7
1.1 Rechtliche Hinweise	8
Warnhinweiskonzept.....	8
Qualifiziertes Personal	8
Entsorgung	9
Symbole auf dem Produkt	9
1.2 Sicherheitshinweise.....	10
Allgemeine Hinweise.....	10
Bestimmungsgemäßer Gebrauch.....	10
Elektrische Sicherheit.....	10
EMV	11
2 Hardware, Schnittstellen und Anzeigen	13
2.1 Hardware-Installation.....	14
2.2 Spannungsversorgung	15
2.2.1 PoE-Versorgung	15
2.2.2 Externe Spannungsversorgung.....	15
2.3 Netzwerkschnittstellen	16
2.4 System- und Error-LED	18
2.4.1 System-LED ☺ (grün).....	18
2.4.2 Service-LED ☹ (rot).....	18
2.5 Service-Taster	19
3 Inbetriebnahme.....	21
3.1 Erstvergabe der IP-Parameter mit WuTility	22
3.2 Inbetriebnahme über die Default-IP-Adresse.....	25
3.2 Initiale Webseite der Erstinbetriebnahme	27
4 Web-Based-Management.....	31
4.1 Start und Navigationskonzept des WBM	32
4.2 Anmelden/Abmelden	33
4.3 Hilfe und Beschreibungstexte	34
5 Betriebsarten und Regel-Konfiguration	35
5.1 Funktionsweise der Microwall Gigabit	36
5.2 Betriebsarten & Umschaltung	37
5.2.1 Modus NAT-Router.....	37
5.2.2 Modus Standard-Router	37
5.2.3 Umschaltung der Betriebsarten	37
5.3 Regel-Übersichten & Label.....	39
5.3.1 Label	39
5.3.2 Erstellen und Verwalten von Labels	40
5.4 Erstellen von Firewall-Regeln.....	41
5.5 Erstellen von Firewall-NAT-Regeln	47

6 Security & Wartung	53
6.1 Firmware-Updates.....	54
6.1.2 Firmware Update mit WuTility	54
6.1.2 Firmware Update per Web-Based-Management	55
6.2 Eigene Zertifikate.....	57
6.3 Deaktivierung nicht benötigter Dienste	60
6.4 Notzugang der Microwall Gigabit	61
6.5 Werkseinstellungen	63
7 Anhang.....	65
7.1 Technische Daten und Bauform.....	66
7.2 Lizenzen	67
Index	74

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:

GEFÄHR

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

WARNUNG

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

VORSICHT

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

ACHTUNG

kennzeichnet eine Gefährdung, die Sachschaden zur Folge haben kann, wenn keine entsprechende 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

W&T

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

Dabei 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 im Handbuch 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 von Wiesemann & Theis ist ein IPv4-Router mit zwei 1000BaseT-Netzwerkanschlüssen und integrierter, Whitelist-basierter Firewall. Sie bindet eine Netzwerkinself an ein übergeordnetes Netzwerk an. Geeignete Filterregeln auf TCP/IP-Ebene schützen beide Netzwerke vor unberechtigter und unerwünschter 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 keiner direkten Sonnenbestrahlung ausgesetzt werden, sowie nicht in der Nähe von Wärmequellen betrieben werden. Bitte beachten Sie hierzu die Einschränkungen in Hinblick auf die

W&T

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 vagabundierende 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 EN60950-1 gewährleisten und „LPS“-Eigenschaft besitzen.

EMV

⚠️ACHTUNG

Zum Netzwerkanschluss der Microwall dürfen ausschließlich geschirmte Netzkabel verwendet werden.

Die Microwalls erfüllen in diesem Fall die industriellen Störfestigkeits-Grenzwerte und die strengeren Emissions-Grenzwerte für Haushalt und Kleingewerbe. Daher gibt es keine EMV-begründeten Einschränkungen in Hinblick auf die Verwendbarkeit der Geräte in diesen Umgebungen.

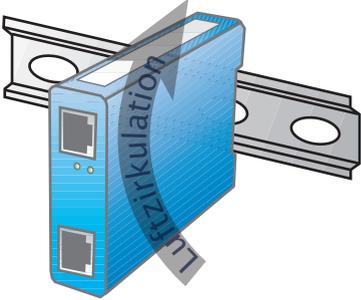
Die vollständigen Konformitätserklärungen zu den in der Anleitung beschriebenen Geräten finden Sie über die jeweiligen Internet-Datenblattseite auf der W&T-Homepage unter <http://www.wut.de>.

2 Hardware, Schnittstellen und Anzeigen

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

2.1 Hardware-Installation

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



i Der Montageort muss den Security-Anforderungen der jeweiligen System-Umgebung angepasst sein. Physikalischer Zugriff auf die Microwall Gigabit 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 Gigabit erfolgt alternativ über PoE oder ein externes Netzteil. Gleichzeitiger Anschluss beider Versorgungen ist nicht zulässig. Die Stromaufnahme kann den technischen Daten entnommen werden.

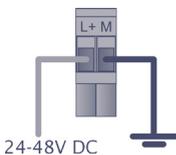
2.2.1 PoE-Versorgung

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

2.2.2 Externe Spannungsversorgung

Alternativ zur PoE-Versorgung, kann die Microwall Gigabit 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 Gigabit 55210 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 EN60950-1 gewährleisten und „LPS“-Eigenschaft besitzen.

2.3 Netzwerkschnittstellen

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



Network 1 (gelb) dient dem Anschluss an das übergeordnete Netzwerk, in welches das Insel-Netzwerk 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.

2.3.1 100/1000BaseT

Beide LAN-Anschlüsse erfolgen über geschirmte RJ45-Buchsen und max. 100m lange, geschirmte Patchkabel. Die Autocrossing-Funktion erlaubt sowohl die Verwendung 1:1 verdrahteter wie auch gekreuzter Patchkabel für die Anbindung des/der LAN-Gerät(e).

Beide Netzwerkanschlüsse sind gegenüber der Versorgungsspannung mit mindestens $500V_{rms}$ galvanisch getrennt.

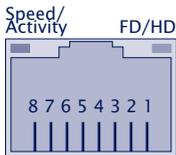
Auto Negotiation: 100/1000BaseT, Full/Half Duplex

Die Netzwerkanschlüsse der Microwall Gigabit arbeiten bei-
de in der Betriebsart *Auto-Negotiation*. Zur Vermeidung von
Problemen wie zum Beispiel ein Duplex-Mismatch, empfehlen

wir angeschlossene Geräte bzw. Switches ebenfalls im Modus *Auto-Negotiation* zu betreiben. Hierbei werden sowohl die Übertragungsgeschwindigkeit wie auch das Duplex-Verfahren automatisch verhandelt und entsprechend in den Geräten eingestellt.

2.3.2 Link-Status

Der Link-Status wird für beide Netzwerkanschlüsse durch jeweils zwei, 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



System-LED

Service-LED

2.4.1 System-LED 🟢 (grün)

ON: Signalisiert normale Betriebsbereitschaft.

Blinken: Die Microwall Gigabit 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 Gigabit ist aktiviert.

Weitere Informationen zum Notzugang enthält das Kapitel *Notzugang*.

i *Der Notzugang öffnet einen nicht-passwortgeschützten HTTPS-Zugang mit der Möglichkeit das aktuelle Passwort zu überschreiben. Starten Sie den Notzugang daher nur mit Vorsicht und 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 Gigabit bereitet eine Reset auf die Werkseinstellungen vor. Wird der Service-Taster weiterhin betätigt, erfolgt nach insgesamt 20s ein Reset auf die Werkseinstellungen.

2.5 Service-Taster



Service-Taster

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

Über den Service-Taster werden die folgenden Aktionen ausgelöst:

Reset/Neustart

Eine kurze Betätigung des Tasters zwischen 0,2 und 3,5s löst einen einfachen Neustart der Microwall Gigabit aus.

Start des Notzugangs

Nach Betätigung des Tasters für mehr als 3,5s, startet die Error-LED mit langsamem Blinken. Wird der Taster während des langsamen Blinkens und vor Ablauf von 10s gelöst, ist der Notzugang der Microwall Gigabit auf beiden Netzwerkan-schlüssen über TCP-Port 446 aktiviert. Erneutes kurzes Betätigen führt einen Reset durch und beendet den Notzugang.

Weitere Informationen zum Notzugang enthält das Kapitel *Notzugang*.

i *Der Notzugang öffnet einen nicht-passwortgeschützten HTTPS-Zugang auf TCP-Port 446 mit der Möglichkeit das aktuelle Passwort zu überschreiben. Starten Sie den Notzugang daher nur mit Vorsicht und 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 dann nach 20s die Microwall auf die Werkseinstellung zurückgesetzt. Ein Lösen des Service-Tasters während die Service-LED schnell blinkt (Zeitfenster 10-20s), führt zu einem Abbruch des Factory-Default-Resets und die Microwall fährt mit dem Standard-Betrieb entsprechend der aktuellem Konfiguration fort.

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

3 Inbetriebnahme

Die Inbetriebnahme der Microwall kann ausschließlich über die Schnittstelle *Network 1* (gelb) erfolgen. Im ersten Schritt wird der Microwall Gigabit die für den initialen Zugriff notwendige IP-Adresse zugewiesen. Bei dem anschließenden ersten Browserzugriff werden dann die weiteren für den Betrieb benötigten Basis-Parameter wie z.B. das Systempasswort konfiguriert.

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

3.1 Erstvergabe der IP-Parameter mit WuTility

Das Windows-Tool *WuTility* unterstützt ab der Version 4.52 die Inventarisierung und das Management der netzwerkbasierenden Parameter der Microwall Gigabit. Ältere *WuTility*-Versionen < 4.52 können nicht verwendet werden.

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

 *Mit Anschluss des Interfaces Network 1 an das Netzwerk ist die initiale Webseite zur Vergabe des Systempasswortes über die Default- oder per *WuTility* vergebene IP-Adresse erreichbar. Stellen Sie daher sicher, dass in dem Zeitraum bis zur Passwortvergabe auf der initialen Webseite keine unberechtigten Zugriffe auf die Microwall Gigabit 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 Gigabit im gleichen physikalischen Netzwerk befinden.

Installation von WuTility

Die Installation erfolgt am schnellsten über den Button *Installieren* von der Startseite der zum Lieferumfang gehörenden Produkt-CD.

Starten Sie *WuTility* anschließend über

Start → *Programme* → *Wutility Version 4* → *WuTility*

Start des Vergabe Dialogs

Stellen Sie sicher, dass das Interface *Network 1* der Microwall Gigabit 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 manuell beliebig oft durch Betä-

tigen des Buttons *Scannen* wiederholen:



Innerhalb der Inventarliste können Sie die gewünschte Microwall Gigabit anhand ihrer MAC-Adresse identifizieren. Ab Werk lautet die IP-Adresse 190.107.233.110.

Unbenannt - WuTility							
Datei	Gerät	Konfiguration	Firmware	Optionen	Hilfe		
Neu	Öffnen	Speichern	Scannen	IP-Adresse	Telnet	Browser	Hilfe
Ethernet-Adresse	IP-Adresse	Netzmaske	Gateway	Produktnummer	Produktname	Version	
00c03d:df3245	190.107.233.110	255.255.255.0	0.0.0.0	#552.10	Microwall Gigabit	1.04	

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



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

Geräteeinstellungen: Netzwerkparameter

dynamisch (DHCP)

statisch

IP-Adresse (muss eindeutig sein): 10 . 40 . 100 . 1

Adressbereich: Netzwerk #0

Diese Adresse ist möglicherweise noch frei. Erneut prüfen

Subnetzmaske: 255 . 255 . 0 . 0

Standardgateway: 10 . 40 . 0 . 254

DNS-Server A: 10 . 40 . 1 . 254

DNS-Server B:

Vorgabe

< Zurück
Weiter >
Abbrechen

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

Die IP-Vergabe mit WuTility kann so lange wiederholt werden, bis die Microwall Gigabit über die initiale Webseite ein Systempasswort erhalten hat. Anschließend ist eine Änderung der IP-Parameter nur noch über das Standard Web-Based-Management möglich.

ment 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*.

3.2 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- oder per WuTility vergebene IP-Adresse erreichbar. Stellen Sie daher sicher, das in dem Zeitraum bis zur Passwortvergabe auf der initialen Webseite keine unberechtigten Zugriffe auf die Microwall Gigabit 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 ein Microwall Gigabit eine neue IP-Adresse erhalten hat, darf die nächste Microwall Gigabit an das Netzwerk angeschlossen werden.*

Rechnerseitig muss hierfür eine der beiden folgenden Voraussetzungen erfüllt sein:

- Die IP-Adresse des verwendeten Rechners liegt im Subnetz-Bereich 190.107.233.0 oder wird temporär auf einen passenden Wert geändert. Für eine Änderung der IP-Adresse des Rechners benötigen Sie Administratorrechte. Klären Sie eine solche Änderung im Vorfeld mit dem zuständigen Netzwerk-Administrator ab.
- Der verwendete Rechner erhält temporär eine feste Route, welche die IP-Adresse 190.107.233.110 in das lokale Netzwerk umlenkt. Für das Einrichten einer solchen Route werden Administratorrechte benötigt. Der Befehlszeilen-Syntax für das Anlegen einer festen Route unter Windows lautet:

```
route ADD 190.107.233.110 MASK 255.255.255.255 [IP-Adresse PC]
```

Die für die Erstinbetriebnahme erforderlichen weiteren Para-

meter werden anschließend über eine initiale Webseite mit Hilfe eines Browsers vorgenommen. Informationen hierzu finden Sie im Kapitel *Initiale Webseite der Erstinbetriebnahme*.

3.2 Initiale Webseite der Erstinbetriebnahme

Die initiale Webseite steht nur bei der Erstinbetriebnahme und nach einem Reset auf Werkseinstellungen zur Verfügung. Sie dient in erster Linie dazu das Passwort für den weiteren Vollzugriff auf das Web-Based-Management der Microwall zu konfigurieren. Gleichzeitig besteht die Möglichkeit die IP-Basisparameter der beiden Netzwerkschnittstellen und die Betriebsart zu bestimmen.

Netzwerkverbindungen zwischen den beiden Netzwerken der Microwall werden die Vergabe der hier verfügbaren Parameter noch nicht erlaubt. Kommunikationsfreigaben müssen später in Form von Whitelist-Regeln für die gewählte Betriebsart ausdrücklich freigegeben werden.

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

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



Soll der Zugriff über die Default-IP-Adresse der Microwall Gigabit 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 selbst-signierten Zertifikat ausgestattet. Entsprechende Warnungen des verwendeten Browsers müssen im Zuge der Erstinbetriebnahme ignoriert und/oder quittiert werden. Nach der Inbetriebnahme kann das Default-Zertifikat über das Web-Based-Management durch ein

eigenes Individual-Zertifikat ersetzt werden kann.

Alle vorgenommenen Einstellungen können später über das Standard Web-Based-Management noch geändert werden.

[Microwall-affe70](#) >> **Erstinbetriebnahme**

Erstinbetriebnahme

Die folgenden Einstellungen helfen Ihnen, die Microwall für den ersten Einsatz zu konfigurieren. Alle hier vorgenommenen Einstellungen können zu einem späteren Zeitpunkt über das Konfigurationsmenü der Microwall geändert werden.

Passwort 
Administrator-Passwort für das Web-Based-Management. Wir empfehlen sichere Passwörter mit mindestens 15 Zeichen, Groß-/Kleinbuchstaben, Ziffern und Sonderzeichen.
Passwort:
<input type="text"/>
Wiederholen:
<input type="text"/>

Netzwerkschnittstelle Network 1 
Die IP-Parameter der Schnittstelle Network 1 für den Anschluss des übergeordneten Intranets. Das angegebene Gateway agiert als Default-Gateway für alle Ziel-Netzwerke ohne statische Route.
IP-Adresse:
<input type="text" value="10.40.21.187"/>
Subnet-Mask:
<input type="text" value="255.255.0.0"/>
Gateway:
<input type="text" value="10.40.0.1"/>
DNS-Server 1:
<input type="text" value="10.40.250.252"/>
DNS-Server 2:
<input type="text"/>

Netzwerkschnittstelle Network 2 
Die IP-Parameter der Schnittstelle Network 2 für den Anschluss der zu schützenden Netzwerk-Insel. Die Net-IDs der Schnittstellen Network 1 und Network 2 müssen unterschiedlich sein.
IP-Adresse:
<input type="text" value="190.107.234.110"/>
Subnet-Mask:
<input type="text" value="255.255.255.0"/>

Betriebsart 
Durch die Wahl der Betriebsart werden noch keine Verbindungen zwischen den Netzwerken freigegeben. Diese müssen später in Form expliziter Freigabe-Regeln erlaubt werden.
Standard-Router: Das Insel-Netz (Anschluss Network 2) muss im Intranet (Anschluss Network 1) bekannt, und in das dortige Routing-Konzept z.B. über statische Routen integriert sein.
NAT-Router: Das Insel-Netz (Anschluss Network 2) wird über eine IP-Adresse des Intranets (Anschluss Network 1) in das dortige Netz eingebunden. Es ist kein Eingriff in das Intranet-Routing-System erforderlich.
<input type="radio"/> Standard-Router
<input type="radio"/> NAT-Router

Passwort (Pflichtfeld)

Vergeben Sie das Passwort für den Zugriff auf das Web-Based-Management der Microwall Gigabit. 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 mit physikalischem Zugriff auf das Gerät und den per Service-Taster aktivierbaren Notzugang oder einen Reset auf die Werkseinstellungen zurückgesetzt werden.*

Network 1 (gelb)

Wenn der Browser-Zugriff über die Default-IP der Microwall Gigabit erfolgt ist, tragen Sie hier jetzt die für ihre Anwendung gültigen Werte ein.

Die Angabe von DNS-Servern ist nur erforderlich, wenn der/die Timeserver für den NTP-Client der Microwall Gigabit in Form eines Hostnames konfiguriert werden.

Network 2 (grün)

Vergeben Sie hier die IP-Adresse und Subnet-Mask für das Interface *Network 2* der Microwall Gigabit. Die Net-IDs der 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 in Form von statischen Routen konfiguriert werden.

Betriebsart (Pflichtfeld)

Wählen Sie die gewünschte Betriebsart der Microwall Gigabit aus. Weitere Informationen hierzu finden Sie im Kapitel *Betriebsarten und Regel-Konfiguration*.

Mit einem Klick auf Anwenden werden eingegebenen Parameter gespeichert und Sie werden automatisch auf die Standard Konfigurationsseiten der Microwall weitergeleitet.

4 Web-Based-Management

Die Konfiguration der Microwall Gigabit ist ausschließlich verschlüsselt per HTTPS möglich. Das WBM (Web-Based-Management) arbeitet sessionorientiert, vorgenommene Änderungen werden mit dem Anwenden-Button jedoch sofort gespeichert und gültig.

■ Navigation innerhalb des WBM

4.1 Start und Navigationskonzept des WBM

Um auf das WBM der Microwall Gigabit zuzugreifen benötigen Sie einen aktuellen Internet-Browser. Session-Cookies und Javascript müssen aktiviert sein.

Der Zugriff auf die Webseiten ist ausschließlich verschlüsselt über über HTTPS möglich. Ab Werk ist der Standardport 443 vorkonfiguriert.

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

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

4.1.1 Navigationskonzept der Microwall Gigabit

Das WBM der Microwall Gigabit arbeitet sessionorientiert über ein passwortgeschütztes Login. Ein Betrieb ohne Passwort ist nicht möglich. Es muss wird im Zuge der Erstinbetriebnahme vergeben werden.

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

Das Beenden einer Konfigurations-Session ist jederzeit über den Button *Abmelden* unterhalb des Navigationsbaums möglich.

4.2 Anmelden/Abmelden

Einstellungen an der Microwall Gigabit werden innerhalb passwortgeschützter Konfigurations-Sessions vorgenommen. Diese sind exklusiv, d.h. zu einem Zeitpunkt kann nur eine Session aktiv sein.

Die Startseite der Microwall bietet nur die Möglichkeit der Passwort-Eingabe für das Login sowie die Umschaltung der Oberflächen-Sprache zwischen Deutsch und Englisch über die Flaggensymbole unter dem Menübaum.

4.2.1 Anmelden



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

i *Zum Schutz vor Brute-Force-Attacks 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* unter dem Navigationsbaum.

4.3 Hilfe und Beschreibungstexte

Sofern die einzelnen Konfigurations-Punkte nicht selbsterklärend sind, erhalten die zugeordneten Info-Symbole die nötigen Beschreibungen, Erklärungen und Hinweise.

Detailinformationen zu den Betriebsarten und den Freigabe-Regeln 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 Funktionsweise der Microwall Gigabit

Die Microwall Gigabit ist als IPv4-Router mit integrierter Whitelist-Firewall konzipiert. Sie lagert schutzbedürftige Netzwerkkomponenten in ein Teilnetzwerk (*Network 2*, grün) aus und erlaubt nur ausdrücklich über Filterregeln freigegebene Kommunikationsverbindungen in das bzw. aus dem übergeordneten Netzwerk (*Network 1*, gelb).

Die beiden nachfolgend beschriebenen Betriebsarten NAT-Router und Standard-Router verfügen über jeweils eigene, auf Quell-/Zieladresse, Quell-/Zielport und Protokoll basierende Regel-Listen.

5.2 Betriebsarten & Umschaltung

5.2.1 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 eine öffentliche IP-Adresse an das Internet anbinden.

Die IP-Adressen der Insel-Hosts werden auf der Intranet-Seite durch die dortige IP-Adresse der Microwall Gigabit ersetzt und sind somit zu keinem Zeitpunkt im Intranet sichtbar. Der Insel-IP-Bereich kann daher 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.

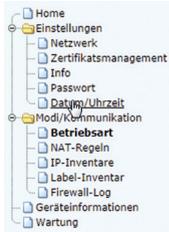
5.2.2 Modus Standard-Router

Im Modus Standard-Router trennt die Microwall Gigabit das Insel-Netzwerk am Anschluss *Network 2* (grün) vom Unternehmens-Intranet am Anschluss *Network 1* (gelb). Das Insel-Netzwerk wird aber zu einem *offiziellen* Subnetz der Intranet-seitigen Infrastruktur. Häufig wird die Insel ein Randnetz sein, in welchem die Microwall Gigabit der einzige Router ist und somit auf den Insel-Hosts als Standardgateway eingetragen werden kann. Intranetseitig sind hingegen häufig weitere Router (z.B. WAN/DSL-Anbindung) vorhanden, so dass hier der Pfad zum Insel-Netzwerk in Form von statischen Routen auf den beteiligten Hosts bekannt gemacht werden muss.

5.2.3 Umschaltung der Betriebsarten

Die Umschaltung der zwischen den Betriebsarten NAT-Router und Standard-Router erfolgt über den Link *Betriebsart* im

Menübaum des Web-Managements.



Microwall-affe70 >> Modi/Kommunikation >> Betriebsart

Betriebsart

Auswahl der Betriebsart Standard-Router oder NAT-Router und ICMP-Handling

Einstellen der Betriebsart

Betriebsart: Router-Modus: ?

- Standard-Router ?
 - Ping auf lokale Interfaces zulassen ?
 - Ping Net 2 Insel -> Net 1 Intranet zulassen
 - Ping Net 1 Intranet -> Net 2 Insel zulassen
- NAT-Router

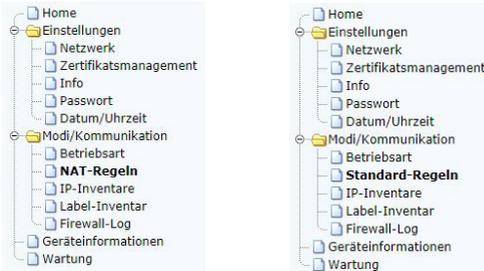
Neben der Betriebsart wird hier jeweils auch die Behandlung und Weiterleitung von ICMP Requests/Replies (ping) festgelegt.

Die Microwall Gigabit verfügt über zwei voneinander unabhängige Regellisten für jede Betriebsart. Der Zugriff ist immer nur auf die zur aktuell aktiven Betriebsart gehörende Regelliste möglich.

Bei Umschaltung der Betriebsart kann entschieden werden, ob die Regeln des vorherigen Modus gelöscht oder gespeichert werden sollen.

5.3 Regel-Übersichten & Label

Je nach gewählter Betriebsart führt der Link *NAT-Regeln* oder *Standard-Regeln* im Menübaum auf die Seite mit der Übersicht aller angelegten Regeln.



Network 1		Network 2									
IP-Adresse(n) Name	Port	IP-Adresse(n) Name	Port								
<table border="1"> <thead> <tr> <th>Web-Traffic to Network 1</th> <th>TCP</th> <th></th> <th>Bearbeiten</th> </tr> </thead> <tbody> <tr> <td>ANY any</td> <td>80, 443</td> <td>10.110.0.0/16 insel-subnet</td> <td>ANY</td> </tr> </tbody> </table>				Web-Traffic to Network 1	TCP		Bearbeiten	ANY any	80, 443	10.110.0.0/16 insel-subnet	ANY
Web-Traffic to Network 1	TCP		Bearbeiten								
ANY any	80, 443	10.110.0.0/16 insel-subnet	ANY								
<p>● Normalbetrieb</p> <p>markierte aktivieren markierte deaktivieren markierte löschen</p>											

Jede Regel wird in einem eigenem Übersichtsblock dargestellt. Dieser enthält Informationen über die verwendeten Quell-/Ziel-Host(s) und Quell-/Ziel-Ports. Die Richtung der Regel aus Sicht des Verbindungsaufbaus ist durch den großen Pfeil der Symbole und dargestellt. Das Symbol gibt an, dass jede Verbindung entsprechend der Regel-Definition einen Eintrag in das Log der Microwall Gigabit erzeugt.

5.3.1 Label

Werden einer Regel bei der Erstellung ein oder mehrere Label zugewiesen, können diese in der Regelübersicht als Anzeige-Filter verwendet werden.

Ist in der Filterung kein Label aktiviert, werden alle Regeln angezeigt. Sobald ein oder mehrere Label aktiviert sind, zeigt die Regelübersicht nur Regeln, die mindestens eins dieser Labels enthalten.

5.3.2 Erstellen und Verwalten von Labels

Neben den beiden ab Werk angelegten Labels *Normalbetrieb* und *Wartung*, können über den Link *Label-Inventar* im Menübaum eigene Label angelegt werden.

[Microwall.affe70](#) >> [Modi/Kommunikation](#) >> **Label-Inventar**

Label-Inventar

Übersicht und Konfiguration der Labels mit denen Filter-Regeln zur übersichtlicheren Darstellung gekennzeichnet werden können.

Labels		
<input type="checkbox"/>	Beschriftung	Kommentar
<input type="checkbox"/>	● Wartung	<input type="button" value="Bearbeiten"/>
<input type="checkbox"/>	● Normalbetrieb	<input type="button" value="Bearbeiten"/>

[markierte löschen](#)

Klicken Sie auf den Button Hinzufügen und vergeben Sie einen Namen, eine optionale Beschreibung und weisen Sie eine beliebige Farbe zu.

5.4 Erstellen von Firewall-Regeln

Die Erstellung von Firewall-Regeln für die Kommunikation ist für die folgenden Betriebsarten und Verbindungs-Richtungen weitestgehend identisch:

- Modus Standard-Router beide Richtungen
- Modus NAT-Router Richtung *Network 2* (grün) nach *Network 1* (gelb)

Abhängig von der gewählten Betriebsart, startet ein Klick auf *NAT-Router* oder *Standard-Router* im Menübaum den Regel-Dialog.

The screenshot shows a dialog box titled "Regel anlegen/bearbeiten" (Create/Edit Rule). It contains the following fields and options:

- Bezeichnung:** Name: [text input], Beschreibung: [text area]
- Richtung:** Radio buttons for "Network 1 >> Network 2" (selected) and "Network 2 >> Network 1".
- Network 1 (yellow background):** Ziel-IP-Adresse(n) | Name: [dropdown menu], Ziel-IP-Adresse(n) / IP-Bereich(e): [text input], Name: [text input], Ziel-Port(s): [text input]
- Network 2 (green background):** Quell-IP-Adresse(n) | Name: [dropdown menu], Quell-IP-Adresse(n) / IP-Bereich(e): [text input], Name: [text input], Quell-Port(s): [text input]
- Protokoll:** Radio buttons for TCP (selected), FTP, and UDP.
- Aktion:** Checkboxes for Loggen and Akzeptieren.
- Aktivieren:** Checkboxes for [] and [] (likely "Aktivieren" and "Deaktivieren").
- Label:** Radio buttons for "Wartung" (selected) and "Normalbetrieb". Below this is the text "Bearbeiten der Labels unter Modi/Kommunikation >> Label-Inventar".

Buttons at the bottom: Anwenden, Abbrechen.

Bezeichnung

Der angegebene individuelle *Name* (Pflichtfeld) indentifiziert die Regel in der Regelübersicht. Die optionale *Beschreibung* dient ausschließlich der Information in diesem Dialog.

Richtung

Festlegung der Richtung für die Regel aus Sicht des Verbindungsaufbaus bei TCP. Bei UDP bestimmt das initiale UDP-Datagramm die Richtung.

Network 1 (gelb) & Network 2 (grün)

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 werden das/die Ziel/Quelle automatisch mit der unter *Name* angegebenen Bezeichnung in das IP-Inventar übernommen.

Zulässige numerische Angaben der Adressen:

- *any*
Schlüsselwort für beliebige IP-Adressen
- *einzelne IP-Adresse*
IP-Adresse in Dot-Notation (z.B. 10.20.0.4)
- *Komma-getrennte IP-Adress-Liste*
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.

Bei der Angabe des/der Port(s) sind folgende Eingaben zulässig:

- *any*

Schlüsselwort für beliebige Portnummer

- *einzelne Portnummer*
z.B. 8000
- *Komma-getrennte 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 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.

Aktion

Akzeptieren erlaubt den durch die Regel definierten Datenverkehr.

Loggen erzeugt für jeden Verbindungsaufbau entsprechend der Regel einen Eintrag im Logfile der Microwall.

Aktivieren

Aktiviert die Regel sofort nach Betätigung des Buttons *Anwenden*.

Ist die Option nicht gesetzt, wird mit Betätigung von *Anwenden* die Regel zwar angelegt aber nicht angewendet;

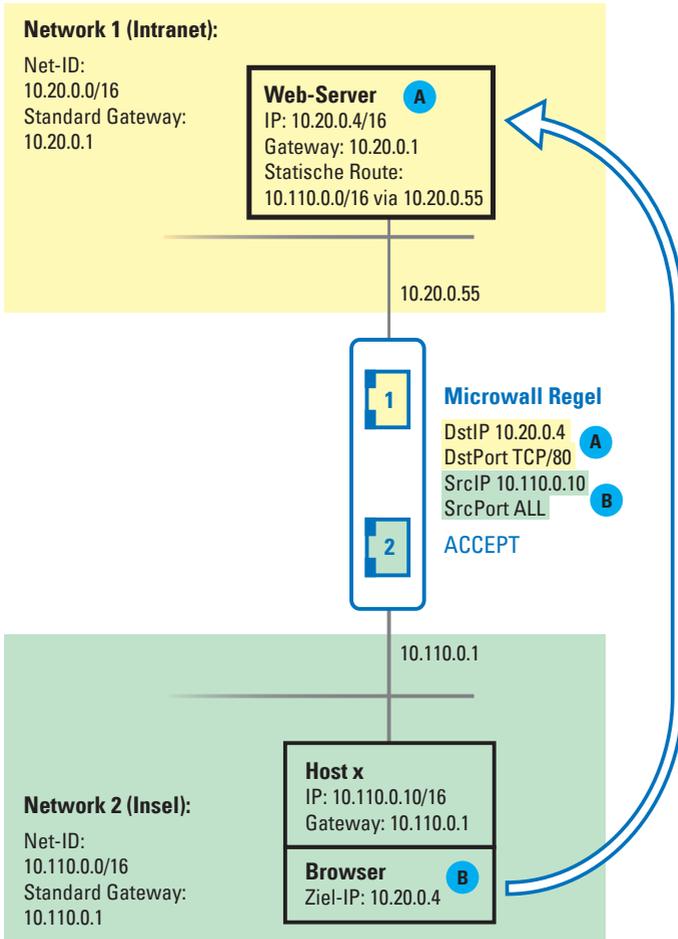
Datenverkehr entsprechend der Regel ist nicht möglich. Eine Aktivierung der Regel kann nachträglich in der Regelübersicht erfolgen.

Label

Zu übersichtlicheren Darstellung bzw. Anzeige-Filterung in der Regelübersicht, können der Regel ein oder mehrere Label zugewiesen werden. Ab Werk sind die Label *Normal mode* und *Service* vorinstalliert. Über den Link *Label-Inventar* im Menübaum können weitere eigene Label angelegt werden.

5.4.1 Beispiel Firewall-Regel

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 Microwall Gigabit selbst ist mit den IPs 10.110.0.1 und 10.20.0.55 in die Netze integriert. Die Regel soll in der Regelübersicht mit dem Label *Normalbetrieb* gekennzeichnet sein.



Der zu diesem Beispiel auszufüllende Regeldialog:

NAT-Regel anlegen/bearbeiten

Bezeichnung: Name: ⓘ

Beschreibung:

Richtung: Network 1 >> Network 2 ⓘ
 Network 2 >> Network 1 ⓘ

Network 1: Ziel-IP-Adresse(n) | Name: ⓘ
Ziel-IP-Adresse(n) / IP-Bereich(e): ⓘ
Name: ⓘ
Ziel-Port(s): ⓘ

Network 2: Quell-IP-Adresse(n) | Name: ⓘ
Quell-IP-Adresse(n) / IP-Bereich(e): ⓘ
Name: ⓘ
Quell-Port(s): ⓘ

Protokoll: TCP ⓘ
 FTP ⓘ
 UDP ⓘ

Aktion: Loggen ⓘ
 Akzeptieren ⓘ

Aktivieren: ⓘ

Label: Wartung ⓘ Normalbetrieb ⓘ
Bearbeiten der Labels unter Modi/Kommunikation >> Label-Inventar

Anwenden Abbrechen

5.5 Erstellen von Firewall-NAT-Regeln

Die Erstellung von Firewall-NAT-Regeln für die Kommunikation ist für die folgende Betriebsart und Verbindungs-Richtung möglich:

- Modus NAT-Router Richtung *Network 1* (gelb) nach *Network 2* (grün)

Ein Klick auf *NAT-Router* im Menübaum startet den Regel-Dialog.

NAT-Regel anlegen/bearbeiten

Bezeichnung: Name:
Beschreibung:

Richtung: Network 1 >> Network 2
 Network 2 >> Network 1

Network 1: Quell-IP-Adresse(n) | Name:
>> Neues Element anlegen oder wählen <<
Quell-IP-Adresse(n) / IP-Bereich(e):
Name:
Ziel-Port(s):

Network 2: Ziel-IP-Adresse | Name:
>> Neues Element anlegen oder wählen <<
Ziel-IP-Adresse:
Name:
Ziel-Port:

Protokoll: TCP
 FTP
 UDP

Aktion: Loggen
 Akzeptieren

Aktivieren:

Label: Wartung Normalbetrieb
Bearbeiten der Labels unter Modi/Kommunikation >> Label-Inventar

Anwenden Abbrechen

Bezeichnung

Der angegebene individuelle *Name* (Pflichtfeld) indentifiziert die Regel in der Regelübersicht. Die optionale *Beschreibung* dient ausschließlich der Information in diesem Dialog.

Richtung

Firewall-NAT-Regeln können nur im Modus NAT-Router für die Richtung von *Network 1* (gelb) nach *Network 2* (grün) angelegt werden. Die Richtung definiert sich bei TCP aus Sicht des Verbindungsaufbaus und bei UDP durch das initiale UDP-Datagramm.

Network 1 (gelb)

Die *Quell-IP-Adresse(n)* aus dem Intranet am Anschluss *Network 1* kann/können entweder über die Select-Box aus der Inventarliste ausgewählt oder direkt numerisch angegeben werden. Bei numerischer Angabe wird die Quelle bzw. der Quellbereich automatisch mit der unter *Name* angegebenen Bezeichnung in das IP-Inventar für *Network 1* übernommen.

Zulässige numerische Angaben der Quell-Adressen:

- *any*
Schlüsselwort für beliebige IP-Adressen
- *einzelne IP-Adresse*
IP-Adresse in Dot-Notation (z.B. 10.20.0.4)
- *Komma-getrennte IP-Adress-Liste*
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.

Der/die Ziel-Port(s) ist die Portnummer, zu welcher der Client im *Network 1* eine Verbindung initiiert. Die Microwall Gigabit überwacht eingehende Pakete mit diesem Zielport und leitet diese an das im Bereich *Network 2* definierte Ziel-System weiter. Bei der Angabe des/der Ziel-Port(s) sind folgende Eingaben zulässig:

- *any*
Schlüsselwort für beliebige Portnummer
- *einzelne Portnummer*
z.B. 8000
- *Komma-getrennte 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.

Network 2 (grün)

Hier erfolgt die Angabe des Zielsystems (Ziel-IP und Ziel-Port) am Anschluss *Network 2*, an welches die im Bereich *Network 1* definierten Verbindungen weitergeleitet werden.

Die *Ziel-IP-Adresse* am Anschluss *Network 2* kann entweder über die Select-Box aus der Inventarliste ausgewählt oder direkt numerisch angegeben werden. Bei numerischer Angabe wird das Ziel automatisch mit der unter *Name* angegebenen Bezeichnung in das IP-Inventar für *Network 2* übernommen.

Zulässige numerische Angaben der Ziel-Adresse:

- *einzelne IP-Adresse*
IP-Adresse in Dot-Notation (z.B. 10.20.0.4)

Bei der Angabe des Ziel-Port ist folgende Eingabe zulässig:

- *einzelne Portnummer*
z.B. 8000

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* automatisch erlaubt und gesperrt.

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

Aktion

Akzeptieren erlaubt den durch die Regel definierten Datenverkehr.

Loggen erzeugt für jeden Verbindungsaufbau entsprechend der Regel einen Eintrag im Logfile der Microwall.

Aktivieren

Aktiviert die Regel sofort nach Betätigung des Buttons *Anwenden*.

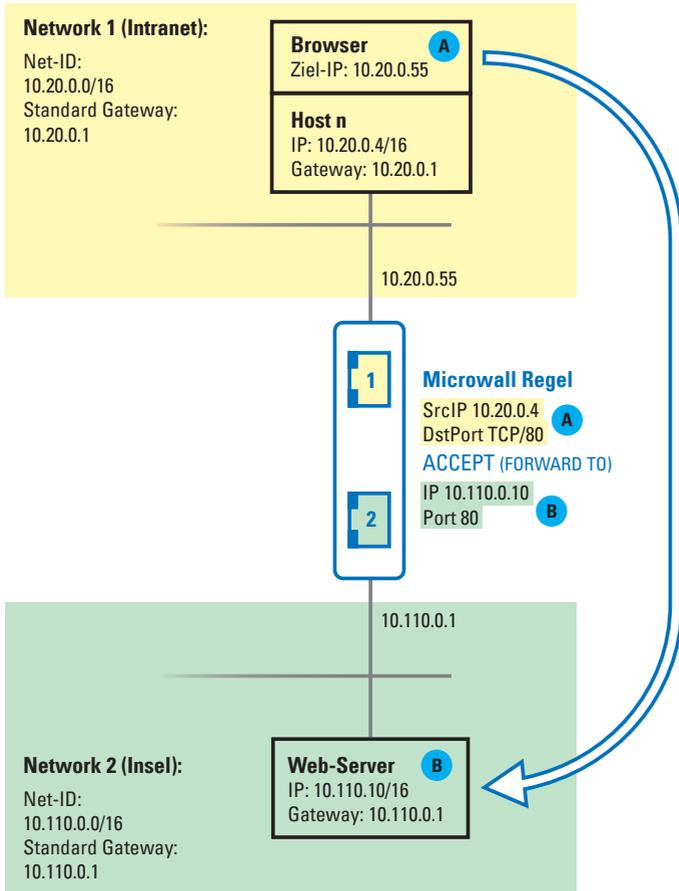
Ist die Option nicht gesetzt, wird mit Betätigung von *Anwenden* die Regel zwar angelegt aber nicht angewendet. Datenverkehr entsprechend der Regel ist nicht möglich. Eine Aktivierung der Regel kann nachträglich in der Regelübersicht erfolgen.

Label

Zu übersichtlicheren Darstellung bzw. Anzeige-Filterung in der Regelübersicht, können der Regel ein oder mehrere Label zugewiesen werden. Ab Werk sind die Label *Normalbetrieb* und *Wartung* vorinstalliert. Über den Link *Label-Inventar* im Menübaum können weitere eigene Label angelegt werden.

5.5.1 Beispiel Firewall-NAT-Regel

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 Gigabit 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 Gigabit verwendet, wo sie dann per Regel durch die Insel-IP 10.110.0.10 ersetzt wird.



Der zu diesem Beispiel auszufüllende Regeldialog:

NAT-Regel anlegen/bearbeiten	
Bezeichnung:	Name: <input type="text" value="Regel 2"/> ⓘ
	Beschreibung: <input type="text" value="Beispiel NAT-Regel"/>
Richtung:	<input checked="" type="radio"/> Network 1 >> Network 2 ⓘ <input type="radio"/> Network 2 >> Network 1
Network 1:	Quell-IP-Adresse(n) Name: <input type="text" value="Intranet-Host"/> ⓘ >> Neues Element anlegen oder wählen << ▾ ⓘ Quell-IP-Adresse(n) / IP-Bereich(e): <input type="text" value="10.20.0.4"/> ⓘ Name: <input type="text" value="Intranet-Host"/> ⓘ Ziel-Port(s): <input type="text" value="80"/> ⓘ
Network 2:	Ziel-IP-Adresse Name: <input type="text" value="Insel Web-Server"/> ⓘ >> Neues Element anlegen oder wählen << ▾ ⓘ Ziel-IP-Adresse: <input type="text" value="10.110.0.10"/> ⓘ Name: <input type="text" value="Insel Web-Server"/> ⓘ Ziel-Port: <input type="text" value="80"/> ⓘ
Protokoll:	<input checked="" type="radio"/> TCP ⓘ <input type="checkbox"/> FTP ⓘ <input type="radio"/> UDP ⓘ
Aktion:	<input type="checkbox"/> Loggen ⓘ <input checked="" type="checkbox"/> Akzeptieren ⓘ
Aktivieren:	<input checked="" type="checkbox"/> ⓘ
Label:	<input type="checkbox"/> <input checked="" type="radio"/> Wartung ⓘ <input checked="" type="radio"/> <input type="radio"/> Normalbetrieb ⓘ Bearbeiten der Labels unter Modi/Kommunikation >> Label-Inventar ⓘ
<input type="button" value="Anwenden"/> <input type="button" value="Abbrechen"/>	

6 Security & Wartung

- Firmware-Updates
- Eigene Zertifikate
- Deaktivierung nicht benötigter Dienste
- Notzugang per Service-Taster
- Reset auf Werkseinstellungen per Service-Taster

6.1 Firmware-Updates

Die Firmware der Microwall Gigabit wird ständig weiterentwickelt. Das folgende Kapitel beschreibt aus diesem Grund das Verfahren einen Upload der Firmware durchzuführen.

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

6.1.1 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:

<http://www.wut.de>

Sie navigieren von dort aus am einfachsten mit Hilfe 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, der auch die Ethernet-Adresse aufweist.

Typnummer



Auf dem Web-Datenblatt der Microwall Gigabit 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.

6.1.2 Firmware Update mit WuTility

Für den 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-Parametern erlauben.

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

Microwall.affe70 >> Einstellungen >> Netzwerk

Netzwerk

Konfiguration der Netzwerk-Interfaces der Microwall und Management der eingehenden Dienste

Basis-Netzwerkeinstellungen

Management	
Browsezugriff:	<input checked="" type="checkbox"/> aktiviert <input checked="" type="checkbox"/> für den Zugriff aus dem Network 1-Netzwerk erlauben <input type="checkbox"/> für den Zugriff aus dem Network 2-Netzwerk erlauben HTTPS-Port: <input type="text" value="443"/>
Inventarisierung (UDP/8513):	<input checked="" type="checkbox"/> aktiviert <input checked="" type="checkbox"/> aus dem Network 1-Netzwerk erlauben <input type="checkbox"/> aus dem Network 2-Netzwerk erlauben
Firmware-Update (TCP/5555):	<input checked="" type="checkbox"/> aktiviert <input checked="" type="checkbox"/> aus dem Network 1-Netzwerk erlauben <input type="checkbox"/> aus dem Network 2-Netzwerk erlauben

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

Für die Übertragung der neuen Firmware an die Microwall Gigabit 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 führt das Gerät automatisch einen Neustart durch und ist anschließend wieder betriebsbereit.

6.1.3 Firmware Update per Web-Based-Management

In Netzwerkumgebungen die den Einsatz von WuTility nicht zulassen oder in denen aus Sicherheitsgründen der Up-

date-Service in der Microwall deaktiviert wurde, kann der Firmware-Update aus dem Web-Based-Management heraus erfolgen.

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

Wartung		⌵
Geräte-Neustart:	<input type="button" value="Neustart"/>	i
Gerät auf Werkseinstellungen setzen:	<input type="button" value="Zurücksetzen"/>	i
Debuginfo herunterladen:	<input type="button" value="Download"/>	
Notzugang per Service-Taster:	<input checked="" type="checkbox"/> HTTPS-Notzugang über Port 446 (Taster 3,5 bis 10s halten) <input checked="" type="checkbox"/> Setzen der Werkseinstellungen (Taster 20s halten)	i
Firmware-Update:	<input type="button" value="Datei auswählen"/> <input type="button" value="Keine ausgewählt"/>	

Wählen Sie die zuvor heruntergeladene und entpackte Firmware-Datei (*.uhd) aus und betätigen dann den Button *Anwenden*. Mit Bestätigung der Sicherheitsabfrage startet wird der Update gestartet.

6.2 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 Gigabit, erzeugt bei aktuellen Browsern entsprechende Sicherheitswarnungen. Diese müssen bei WBM-Zugriffen explizit quittiert und/oder mit geeigneten Ausnahme-Regeln bestätigt werden.

In Netzwerkkumgebungen mit erhöhten Sicherheitsanforderungen oder in denen diese Ausnahmen nicht erwünscht sind, kann das Werks-Zertifikat durch ein individuelles Zertifikat ersetzt werden.

Erzeugung, Signatur und Installation eines eigenen Zertifikates unterteilen sich hierbei in die folgenden groben Schritte:

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

Klicken Sie im Menübaum auf den Link *Zertifikatsmanagement*. Neben Informationen zu dem aktuell installierten Zertifikat, sind hier alle Funktionen für das Handling individueller Zertifikate enthalten:

Zertifikatsmanagement

Erstellung, Upload, Download und Installation individueller Zertifikate

Aktuelle Installation	
Aktuelles Zertifikat:	Installationsart: <input type="text" value="Selbstsigniertes Zertifikat"/> i Gültig bis: 13.12.2026
CSR (Certificate Signing Request)	
Informationen:	Common Name: <input type="text"/> i Organization Name: <input type="text"/> Organizational Unit: <input type="text"/> City or Locality: <input type="text"/> State or Province: <input type="text"/> Country (2 Letter Code): <input type="text"/> Email-Address: <input type="text"/> Alternative Names: <input type="text"/>
Aktion:	CSR erstellen: <input type="button" value="Erstellen"/> i CSR löschen: <input type="button" value="Löschen"/> i
Selbstsigniertes Zertifikat	
Aktion:	Selbstsigniertes Zertifikat erstellen und installieren: <input type="button" value="Installieren"/> i
Extern signiertes Zertifikat	
Download:	CSR Download: <input type="button" value="Download"/> i
Upload:	Zertifikat: <input type="button" value="Datei auswählen"/> Keine ausgewählt i Zertifikats-Kette: <input type="button" value="Datei auswählen"/> Keine ausgewählt
Aktion:	Zertifikat installieren: <input type="button" value="Installieren"/> i

Erzeugen ein 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 Gigabit später im Browser aufgerufen wird. Unter *Alternative Names* können zusätzliche Namen, IP-Adressen und auch Wildcard-Namen eingegeben werden. Der in *Common Name* eingetragene Name wird automatisch in die Alternative Names übernommen.

Durch Klick auf *Erstellen* generiert die Microwall Gigabit ein RSA-Schlüssel-Paar und erstellt aus dem Public-Key und den getätigten Angaben ein CSR.

Installation eines selbstsignierten Zertifikates

Durch Klick auf *Installieren* unter *Selbstsigniertes Zertifikat*, kann das CSR 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 *Download* zum Zweck einer externen Signatur von der Microwall Gigabit heruntergeladen werden. Der Download erfolgt im PEM-Format

Nach der Signatur durch die Zertifizierungsstelle (CA) können das Zertifikat sowie eine eventuell benötigte Zertifikats-Kette über die entsprechenden Upload-Buttons in die Microwall Gigabit 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, der Zertifikats-Kette und das Gültigkeits-Datum.

6.3 Deaktivierung nicht benötigter Dienste

Die Microwall Gigabit stellt drei eingehende eigene Dienste zur Verfügung:

Port-/Socket-nummer	Anwendung	System-passwort-Schutz?	Konfigurier-/abschaltbar?
443 (TCP)	HTTPS-Management	ja	ja/ja
8513 (UDP)	Inventarisierung	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.

i *In Netzwerkkumgebungen mit erhöhten Sicherheitsanforderungen kann es sinnvoll sein, nach der Einrichtung der Kommunikations-Regeln im operativen Betrieb alle eingehenden Dienste zu deaktivieren. Für eventuelle später erforderliche Änderungen kann der Webzugriff über den per Service-Taster zugänglichen Notzugang bedarfsgesteuert jederzeit wieder aktiviert werden. (s. Kapitel Notzugang per Service-Taster).*

6.4 Notzugang der Microwall Gigabit

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.



Service-Taster

Start 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 mit langsam blinkt. Wenn Sie den Taster jetzt lösen, ist der Notzugang aktiviert.

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

i *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](https://[IP-Adresse|Hostname]:446)

Ohne Passwort-Abfrage gelangen Sie auf die folgende Webseite:

Microwall-08686c >> Notzugang

Notzugang

Ändern Sie hier das Loginpasswort		⌵
Einstellungen:	Passwort ändern:	ⓘ
<input type="checkbox"/>		
Management		⌵
Browserzugriff:	<input checked="" type="checkbox"/> aktiviert	
	<input checked="" type="checkbox"/> für den Zugriff aus dem Network 1-Netzwerk erlauben	
	<input type="checkbox"/> für den Zugriff aus dem Network 2-Netzwerk erlauben	
HTTPS-Port:	<input type="text" value="443"/>	
<input type="button" value="Anwenden"/>		<input type="button" value="Abbrechen"/>

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 Giga-bit 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 wieder der Zugriff auf das passwortgeschützte Standard Web-Interface über den konfigurierten TCP-Port möglich.

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

6.5 Werkseinstellungen

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



Service-Taster

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 Standard-Betrieb entsprechend der aktuellem Konfiguration fort.

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

7 Anhang

- Technische Daten und Bauform
- Lizenzen

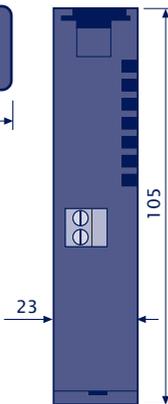
7.1 Technische Daten und Bauform

Spannungsversorgung ...	
Power-over-Ethernet:	37-57V DC aus PSE
Externe Speisung, Schraubklemme	DC 24-48V (+/-10%)
Stromaufnahme ...	
Power-over-Ethernet:	PoE Class 2 (3,84 W - 6,49W)
Ext. Speisung	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	-40 ... +85°C
... Betrieb, nicht angereicherte Montage	0 ... +50°C
Zulässige rel. Luftfeuchtigkeit	0 - 95% (nicht kondensierend)
Abmessungen	105 x 75 x 22mm
Gewicht	ca. 120g

Frontansicht 55210



Unterseite 55210



Maße in mm, +/-1mm

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**A**

Abmelden 33
Anmelden 33
Autocrossing 16
Auto Negotiation 16

B

Bauform 66
Betriebsarten 37

C

Certificate Signing Request
58

D

Default-IP-Adresse 25
Dienste 60

E

Erstinbetriebnahme 27

F

Firewall-Regeln 41
Firmware-Updates 54

H

Hardware-Installation 14
Hutschiene 14

I

Inbetriebnahme 21

L

Label 39
LED 17
Link-Status 17
Lizenzen 67

N

NAT-Regeln 47
NAT-Router 37
Navigationskonzept 32
Netzwerkschnittstellen 16
Notzugang 61
Notzugangs 19

P

PoE 15

R

Regel-Übersichten 39
Reset 19

S

Security 53
Service-Taster 19, 61, 63
Spannungsversorgung 15
Standard-Router 37
System LED 18

T

Technische Daten 65

W

Web-Based-Management 31
Werkseinstellung 19
Werkseinstellungen 63
WuTility 22

Z

Zertifikate 57

