Microwall Gigabit application example:

Isolating a CNC milling machine

In our company we use a CNC milling machine for fabricating prototypes and small series. A Windows 7 embedded standard with the latest patch level runs on the control computer which is incorporated into our production network. Since Microsoft will no longer provide expanded support for this operating system as of 2020, this milling machine has been isolated as a precaution. Using the "Microwall Gigabit" firewall router a dedicated network segment is assigned to it and communication with this network segment highly filtered.

Greater network security through isolation

In 2017 WannaCry gained worldwide attention as it wreaked havoc in networks. This ransomware cryptoworm exploited a vulnerability in the file and printer sharing protocol of Windows networks. It was so damaging that Microsoft not only patched the current operating systems, but also provided security updates for products for which support had already expired.

WannaCry demonstrated effectively how great the risk is from running unneeded network services.

It seems obvious that non-essential services should simply be disabled. But it's not always clear which services are in fact needed between sub-components in a system. Furthermore changes to machines could be made which under some circumstances could result in a loss of certification and thereby to a transfer of liability over to the operator.

And so we have developed Microwall Gigabit as an easy to use alternative for protecting production systems. This is a simple 2-port firewall which uses the whitelist principle. This means: all allowed connections must be explicitly released.

Objective

The milling machine is equipped with a Windows control computer on which the CNC software runs. It uses two network interfaces: one connects the computer to the milling machine itself, and the other incorporates it into the production network. If a security hole in the current status of the operating system is discovered, Microsoft will provide a timely security update. After the end of extended support in 2020 however no more security updates will be provided in normal cases. An attacker could try to compromise the control computer and if successful threaten not only the device itself, but even the surrounding network.

This is why the milling machine needs to be isolated using the islandization strategy. Microwall places the milling machine in its own network segment and severely restricts what communication is possible with this network segment through the use of firewall rules.

Vulnerability

A brief analysis of the current situation with the port scanner nmap [Tutorial: Finding open ports in the network] reveals something unsettling: the control computer shows twelve open ports that can be reached in the network, including a web server.

A second, intensive scan finds a total of 24 open TCP ports. The web server is an unconfigured internet information server 7.5 which shows known weaknesses which can result in remote code execution. This means that an attacker can run any program he wishes over the network. A lottery win for cyber warriors. An ironic detail: the web server seems to serve no other purpose than as an information page, and so is in all likelihood as superfluous as the other open ports. We are happy that we took the time for an intensive scan and will commence with islandization immediately.

Procedure

Step 1: Determine the mode and the necessary firewall rules

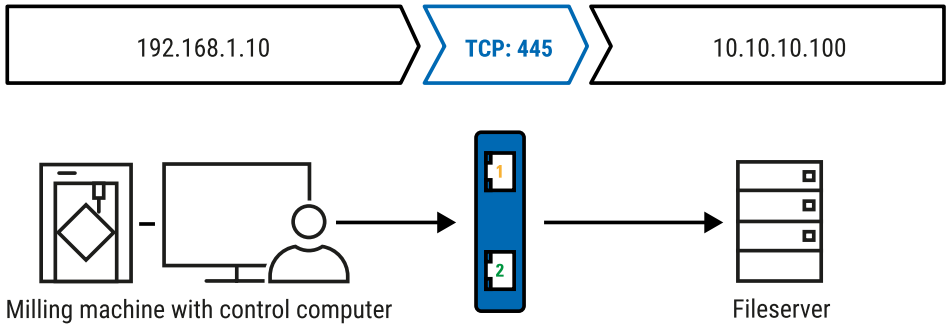
To keep the configuration as simple as possible, we run the Microwall in NAT mode. The control computer for the milling machine doesn't even appear, rather the Microwall more or less takes on its role in the network.

Actually there is only one situation in which the milling machine should communicate over the network. To be able to access production data it must be allowed to open a connection to the central Windows file server. All other connections are prohibited.

Since the control computer itself does not provide any resources in the network, incoming connections are completely blocked. Furthermore the file server release which is supposed to allow access by the CNC software is known and unambiguous. Since the IP address of the file server is also known, no name resolution is required. Convenience functions such as searching for computers and releases over the network are superfluous, likewise the NetBIOS transport protocols. Ports 137, 138 and 139 can therefore be ignored and even blocked. For automatic time updates UDP port 123 could be enabled, and for name resolution via DNS UDP port 53. Since these functions are however also not needed for functioning of the milling machine, they remain closed as well.

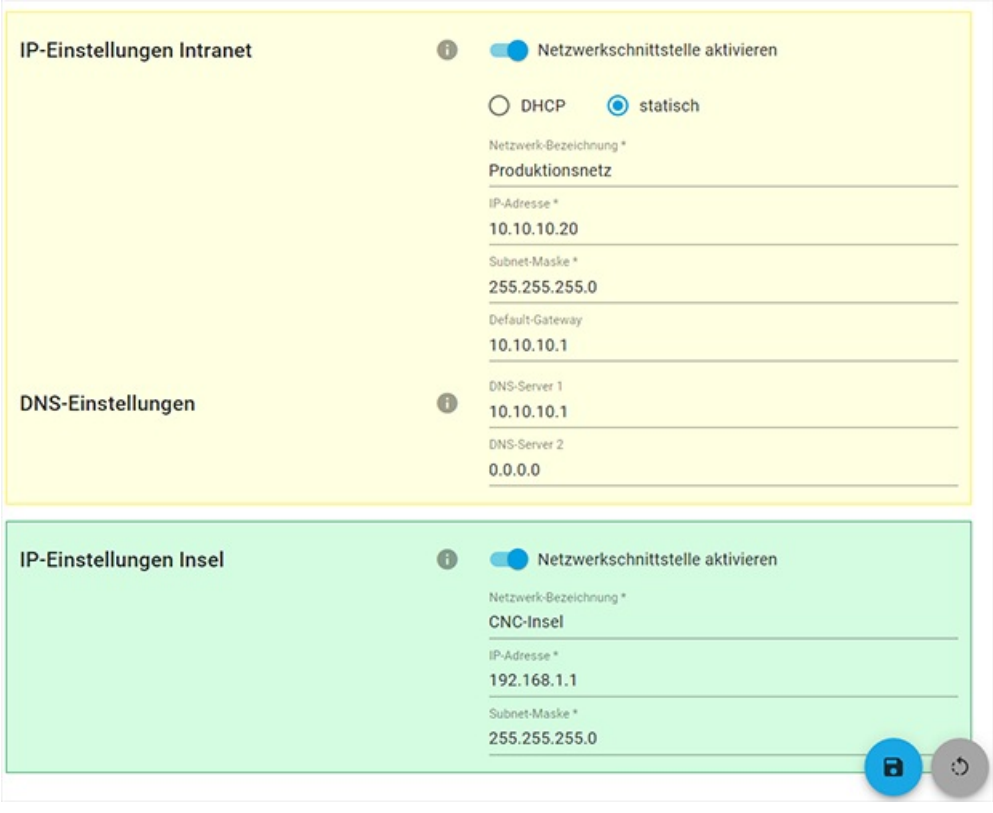
Patch management is handled by our IT department, which is why the ports remain closed even for an automatic update. Otherwise we would have to allow TCP connections to the WSUS server.

The control computer needs only to be able to open an SMB connection to the file server with the known IP address. This happens using destination port 445. Since this is TCP communication, the back channel is directly included in the connection. **By specifying just a single rule the milling machine is permanently secured. At the same time its function is also ensured!**



Step 2: Device configuration

In its function as a router the Microwall connects the surrounding network to an isolated segment. It does however an IP configuration for the interfaces to the two networks.



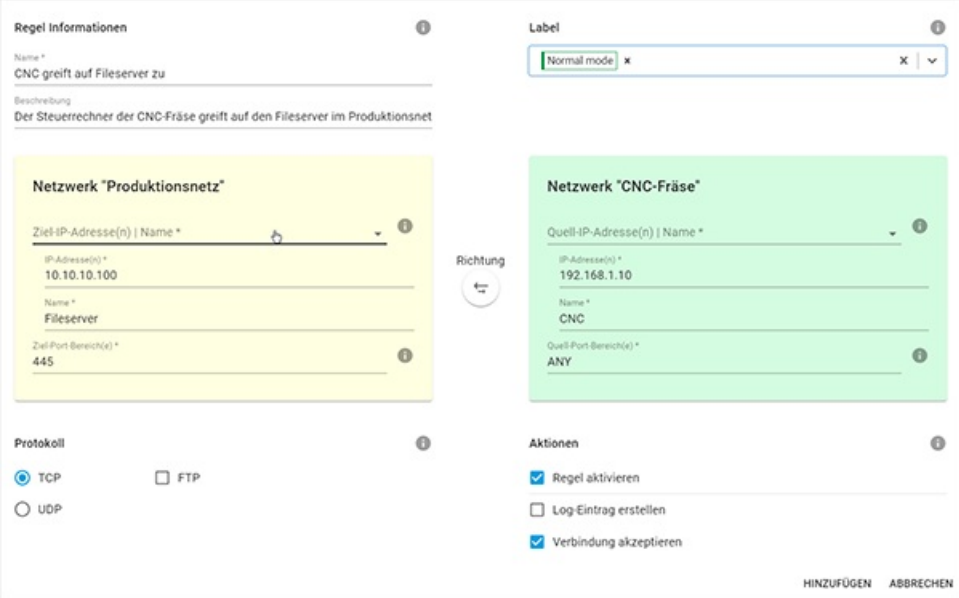
1 Specifying a network name makes it easier for the administrator to later assign rules.

2 The original IP configuration of the control computer (i.e. 10.10.10.20) is taken on for the public interface. Other than the hardware address nothing in the surrounding network changes.

3 On the island side, for simplicity's sake we choose the traditional 192.168.1.0/24 network. For this network the Microwall serves as a standard gateway is gets address 192.168.1.1

IP configuration of the control computer
The control computer is given IP 192.168.1.10. As a standard gateway it is assigned the Microwall with IP address 192.168.1.1.

Firewall rules for file server access
In the last step we set up the necessary firewall rules. The control computer with IP address 192.168.1.10 must be able to open a connection through port 445 to the production data server having IP address 10.10.10.100.



Step 3: Test run

The test run over several weeks shows that the milling does its job as usual.

Summary

With the help of Microwall the CNC milling machine was able to be isolated in its own network segment in a matter of minutes. To ensure proper function only a single firewall needed to be applied. As a side-effect the NetBIOS protocols for file and printer release were blocked so that details about the milling machine are hidden behind the Microwall.

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.)

W&T
www.WuT.de

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