Background information:

Important firewall rules

for configuring the W&T Microwall

To the topic of isolation
To firewalls

These standard firewall rules help you to implement typical applications for the Microwall.

For the sake of simplicity we shall use the following configuration:

The isolated network segment has the network address 10.10.20.0/24 assigned to it, and the surrounding network has network 10.10.10.0/24.

In the following rules the device on the island always has the IP address 10.10.20.**20**, and the device in the surrounding network has IP address 10.10.10.**10**.

File access from the island computer to a file server (TCP/IP)

TCP/IP Windows file access release
File access is via SMB Protocol. Here the isolated host must open a TCP connection to port 445 of the file server. If access is directly through the IP address of the file server, this rule is sufficient.

Island network	TCP	Surrounding network
IP: 10.10.20.20 **Port: any**	→	**IP 10.10.10.10** **Port: 445**

File access from island computer to a file server (NetBIOS)

If older computers - using Windows XP for example - also need to be access the Windows network, you must also approve the session-based NetBIOS transport protocol on Port 139/TCP in addition to the TCP port 445.

Please note that these older operating system versions are unsafe!

Rule 1: Release of the NetBIOS session service
Permit data transport over the connection-based session service.

Island network	TCP	Surrounding network
IP: 10.10.20.20 **Port: any**	→	**IP 10.10.10.10** **Port: 139**

Rule 2: Release of file access
Open TCP connection to Port 445 of the file server.

Island network	TCP	Surrounding network
IP: 10.10.20.20 **Port: any**	→	**IP 10.10.10.10** **Port: 445**

Permit name resolution via DNS

Resolve host name via DNS
Using the Domain Name System (DNS) you obtain the IP address of a computer which is accessed by its computer name. This is a short data exchange via UDP.

Island network	UDP	Surrounding network
IP: 10.10.20.20 Permit return direction: yes		IP 10.10.10.10 Port: 53

Obtain current time over the network (NTP)

Time updates with (S)NTP via UDP
Time servers provide the current time using Simple Network Time Protocol (SNTP) or Net Time Protocol (NTP).

Island network	UDP	Surrounding network
IP: 10.10.20.20 Permit return direction: yes		IP 10.10.10.10 Port: 123

Access to a web interface in the island network

Permit unencrypted HTTP
For access to unencrypted web sites TCP port 80 must generally be opened.

Island network	TCP	Surrounding network
IP: 10.10.20.20 Port: 80		IP 10.10.10.10 Port: any

(Alternative): Permit encrypted HTTPS
For access to encrypted web sites TCP port 443 must generally be opened.

Island network	TCP	Surrounding network
IP: 10.10.20.20 Port: 443		IP 10.10.10.10 Port: any

Sending email from the island network

In the following rules it is assumed that the IP addresses of the mail servers are known.

Send emails via SMTP (with/without StartTLS)
Unencrypted and StartTLS-protected email sending via SMTP.

Island network	TCP	Surrounding network
IP: 10.10.20.20 Port: any		IP 10.10.10.10 Port: 587

(Alternative): Send emails via SMTPS.
Encrypted email sending using SMTPS.

Island network	TCP	Surrounding network

IP: 10.10.20.20 Port: any		IP 10.10.10.10 Port: 465

Access emails from within the island using IMAP

Access email accounts using IMAP (with/without StartTLS)
Access email accounts from within the island - unencrypted or protected by StartTLS.

Island network	TCP	Surrounding network
IP: 10.10.20.20 Port: any		IP 10.10.10.10 Port: 142

(Alternative): Access emails using IMAPS (with/without StartTLS)
Access email accounts from within the island, TLS protected

Island network	TCP	Surrounding network
IP: 10.10.20.20 Port: any		IP 10.10.10.10 Port: 992

Sending an SNMP trap from within the island

Unencrypted SNMP trap from within the island

Island network	UDP	Surrounding network
IP: 10.10.20.20 Permit return direction: no		IP 10.10.10.10 Porto: 162

SNMP polling from outside

Permit unencrypted SNMP polling by a manager outside the island
An SNMP manager can access the island for querying the values there by polling.

Island network	UDP	Surrounding network
IP: 10.10.20.20 Permit return direction: yes SNMP: yes		IP 10.10.10.10 Port: 161

Use Secure Shell to access an island device

SSH connection to the island
You can use an encrypted terminal session to control a computer on the island.

Island network	TCP	Surrounding network

IP: 10.10.20.20 Port: 22		IP 10.10.10.10 Port: any

IoT communication using MQTT broker

MQTT connection to the island
MQTT is a standard protocol for the Internet of Things. Using an MQTT broker you can exchange messages even across islands.

Island network	TCP	Surrounding network
IP: 10.10.20.20 Port: any		IP 10.10.10.10 Port: 1883

Query MySQL database on the island

Open connection to database server on the island
If a database server on the island needs to be polled, TCP port 3306 must be released.

Island network	TCP	Surrounding network
IP: 10.10.20.20 Port: 3306		IP 10.10.10.10 Port: any

Permit W&T - Box-2-Box mode (Web-IO Digital 4.0)

Connection to Box-2-Box slave on the island
To open a Box-2-Box connection to an island device, you must use one of the two Box-2-Box slave ports.

Island network	TCP	Surrounding network
IP: 10.10.20.20 Port: 49157, 49158		IP 10.10.10.10 Port: any

Permit W&T OPC access (Web-IO Digital 4.0)

Permit access for the W&T OPC server
To detect island devices in the W&T OPC server you must enable TCP port 49159.

Island network	TCP	Surrounding network
IP: 10.10.20.20 Porot: 49159		IP 10.10.10.10 Port: any

Permit W&T ASCII protocol (Web-IO Digital 4.0)

Permit access using W&T ASCII protocol
By exchanging simple command strings you can for example read inputs and counters on Web-IOs and set outputs.

Island network	TCP	Surrounding network
IP: 10.10.20.20 **Porto: 42280**	←	**IP 10.10.10.10** **Port: any**

Permit W&T - Binary protocol

Permit access to binary servers in the island segment
The W&T Binary mode allows multiple TCP connections between devices.

Island network	TCP	Surrounding network
IP: 10.10.20.20 **Port: 49153 - 49156**	←	**IP 10.10.10.10** **Port: any**

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