Secure OT with Industrial NAT Gateway and firewall ***WALL IE*** from Helmholz

STREAMLINED, COMPACT, AND SIMPLE SOLUTIONS FOR CYBER-SECURE MACHINERY

No new machine can still do without its own machine network. Already just as self-explanatory today is the securing of this network against unwanted external access. At the latest with new specifications such as IEC 62443 and the European Machinery Regulation, corresponding cybersecurity measures will now be obligatory for all those who bring machinery into circulation. More than ever before, practicable solutions for cyber-secure machinery are thus called for – like the Industrial NAT Gateway WALL IE from Helmholz.

With the triumphal march of Ethernet networking in machinery and production systems, cybersecurity must also play an entirely central role there. This necessity is reflected accordingly in the current norm and guideline situation: the international norm series IEC 62443, for example, most recently revised in 2023, deals with the cybersecurity of "Industrial Automation and Control Systems" (IACS), thereby pursuing a holistic approach for operators, integrators, and manufacturers. It thus impacts all those involved in the manufacture and operation of machinery and defines appropriate responsibilities for mechanical engineers, suppliers, and end customers. The European Union has also acknowledged the seriousness of the situation and is reacting, for example, with the NIS-2 Directive (Network and Information Security Directive, in force since 2023) and the Cyber Resilience Act (CRA).

The European Commission has also revised the Machinery Directive 2006/42/EC. The Directive has also been adapted to the New Legislative Framework (NLF) in the process. In addition, new technological developments like artificial intelligence, autonomy, and networking have also been considered in the adjustment of the fundamental safety and health protection requirements of the Directive. The corresponding new European Machinery Regulation 2023/1230 will be applied as of January 20, 2027 for the putting into circulation of machinery.

INTEGRATING MACHINERY NETWORKS SECURELY

Not only these current specifications show: the theme of machine security affects everyone in the meantime. In the process, the central task is to securely integrate machine networks into the higher level production network.

The keyword here is "Secure OT", meaning secure operative technology consisting of software and hardware for the control, securing, and monitoring of industrial control systems, devices, and processes. In the face of growing amounts of data, there is no way around the separation or segmentation of networks against this background.

YOUR NETWORK COACH – MORE THAN JUST A FIREWALL!

High level of security
through access restriction
with packet filters (IPv4 addresses, protocol (TCP/UDP), ports, MAC addresses).

Time savings
through automatic translation of IP addresses (NAT) without changing the existing network configuration of the machine.

Smooth production process
through network segmentation
for better performance in the network. Through the avoidance of large broadcasts.

View video

Concepts with zones and secure zone transitions (Zones & Conduits) have proven especially effective here. IEC 62443 therefore also prescribes a corresponding protection concept: in keeping with this, it is often inappropriate for large or complex systems to utilize the same protection needs for all components, as these demonstrate different threats and risks. Differences can be represented through the concept of the "security zone". A security zone is a logical grouping of relevant physical objects that have the same protection needs. The boundary of the security zone defines which components lie within and which outside of the zone. In order to assure the required information flow into and out of a security zone, so-called communication conduits are defined. Communication outside of conduits is thereby not permitted.

ROBUST AND COST-EFFICIENT SECURING WITH WALL IE

At this point, the question arises of how such a zones & conduits protection concept can be implemented in concrete terms for networked machinery. The market offers numerous high-end solutions for this, which are, however, most often too large for securing a single machine network. This generally also means: excessively complex, not to mention unnecessarily expensive. Especially the medium-sized mechanical engineering segment and its customers are therefore searching for more practicable solutions, which should be not only secure and reliable, but also be realizable in a streamlined, efficient, and simple manner. Such a solution is the NAT Gateway WALL IE from Helmholz: installed once and permanently between the machine and the production network, the robust and especially compact Ethernet components connect bridge and firewall functions in the scope actually required.

In concrete terms, the components protect the networks in that they precisely regulate which participants may exchange data with which device. The prerequisite for this is created by a packet filter functionality: this enables the limitation of access between the production network and the automation cell. Contributing to the simplicity and security of the solution is the fact that the WALL IE, together with the machine network behind it in the production network, can only be displayed as a single IP address.
As another special feature, WALL IE can be used in both the NAT operating mode and as a bridge. In the bridge operating mode, it acts as a switch. In contrast with normal switches, however, packet filtering is also possible in this operating mode. This means that the restriction of access to individual areas of your network can be achieved without having to use different networks for this purpose.

In the NAT operating mode, which is used by most users, the WALL IE forwards the data traffic between various IPv4 networks (Layer 3) and uses packet filters for limiting access to the automation network behind it. In the process, address translation by way of Network Address Translation (NAT) is supported. The use of NAT also makes it possible to incorporate several automation cells of the same kind with the same address range into the production network. WALL IE supports two NAT functionalities in the NAT operating mode: basic NAT (also referred to as "1:1 NAT" or "Static NAT") and NAPT (Network Address and Port Translation, also referred to as "1:N NAT" or "Masquerading").

EVEN MORE POSSIBILITIES THROUGH NEW VARIANTS

This has been proven thousands of times since the market launch of WALL IE in 2015. The functional scope has grown

constantly since then, mostly as a reaction to concrete customer inquiries. Since 2024, two new variants now complement the previous “standard” version (with four ports and a transmission rate of 100 Mbps). Both are equipped with a faster processor with Ethernet up to 1 Gbit/s, thus opening up new application areas. The new “Compact” version is thereby limited to two ports - one for the company network (WAN), one for the machine network (LAN). The “Plus” version on the other hand offers eight ports.

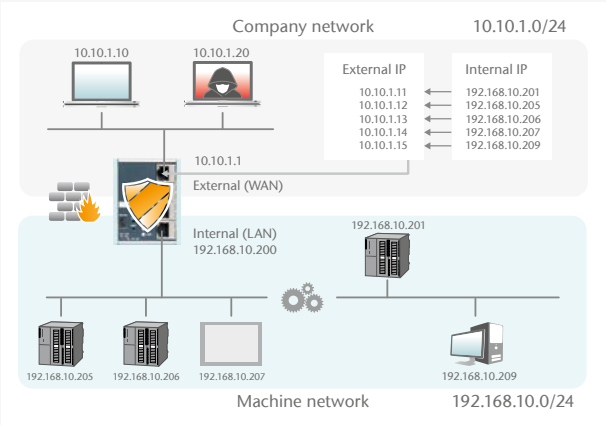
The ports can be used freely configurable as switches for LAN or WAN. The advantage: smaller networks can thus be realized without additional switches or with a single device.

All three WALL IE variants have in common that only basic network knowledge is required for commissioning. Thus, for example, no adjustment of the network configuration in the LAN network is necessary. Series machines can also be easily integrated with identical IP addresses.

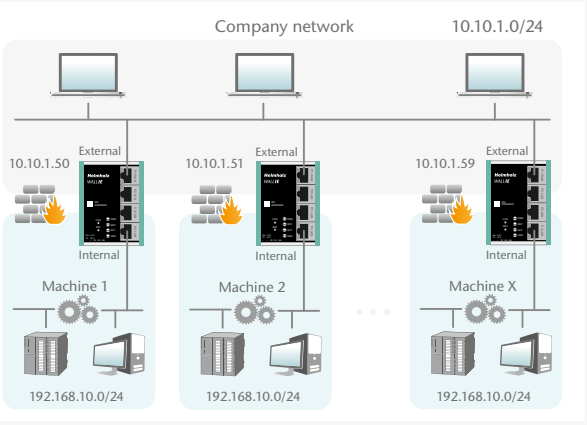
SUMMARY

In the networked industry of the future, the security of machines and systems will be decisive for a stable and malfunction-free process. Processes can be easily optimized through network segmentation and secure access to the machine network. The easily configurable NAT Gateways or machine firewalls of the WALL IE series from Helmholz offer customized protection of sensitive data and protect critical systems from cyber threats with little effort.

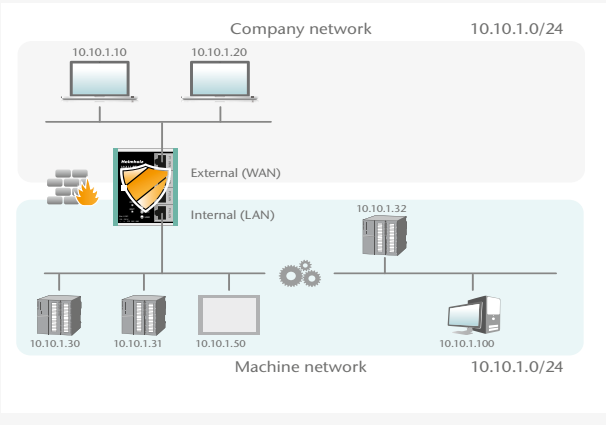
NAT operating mode (Basic NAT)



NAT application



Bridge operating mode



NAPT: Network Address and Port Translation