

W&T

www.WuT.de

Anleitung

Inbetriebnahme und Anwendung

Microwall

gültig für folgende Modelle:

#55211: Microwall VPN
ab Firmware 1.36

#55212: Microwall IO
ab Firmware 1.12

Release 1.07 04/2023

© 04/2023 by Wiesemann und Theis GmbH

Microsoft und Windows, sind eingetragene Warenzeichen der Microsoft Corporation.

WireGuard und das WireGuard Logo sind eingetragene Warenzeichen von Jason A.Donenfeld

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. Weitere Informationen hierzu finden Sie auf Ihrem Gerät.

Zugehörige Quelltexte können Sie 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.

Einleitung

Die Microwall VPN und Microwall IO sind industrietaugliche IPv4-Router mit zwei 1000BaseT-Netzwerkanschlüssen, integrierter, whitelist-basierter Firewall sowie einem WireGuard VPN-Zugang. Sie binden eine Netzwerkinsel z.B. mit Automatisierungskomponenten an ein übergeordnetes lokales Netzwerk an. Parallel hierzu kann über das Wireguard VPN als Client oder Server ein sicherer Fernzugriff auf die Teilnehmer des Inselnetzwerkes erfolgen. Geeignete Filterregeln auf TCP/IP-Ebene schützen alle Netzwerke vor unberechtigter, unerwünschter und schädlicher Kommunikation.

Die Microwall IO verfügt über 2 digitale Eingänge und 2 digitale Ausgänge, welche in Automatisierungsumgebungen die Steuerung von Router-/Firewall-Funktionen und das Auswerten von Meldungen erlauben

1 Rechtliche Hinweise und Sicherheit	7
1.1 Rechtliche Hinweise	8
1.2 Sicherheitshinweise.....	10
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 IP-Vergabe per DHCP.....	22
3.2 Erstvergabe der IP-Parameter mit WuTility	23
3.3 Inbetriebnahme über die Default-IP-Adresse.....	26
3.4 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 DHCP-Server & Discover-Assistent.....	35
5.1 DHCP-Server	36
5.2 Discover-Assistent	38
6 Betriebsarten und Regel Konfiguration.....	39
6.1 Modus NAT-Router.....	40
6.2 Modus Standard-Router	42
6.3 Modus Standard-Router mit Static-NAT.....	44
6.4 IP-Inventare.....	46
6.4.1 Scannen von Network 2	47
6.5 Erstellen von Firewall-Regeln.....	48
6.5.1 Verwendung von Hostnamen als Ziel einer Regel	51
6.6 Beispiele Firewall-Regeln	52
6.6.1 Modus Standard-Router, Network 2 nach Network 1.....	52
6.6.2 Modus NAT-Router, Network 1 nach Network 2.....	54

7 Wireguard VPN-Server	57
7.1 Übersicht WireGuard VPN-Server	58
7.2 VPN-Umgebung.....	59
7.3 VPN-Client Inventar	61
7.3.1 Neue VPN-Clients - Standard Konfiguration	61
7.3.2 Neue VPN-Clients - Erweiterte Konfiguration.....	63
7.4 VPN-Regeln.....	65
7.5 Schritt für Schritt: VPN-Zugang für ein Mobilgerät	68
8 Wireguard VPN-Client.....	75
8.1 Übersicht WireGuard VPN-Client.....	76
8.2 VPN-Client	77
9 Wireguard-VPN Box-to-Box	81
9.1 Übersicht WireGuard-VPN Box-to-Box	82
9.1.1 Konfigurationsbeispiel VPN Box-to-Box	82
10 Digitale Ein-/Ausgänge (nur Microwall IO)	89
10.1 Digitale Eingänge.....	90
10.1.1 Beschaltung der digitalen Eingänge.....	90
10.2 Digitale Ausgänge.....	92
10.2.1 Beschaltung der digitalen Eingänge.....	92
11 Security & Wartung	93
11.1 Security-Hinweise.....	94
11.1.1 Funktion und typische Anwendung	94
11.1.2 Anforderungen an Integratoren und Betreiber	94
11.1.3 Installationsort	95
11.1.4 Inbetriebnahme	96
11.1.5 Betrieb und Konfiguration	97
11.1.6 Service, Wartung und Außerbetriebnahme.....	99
11.2 Up-/Download von Konfigurations-Backups.....	100
11.3 Firmware-Updates	102
11.3.1 Wo ist die aktuelle Firmware erhältlich?.....	102
11.3.2 Firmware-Update mit WuTility	103
11.3.3 Firmware Update per Web-Based-Management	104
11.4 Eigene Zertifikate.....	106
11.5 Notzugang der Microwall	108
11.6 Werkseinstellungen	110
Anhang	111
Technische Daten und Bauform.....	112
Microwall VPN, #55211	112
Microwall IO, #55212.....	113
Index	114

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:

GEFÄHRDUNG

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

W&T

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 VPN und Microwall IO sind industrietaugliche IPv4-Router mit zwei 1000BaseT-Netzwerkanschlüssen, integrierter, whitelist-basierter Firewall und einem WireGuard VPN-Client/Server. Sie binden eine Netzwerkinself an ein übergeordnetes lokales Netzwerk an. Parallel hierzu kann über das Wireguard VPN ein sicherer Fernzugriff auf die Teilnehmer des Inselnetzwerkes erfolgen. Geeignete Filterregeln auf TCP/IP-Ebene schützen alle Netzwerke vor unberechtigter, unerwünschter und schädlicher Kommunikation.

Die Microwall IO verfügt über 2 digitale Eingänge und 2 digitale Ausgänge, welche in Automatisierungsumgebungen die Steuerung von Router-/Firewall-Funktionen und das Auswerten von Meldungen erlauben.

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!

W&T

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 VPN 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 Netzkabel 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.

W&T

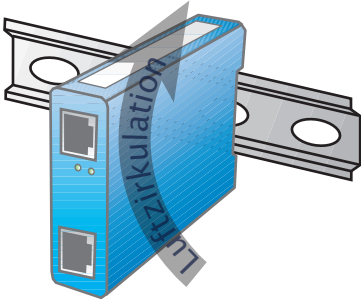
Die vollständigen Konformitätserklärungen zu den in der Anleitung beschriebenen Geräten finden Sie über die jeweiligen Internet-Datenblattseite auf der W&T-Homepage unter <http://www.wut.de>.

2 Hardware, Schnittstellen und Anzeigen

- Hardware-Installation
- Spannungsversorgung
- Netzwerkschnittstellen
- Service-Taster
- Digitale EAs (nur Mircrowall IO)

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.



i 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.

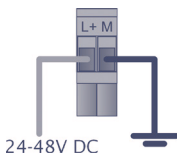
2.2.1 PoE-Versorgung

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%)



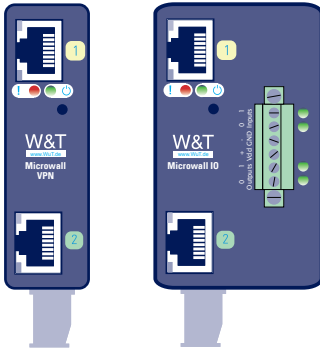
⚠️ WARNUNG

Für die externe Versorgung der Microwall 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 EN62368-1 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

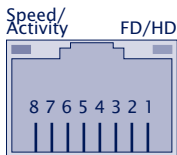
Gegenüber der Versorgungsspannung besteht eine galvanische Trennung mit mindestens $500V_{rms}$

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



System-LED

Service-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*.

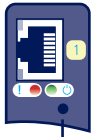
Langsames Blinken: Der Service-Taster wurde zwischen 3,5s und 10s betätigt. Der Notzugang der Microwall ist aktiviert.

Weitere Informationen zum Notzugang enthält das Kapitel *Notzugang*.

i *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



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*.

i *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-Basisparameter 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*.

i *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).*


i *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 Netzwerkbasisparameter 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>

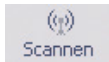
Der Start erfolgt nach der Installation über

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.

Unbenannt - WuTility							
Datei Gerät Konfiguration Firmware Optionen Hilfe							
Neu Öffnen Speichern Scannen IP-Adresse Telnet Browser Registrierg. Firmware Hilfe							
	Ethernet-Adresse	IP-Adresse	Netzmaske	Gateway	Produktnummer	Produktname	Version
	00c03d:df3245	190.107.233.110	255.255.255.0	0.0.0.0	#55211	Microwall VPN	1.04

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.

Geräteeinstellungen: Netzwerkparameter

dynamisch (DHCP)

statisch

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

Adresbereich: Netzwerk #0

Diese Adresse ist möglicherweise noch frei. Erneut prüfen

Subnetzmaske: 255 . 255 . 0 . 0

Vorgabe: Dropdown

Standardgateway: 10 . 10 . 0 . 254

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

DNS-Server B:

< Zurück Weiter > Abbrechen

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-

parameter 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.

i *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).*

i *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 folgende Voraussetzungen erfüllt sein:


- Der Netzwerkanschluss des verwendeten Rechners muss eine IP-Adresse im Bereich 190.107.233.0/24 haben. Eine 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, 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).*

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.

Initialisierung

Loginpasswort

Loginpasswort	<input type="text"/>	<input type="text"/>
	<input type="text"/>	<input type="text"/>

Netzwerk 1

IP-Einstellungen Intranet	<input type="radio"/> DHCP	<input checked="" type="radio"/> statisch
	Netzwerk-Bezeichnung *	
	Network 1	
	IP-Adresse *	
	192.168.0.100	
	Subnet-Maske *	
	255.255.255.0	
	Default-Gateway	
	192.168.0.1	

Netzwerk 2

IP-Einstellungen Insel	<input type="radio"/> DHCP	<input checked="" type="radio"/> statisch
	Netzwerk-Bezeichnung *	
	Network 2 (Island)	
	IP-Adresse *	
	10.10.0.1	
	Subnet-Maske *	
	255.255.0.0	

Routermodus

Routermodus	<input type="radio"/> Standard-Router
	<input checked="" type="radio"/> NAT-Router


Konfigurations-Backup

Konfigurations-Backup	Backup Passwort
	<input type="text"/>
	<input type="button" value="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.

Konfigurations-Backup

Erlaubt das Hochladen eines zuvor 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.

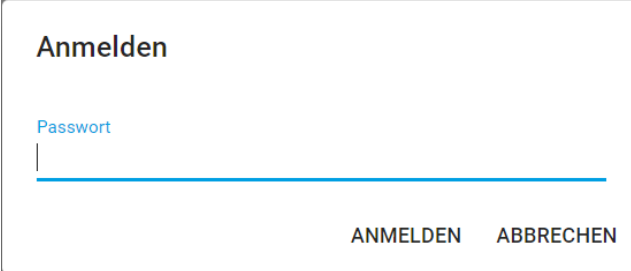
Nach dem Login werden vorgenommene Änderungen mit Betätigung des Buttons *Speichern* auf der jeweiligen Seite sofort übernommen. Sollte die Übernahme der Parameter einen Neustart der Microwall erfordern, erfolgt nach Betätigung von *Speichern* ein entsprechender Hinweis.

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



The screenshot shows a login interface with the following elements:

- Title: **Anmelden**
- Label: **Passwort**
- Input field: A horizontal line representing the password input area.
- Buttons: **ANMELDEN** and **ABBRECHEN**

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-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*.

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, den Freigaberegeln sowie der VPN-Einrichtung enthält diese Anleitung im Kapitel *Betriebsarten und Regel konfiguration*.

5 DHCP-Server & Discover-Assistent

- DHCP-Server für *Network 2*
- Statische oder dynamische Leases
- Kontrollierte Inbetriebnahme neuer/fremder Geräte
- Identifizierung unerwünschter Verbindungen

5.1 DHCP-Server

Die Microwall kann in *Network 2* als DHCP-Server arbeiten. Aktivierung und Konfiguration des DHCP-Servers erfolgen im Menüweig *Grundeinstellungen* -> *DHCP-Server*.

Dynamische Leases im Servicefall

Ausschließlich für Serviceeinsätzen z.B. für den schnellen Anschluss eines Notebooks, unterstützt der DHCP-Server die dynamische Zuweisung von IP-Adressen aus einem konfigurierbaren Adresspool.


Der DHCP-Server der Microwall erstellt *keine* Bindung zwischen einer dynamisch vergebenen IP-Adresse und der MAC-Adresse des jeweiligen Clients. Auf neue Anfragen hin wird immer die erste freie Adresse aus dem Pool vergeben, unabhängig davon, ob dem Host zuvor eventuell bereits eine andere Adresse zugewiesen wurde.

Aus diesem Grund *müssen* für DHCP-Clients, welche im operativen Betrieb in Freigaberegeln verwendet werden, statische Leases angelegt werden.


Statische Leases

Zur Unterstützung statischer DHCP-Leases stellt die Microwall auf 3 Listen zur Verfügung.


DHCP-Lease-Anfragen

Hier werden alle von der Microwall an Netzwerk 2 empfangenen Anfragen aufgeführt, für welche noch keine statische Lease vergeben ist. Der Button  startet den Dialog für das Anlegen einer statischen Lease für das jeweilige Gerät.

Statische DHCP-Leases

Hier werden alle angelegten statischen Leases aufgeführt und können editiert werden. Der -Button erlaubt das manuelle Anlegen einer neuen Lease.

Als Vorgabe für den DNS-Server vergibt die Microwall ihre IP-Adresse in *Network 2* und arbeitet dort als DNS-Proxy.

 Die Vergabe der Microwall als DNS-Proxy für die Clients ist die Voraussetzung für die Nutzung des Discover-Modus. Bei der Nutzung externer, über Network 1 erreichbarer DNS-Server muss zusätzlich beachtet werden, dass eine entsprechende Firewall-Regel erforderlich ist.

Aktuelle DHCP-Leases

Auflistung aller von der Microwall mit einer Lease versehenen Geräte.

5.2 Discover-Assistent

Der Discover-Assistent erlaubt die kontrollierte Inbetriebnahme neuer Geräte im *Netzwerk 2* (grün). Ausgehenden Verbindungsversuche ausgewählter Hosts werden aufgezeichnet und zusammen mit dem vorher ggf. aufgelösten Hostnamen dargestellt. Die Verbindungen bleiben allerdings blockiert bis für gewünschte Kommunikation per Mausklick eine entsprechende Freigaberegeln generiert wird.

Discover-Assistent

Beobachten Sie Kommunikations-Versuche und erlauben Sie gewünschte Verbindungen per Mausklick.

Modus

Inventareintrag

Individuelle IP

IP-Adresse eingeben

10.120.0.78

▶ START

Alle Geräte

Verbindungsversuche

Zeitstempel	Ziel (Intranet)	Quelle (Insel)	Firewall-Regeln
14.06.2022 12:04:14	www.wut.de (92.204.239.49) TCP/80	10.120.0.78 TCP/47018	Neue Regel ⊕
14.06.2022 12:04:17	virenschleuder.de (217.160.231.199) TCP/443	10.120.0.78 TCP/33970	Neue Regel ⊕

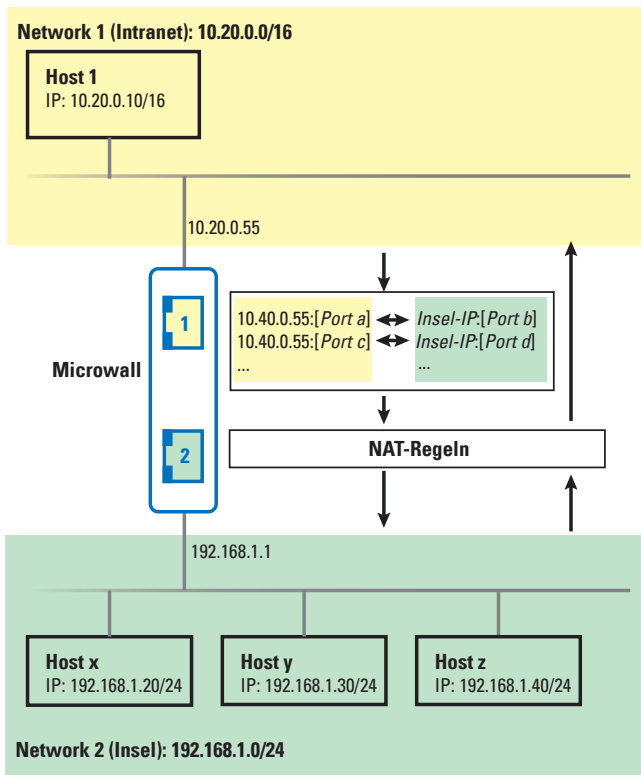
6 Betriebsarten und Regel Konfiguration

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

6.1 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.

Betriebsart

Wählen Sie hier die Betriebsart und das Ping-Verhalten.

Routermodus	<input type="radio"/> Standard-Router	<input checked="" type="radio"/> NAT-Router
ICMP	<input type="checkbox"/> Ping auf lokale Interfaces zulassen	<input type="checkbox"/> "Network 2" -> "Network 1" zulassen

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

Um nach der Aktivierung des Modus *NAT-Router* Kommunikation zwischen Teilnehmern aus dem Intranet und des Inselnetzwerks zu erlauben, müssen ausdrückliche Freigabe-Regeln in folgendem Untermenü konfiguriert werden. Es existieren keine ab Werk vorgegebenen Regeln.

Firewalleinstellungen ^

Betriebsart

Standard-Regeln

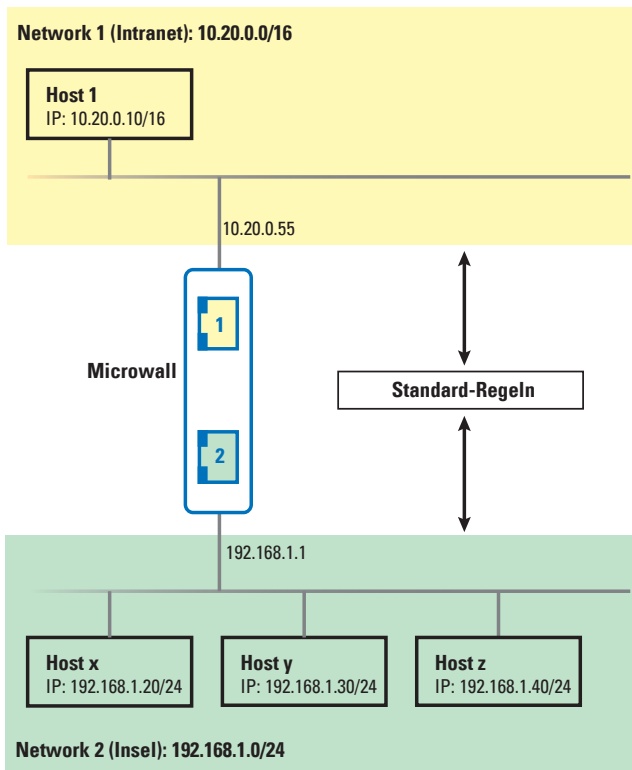
NAT-Regeln

6.2 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 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.

Betriebsart

Wählen Sie hier die Betriebsart und das Ping-Verhalten.

Routermodus Standard-Router NAT-Router

ICMP Ping auf lokale Interfaces zulassen
 "Network 2" -> "Network 1" zulassen
 "Network 1" -> "Network 2" zulassen



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

Um nach der Aktivierung des Modus *Standard-Router* Kommunikation zwischen Teilnehmern aus dem Intranet und des Inselnetzwerks zu erlauben, müssen ausdrückliche Freigabe-Regeln in folgendem Untermenü konfiguriert werden. Es existieren keine ab Werk vorgegebenen Regeln.

Firewalleinstellungen ^

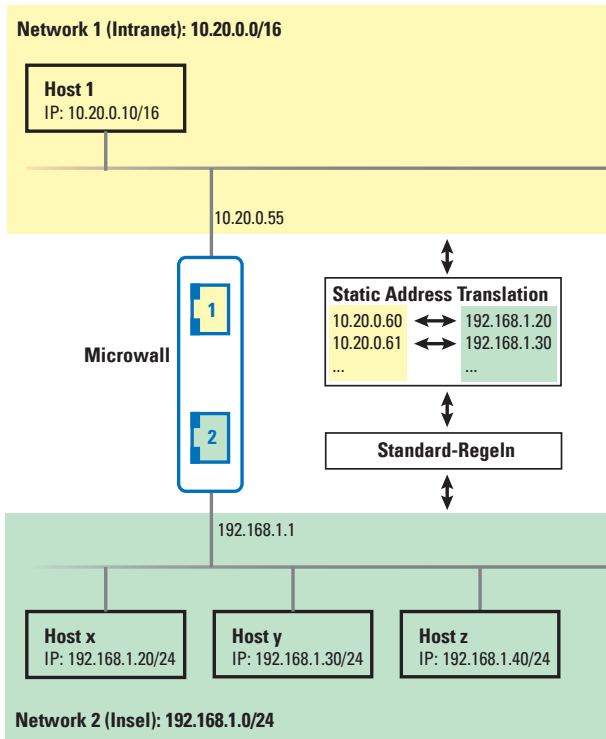
Betriebsart

Standard-Regeln

6.3 Modus Standard-Router mit Static-NAT

Der Modus Standard-Router bietet als Option eine feste 1:1-Zuordnung von IP-Adressen aus dem Unternehmensintranet am Anschluss *Network 1 (gelb)* zu IP-Adressen aus dem Inselnetzwerk. Die Microwall erhält hierzu neben der primären IP-Adresse aus dem Intranet, zusätzliche sekundäre Adressen aus dem Intranet. In der Übersetzungstabelle für das Static NAT werden diese den gewünschten Hosts in der Insel zugewiesen. Über die sekundären IP-Adressen besteht kein Zugang zu Diensten der Microwall (WBM, Update, Ping etc.)

Mit Hilfe des Static-NATs erscheinen Insel-Hosts im Intranet so, als wären sie Teilnehmer des lokalen Netzwerks. Für eine Kommunikation mit den Insel-seitigen Hosts müssen geeignete Firewall-Regeln konfiguriert werden. Ein Eingriff in das Intranet-seitige Routing-Konzept ist nicht erforderlich.



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.

Betriebsart

Wählen Sie hier die Betriebsart und das Ping-Verhalten.

Routermodus
 Standard-Router
 NAT-Router

ICMP
 Ping auf lokale Interfaces zulassen
 "Network 2" -> "Network 1" zulassen
 "Network 1" -> "Network 2" zulassen

+
↺

Der Button *Plus* am oberen rechten Rand der Tabelle für *Statisches NAT* öffnet den Dialog für das Anlegen neuer Zuordnungen. Bestimmen Sie in dem folgenden Dialog welche IP-Adresse des Intranets (*Network 1, gelb*) der gewünschten IP-Adresse im Insel-Netzwerk (*Network 2, grün*) zugeordnet werden soll.

Statisches NAT (1-zu-1) +

Geräte-IP (Intranet)	Ziel-IP (Insel)
Keine Daten verfügbar...	

Bitte beachten Sie, dass Sie auch entsprechende Firewall-Regeln für den Zugriff auf die Ziel-IP(s) definieren müssen.

Über den Button *Speichern* wird der Modus *Standard-Router* mit der zugehörigen Tabelle für das Static-NAT aktiviert und der zugehörige Regel-Satz geladen.

Um nach der Aktivierung des Modus *Standard-Router* Kommunikation zwischen Teilnehmern aus dem Intranet und des Inselnetzwerks zu erlauben, müssen ausdrückliche Freigabe-Regeln in folgendem Untermenü konfiguriert werden. Es existieren keine ab Werk vorgegebenen Regeln.

- Firewalleinstellungen ^
- Betriebsart
- Standard-Regeln







6.4 IP-Inventare

Im Menüweig *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.







MicrowallVPN-08B7B2 / Firewalleinstellungen / IP-Adressen-Inventar

ABMELDEN 

Netzwerk "Network 1 (LAN)"

<input type="checkbox"/>	IP-Adresse(n)	Name Beschreibung	Verwendung		
<input type="checkbox"/>	ANY	Any	1		
<input type="checkbox"/>	192.168.10.1	DNS	1		
<input type="checkbox"/>	192.168.10.254	Srv-1	0		

Netzwerk "Network 2 (Island)"

<input type="checkbox"/>	IP-Adresse(n)	Name Beschreibung	Verwendung		
<input type="checkbox"/>	10.10.0.0/16	Subnet Island	3		
<input type="checkbox"/>	10.10.0.78	SRV-2	3		
<input type="checkbox"/>	10.10.0.200	hp switch	2		

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)

6.4.1 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.

6.5 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.

MicrowallVPN-08B7B2 / Firewalleinstellungen / Standard-Regeln

ABMELDEN 

[Modus] -Regeln

 Das Gerät ist im Standard-Modus.
Die Standard-Regeln sind aktiv.

Erstellen und verwalten Sie hier Ihre (Standard-)Firewall-Regeln. 

Filter auswählen...

v

✓ ALLE AKTIVIEREN
✗ ALLE DEAKTIVIEREN

ALLE LÖSCHEN

IP-Bereich "Network 1"	Port(s)	IP-Bereich "Network 2 (Island)"	Port(s)
------------------------	---------	---------------------------------	---------

Keine Suchergebnisse oder (noch) keine Regeln angelegt...

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/regelbeispiele>.*

Regel Informationen

Name *

Beschreibung

Netzwerk "Network 1 (LAN)"

Quelle IP-Bereichen Name

IP-Adresse(n) hinzufügen

IP-Adresse(n) *

Name *

NAT-Port *

➔

Richtung
auswählen

⬅

Label

Label auswählen...

Netzwerk "Network 2 (Island)"

Ziel IP-Bereichen Name

IP-Adresse hinzufügen

IP-Adresse *

Name *

Ziel-Port *

Protokoll

TCP FTP

UDP

Aktionen

Regel aktivieren

Log-Eintrag erstellen

Verbindung akzeptieren

Bitte mindestens eine Aktion auswählen!

HINZUFÜGEN ABBRECHEN

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 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*) arbei-

tet. 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.

6.5.1 Verwendung von Hostnamen als Ziel einer Regel

In Regeln, welche Verbindungen in Richtung *Network 1* freigeben, kann das Ziel auch in Form eines Hostnamen angegeben werden (z.B. *www.wut.de*). Voraussetzung hierfür ist, dass die initiierenden Teilnehmer in *Network 2* die dortige IP-Adresse der Microwall als DNS-Server verwenden.

 *Arbeitet die Microwall für Teilnehmer im Network 2 als DNS-Proxy, muss für eine korrekte Auflösung der Anfragen der auf Network 1 konfigurierte DNS-Server erreichbar sein.*

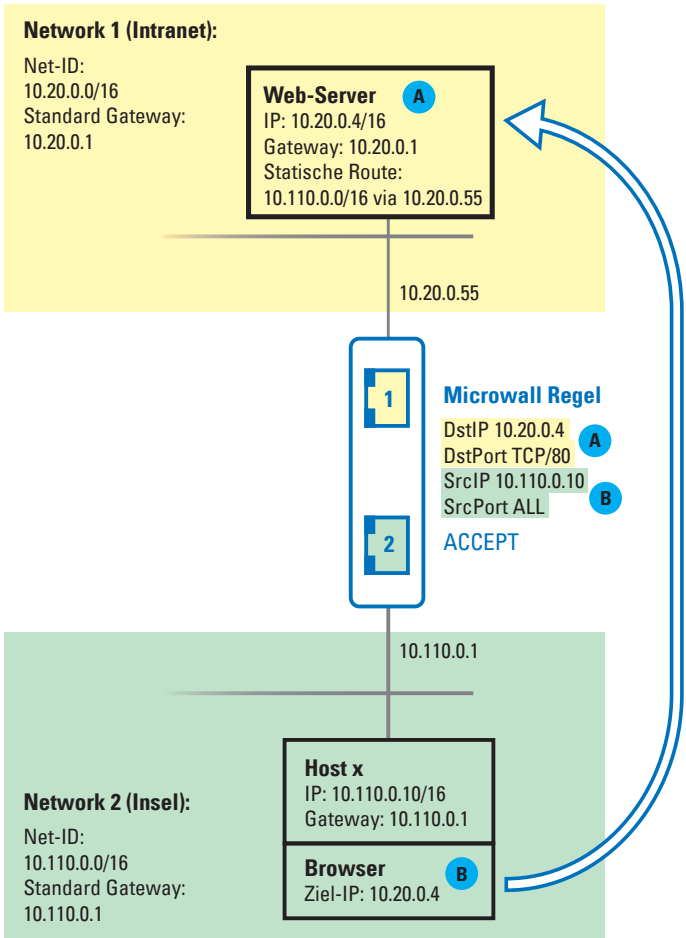
Es können einzelne Hostnamen sowie komma-getrennte Hostlisten verwendet werden (z.B. *www.wut.de, www.timeair.de*).

Als Wildcard in einem Hostnamen kann das *-Zeichen eingesetzt werden. innerhalb eines Hostnamen ist *eine* Wildcard erlaubt und diese *muss* am Anfang stehen (z.B. **.wut.de*). Innerhalb von Namenslisten gilt das für jeden Hostnamen.

6.6 Beispiele Firewall-Regeln

6.6.1 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:

Regel Informationen

Name * **Beispiel Web-Zugriff**

Beschreibung

Netzwerk "Network 1 (LAN)"
Ziel (IP-Adresse(n) / Name) *
IP-Adresse(n) hinzufügen
IP-Adresse(n) * **10.20.0.4**
Name * **Intranet Server**
Ziel (Port-Bereich) * **80**

Netzwerk "Network 2 (Island)"
Quelle (IP-Adresse(n) / Name) *
IP-Adresse(n) hinzufügen
IP-Adresse(n) * **10.110.0.10**
Name * **Insel Browser**
Quelle (Port-Bereich) * **ANY**

Richtung

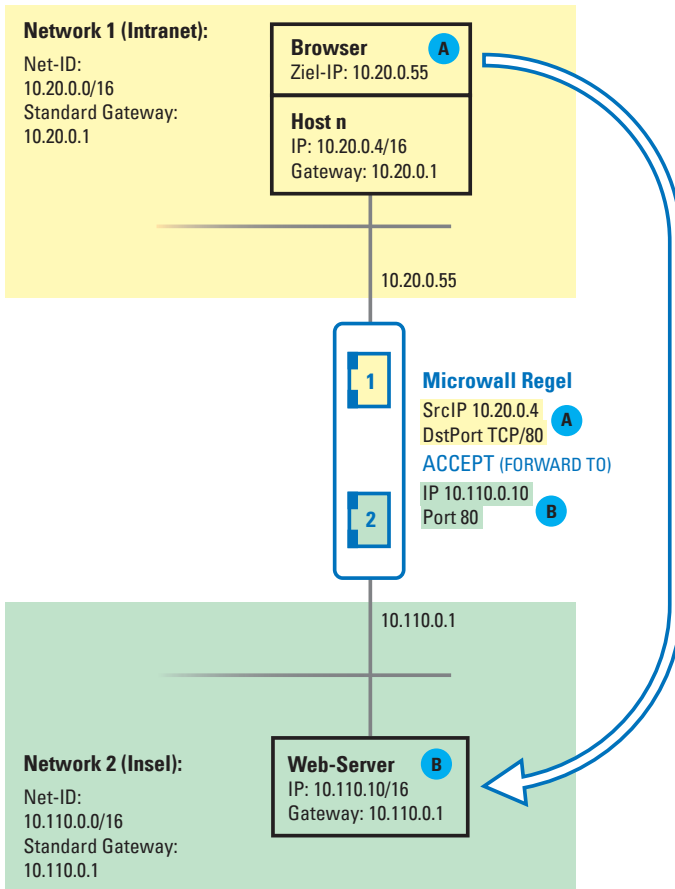
Protokoll
 TCP FTP
 UDP

Aktionen
 Regel aktivieren
 Log-Eintrag erstellen
 Verbindung akzeptieren

HINZUFÜGEN ABBRECHEN

6.6.2 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:

Regel Informationen

Name* **Beispiel Web-Zugriff**

Beschreibung

Netzwerk "Network 1 (LAN)"
Zur IP-Adresse(n) Name*
IP-Adresse(n) hinzufügen
10.20.0.4
Name* **Browser Intranet**
NAT-Port* **80**

Netzwerk "Network 2 (Island)"
Zur IP-Adresse(n) Name*
IP-Adresse hinzufügen
10.110.0.10
Name* **Insel Server**
Ziel-Port* **80**

Richtung auswählen


Protokoll

TCP FTP
 UDP

Aktionen

Regel aktivieren
 Log-Eintrag erstellen
 Verbindung akzeptieren

HINZUFÜGEN ABBRECHEN

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

7 Wireguard VPN-Server

- Konfiguration der Microwall als VPN-Server mit erlaubten Clients
- Erstellen von Firewall-Regeln für den VPN-Server-Modus

7.1 Übersicht WireGuard VPN-Server

WireGuard ist eine VPN-Architektur, deren Schwerpunkt neben hohen Sicherheitsanforderungen durch moderne Kryptographie auch auf einer einfachen Konfiguration bei gleichzeitig hoher Geschwindigkeit liegt.

Details sowie aktuelle Informationen zu Konzept, Funktion und Entwicklungsstatus dieses Open-Source-Projektes finden Sie unter folgendem Link. Dort stehen auch Download-Möglichkeiten für WireGuard-VPN-Clients aller gängigen Betriebssysteme (Windows, Linux, Android, IOS, MacOS) zur Verfügung.

<https://www.wireguard.com>

WireGuard Funktionsweise

WireGuard tunnelt IP-Pakete durch einen verschlüsselten UDP-Kanal zwischen dem VPN-Client und VPN-Server in einem virtuellen IP-Subnetz. Verschlüsselung und gegenseitige Authentifizierung erfolgen hierbei asymmetrisch über Schlüssel-paare mit jeweils öffentlichem und privatem Teil (Public-Key/Private-Key). Die Public-Keys eines VPN-Servers und -Clients müssen gegenseitig bekannt sein.

Modus WireGuard Server

Die Microwall stellt auf der LAN-Seite einen WireGuard-Server zur Verfügung, auf welchen sich registrierte VPN-Clients verbinden können und sicheren Zugriff auf Teilnehmer des Insel-Netzwerks erhalten. Alle Verbindungen in das Insel-Netzwerk müssen über eine Whitelist-basierte Firewall ausdrücklich erlaubt werden.

Anwendungsbeispiel

Externe WireGuard-Clients unter Windows, Linux, Android oder IOS bauen einen VPN-Tunnel zur Microwall auf um sich hierüber z.B. für eine Fernwartung auf Teilnehmer des Insel-Netzwerkes zu verbinden.

7.2 VPN-Umgebung

Im Menüweig *VPN-Server* → *VPN-Umgebung* erfolgen die Grundeinstellungen des VPN-Server-Modus sowie die Verwaltung und Steuerung der zulässigen VPN-Clients.

[MicrowallVPN-08B7B2](#) / [VPN-Einstellungen](#) / VPN-Umgebung

VPN-Umgebung

VPN-Server

VPN aktivieren

VPN-Server Einstellungen

i
 aktivieren

VPN-Server Public Key
h0qf/kNvgEsMr8gWF09ah+QqbzS0SXBkUAEefXAVdm0=

NEUER KEY

Virtuelle IP/Subnet *
10.3.3.1/16

UDP Listenport *
10001

Wireguard-Version: 0.0.20200215

VPN aktivieren

Die Check-Box aktiviert den VPN-Server mit den eingestellten Parametern auf dem Anschluss *Network 1* (gelb) der Microwall VPN.

VPN-Server Einstellungen – Public-Key/Neuer Key

Der angezeigte Public-Key des VPN-Servers muss jedem VPN-Client bekannt sein und kann hier aus dem Textfeld z.B. in eine Datei kopiert werden.

Über den Button *Neuer Key* wird ein neues Schlüsselpaar (Private-Key und Public-Key) für den VPN-Server generiert.

i *Innerhalb einer bestehenden VPN-Umgebung muss der Public-Key eines neu erzeugten Schlüsselpaares an alle VPN-Clients ausgerollt werden. Eine Kommunikation über das alte Schlüsselpaar ist nicht mehr möglich.*

VPN-Server Einstellungen – Virtuelle IP/Subnet

Die virtuelle IP-Adresse und Subnet Mask des VPN-Servers in CIDR-Notation legt die NetID des gesamten VPNs fest. Die

IP-Adressen aller VPN-Clients müssen sich im gleichen Subnet befinden. Der IP-Bereich des VPNs darf nicht mit den Adressbereichen von *Network 1* und *Network 2* kollidieren. Auch der Konflikt mit dem/den IP-Bereich/en auf der VPN-Client-Seite muss verhindert werden.

VPN-Server-Einstellungen → UDP Listenport

Bestimmt den UDP-Listenport, auf welchem der VPN-Server Verbindungen von VPN-Clients entgegen nimmt. Der hier konfigurierte UDP-Port muss in allen VPN-Clients als Zielport verwendet werden.




Wenn VPN-Clients sich über einen serverseitig vorgeschalteten Router oder eine Perimeter-Firewall verbinden, muss diese Portnummer mit der IP-Adresse von *Network 2* ggf. über eine Firewall- oder NAT-Regel freigeschaltet werden.

Aktivierte Clients

[MicrowallVPN-08B7B2](#) / [VPN-Einstellungen](#) / [VPN-Umgebung](#)

VPN-Umgebung

VPN-Clients

Aktivierte Clients	
<input checked="" type="checkbox"/>	10.3.3.2 (Clt-10) 
<input checked="" type="checkbox"/>	10.3.3.3 (Clt-20) 
<input type="checkbox"/>	10.3.3.5 (Clt-30) 

Der Abschnitt enthält alle im VPN-Client-Inventar angelegten VPN-Clients. Die Checkbox aktiviert den jeweiligen Client und erlaubt die Verbindung zum VPN-Server. Für Verbindungen zu Teilnehmern im Inselnetz sind zusätzlich entsprechende Freigaben/Regeln auf der Seite *VPN-Regeln* erforderlich.

Die Weltkugel hinter einem Client-Eintrag zeigt an, dass der Client auf die Konfigurationseiten der Microwall zugreifen darf.

7.3 VPN-Client Inventar

Die Seite erlaubt das Anlegen, Löschen und Verwalten von VPN-Clients.

[MicrowallVPN-08B7B2](#) / [VPN-Einstellungen](#) / [Client-Inventar](#)

Client-Inventar

VPN-Clients



<input type="checkbox"/>	Virtuelle IP-Adresse	Name Beschreibung	Verwendung	
<input type="checkbox"/>	10.3.3.2 Client ist aktiviert.	Clt-10	1	
<input type="checkbox"/>	10.3.3.3 Client ist aktiviert.	Clt-20	2	

Auf der Seite VPN-Client-Inventar erfolgt lediglich die Verwaltung der VPN-Clients. Die Freischaltung für tatsächliche VPN-Verbindungen erfolgt auf der Seite VPN-Umgebung.

7.3.1 Neue VPN-Clients - Standard Konfiguration

Der Button am oberen rechten Rand der Tabelle startet den Dialog für das Anlegen neuer VPN-Clients.

VPN-Client hinzufügen

Virtuelle IP/Subnet des VPN-Servers: 10.3.3.1/16

Virtuelle IP-Adresse (des VPN-Clients) *

10.3.3.11



Name *

Clt-55

Beschreibung

Public Key



IP-Bereich Site-to-Site



Pre-shared Key (PSK)

 PSK ERZEUGEN



Zugriff auf diese Webkonfigurationsoberfläche erlauben

VPN-Client aktivieren



Erweiterte Konfiguration

Die Standard-Konfiguration setzt voraus, dass die VPN-Konfiguration des Clients manuell erzeugt wird und dort bereits ein Schlüsselpaar erzeugt wurde.

Virtuelle IP-Adresse des VPN-Clients

Die hier eingegebene virtuelle IP-Adresse muss im gleichen Subnetz des VPN-Servers liegen. Sie darf nicht mit der Adresse anderer VPN-Clients kollidieren.

Name & Beschreibung

Frei wählbare(r) Name (Pflichtfeld) und Beschreibung des VPN-Clients.

Public-Key

Public-Key des auf dem VPN-Client erzeugten Schlüsselpaars.

IP-Bereich Site-to-Site

Falls der VPN-Client für eine Site-to-Site-Verbindung zu einer anderen Microwall genutzt werden soll, muss hier die Net-ID der Client-Insel angegeben werden.

Client-Einstellungen → Pre-shared Key (PSK)

Mit dem PSK wird die VPN-Kommunikation zusätzlich verschlüsselt. Der PSK muss auf dem VPN-Client und dem VPN-Server identisch sein. Wie auch der Public-/Private-Key ist der Syntax des PSK WireGuard-spezifisch und nicht frei wählbar. Die Erzeugung erfolgt in der Regel auf dem VPN-Server oder auf einem Drittsystem mit Hilfe der WireGuard-Tools.

Option: Zugriff auf Webkonfiguration zulassen


Mit Aktivierung dieser Option wird dem VPN-Client gestattet auf die Konfigurationsseiten der Microwall zuzugreifen.

Option: VPN-Client aktivieren

Mit Aktivierung dieser Option wird der angelegte VPN-Client mit Betätigung des Buttons *Hinzufügen* sofort aktiviert. Für Zugriffe auf Teilnehmer des Inselnetzwerkes müssen entsprechende Regeln unter VPN-Regeln angelegt werden.

7.3.2 Neue VPN-Clients - Erweiterte Konfiguration

Das Aktivieren der Option *Erweiterte Konfiguration* erlaubt das Erstellen einer vollständigen Konfigurationsdatei für den neuen VPN-Client. WireGuard-Clients für Windows, Android und IOS erlauben den Import solcher Konfigurationen als Datei oder per QR-Code.

 *Das Schlüsselpaar für den neuen VPN-Client wird in diesem Fall durch die Microwall erzeugt und der sensible Private-Key ist Bestandteil der Konfigurationsdatei. Diese Methode darf daher nur verwendet werden, wenn die Datei auf sicherem Weg an den Client übertragen werden kann.*

Private Key und Button Key erzeugen

Der Button *Key erzeugen* generiert ein Schlüsselpaar für die Verwendung im VPN-Client. Der für die spätere Authentifizierung des Clients benötigte Public-Key wird von der Microwall VPN automatisch gespeichert. Der zugehörige Private-Key steht nur bis zur Erzeugung der Konfigurationsdatei zur Verfügung und wird mit dem Schließen des Dialoges gelöscht.

Endpunkt (VPN-Server)

Die aus Sicht des VPN-Clients benötigte Adressinformation für die Verbindung zum VPN-Server in folgendem Format

[URL|IP-Adresse]:[UDP-Listenport]

Vorgegeben sind die IP-Adresse von *Network 1* und der in der *VPN-Umgebung* konfigurierte *UDP-Listenport*.

Erlaubte IPs


Eine Komma-getrennte Liste von IP-Adressen in CIDR-Notation, von denen eingehender Verkehr für diesen Peer zugelassen wird und an die ausgehende Verkehr für diesen Peer weitergeleitet wird.

Vorgegeben ist der virtuelle IP-Bereich des VPNs und der IP-Bereich des Inselnetzwerks an *Network 2*. Änderungen und Erweiterungen sind nur in Ausnahmefällen erforderlich, wenn z.B. über im Inselnetzwerk befindliche Router weitere Netzwerke erreichbar sind.

Keep Alive

Angabe des Intervalls in Sekunden, mit dem der VPN-Client Wireguard-Keep-Alive Pakete generiert, um den UDP-Tunnel in evt. der Infrastruktur befindlichen Routern offen zu halten.

7.4 VPN-Regeln

Mit welchen Teilnehmern und Diensten im Inselnetzwerk ein aktiver VPN-Client kommunizieren darf, muss über entsprechende VPN-Regeln ausdrücklich erlaubt werden. Das Erstellen solcher Firewall-Regeln für das VPN erfolgt auf der Seite *VPN-Einstellungen* -> *VPN-Regeln*. Neben einer Übersicht der bereits existierenden Regeln können über den Button  neue Regeln angelegt und definiert werden.

Name

Frei wählbarer Name der Regel.

Beschreibung

Optionale frei wählbare Beschreibung der Regel.

Label

Zur übersichtlicheren Darstellung bzw. Anzeige-Filterung in der Regel-Übersicht, 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 der getunnelten Verbindung. Bei TCP wird die Richtung durch den Verbindungsaufbau bestimmt. Bei UDP wird sie durch das initiale UDP-Datagramm festgelegt.

VPN-Client Network 1 (gelb) & Network 2 (grün)

Konfiguration der innerhalb des VPN-Tunnels zulässigen Kommunikationsverbindungen zwischen dem VPN-Client und Inselteilnehmern. In welchem Netzwerk sich Quelle oder Ziel befinden, wird dynamisch über die gewählte Richtung der Regel bestimmt.

Bei der Auswahl des VPN-Clients in *Network 1* (gelb) kann nur ein zuvor im entsprechenden Inventar angelegter VPN-Client ausgewählt werden. Dessen Kommunikationspartner im Inselnetz an *Network 2* (grün) kann 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 IP-Inventar für *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 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 Verlauf einer FTP-Session 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 nachträglich in der Regelübersicht erfolgen.

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

Verbindung akzeptieren erlaubt den durch die Regel definierten Datenverkehr.

7.5 Schritt für Schritt: VPN-Zugang für ein Mobilgerät

Im Insel-Netz befindet sich eine Maschine, auf deren internes Web-Interface über das Internet von einem Android-Mobilgerät aus zugegriffen werden soll.

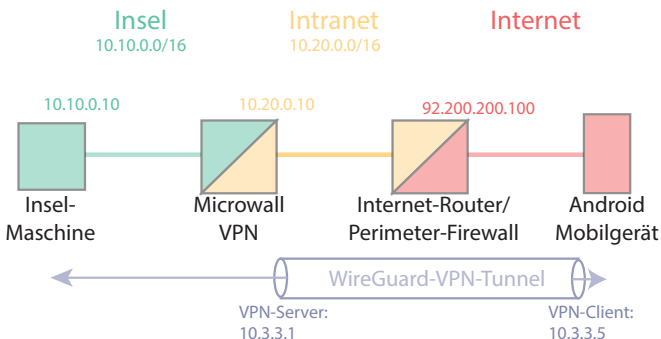
Das Beispiel geht davon aus, dass die Microwall bereits als NAT-Router zwischen dem Intranet an *Network1* (gelb) und der Netzwerk-Insel an *Network2* (grün) eingerichtet ist.

1. Vorbereitungen

Android WireGuard APP - Diese muss auf dem Android-Mobilgerät installiert sein. Geben Sie hierfür in der Playstore-Suche „Wireguard“ ein.

Internet-Router/Perimeter-Firewall - In der für die Anbindung des Intranets an das Internet oder ein anderes übergeordnetes Netzwerk zuständigen Perimeter-Firewall (ggf. DSL-Router) ist eine NAT-Regel erforderlich. Diese muss internetseitig eingehende UDP-Pakete mit dem Zielport 10001 an die intranetseitige IP-Adresse der Microwall VPN weiterleiten.

Dynamische IP-Adressen - Verfügt der Internetanschluss des Intranets WAN-seitig nur über dynamische IP-Adressen des Providers, muss der Dienst eines DynDNS-Anbieters genutzt werden. Als Endpunkt in der VPN-Client-Konfiguration muss in diesem Fall die IP-Adresse durch den entsprechenden Hostnamen ersetzt werden.



2. Einrichtung der VPN-Server-Umgebung


Wechseln Sie auf die Seite *VPN-Einstellungen* -> *VPN-Umgebung*:

[MicrowallVPN-0887B2](#) / [VPN-Einstellungen](#) / [VPN-Umgebung](#)


VPN-Umgebung

VPN-Server

VPN aktivieren	①	<input checked="" type="checkbox"/> aktivieren
VPN-Server Einstellungen	②	VPN-Server Public Key h0qf/rkNvgEsr8gWF09ah+QqbzS0SXBkUAeefXAVdm0= <input type="text" value="NEUER KEY"/>
	③	Virtuelle IP/Subnet * 10.3.3.1/16
	④	UDP-Listenport * 10001
Wireguard-Version: 0.0.20200215		

- ① Aktivieren Sie den VPN-Server
 - ② Erzeugen Sie ein Schlüsselpaar für den VPN-Server. Der öffentliche Teil des Schlüssels (Public-Key) wird angezeigt.
 - ③ 10.3.3.1/24
Legt die IP-Adresse des VPN-Servers und Net-ID für das virtuelle VPN-Netzwerk fest. Der Bereich ist weitestgehend frei wählbar, darf aber mit keinem der anderen beteiligten Bereiche kollidieren.
 - ④ 10001
Der UDP-Listenport, auf welchem der VPN-Server eingehende Client-Verbindungen entgegennimmt.
-  Speichert und aktiviert die Änderungen.

3. Anlegen des VPN-Clients im Inventar

Wechseln Sie auf die Seite *VPN-Einstellungen* -> *VPN-Inventar* und klicken auf den -Button am oberen rechten Rand der Tabelle.

VPN-Client hinzufügen

Virtuelle IP/Subnet des VPN-Servers: 10.3.3.1/16

Virtuelle IP-Adresse (des VPN-Clients) *

10.3.3.5

①



Name *

Android Service 1

②

Beschreibung

Public Key



IP-Bereich Site-to-Site



Pre-shared Key (PSK)

PSK ERZEUGEN



Zugriff auf diese Webkonfigurationsoberfläche erlauben

VPN-Client aktivieren

③



Erweiterte Konfiguration

④

① 10.3.3.5

Die IP-Adresse des VPN-Clients aus dem Bereich des virtuellen VPN-Netzwerkes.

② Android Service 1

Frei wählbarer Name des VPN-Client.

③ Der VPN-Client soll Zugriff auf die Konfigurationsoberfläche der Microwall VPN erhalten und nach dem Anlegen auch sofort aktiviert sein. Aktivieren Sie daher die beiden Optionen.

④ Die Microwall soll die gesamte Konfigurationsdatei für den VPN-Client erzeugen. Aktivieren Sie hierfür den Schalter *Erweiterte Konfiguration*.

i Dieser Weg sollte nur gewählt werden, wenn gewährleistet werden kann, dass die Konfigurationsdatei sicher an den Client übermittelt werden kann.

i Optional kann die VPN-Verbindung netzwerkseitig auch zusätzlich über einen Pre-shared-Key (PSK) verschlüsselt werden. Klicken Sie für die Erzeugung eines PSK auf den entsprechenden Button. Der PSK wird automatisch in die per QR-Code übertragene Client-Konfiguration aufgenommen.

Erweiterte Konfiguration

Sie können hier ein Private-/Public-Schlüsselpaar generieren und damit eine vollständige Konfigurationsdatei für Ihr Endgerät erzeugen. Wireguard-Clients für Windows, Android und iOS können diese direkt als Datei oder per QR-Code importieren.

Insbesondere der Private Key darf dabei nicht in falsche Hände geraten!

Bitte verwenden Sie diese Variante nur, wenn Sie die Konfigurationsdatei auf einem sicheren Weg an Ihr Endgerät übermitteln können.

Private Key * 5 i

Endpunkt (VPN-Server) 6 i

Erlaubte IPs 7 i

Keep-Alive 8 i


9 i


10


5 Der Button *Keys erzeugen* erstellt ein Schlüsselpaar für den VPN-Client. Der Private-Key wird von der Microwall VPN ausschließlich für die Dauer dieses Erstellungsdialoges gespeichert und anschließend gelöscht.


6 92.200.200.100:10001
Endpunkt, unter welchem der VPN-Server erreichbar ist. In diesem Beispiel ist das die WAN-seitige offizielle IP-Ad-

resse des DSL-Routers, welcher das Intranet an das Internet anbindet. Doppelpunktgetrennt muss der UDP-Listenport des VPN-Servers angegeben sein.

 *Beachten Sie hierzu auch die im Abschnitt Vorbereitungen beschriebene NAT-Regel in der Perimeter-Firewall des Intranets.*

 10.3.3.1/32,10.10.0.0/16
IP-Adressen und IP-Bereiche in CIDR-Notation, welche im Rahmen der VPN-Verbindung auftreten und akzeptiert werden sollen. Befindet sich der gewünschte Kommunikationspartner direkt im Inselnetz, ist eine Änderung der Vorgaben in der Regel nicht erforderlich.

 20
Intervall, in welchem der WireGuard-VPN-Client Keep Alive Pakete zur Aufrechterhaltung des UDP-Tunnels in den beteiligten Routern generiert.

 Der Button *QR-Code Anzeigen* erzeugt abschließend den QR-Code mit dem Inhalt der VPN-Client-Konfiguration. Starten Sie die WireGuard-App auf dem Mobilgerät und wählen dort die Option *Import from QR-Code*. Wurde der QR-Code erfolgreich gelesen, vergeben Sie einen Namen für die neue VPN-Verbindung.

 *Hinzufügen* schließt den Konfigurationsdialog und führt auf die Übersichtsseite des VPN-Client-Inventars.

 Speichert und aktiviert die Änderungen.

4. VPN-Regel für den Zugriff auf das Insel-Gerät

Wechseln Sie auf die Seite *VPN-Einstellungen* -> *VPN-Regeln* und klicken auf den Button  am oberen rechten Rand der Tabelle.

The screenshot shows the configuration page for a rule named "VPN-Zugriff Android Service 1". The interface is divided into several sections:

- Regel Informationen:** Shows the rule name (1) and a description field.
- Label:** A dropdown menu to select a label.
- Netzwerk "Network 1 (LAN)" (VPN):** The source network configuration, including:
 - Quell-VPN-Client | Name: 10.3.3.5 | Android Service 1 (2)
 - Quell-Port-Bereich: Any (3)
- Netzwerk "Network 2 (Island)":** The destination network configuration, including:
 - Ziel-IP-Adresse | Name: 10.10.0.10 (4)
 - Ziel-Port-Bereich: 80,443 (5)
- Richtung:** A right-pointing arrow indicating the direction of traffic.
- Protokoll:** Radio buttons for TCP (selected) and UDP.
- Aktionen:** Checkboxes for "Regel aktivieren" (6), "Log-Eintrag erstellen", and "Verbindung akzeptieren".
- Buttons:** "HINZUFÜGEN" and "ABBRECHEN" (7) at the bottom right.

- 1 VPN-Zugriff Android Service 1
Frei wählbarer Name der VPN-Regel
 - 2 10.3.3.5 | Android Service 1
Auswahl des VPN-Clients aus dem VPN-Inventar als Quelle der freizugebenden TCP-Verbindung.
 - 3 Any
Der Quell-Port der TCP-Verbindung ist beliebig.
 - 4 10.10.0.10
Auswahl des Zielhosts im Inselnetzwerk als Ziel der freizugebenden TCP-Verbindung.
 - 5 80,443
Der Ziel-Port der TCP-Verbindung. Der Web-Service auf dem Zielsystem wird über die TCP-Ports 80 oder 443 angesprochen.
 - 6 Das Protokoll der Verbindung ist TCP. Verbindungen entsprechend den Einstellungen sollen akzeptiert werden und in der Log-Datei der Microwall VPN dokumentiert werden. Die formulierte Regel soll sofort aktiviert werden.
 - 7 *Hinzufügen* schließt den Regel-Dialog und führt auf die Übersichtsseite der VPN-Regeln.
- Speichert und aktiviert die Änderungen.

5. Test der VPN-Verbindung

Öffnen Sie auf dem Android-Gerät die WireGuard App und aktivieren Sie den zuvor angelegten VPN-Tunnel. In der Android-Status-Zeile sollte jetzt ein Schlüsselsymbol die VPN-Verbindung signalisieren. Starten Sie einen Browser und geben in der Adresszeile die IP-Adresse des Insel-Hosts an:

http(s)://10.10.0.10

Für den Zugriff auf die Konfigurationsseiten der Microwall VPN verwenden Sie als Ziel die virtuelle IP-Adresse des VPN-Servers:

`https://10.3.3.1`

8 Wireguard VPN-Client

- Konfiguration der Microwall als VPN-Client

8.1 Übersicht WireGuard VPN-Client

WireGuard ist eine VPN-Architektur, deren Schwerpunkt neben hohen Sicherheitsanforderungen durch moderne Kryptographie auch auf einer einfachen Konfiguration bei gleichzeitig hoher Geschwindigkeit liegt.

Details sowie aktuelle Informationen zu Konzept, Funktion und Entwicklungsstatus dieses Open-Source-Projektes finden Sie unter folgendem Link.


<https://www.wireguard.com>

WireGuard Funktionsweise

WireGuard tunnelt IP-Pakete durch einen verschlüsselten UDP-Kanal zwischen dem VPN-Client und VPN-Server in einem virtuellen IP-Subnetz. Verschlüsselung und gegenseitige Authentifizierung erfolgen hierbei asymmetrisch über Schlüssel-paare mit jeweils öffentlichem und privatem Teil (Public-Key/Private-Key). Die Public-Keys eines VPN-Servers und -Clients müssen gegenseitig bekannt sein.

Modus WireGuard Client

Alternativ zum Server-Modus kann die Microwall auf dem Anschluss *Network 1* auch als WireGuard-Client betrieben werden. Sie baut den VPN-Tunnel zu einem WireGuard VPN-Server auf.

 *Die Microwall VPN verfügt im VPN-Client-Modus über keine eigene Firewall für den Zugriff in das Inselnetzwerk. Zugriffsbeschränkungen müssen ggf. auf der Seite des VPN-Servers implementiert werden.*

Anwendungsbeispiel

Die Microwall verinselt ein internes Maschinen- oder Anlagen-Netzwerk. Im Service- oder Wartungsfall soll die Microwall eine VPN-Verbindung zum Hersteller aufbauen.

8.2 VPN-Client

Im Menüweig *VPN-Client* erfolgen die Grundeinstellungen des VPN-Client-Modus.

MicrowallVPN-08F142 / VPN-Client

Client aktivieren	<input checked="" type="checkbox"/> aktivieren [Status Tunnel]
Client-Einstellungen	Öffentlicher Schlüssel (VPN-Client) SVN/B3v66PnHQFmyVJS2jNkNFVxW+JbjznMnK/zAms= <input type="button" value="NEUER KEY"/> Virtuelle IP-Adresse Client (CIDR) * <input type="text"/> IP-Adresse/Hostname VPN-Server * <input type="text"/> UDP-Port VPN-Server * <input type="text"/> Öffentlicher Schlüssel VPN-Server * <input type="text"/> Erlaubte IPs * <input type="text"/> Keep-Alive * 20 Pre-shared Key (PSK) <input type="text"/> <input checked="" type="checkbox"/> Zugriff auf das WBM über die VPN-Verbindung erlauben
Konfiguration einspielen	<input type="button" value="HOCHLADEN"/>
Konfigurationsvorlage	<input type="button" value="HERUNTERLADEN"/>

Client aktivieren

Die Check-Box aktiviert die VPN-Verbindung zu dem WireGuard VPN-Server mit den angegebenen Parametern.

Bei aktiviertem VPN-Tunnel enthält die Zeile unter der Check-box den aktuellen Status und die Menge der transferierten Daten. Bedingt durch das von WireGuard verwendete verbindungslose UDP-Protokoll, kann die Aktualisierung des Tunnelstatus bis zu ca. 3 Minuten verzögert sein.

Client-Einstellungen → Neuer Key

Der Button *Neuer Key* generiert ein neues Schlüsselpaar für den Client-Modus der Microwall. Der angezeigte Public-Key wird für die Konfiguration des VPN-Servers benötigt und muss diesem mitgeteilt werden.

Client-Einstellungen → Virtuelle IP-Adresse Client (CIDR)

Die virtuelle IP-Adresse des Clients innerhalb der VPN-Umgebung. In der Regel erhalten Sie diese Adresse vom Betreiber de VPN-Servers und müssen diese hier eintragen.

Client-Einstellungen → IP-Adresse/Hostname VPN-Server

IP-Adresse/Hostname unter welcher der WireGuard VPN-Server erreicht wird. In der Regel erhalten Sie diese Adresse vom Betreiber des VPN-Servers und müssen diese hier eintragen.

Client-Einstellungen → UDP-Port VPN-Server

UDP-Portnummer unter welcher der WireGuard VPN-Server erreicht. In der Regel erhalten Sie die Portnummer vom Betreiber des VPN-Servers und müssen diese hier eintragen.

Client-Einstellungen → Öffentlicher Schlüssel VPN-Server

Public-Key des WireGuard VPN-Servers. Sie erhalten diesen vom Betreiber des VPN-Servers und müssen diesen hier eintragen.

Client-Einstellungen → Erlaubte IPs

Liste von IP-Adressen oder Adressbereichen (CIDR-Notation), die innerhalb des VPN-Tunnels erlaubt sind. Die Microwall VPN trägt hier automatisch die virtuelle IP-Adresse des VPN-Servers, die Net-ID des Insel-Netzwerks (vgl. Grundeinstellungen → Netzwerk) sowie die Net-ID des LANs auf der VPN-Server-Seite ein.

Client-Einstellungen → Keep-Alive

In dem hier konfigurierten Abstand in Sekunden werden Keep-Alive-Pakete vom VPN-Client an den VPN-Server gesendet, um den für das VPN benötigten UDP-Kanal offen zu halten. Die Zykluszeit für Keep-Alive-Pakete hat darüber hinaus Einfluss auf die Aktualisierung des Tunnelstatus, so dass wir einen Wert von 20s empfehlen.

Client-Einstellungen → Pre-shared Key (PSK)

Mit dem PSK wird die VPN-Kommunikation zusätzlich verschlüsselt. Der PSK muss auf dem VPN-Client und dem VPN-Server identisch sein. Wie auch der Public-/Private-Key ist der Syntax des PSK WireGuard-spezifisch und nicht frei wähl-

bar. Die Erzeugung erfolgt in der Regel auf dem VPN-Server oder auf einem Drittsystem mit Hilfe der WireGuard-Tools.

Client-Einstellungen → Zugriff auf WBM über VPN erlauben


Mit Aktivierung dieser Option werden Zugriffe auf das Web-Based-Management der Microwall durch die Tunnel-Verbindung erlaubt.

Konfiguration einspielen

Die gesamte Konfiguration des VPN-Clients inkl. des Private-Keys kann auch extern in einer Config-Datei erzeugt und in die Microwall VPN geladen werden.

Konfigurationsvorlage

Es kann eine Konfigurationsvorlage heruntergeladen werden, anhand derer die VPN-Client Konfiguration extern vorgenommen werden kann. So erstellte Konfigurationsdateien können über den Button *Konfiguration einspielen* in die Microwall geladen werden.

 *Die Microwall VPN verfügt im VPN-Client-Modus über keine eigene Firewall für den Zugriff in das Inselnetzwerk. Zugriffsbeschränkungen müssen ggf. auf der Seite des VPN-Servers implementiert werden.*

9 Wireguard-VPN Box-to-Box

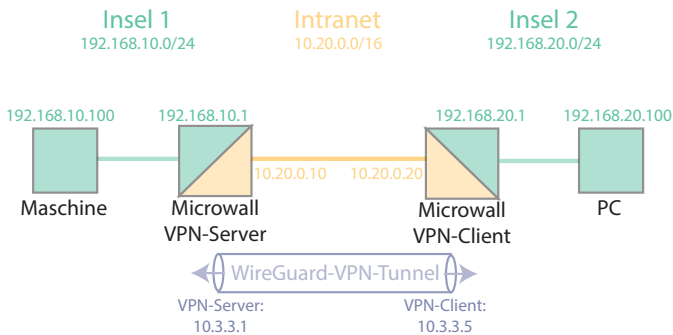
- VPN-Tunnel zwischen Insel-Netzwerken
- Konfiguration der Server-Microwall
- Konfiguration der Client-Microwall

9.1 Übersicht WireGuard-VPN Box-to-Box

Die Betriebsart Box-to-Box baut zwischen zwei Microwalls einen VPN-Tunnel auf, durch welchen die Insel-Netzwerke verschlüsselt und authentifiziert kommunizieren.

Im Box-to-Box-VPN arbeitet eine Microwall als VPN-Server, zu welchem sich andere, als VPN-Client konfigurierte Microwalls verbinden.

9.1.1 Konfigurationsbeispiel VPN Box-to-Box



Voraussetzungen

Die Microwalls sind mit den in der Skizze angeführten Adressen vorkonfiguriert und per Browser aus dem Intranet heraus erreichbar. Als Gateway in den Netzwerkteilnehmern der Inselnetze ist die dortige Microwall vorgegeben.

i In diesem Beispiel wird die Konfigurations-Datei für den VPN-Client auf der VPN-Server-Microwall erstellt. Diese Datei enthält den Private-Key des Clients sowie den ggf. verwendeten Preshared-Key und muss vertraulich behandelt werden. Für kritische Anwendungen empfiehlt es sich die Client-Konfiguration manuell über die Weboberfläche durchzuführen. Hierbei ist der Private-Key nicht auslesbar.

i Sollten Sie andere, als die hier verwendeten IP-Bereiche verwenden, beachten Sie, dass alle Netzwerke über unterschiedliche Net-IDs verfügen müssen.

1. Grundeinstellungen VPN-Server

Öffnen Sie in einem Browser die Webseite der als VPN-Server arbeitenden Microwall und loggen sich ein.

Navigieren Sie auf die Seite

VPN-Server → VPN-Umgebung

Nehmen Sie die folgenden Einstellungen vor und kopieren den angezeigten öffentlichen Schlüssel, um diesen später in die Konfiguration des VPN-Clients einzufügen:

VPN-Umgebung

VPN-Server


Server aktivieren	<input checked="" type="checkbox"/> aktivieren
Server-Einstellungen	<p>Öffentlicher Schlüssel 2Cv3lxsBZ5OzOlrX2TMPvsAr62wQNb1vSzuHWkk77WM= <input type="text" value="NEUER KEY"/></p> <p>Virtuelle IP/Subnet * 10.3.3.1/24</p> <p>UDP-Listenport * 4444</p>

Speichern Sie die Änderungen über 

2. Anlegen und Authentifizieren des VPN-Clients

Navigieren Sie auf die Seite

VPN-Server → Client-Inventar

Für das Hinzufügen eines neuen VPN-Clients klicken Sie auf  und nehmen die folgenden Einstellungen vor: Zur Erzeugung der Keys klicken sie den zugehörigen Button neben den Eingabefeldern.

VPN-Client hinzufügen

Virtuelle IP/Subnet des VPN-Servers: 10.3.3.1/24

Virtuelle IP-Adresse (des VPN-Clients) *

10.3.3.5



Name *

Client 1

Beschreibung

Public Key *

LDmqxYwkUe6jlxT1cl9+pGhQo0OXzi8V+RxTqj68Lic=



IP-Bereich Site-to-Site

192.168.20.0/24



Pre-shared Key (PSK)

rhOtuqLARA6WfFZMYGNkqsjMgDvP14Tg00tvS5

PSK ERZEUGEN



Zugriff auf diese Webkonfigurationsoberfläche erlauben

VPN-Client freischalten



Erweiterte Konfiguration

Sie können hier ein Private-/Public-Schlüsselpaar generieren und damit eine vollständige Konfigurationsdatei für Ihr Endgerät erzeugen. Wireguard-Clients für Windows, Android und iOS können diese direkt als Datei oder per QR-Code importieren.

Insbesondere der Private Key darf dabei nicht in falsche Hände geraten!

Bitte verwenden Sie diese Variante nur, wenn Sie die Konfigurationsdatei auf einem sicheren Weg an Ihr Endgerät übermitteln können.

Private Key *

MKCLoQ4EjsSdxS+37/t3Buy08W/vmcs6DcA

KEYS ERZEUGEN



Endpunkt (VPN-Server)

10.20.0.10:4444



Erlaubte IPs

192.168.10.0/24



Keep-Alive

20



CONFIG-DATEI HERUNTERLADEN

QR-CODE ANZEIGEN

HINZUFÜGEN ABBRECHEN

Laden Sie die Konfigurationsdatei über den entsprechenden Button herunter unter speichern diese. Diese Datei enthält den Private-Key des Clients sowie den ggf. verwendeten Preshared-Key und muss vertraulich behandelt werden.

Über *Hinzufügen* gelangen Sie zurück in die Inventar-Übersicht.

Client-Inventar

VPN-Clients



<input type="checkbox"/>	Virtuelle IP-Adresse	Name Beschreibung	Verwendung	
<input type="checkbox"/>	10.3.3.5	Client 1	0	

Speichern Sie die Änderungen über .

3. Grundeinstellungen VPN-Client

Öffnen Sie in einem Browser die Webseite der als VPN-Client arbeitenden Microwall und loggen sich ein.



Navigieren Sie auf die Seite

VPN-Client

Klicken Sie unter *Konfiguration einspielen* auf den Button *Hochladen* und senden die auf dem VPN-Server erzeugte Konfigurationsdatei in den VPN-Client.

Alle Eingabefelder werden automatisch ausgefüllt und es muss nur noch die Option *Client aktivieren* angeklickt werden.

VPN-Client

Client aktivieren	<p> <input checked="" type="checkbox"/> aktivieren</p> <p>Vor Kurzem aktiv (460 B empfangen, 2.0 KB gesendet). Status VPN-Tunnel: offen</p>
Client-Einstellungen	<p> Öffentlicher Schlüssel (VPN-Client) LDmqxYwkUe6jlxT1cl9+pGhQo0OXzi8V+RxTqj68Lic=</p> <p><input type="text" value="NEUER KEY"/></p> <p>Virtuelle IP-Adresse Client (CIDR) * 10.3.3.5/24</p> <hr/> <p>IP-Adresse/Hostname VPN-Server * 10.20.0.10</p> <hr/> <p>UDP-Port VPN-Server * 4444</p> <hr/> <p>Öffentlicher Schlüssel VPN-Server * 2Cv3lxsBZ5OzOlrx2TMPvsAr62wQNb1vSZuHWkk77WM=</p> <hr/> <p>Erlaubte IPs * 192.168.10.0/24</p> <hr/> <p>Keep-Alive * 20</p> <hr/> <p>Pre-shared Key (PSK) QJpl94auygj13xDVoSZui7cc+/DpUL2wJijm7HQEV/U=</p>

Speichern Sie die Änderungen über  .

Die Konfiguration des VPN-Clients ist hiermit abgeschlossen.

Der VPN-Tunnel wird jetzt aufgebaut und nach einigen Sekunden im Status sowohl gesendete wie auch empfangene Daten angezeigt.

4. Konfiguration der statischen Routen

Das Inselnetzwerk der jeweils gegenüber liegenden Seite muss sowohl dem VPN-Server als auch dem VPN-Client in Form einer statischen Route bekannt gemacht werden.

Navigieren Sie im VPN-Server und VPN-Client auf die Seiten

Grundeinstellungen → *Netzwerk*

Unter *Statische Routen* klicken auf  und nehmen folgende Einstellungen vor:

VPN-Server:

Route hinzufügen

Net-ID *

192.168.20.0

Subnet-Maske *

255.255.255.0

Gateway *

10.3.3.1

HINZUFÜGEN ABBRECHEN

VPN-Client:

Route bearbeiten

Net-ID *

192.168.10.0

Subnet-Maske *


255.255.255.0

Gateway *

10.3.3.5

Warnung: Das angegebene Gateway passt nicht zu den IP-Einstellungen des Geräts.

HINZUFÜGEN ABBRECHEN

Speichern Sie im VPN-Server und VPN-Client die Änderungen über .

5. Erstellen der Whitelist-Regel im VPN-Server

Alle Kommunikations-Verbindungen zwischen den beiden Insel-Netzwerken müssen in der VPN-Firewall in Form einer entsprechenden Regel explizit erlaubt werden.

Navigieren Sie im VPN-Server auf die Seite

VPN-Server → *VPN-Regeln*

Klicken Sie in der Regel-Übersicht auf  und nehmen Sie folgenden Einstellungen vor:

Regel Informationen

Name *
PC zu Maschine TCP/443

Beschreibung

Label

Label auswählen...

Netzwerk "Network 1" (VPN)

Quell-IP-Adresse(n) / VPN-Client | Name *
IP-Adresse(n) *
192.168.20.100
Quell-Port-Bereich(e) *
ANY

Richtung auswählen

→
 ←

Netzwerk "Network 2 (Island)"

Ziel-IP-Adresse(n) | Name *
IP-Adresse(n) *
192.168.10.100
Name *
Maschine Insel 1
Ziel-Port-Bereich(e) *
443

Protokoll


TCP FTP
 UDP

Aktionen

Regel aktivieren
 Log-Eintrag erstellen
 Verbindung akzeptieren

HINZUFÜGEN ABBRECHEN

Diese Regel erlaubt eine am VPN-Server über das VPN eingehende TCP-Verbindung von 192.168.20.100 zu der im Insel-Netzwerk angeschlossenen Maschine 192.168.10.100 auf dem Port TCP/443.

Klicken Sie *Hinzufügen* und in der Regel Übersicht auf  um die Regel zu speichern sowie zu aktivieren.

10 Digitale Ein-/Ausgänge (nur Microwall IO)

- Beschaltung der Ein-/Ausgänge
- Funktionen der digitalen Eingänge
- Funktionen der digitalen Ausgänge

Das folgende Kapitel ist ausschließlich für die Microwall IO und deren digitale Ein- und Ausgänge gültig.

10.1 Digitale Eingänge

Die Microwall IO verfügt über 2 per Schraubklemme zugängliche digitale Eingänge mit folgenden elektrischen Eigenschaften:

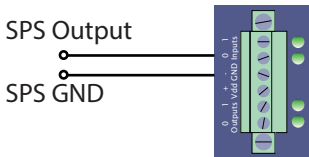
- Zulässige Eingangsspannung -30VDC - +30VDC
- Schaltschwelle 8V +/-1,5V
- Stromziehend (Strom ON ca. 2,2 mA)

Der aktuelle Status der Eingänge wird durch zwei zugehörige LEDs signalisiert.

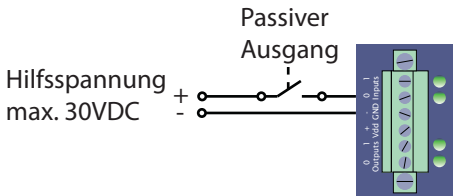
10.1.1 Beschaltung der digitalen Eingänge

Beide Eingänge sind stromziehend und müssen mit aktiven Ausgängen belegt werden, welche mindestens 2,2mA Strom liefern müssen.

Beispiel: Anschaltung aktiver SPS-Ausgang



Beispiel: Anschaltung potentialfreier Ausgang/Schalter



10.1.2 Verfügbare Aktionen der digitalen Eingänge

Die Zuordnung, der bei einem Statuswechsel des Eingangssignals auszuführenden Aktionen erfolgt im WBM-Menüszweig *I/O-Events*. Die Ereignisse werden unterschieden nach steigender und fallender Flanke. Jedem Ereignis können mehrere Aktionen zugewiesen werden.

Die folgenden Aktionen stehen zur Verfügung:

- Aktivierung/Deaktivierung des VPN-Tunnels als Client oder Server
- Aktivierung/Deaktivierung des Netzwerkschnittstellen
- Aktivierung/Deaktivierung von Firewall-Regeln mit bestimmten Labeln

10.2 Digitale Ausgänge

Die Microwall IO verfügt über 2 per Schraubklemme zugängliche digitale Ausgänge mit folgenden elektrischen Eigenschaften:

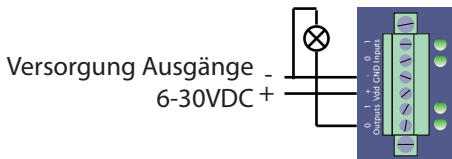
- Separate Ausgangsspannung 6-30VDC
- max. Ausgangsstrom 500mA/Ausgang, kurzschlussfest

Der aktuelle Status der Ausgänge wird durch zwei zugehörige LEDs signalisiert.

10.2.1 Beschaltung der digitalen Eingänge

Die Ausgänge verfügen über eine separate Versorgungsspannung und schalten im Status ON die an der Klemme *Vdd* anliegende Spannung durch.

Beispiel-Beschaltung Ausgang



10.2.2 Verfügbare Aktionen der digitalen Ausgänge

Die Zuordnung welches interne Ereignis der Microwall welchen Ausgang schaltet, erfolgt im WBM-Menüzweig *I/O-Events*. Ereignisse können einen Ausgang Einschalten, Ausschalten oder Toggeln.

Die folgenden auslösenden Ereignisse stehen aktuell zur Verfügung:

- Aktiver/deaktiver VPN-Tunnel (Client oder Server)
- Aktive/deaktive Konfigurations-Session WBM
- Aktiver/deaktiver Notzugang

11 Security & Wartung

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

11.1 Security-Hinweise

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

11.1.1 Funktion und typische Anwendung

Die Microwall ist eine als IPv4-Router konzipierte, strikt Whitelist-basierte Kleinfirewall mit zwei Ethernet-Anschlüssen und einem integrierten WireGuard-VPN-Zugang, welcher wahlweise als Client (ausgehend) oder als Server (eingehend) genutzt werden kann.

Die typische Anwendung besteht darin, eine Netzwerkinsel von einem übergeordneten Intranet logisch zu entkoppeln. Sie unterstützt den Betreiber hiermit bei der Segmentierung des Netzwerkes als eine Basis-Maßnahme vieler IT-Security-Konzepte. Die Intranet-Seite der Microwall (*Network 1, gelb*) kann über weitere Router und Perimeter-Firewalls mit dem Internet verbunden sein. Aus Sicht einer Defense-in-Depth-Strategie erfolgt der Einsatz der Microwall somit immer hinter mindestens einer Perimeter-Firewall und außerhalb einer DMZ.

Zum Zweck der Fernwartung verfügt die Microwall auf der Intranetseite (*Network 1, gelb*) über einen WireGuard-VPN-Endpunkt. Dieser ermöglicht als Client oder Server einen verschlüsselten, authentifizierten sowie über eine eigene Firewall geschützten Fernzugriff auf Teilnehmer des Inselnetzwerks. Ein Querzugriff auf das Intranet am Anschluss *Network 1* über das VPN ist nicht möglich

11.1.2 Anforderungen an Integriatoren und Betreiber

Die Werkseinstellungen der Microwall orientieren sich an einer universellen und möglichst barrierefreien Erstinbetriebnahme in einem Intranet.

Abhängig von der individuellen Netzwerkkumgebung und

den Security-Anforderungen müssen diese Vorgaben für den operativen Betrieb überprüft werden. Es können Änderungen und/oder zusätzliche Maßnahmen durch den Integrator oder Betreiber erforderlich werden. Hierzu zählen insbesondere:

- Wahl eines sicheren Passwortes hinsichtlich Länge und Zusammensetzung
- Deaktivierung nicht benötigter Dienste bzw. Beschränkung von deren Verfügbarkeit auf das benötigte Netzwerk-Interface
- Möglichst eng formulierte Firewallregeln (z.B. Vermeidung von Any/Any-Freigaben)
- Installation eines individuellen Gerätezertifikats innerhalb einer PKI-Umgebung
- Sicheres Management der WireGuard-Kommunikationspartner und sichere Handhabung der zugehörigen Keys.
- Schutz der Microwall vor unauthorisiertem physikalischen Zugriff

Weitere Details hierzu finden Sie in der Folge dieses Kapitels sowie in den vorhergehenden funktionspezifischen Kapiteln dieser Anleitung.

11.1.3 Installationsort

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

- Außerbetriebnahme des Gerätes (Entfernen Netzwerkkabel, Spannungsversorgung ...) 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 oder unauthorisierte VPN-Clients anzulegen.

11.1.4 Inbetriebnahme

Die Inbetriebnahme einer Microwall unterteilt sich in die Vergabe einer IP-Adresse per DHCP oder mit dem Tool *WuTility* und dem anschließenden Aufruf der initialen Webseite. Auf dieser erfolgen die Konfiguration des Passwortes sowie der netzwerkseitigen Basisparametern. Erst nach diesem Schritt ist der Zugang zur Managementoberfläche der Microwall VPN durch das Passwort geschützt.

IP-Vergabe

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 Inbetriebnahme über eine Punkt-zu-Punkt-Verbindung mit dem konfigurierenden Rechner durchzuführen. Erst anschließend wird die Microwall dann mit den eigentlichen Zielnetzwerken verbunden.

Passwort

Der operative Einsatz der Microwall ohne Passwort ist nicht möglich. Das Passwort 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.

11.1.5 Betrieb und Konfiguration

Individuelles Geräte-Zertifikat

Der Zugriff auf das Web-Based-Management kann ausschließlich verschlüsselt per HTTPS erfolgen. Ab Werk wird hierfür ein geräteindividuelles, 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 zum Schutz vor Man-in-the-Middle-Attacken das Default-Zertifikat durch ein individuelles eigenes Zertifikat zu ersetzen.

Deaktivierung nicht benötigter Dienste

Die Microwall unterstützt die folgenden eingehenden und ausgehenden Dienste:

Portnr.	Anwendung	Passwort?	Konfigurier-/abschaltbar?
Eingehend:			
443 (TCP)	HTTPS-Management Default: aktiv/Network 1	ja	ja/ja
8513 (UDP)	Inventaris. WuTility Default: aktiv/Network 1	nein	nein/ja
5555 (TCP)	Firmw.-Update WuTility Default: aktiv/Network 1	ja	nein/ja
446 (TCP)	HTTPS Notzugang Default: deaktiv, (manuelle Aktivierung über Service-Taster)	nein	nein/ja
161 (UDP)	SNMP Default: deaktiv, (Aktivierung per Web-Management und nur lesend)	ja (SNMPv3)	ja/ja
ICMP	Echo-Request Default: deaktiv	-	nein/ja
Ausgehend:			
123 (UDP)	NTP Timeserver Default: deaktiv	-	nein/ja

53 (UDP)	DNS Client Default: deaktiv (Aktivierung automatisch bei Bedarf)	-	nein/nein
514 (UDP)	Syslog Client Default: deaktiv	-	ja/ja
67 (UDP)	DHCP Client Default: aktiv (Deaktivierung durch statische IP)	-	nein/ja

Konfiguration und Aktivierung/Deaktivierung der ausgehenden 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 ab Werk über keine Freigabe-Regeln zur Kommunikation zwischen den beiden Netzwerkan schlüssen oder für einen VPN-Client. Bei der Formulierung von Regeln empfehlen wir, diese nach dem Need-to-know-Prinzip so eng wie möglich zu formulieren. 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 sowie für die Authentifizierung innerhalb des WireGuard VPN-Protolls verwendet. Beide Private-Keys der Microwall sind nicht auslesbar.

Bei der Einrichtung von WireGuard-VPN-Clients besteht aus

Gründen der Benutzerfreundlichkeit optional die Möglichkeit, das Schlüsselpaar des neuen Clients von der Microwall erzeugen zu lassen. Wählen Sie diesen Weg nur, wenn Sie eine vertrauliche Übertragung dieses Schlüssels an den VPN-Client gewährleisten können. Für Anwendungen mit erhöhtem Schutzbedarf empfehlen wir das Schlüsselpaar auf dem VPN-Client zu generieren und dann den unkritischen Public-Key auf anderem Weg an die Microwall zu übertragen.

11.1.6 Service, Wartung und Außerbetriebnahme

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

Bei der Außerbetriebnahme sollte zum Schutz aller in der Microwall gespeicherten vertraulichen Informationen (IP-Bereiche, Freigabe-Regeln, VPN-Zugänge etc.) auf die Werkseinstellungen zurückgesetzt werden. Dieses kann entweder über das Web-Based-Management oder den Service-Taster erfolgen.


11.2 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-/VPN-Regeln, VPN-Keys, 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 andere 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.

11.3 Firmware-Updates

Zur Behebung funktionaler Fehler, eventuell entdeckter Schwachstellen oder auch zur Funktions-Erweiterung veröffentlicht W&T Firmware-Updates für die Microwall. Der Upload in das Gerät erfolgt entweder mit Hilfe des Management-Tools WuTility oder über das Web-Based-Management der Microwall.

Zum Schutz vor Manipulationen der Firmware-Dateien und somit einer möglichen Kompromitierung der Geräte, sind alle Update-Dateien für die Microwall verschlüsselt und von W&T signiert.

Update-Dateien beinhalten immer die gesamte Firmware bzw. das gesamte System der Microwall. Aus diesem Grund sind Firmware-Updates immer mit einem Neustart der Microwall und somit auch einer Unterbrechung des operativen Betriebes verbunden. Individuelle Konfigurationsdaten (IP-Parameter, Firewall-Regeln etc.) werden von einem Firmware-Update nicht beeinflusst und bleiben erhalten.

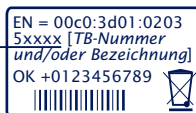
11.3.1 Wo ist die aktuelle Firmware erhältlich?

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. Sie finden diese auf dem an der Gehäuseschmalseite befindlichen Aufkleber.

Typnummer



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.


11.3.2 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.

Web-Zugriff



 zulassen

Zugriff erlauben aus:


Network 1 (LAN)

Network 2 (Island)

HTTPS-Port *

443

WuTility-Management


 zulassen (UDP/8513)

Zugriff erlauben aus:

Network 1 (LAN)

Network 2 (Island)


Firmware-Update

 zulassen (TCP/5555)

Zugriff erlauben aus:

Network 1 (LAN)

Network 2 (Island)

 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 betriebsbereit.





11.3.3 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 deaktiviert wurde, kann das Firmware-Update aus dem Web-Based-Management heraus erfolgen.

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

Wartung

Führen Sie hier Neustarts und andere Wartungsaufgaben durch.

Neustarten		<input type="button" value="NEUSTART GERÄT"/>
Zurücksetzen		<input type="button" value="WERKSEINSTELLUNGEN"/>
Service-Taster-Funktionen		<input checked="" type="checkbox"/> HTTPS-Notzugang <input checked="" type="checkbox"/> Werkseinstellungen setzen
Firmware-Update		<input type="button" value="DATEI HOCHLADEN"/> <small>(Bisher) keine Datei hochgeladen... Aktuelle Firmwareversion: 1.05</small> <input type="button" value="UPDATE INSTALLIEREN"/> <input type="button" value="UPLOAD VERWERFEN"/>

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. Die Microwall entschlüsselt die Firmware, prüft die Signatur und schreibt die Firmware in ihr internes Flash. Abschließend wird automatisch ein Neustart durchgeführt und die Microwall ist wieder betriebsbereit.

11.4 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 Netzwerkkumgebungen 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 vertrauenswürdige 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 VPN später im Browser aufgerufen werden. Unter *Alternative Names* können zusätzliche Namen, IP-Adressen und auch Wildcard-Namen 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.

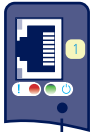
Nach einer formalen Prüfung wird das Zertifikat durch Klick auf *Installieren* unter *Extern signiertes Zertifikat* in das System integriert und bei allen Web-Zugriffen verwendet.

Informationen und Ablauf von Zertifikaten

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

11.5 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.



Service-Taster

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.

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`

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.

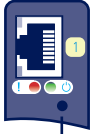
Beenden des Notzugangs

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.

11.6 Werkseinstellungen

Ein 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 3,5s 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*.

Anhang

- Technische Daten und Bauform

Technische Daten und Bauform

Microwall VPN, #55211

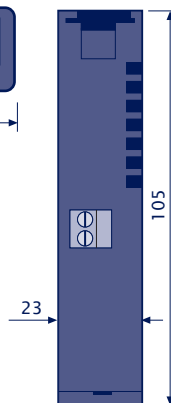
Spannungsversorgung ...	
Power-over-Ethernet:	37-57V DC aus PSE
Externe Speisung, Schraubklemme	DC 24-48V (+/-10%)
Stromaufnahme ...	
Power-over-Ethernet:	PoE Class 2 (3,84 W - 6,49W)
Ext. Speisung	typ. 150mA@24V DC max. 200mA@24V DC
Galvanische Trennung	Netzwerkanschlüsse: min 500V
LAN-Port Network 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 55211



Maße in mm, +/-1 mm

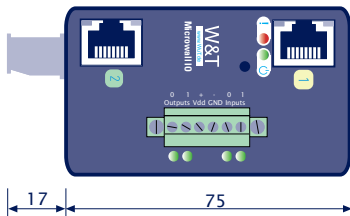
Unterseite 55211



Microwall IO, #55212

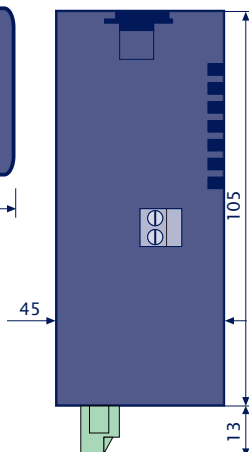
Spannungsversorgung ... Power-over-Ethernet: Externe Speisung, Schraubklemme	37-57V DC aus PSE DC 24-48V (+/-10%)
Stromaufnahme ... Power-over-Ethernet: Ext. Speisung	PoE Class 2 (3,84 W - 6,49W) typ. 150mA@24V DC max. 200mA@24V DC
Galvanische Trennung	Netzwerkanschlüsse: min 500V
LAN-Port Network 1	10/100/1000BaseT auf RJ45, autosensing, autocrossing, PoE
LAN-Port Network 2	10/100/1000BaseT auf RJ45, autosensing, autocrossing
Digitale Eingänge	2 x auf Schraubklemme Eingangsspannung +/-30VDC Schaltschwelle 8V +/-1,5V Eingangsstrom min. 2,2mA
Digitale Ausgänge	2 x auf Schraubklemme 6-30VDC, 500mA/Ausgang
Zulässige Umgebungstemperatur Lagerung ... Betrieb, nicht angereicherte Montage	-40 ... +85°C 0 ... +50°C
Zulässige rel. Luftfeuchtigkeit	0 - 95% (nicht kondensierend)
Abmessungen	105 x 75 x 45mm
Gewicht	ca. 180g

Frontansicht 55212



Maße in mm, +/-1mm

Unterseite 55212



Index**A**

Abmelden 33
Anmelden 33

B

Backup-Datei 100
Bauform 112
Beschaltung Ausgang 92
Beschaltung Eingang 90
Box-to-Box 82

C

Certificate Signing Request
106

D

Default-IP-Adresse 26
DHCP 22
DHCP-Server 36
Digitale Ausgänge 92
Digitale Eingänge 82, 90
Discover-Assistent 38
DNS-Proxy 51
DNS-Server 51

E

Erstinbetriebnahme 27

F

Firewall-Regeln 48

H

Hardware-Installation 14
Hostnamen 51
Hutschiene 14

I

Inbetriebnahme 21

K

Konfigurations-Backup 30
Konfigurationsdateien 30, 100

L

LED 17
Link-Status 17

N

Navigationskonzept 32
Netzwerkschnittstellen 16
Notzugang 19, 108

P

PoE 15
Preshared Key 63, 78
Preshared-Key 71, 85
PSK 63, 71, 78

R

Reset 19

S

Security 93
Service-Taster 19, 108, 110
Spannungsversorgung 15
Standard-Router 42
Static-NAT 44
System LED 18

T

Technische Daten 111

V

VPN-Clients 60
VPN-Regeln 65

W

Web-Based-Management 31

Werkseinstellung 19

Werkseinstellungen 110

WlreGuard Client 76

WuTility 23

Z

Zertifikate 106