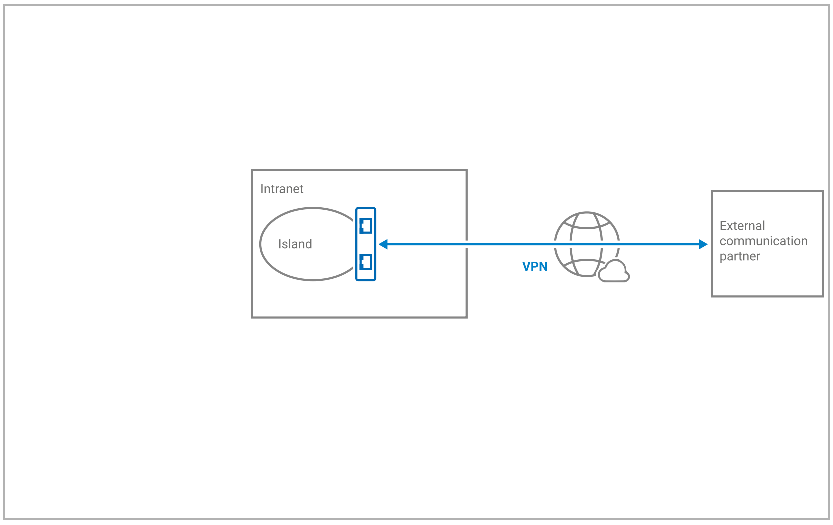
Data sheet:

Microwall VPN



Article no.: 55211

EUR 448.00

*Net price for
commercial users

Click on the image for a larger view

□ □ □

Secure communication for machines and systems

Secure communication = secure operation - The Microwall VPN is a firewall that uses appropriate rules to protect your critical machines or systems from undesired or harmful access. Communication from and to the island is restricted to what is essential for operation, thereby significantly reducing the potential attack area. Harmful events such as load spikes, broadcast storms etc. remain locally limited and have no effects on the other respective segment.

Secure commissioning - In contrast to many other routers which often permit unrestricted outgoing data communication, the Microwall VPN blocks any cross-network data traffic. In Discover mode outgoing communication attempts of the island-side connected devices and including the associated host name of the destination server are documented. Permitted destinations are used with a mouse click to create a release rule, whereas undesired communication remains blocked.

Secure remote access via VPN - For remote maintenance and remote access to the island network the Microwall VPN provides a WireGuard®-VPN endpoint which can be operated actively as a VPN client or passively as a VPN server.

More info: Learn more about how the Microwall VPN workshere.

Properties | Run modes | Technical data | Accessories

Properties:

Interfaces:

- **2x Ethernet 100/1000BaseT**
  - Autosensing and Auto-MDIX
- **High data throughput**
  - Gigabit Ethernet
  - max. 900 mbps in router mode, max. 300 mbps VPN
  - Low latency times thanks to powerful hardware platform

Connectivity:

- **Mode: Standard router**
  - Integration into the routing concept of the intranet
  - Static NAT can be used for 1:1 mapping of intranet IPs on island hosts.
- **Mode: NAT router**
  - Integration of the islands via a single Intranet IP
- **Discover mode**
  - Assisted and secure commissioning of new/unknown devices
  - Recording of outgoing connection attempts including DNS host names
  - Creating release rules with the click of a mouse
- **WireGuard VPN server & VPN client**
  - Secure VPN connection to the island for Windows, Linux, Android, MacOS, IOS clients, Microwalls
  - Access control of VPN clients using dedicated firewall
  - In Client mode VPN connection to your manufacturer/service network

- **Wire Guard VPN Box-to-Box**
  - VPN tunnel between two Microwalls
  - Secure connection of island networks using the intra/internet

Management & Security:

- **Secure firmware concept with Secure Boot**
  - No uploading of manipulated firmware or third-party firmware
- **Configuration via HTTPS-Only Mode**
  - Supports individual certificates
  - Fast startup using WuTility or DHCP
  - Required password without default login
- **Port management for all local services**
  - All service/management services can be configured/deactivated
- **Consistent whitelist-based firewall concept**
  - Filter rules based on IPv4 addresses, host names and TCP/UDP port numbers
  - Dedicated firewall for incoming VPN connections
- **Logging**
  - Identification of undesired communication attempts
- **Network management systems**
  - Optional support for SNMPv2c/3 (read)

Supply Voltage

- **External power**
  - Screw terminals, 24V-48V DC
- **Power-over-Ethernet (PoE)**

Standards & more

- **Conforms to standards both in office and industrial environments:**
  - High noise resistance per EN 61000-6-2
  - Low noise emission per EN 55032:2015 + A1 Cl. B, EN 61000-3-2 & EN 61000-3-3
- **5 year guarantee**

Wish for something!
Your suggestions for improvement and additions

Operating modes:

The Microwall VPN remotes sensitive components or subnets into a separate island network and separates it from the higher level company intranet. For remote maintenance, remote support, etc. a WireGuard VPN server is available which provides selected VPN clients with secure and dedicated firewall protected access to the island stations.

All connections between the networks must use rules based on source/destination IP and the used TCP/UDP port numbers to obtain an express release. For outgoing connections host names can be used as a destination within the rules. Communication of undocumented and/or undesired services is prohibited and harmful events such as overload are kept away from the island.

NAT router mode

Similar to a traditional DSL internet connection, the entire island network is incorporated via just an IP address of the intranet into the network there. No intervention into the routing concept of the intranet is necessary. Operation of multiple island networks having the same IP ranges is also possible in this mode. This gives machines and systems manufacturers the possibility of operating internal network with a uniform series IP configuration - no cumbersome adaptations to the customer’s infrastructure.

Standard router mode

The Microwall VPN operates like a traditional router, while the island network appears in the intranet in the form of static routing. Static NAT can also be used for 1:1 mapping of intranet addresses to fixed IPs in the island network. These island hosts thereby become quasi-local components of the intranet while still enjoying the protection of appropriate firewall rules.

Discover mode

Connection attempts on the island side to connected hosts are recorded and logged including whatever destination host names were used. For desired connections, a release rule is created just by a mouse click. Unknown, undesired or harmful connections remain blocked.

WireGuard VPN

The Microwall VPN uses the WireGuard platform as a VPN solution for remote access. Compared with other VPN solutions this offers advantages such as high data throughput and simple management with a high level of security and stability. Details and current information about WireGuard can be found at https://www.wireguard.com. The Microwall VPN can provide a VPN client or VPN server terminal point on your intranet connection. Depending on the application external WireGuard clients can dial in to the islands or the Microwall connects as a VPN client - for example into your service network.

Technical data:

Connections and displays:

Network:	2x 100/1000BaseT Autosensing/Auto-MDIX RJ45 IPv6 on request
Data throughput:	Router mode (unidirectional TCP): max. 900MBit/s VPN tunnel (unidirectional TCP): max. 300MBit/s
Electrical isolation:	Network connections min. 1500 V
Supply voltage:	Power-over-Ethernet (PoE) or DC 24V .. 48V (+/-10%) and
Supply connection:	Plug-in screw terminal, 5.08mm spacing Labeled "L+" and "M"
Current consumption:	PoE Class 2 (3.84 W to 6.49 W) or for external supply: typ. 150mA @24V DC max. 200mA @24VDC
Indicators:	2x LEDs for network status 1x LED for Error

Housing and other data:

Enclosure:	Plastic compact housing for top-hat rail mount 105x22x75mm (LxWxH)
Enclosure rating:	IP20
Weight:	approx. 120g
Ambient temperature:	Storage: -40..+85°C Operating 0..+50°C (no stack mounting)
Permissible relative humidity:	5..95% RH, non-condensing
Scope of delivery:	1x Microwall VPN 1x Quick Guide

Accessories

*Net unit price for commercial users

Power supplies

Plug-in power supply, 24V / 500mA DC with Euro plug	11021	21.00€	🛒
Plug-in Power Supply, 24V / 750mA DC with Euro, US and UK plug	11026	38.00€	🛒
Power supply for DIN rail, 24V / 630mA DC (merchandise, 2-year manufacturer's guarantee)	11080	33.00€	🛒

Mechanical Accessories

Wall mount housing, enclosure rating IP66 / IP67	11120	54.00€	🛒
Mounting bracket for wall mounting	58812	11.20€	🛒
19" DIN rail	58813	21.00€	🛒

Supplementary network products

Ethernet Switch Industry, 4 Ports	55604	218.00€	🛒

Software

WuTility	00104	free	⬇

* Our offering is intended only for commercial users. We will be happy to refer private end customers to trading partners through whom our products can be purchased.

We are available to you in person:

Wiesemann & Theis
GmbH
Porschestr. 12
42279 Wuppertal
Phone: +49 202/2680-110 (Mon.-Fri. 8 a.m. to 5
p.m.)
Fax: +49 202/2680-265
info@wut.de

Data Privacy