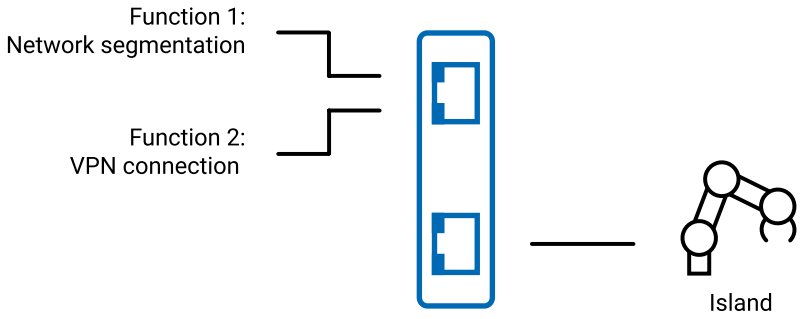
Function description:

Secure communication for machines and systems

with near and distant communication partners



Linking critical systems to the intranet - isolation using the Microwall

Segmenting of individual function units is a common practice in companies for enhancing network security. Firewall routers monitor and control communication between the individual segments. Depending on the size of the company and units the necessary firewall rules become quickly evident. The Microwall is located as close to the vulnerable equipment as possible and creates a network island around the respective function unit.

Filtering rules in the form of a white list can be used to protect the equipment itself as well as the remainder of the network and data contained in it, so that now only expressly permitted communication is allowed between the island and the surrounding network. The set of filtering rules needed for securing the island is thereby usually reduced to a manageable degree.

Here you will find more detailed information:

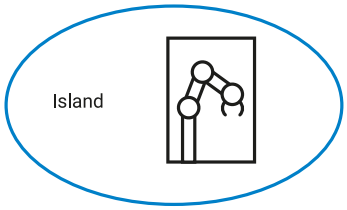
- Firewalls, segmenting and isolation
- Application example: Isolating a CNC milling machine

Secure remote access with VPN end point directly on the equipment

A VPN tunnel is used for communication with external communication partners such as service technicians at the machine or employees in the home office. By using WireGuard VPN a secured and authenticated connection between the isolated unit and the trustworthy connection partner is established over which the data packets can be sent and received. The surrounding intranet is tunneled by the connection and cannot be accessed by the communication partner or any possible attackers of the segmented unit.

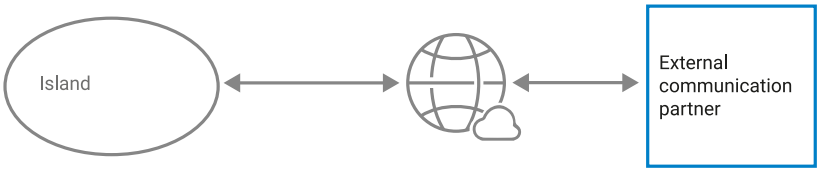
Entities

Island



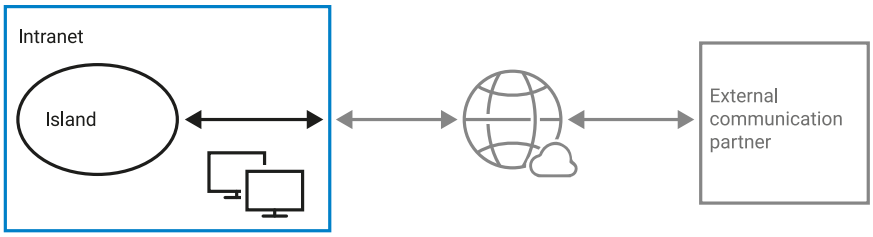
Network islands are small subnetworks which are located within a higher level network. In this way individual areas in the company are separated according to function. Potential attackers and malware cannot reach the overall company network. But the more entities are included in a network the more extensive and complex the necessary filter rules in the firewall. Therefore it can make sense to isolate individual systems or even single machines or computers which communicate not only over the intranet but also over the Internet.

The external communication partner



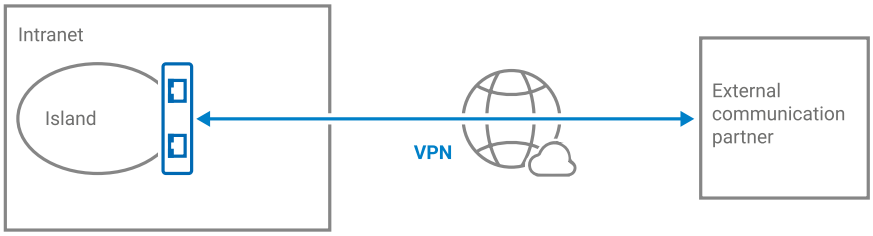
In some applications the communication partner of machines, systems or computers is not located in the same network as the unit itself. This is always the case for example in situations where remote maintenance has to be performed on machines, where unmanned equipment is operated at difficult to access locations, or machine data are collected from an external point. In such cases the connection has to be made over the Internet. Even when the communication partner is known and authenticated, data can be picked up and read anywhere along the connection. To prevent this and to bring the two communication partners together securely, VPN tunnels are used.

The intranet



The path from the external communication partner to the respective location in the organization generally passes not only through the Internet but also over the intranet. Many other devices are connected there to the network: Employee PCs, machines, equipment, servers, firewalls or other network segments. The VPN tunnel that passes uninterrupted to the network island thereby increases the security of the tunneled data while also preventing any access to all other network devices. The pass-through must be ensured through all firewalls and routers on the intranet line.

The solution: Microwall VPN



With its two network interfaces the Microwall VPN isolates parts of a network in a separate segment and connects them to the intranet according to user-configured firewall rules. As the VPN termination point on the edge of the network island the Microwall can also open an encrypted connection to a communication partner outside the company. This requires only that the partner install the corresponding WireGuard software and perform the corresponding authentication. Once the connection is established the two communication partners behave as if they were in the same network.

Could you use some assistance?

If you have questions or need a consultation please don't hesitate to contact me.

+49 202/2680-110 t.clever@wut.de

Thomas Clever

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