



HIRSCHMANN

A BELDEN BRAND

Understanding firewall technology for industrial connectivity

White Paper



Prof. Dr. Tobias Heer | Principal Technology Architect

Dr. Oliver Kleineberg | VP, Technology

Divij Agarwal | Senior Director, Technology Platforms

Executive summary: firewalls, firewalls and firewalls

Firewalls are indispensable tools for network security. As industrial systems have adopted Ethernet infrastructure and become interconnected with corporate IT systems, firewalls have become essential components for ensuring network security and enhancing system robustness and resiliency. Rather than being a one-size-fits-all solution, firewalls come in various form factors with a range of features and technologies optimized to fulfill different roles within a comprehensive security architecture. There are firewalls designed for enterprise use and those specifically tailored for industrial applications. This white paper explores the various types of industrial firewalls and discusses how they can be utilized to enhance the security, robustness and resiliency of industrial systems.

Table of contents

Executive Summary	1
Firewalls: an essential component of industrial network security	2
General function of a firewall	2
Firewalls in an industrial environment: applications and requirements	3
Firewalls at network boundaries	3
Security in other network infrastructure	5
Differences in filtering	5
Management of firewalls	6
Summary	8
References	8
About Belden	9



Firewalls: an essential component of industrial network security

Modern security models adopt a holistic approach, considering not only technology but also the processes and people involved. Consequently, firewalls alone have not been promoted as a sufficient or exclusive measure for securing industrial plants and networks for quite some time. However, firewalls remain core elements in network segmentation and are therefore essential parts of any network security strategy.

Over time, the term “firewall” has come to encompass a broad range of technologies with different methods of operation and objectives.

Today, the diverse array of firewalls includes stateless and stateful firewalls, transparent firewalls and firewalls at various levels of network reference architectures. Additionally, there are firewalls with deep packet inspection and even firewalls with intrusion detection features.

Additionally, there are methods such as access control lists that can control and limit network traffic. This variety leaves system designers with the critical task of determining which type of firewall is appropriate for each specific use case.



General function of a firewall

Firewalls are devices that protect networks or network devices, such as industrial PCs, control systems and cameras, from unauthorized access. They achieve this by preventing network traffic to or from these systems. The primary distinction is between host firewalls and network firewalls. Host firewalls are installed on a computer (host) or provided by the operating system as a software feature, such as the Windows system firewall or the iptables firewall in most Linux systems.

In contrast, network firewalls are specifically developed for use as firewalls and are placed within the network rather than on a PC. These network or hardware firewalls are crucial elements in industrial facilities, especially when connected to additional networks (e.g., office networks). They are also essential when wired transmissions are combined with wireless technologies. In these situations, a network firewall establishes the network boundary as the first line of defense against attacks, allowing only desired traffic into and out of the network.

The fundamental technical function of any firewall is to filter packets. The firewall inspects each packet it receives to determine whether it corresponds to a desired template for traffic patterns. The firewall then filters (drops or discards) or forwards packets that match these templates, which are modeled in the form of rules.

For example, a firewall at the boundary of a network might include rules such as “A communication link within the network can only take place with a specified server” or “Only the PCs for remote maintenance can be reached outside the network, not any other devices.”

A firewall protecting an operational zone of a plant floor might contain rules for industrial protocols, such as Modbus/Transmission Control Protocol (TCP), like “Write commands for the Modbus/TCP protocol, coil 56, are permitted only from the maintenance terminal.”

Given the significance of network-based firewalls for industrial facilities, this white paper focuses on that sub-genre. But where are these firewalls used in today’s security models?

Firewalls in an industrial environment: applications and requirements

Firewalls are crucial components in today's security strategies. Different types of firewalls are deployed in various locations within the network to provide different types of protection as part of a Defense in Depth strategy. Firewalls can secure the link between a company network and the industrial network to protect against external hacker attacks. Other types of firewalls separate devices within a network from each other. They also permit only specified communications between devices to protect against malicious attacks and device or operator error. The concept of precisely limiting communication between participants in internal networks, as well as partitioning various network areas from each other, is known as Zones and Conduits. Zones and Conduits are a central component of the international standard IEC 62443 and a key element of a Defense in Depth security strategy.

Defense in Depth is a strategy where multiple layers of defense are implemented, rather than relying on a single defense mechanism, such as a single firewall. The reason why Zones and Conduits and Defense in Depth complement each other so well is that key elements of both strategies enhance each other. On one hand, Defense in Depth hampers attacks against networks through a set of layered defenses "in depth" – an attacker must defeat multiple security levels, not just a single obstacle. On the other hand, partitioning a network into multiple communication zones and implementing a "need to communicate" strategy according to Zones and Conduits implicitly adds additional defense layers – layers that enhance the resilience of the network in the event that one of the areas is compromised by an attacker. In this case, only the partitioned area that the attacker has been able to reach is compromised; the remainder of the network remains protected.

Moreover, the bulk of cyber incidents are related to device failure, software error, human error or malware. Zones and Conduits increase system reliability and robustness by preventing incidents in one zone from spreading to another.

The strategies of Defense in Depth and Zones and Conduits are not new. If you look at castle construction in any culture, you will see that layers of security were built into the design – moats, multiple walls and turrets. Individual zones of the castle are separated from each other by controlled conduits – gates, drawbridges and iron bars – to contain attackers and make their movements more difficult.

In communication networks, the isolation of groups of networked devices into Zones and Conduits represents the gates. This procedure should be applied in combination with a stacked Defense in Depth strategy, since gates are useless without walls. To implement these best practices in communication networks, numerous firewalls are used at various locations within the network.

Firewalls at network boundaries

Firewalls play various roles in partitioning networks. They can be used to protect a company's enterprise networks against external threats. In this case, overall protection is the domain of IT firewall solutions placed in a company's data center. Firewalls can also protect networks from each other, for example, by separating a production network from the company's enterprise network.

Firewalls in small cells or external sites

Industrial firewalls with router functions are ideal for smaller external sites. This allows, for example, distribution stations or remote work sites to connect to the company's control infrastructure via a cellular network. The firewall controls the flow of network traffic into and out of the external site's local network. Because such a firewall represents the border between the company's network (the external site) and an external network (a provider network or the Internet), it must have full capabilities for packet filtering and traffic filtering between various networks. Such a firewall is called an IP firewall since it processes Internet Protocol (IP) traffic. Given that these firewalls are often installed near the actual facility, industrial hardening must be considered. Extended temperature ranges and/or approval for use in special areas (e.g., energy supply, hazardous locations and transportation) are crucial.

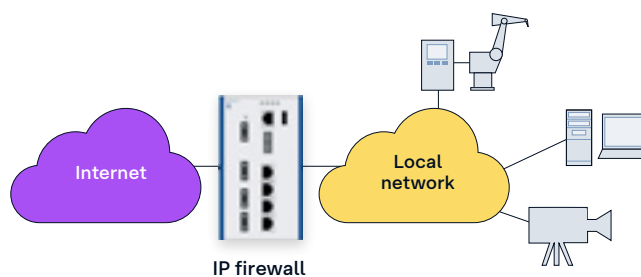


Fig. 1: Firewall between the Internet and the local company network

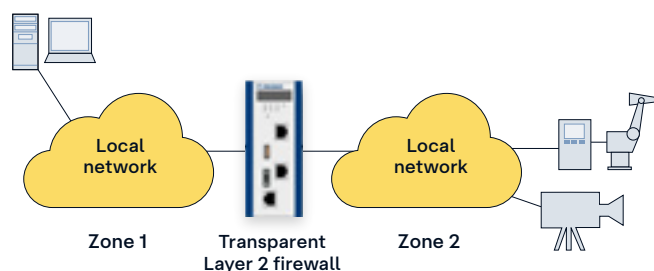


Fig. 2: Firewall within a local network

Firewall at the field level

Protecting only the external boundaries of a network is rarely sufficient, as many threats originate from within. Industry studies indicate that most “cyber incidents” stem from software or device failures and human error, rather than intentional external attacks. In a networked control system, errors and mistakes can quickly propagate unless proper design steps are taken to isolate and contain failures. Therefore, an effective cybersecurity strategy is not just about security but also about ensuring the safety, resiliency and reliability of your system.

Firewalls can enhance overall resiliency against unintentional errors by limiting communication between different zones of the local network (see figure 2). This requires a firewall tailored to this specific use case. If communication from outside the facility is only supposed to be possible with a single device, the firewall should specifically permit this connection while preventing other communication attempts.

The demands on a firewall used within a network differ from those on a firewall used between networks. Therefore, a transparent Layer 2 firewall at the Ethernet level is required instead of an IP firewall. The key characteristic of a transparent Layer 2 firewall is shown in figure 3. It implements filtering functions on local communication, which usually occurs at the Ethernet level or “Layer 2” in the Department of Defense (DoD) or ISO–Open Systems Interconnection (OSI) layering model.

In contrast, pure Layer 3 firewalls are usually unaware of Layer 2 traffic. Thus, the Layer 2 firewall is transparent to the upper protocol layers but performs a critical security function in local networks.

Since these firewalls are typically implemented at the field level, application parameters such as temperature, vibration and other environmental factors must be considered. Additionally, necessary approvals are required.

This results in significant functional differences compared to conventional IT firewalls, including differences in outward appearance, device sizes and housing. Additionally, cooling (usually only passive cooling is possible) and supported network media and transceiver technology also vary.

Firewall in a WLAN

Communication between wireless and wired networks can be controlled by firewalls. When a client connects to a WLAN, it can, in principle, communicate directly with all other devices in the same network. This means an attacker could potentially extend a successful attack on a WLAN-connected client to any other device on the Ethernet network.

This issue can be mitigated by restricting message forwarding between WLAN clients using a firewall at the WLAN access point. For instance, the communication of a tablet connected to a device via WLAN can be restricted to accessing data only through the user interface. This prevents it from reaching additional subsystems or other connected devices.

This is why Belden industrial wireless LAN access points are equipped with firewall functionality. In this scenario, the network requires a transparent Layer 2 firewall capable of filtering communication within the network (directly between WLAN devices). To achieve this, the firewall must be implemented directly at the access point. Industrially hardened devices are also crucial in this context.

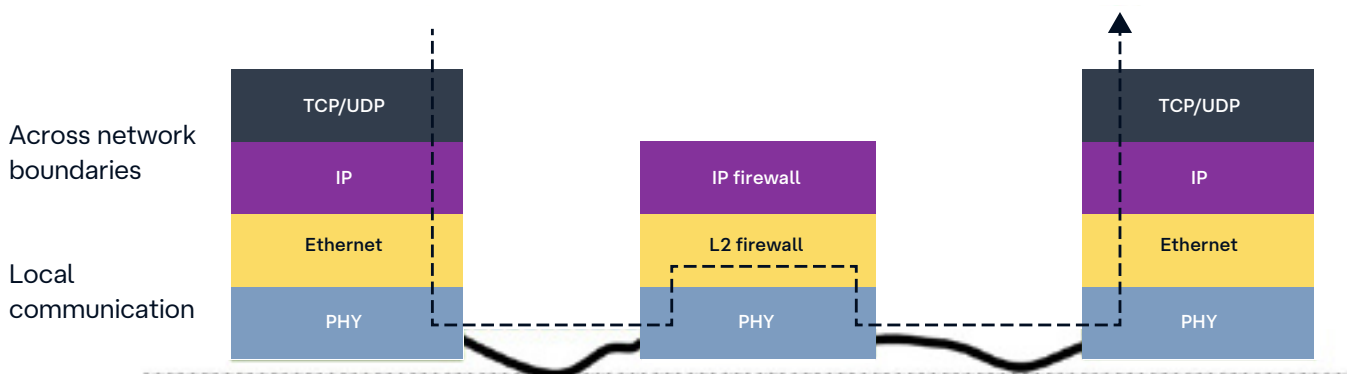


Fig. 3 – Layer 2 transparent firewall

Security in other network infrastructure

As part of a Defense in Depth strategy, it is beneficial to restrict communication to desired patterns and relationships at all points in the network. However, because firewalls introduce transmission latency and reduce network throughput, using dedicated firewalls throughout the entire network may not be feasible. Instead, internal network protection is achieved through high-quality network switches and routers with powerful stateless filtering rules, as further described in the next section. These rules are typically referred to as Access Control Lists (ACLs) rather than firewall rules. ACLs are ideal for situations where rapid filtering must occur within a network.

Differences in Filtering

The environment and placement within the network are not the only factors determining firewall requirements. Different use cases impose varying demands on the filtering mechanisms needed. It is crucial to differentiate how deeply a firewall can observe communication between devices. A broad range of solutions is available, from firewalls that perform simple pattern recognition on packets (often called signatures) to those that understand the functions and procedures in industrial protocols. This allows them to prevent specific communication templates in a targeted manner.

Combining different security characteristics, such as various firewall mechanisms, can enhance security when implementing Defense in Depth. The master builders of the Middle Ages provide inspiration for this concept of diversity in defense mechanisms: in castles and other fortifications, high walls were often combined with other methods of defense, such as moats. An attacker had to develop a more sophisticated strategy to overcome both the wall and the moat.

In modern communication networks, it is equally advisable to implement diverse firewall mechanisms and combine them with Defense in Depth measures or other security mechanisms. The following filter mechanisms are commonly known:

Stateless Firewalls

Communication relationships between devices can exist in various phases (states). Typically, the communication relationship is initiated in the first phase, active communication occurs in the second phase and the connection is terminated in the third phase. A concrete example of a protocol that follows this procedure is the Transmission Control Protocol (TCP), often combined with the Internet Protocol (IP) to form TCP/IP.

As the name implies, stateless firewalls do not react to the state of a communication connection nor do they differentiate between the various phases.

Stateless firewalls only determine which individual devices or applications may communicate with one another. However, they cannot ascertain whether the participants are conducting the communication according to the normal procedure.

Consequently, a stateless firewall cannot recognize or prevent attacks resulting from abnormal protocol behavior. This vulnerability puts industrial devices with minimal self-defense at risk of being targeted by attacks such as denial of service (DoS).

A DoS attack can be executed by deliberately flooding the communication interface of an industrial device with traffic. This overloads it with forged or erroneous communication requests.

Stateful Firewalls

In contrast, stateful (state-aware) firewalls monitor the communication process of the participants. They use this recorded information, such as the initiation or termination of the connection, as the basis for packet filtering.

This enables stateful firewalls to recognize and prevent attacks that attempt to communicate over already established connections. Similarly, they can prevent attacks that exploit a known faulty connection to load and overload a system.

Deep Packet Inspection

Deep Packet Inspection (DPI) is an extension of Stateful Packet Inspection. While stateful firewalls typically examine only the header at the beginning of a packet, DPI goes further. It analyzes the entire packet, including the payload, to provide more comprehensive security.

It allows examination beyond the communication header to the payload, such as control protocols of industrial applications, of a packet.

This enables the discovery of highly specialized attack patterns hidden deep within the communication flow.

To achieve this, the firewall must be capable of interpreting the respective communication protocol to differentiate between well-formed, “good” packets and malicious packets or harmful payloads. Therefore, DPI firewalls are often implemented as additional components of a Stateful Packet Inspection firewall. They are specifically used for select protocols and application purposes, such as industrial protocols.

A DPI firewall offers a high degree of security, often with a highly individualized and finely configured rule set, but it demands more computing power. Additionally, a specialized configuration interface is necessary for establishing the firewall rules. Fortunately, leading products include built-in tools to simplify this process.

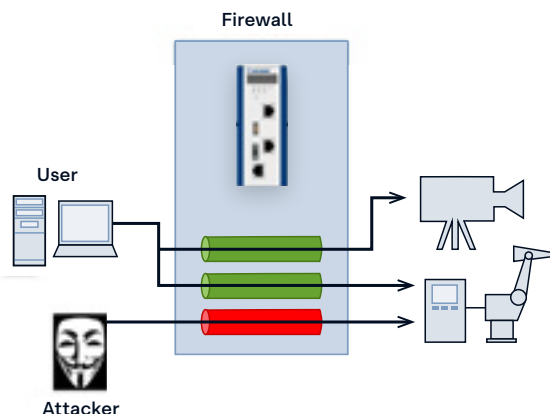
Due to their ability to provide very granular protection, DPI firewalls are well-suited to secure the conduits between various industrial zones. They not only determine which devices communicate with each other but also understand control protocols. This allows them to permit only certain types of communications.

By carefully deploying them at select points within the network, DPI firewalls significantly enhance the security of industrial communications.

Sometimes, the term DPI is used to describe a different security mechanism that employs a signature database rather than fully decoding the application protocol. Signature files offer a different type of protection by matching packet bits to a set of signatures. This helps identify and block previously identified vulnerabilities.

While signature files can protect against known vulnerabilities, they do not offer the broad protection against malformed packets that protocol-level DPI provides. Additionally, they do not allow the message flow to be tightly configured. DPI enables communications to be restricted to those that make sense for the specific system.

Firewall configured too liberally



Firewall configured too restrictively

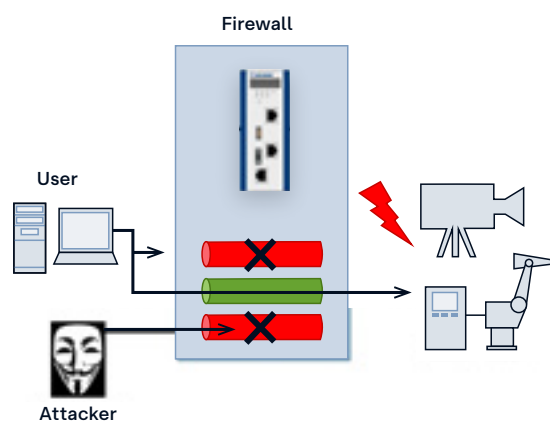


Fig.4: Integrating a firewall into an existing industrial network may lead to too liberally or too restrictively configured rule sets.

Management of firewalls

Just as there are differences in the application areas and capabilities of packet filters, there are differences in the additional functions of firewalls. An easy-to-use firewall can be the difference between a feasible solution and one that becomes an obstacle rather than an enabler in implementing a security strategy. This can be demonstrated by reviewing two typical management tasks: a) integrating a new firewall into an existing industrial network and b) managing multiple firewalls with network management tools.





Learning firewalls

Deploying a new firewall in an existing industrial network is no trivial matter. In such applications, there are generally numerous communication relationships that are rarely completely and correctly summarized and documented. Since the main function of a firewall is to prevent unknown network traffic, the initial configuration of these devices is particularly challenging. If the firewall is configured too liberally, the control and monitoring traffic of the facility can flow without problems. However, the firewall also presents no significant obstacle to an attacker. It offers no protection against misbehaving devices or malware.

Conversely, if the firewall is configured too restrictively, it blocks potential attacker communication but also hinders regular traffic, causing the facility to malfunction in certain situations. This can lead to delays and costly repairs. Therefore, it is crucial to configure the firewall properly to permit desired communication while simultaneously preventing undesired traffic. Without a complete view of all communication relationships, integrating a firewall into an existing network can be a nerve-wracking experience (see figure 4).

Modern, high-quality industrial firewalls support employees during commissioning by offering special analysis modes.

Such a mode, for example, a Firewall Learning or Test Mode, enables the firewall to analyze the communication relationships in a network during a learning phase. During this phase, the firewall records all communication relationships without restricting any of them. With the help of connection analysis, an administrator can quickly and easily detect desired or undesired communication relationships and create a custom configuration of the firewall (semi-) automatically. This saves time and enables a functional and secure configuration without risking downtime and failures. The duration of the learning period must be freely configurable since the firewall must observe all communication relationships during this phase. For sporadic communication relationships, such as those during regularly scheduled maintenance, the timeframe must be set accordingly. This ensures that the sporadic communication is captured effectively.

Management of multiple firewalls

Using firewalls to isolate various devices and facility components from one another is a crucial aspect of a Defense in Depth strategy. If an attacker overcomes an initial obstacle and penetrates the network, additional firewalls with more specific rules can prevent further penetration into more sensitive facility components.

However, managing and configuring multiple IP firewalls and transparent Layer 2 firewalls can be challenging. Without a powerful management tool for simple mass configuration, this task can become very time-consuming and error-prone. This is especially true when changes to the network infrastructure are required.

Therefore, it is essential that firewalls can be managed and monitored centrally by network management tools to streamline this process.

With proper tools like Industrial HiVision, standard configurations can be quickly implemented on newly installed firewalls. Additionally, mass configuration changes can be made to adapt to network infrastructure changes.

For example, if a new log server needs to be accessible by all devices in the production network, configuring each firewall individually to set the IP address and port of the log server would be time-consuming. This process is also prone to errors.

Using a centralized network management tool can streamline the configuration process and reduce the risk of mistakes. This tool allows for mass configuration, enabling the task to be performed simultaneously and reliably for all firewalls at once.



Summary

While firewalls are just one of many essential components in modern security practices, they remain a pivotal element that no security model can do without. Implementing key principles from international standards and best practices relies heavily on the use of firewalls.

Firewalls are not a single type of device but rather a diverse collection with varying technical characteristics, hardware features and regulatory and industry approvals. These factors influence the types of industrial environments in which they can be used and the use cases they best serve.

Therefore, it is crucial to select the appropriate firewall for each area within the industrial network. To maximize their effectiveness, network designs should adhere to the best practices of Zones and Conduits as well as Defense in Depth.

Integrating different firewall functions into an overall network defense strategy allows for a robust and comprehensive security approach. Positioning various types of firewalls where they can leverage their strengths ensures optimal protection. This strategic design makes networks future-proof and resilient against evolving threats.

References

1. National Institute of Standards and Technology NIST, Guidelines on Firewalls and Firewall Policy, Revision 1, 2009
2. Belden blog “Cyber Security for Industrial Applications: Defense in Depth”, <http://www.belden.com/blog/industrialethernet/Cyber-Security-for-Industrial-Applications-Defense-in-Depth.cfm>
3. National Institute of Standards and Technology NIST, Guide to Operational Technology (OT) Security, 2023 <https://csrc.nist.gov/pubs/sp/800/82/r3/final>



Connect to what's possible.

White Paper



About Belden

Belden Inc. delivers complete connection solutions that unlock untold possibilities for our customers, their customers and the world. We advance ideas and technologies that enable a safer, smarter and more prosperous future. Throughout our 120+ year history we have evolved as a company, but our purpose remains – making connections. By connecting people, information and ideas, we make it possible. We are headquartered in St. Louis and have manufacturing capabilities in North America, Europe, Asia and Africa.

For more information, visit us at:
belden.com

follow us on



© 2025 | Belden and its affiliated companies claim and reserves all rights to its graphic images and text, trade names and trademarks, logos, service names, and similar proprietary marks, and any other intellectual property rights associated with this publication. BELDEN® and other distinctive identifiers of Belden and its affiliated companies as used herein are or may be pending or registered or unregistered trademarks of Belden, or its affiliates, in the United States and/or other jurisdictions throughout the world. Belden's trade names, trademarks, logos, service names, and similar proprietary marks shall not be reprinted or displayed without Belden's or its affiliated companies' permission and/or in any form inconsistent with Belden's business interests. Belden reserves the right to demand the discontinuation of any improper use at any time.