Background information:

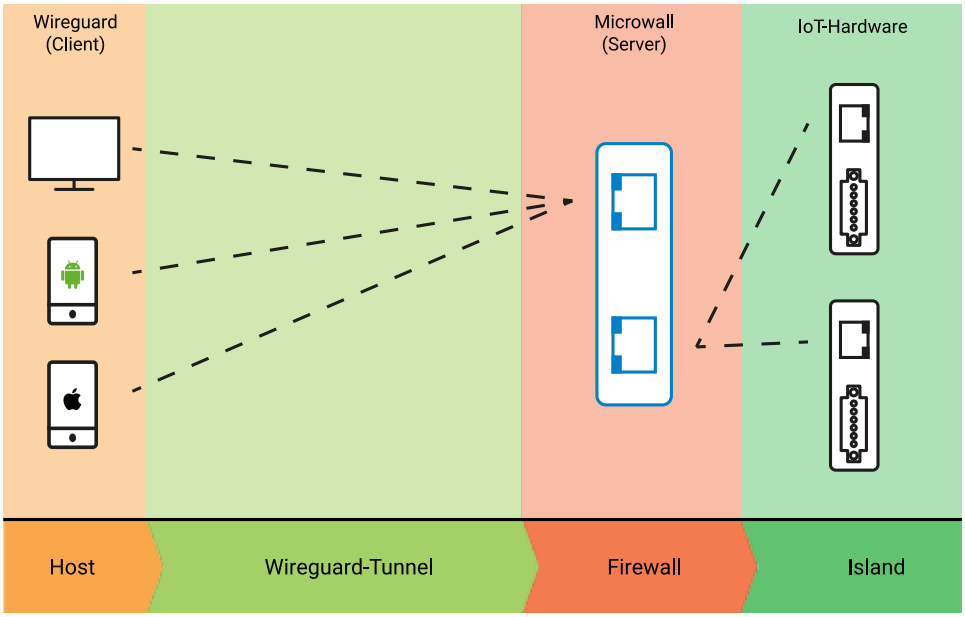
VPN scenarios

The Microwall combines various network devices into a protected network island.
Communication in and out is through an encrypted and authenticated VPN tunnel. It must be decided from where the initiative for opening the connection comes.

Initiating the connection	from the outside	island side	configuration-dependent
	e.g. from mobile workers, service providers, by the integrator or manufacturers	e.g. by the operator, the machine or the sensor	
	Host-to-Island	Island-to-Host	Island-to-Island

1. Host-to-Island

A Microwall is installed at the customer/operator and configured as a VPN server. The communication partner can be various hosts using Windows, Linux, Android, MacOS or iOS and with the aid of corresponding software used as VPN clients.



A VPN client can at any time open an encrypted and authenticated connection to the partner in the segmented network. This gives manufacturers and integrators the ability when needed to access the corresponding network sector for service or maintenance purposes without having to be on site. By segregating the corresponding network segment as well as using the VPN firewall the operator can be assured that external communication partners only have access to allowed areas.

Other possible applications include far distant or difficult to access locations such as wind power and photovoltaic equipment.

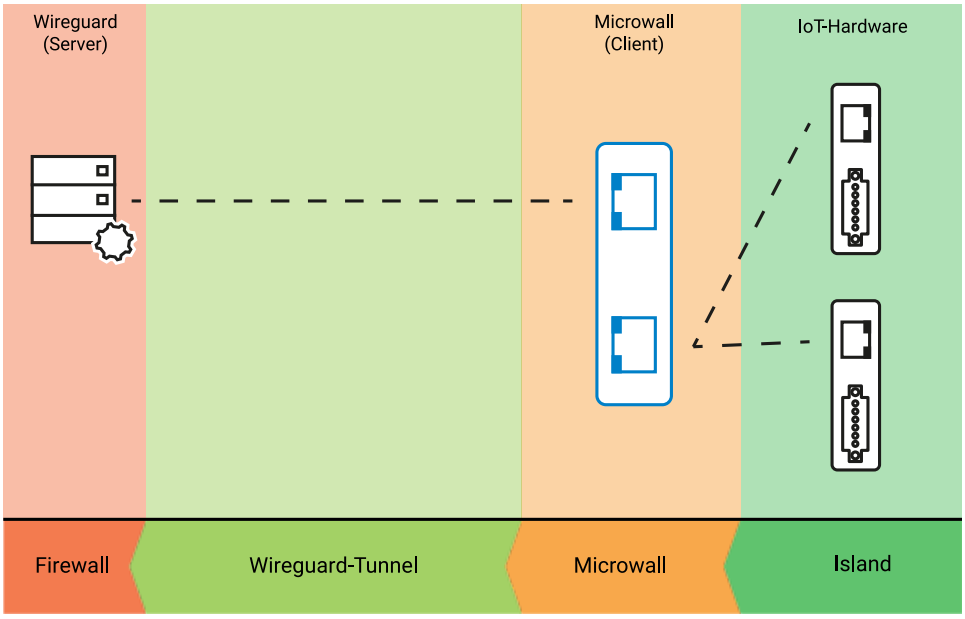
Use the smartphone to securely access a Web-IO

Lean how you can use a smartphone and VPN tunnel to access a Web-IO. In the following tutorial we show you step-by-step how to configure this.

Go to the tutorial

2. Island-to-Host

The Microwall installed at the operator is configured as a VPN client and when needed opens an encrypted and authenticated connection to the VPN server.



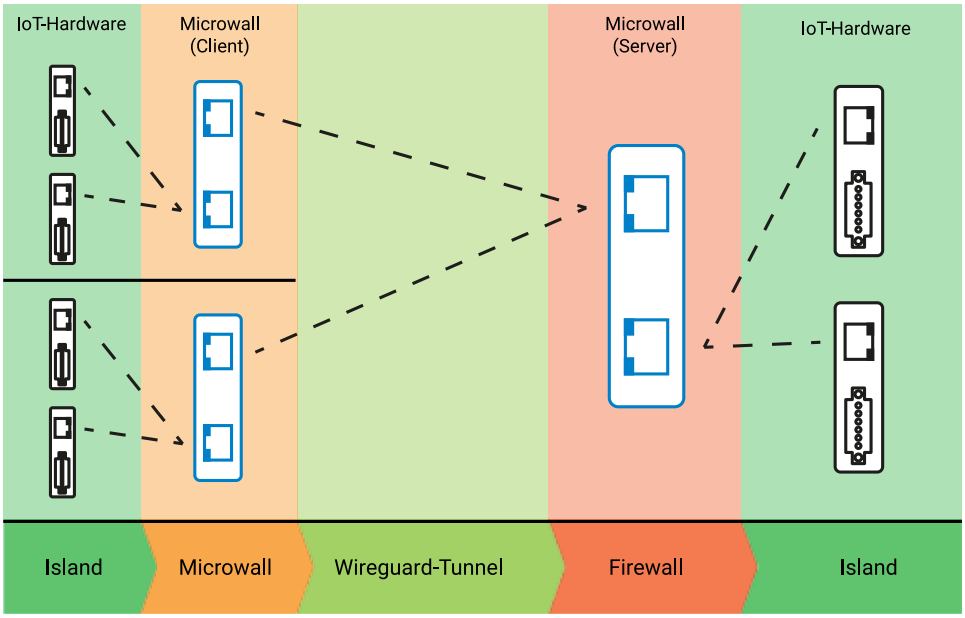
Once the VPN connection has been initiated on the operator side, the operator can access a remote service or maintenance network at the manufacturer or integrator. The prerequisite on the manufacturer side is an Linux operating system or an additional installed Microwall.

This application scenario is particularly relevant for regular maintenance requirements and for checking fault messages in hard to access systems, such as wind power or photovoltaic plants.

Here follows a tutorial for realizing the Island-to-Host scenario.

3. Island-to-Island

In the Island-to-Island scenario a VPN connection between two Microwalls is opened. The resulting encrypted and authenticated VPN tunnel lets any network device which is listening to one of the two islands act as a communication partner of the other network island.



In this way network sections can also be securely connected to each other through non-secure network environments. This protects information and data especially in public or highly complex networks.

WireGuard VPN tunnel between 2 networks

A PC in Island 1 needs to use a VPN tunnel to access the web page of a Web-IO in Island 2. The steps for configuration are explained in this tutorial.

Go to the tutorial

The proof of the pudding is in the eating!

We are happy to provide you with a Microwall at no charge for a period of four weeks.

Request test unit

Thomas Clever
t.clever@wut.de

You can reach our engineers by phone at +49 202/2680-110 (Mon.-Fri. 8 a.m. to 5 p.m.)

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