HIRSCHMANN
A BELDEN BRAND

White Paper

Understanding Firewall Technology

for Industrial Cybersecurity

Prof. Dr. Tobias Heer – Senior Architect CTO Office, Hirschmann Automation and Control GmbH

Dr. Oliver Kleineberg – Global CTO Industrial Networking, Hirschmann Automation and Control GmbH

Divij Agarwal – Senior Product Manager, Belden

Executive Summary: Firewalls, Firewalls and Firewalls

Firewalls represent an indispensable tool for network security. As industrial systems have adopted Ethernet infrastructure and become interconnected to corporate IT systems, firewalls have become essential components for ensuring network security and increasing system robustness and resiliency. Rather than being a one-size-fits-all device, firewalls come in a variety of form factors with a range of features and technologies optimized to play different roles as part of a comprehensive security architecture. There are firewalls designed for enterprise use and firewalls designed for use in industrial applications. This article presents the various types of industrial firewalls and describes where and how they can be used to enhance the security, robustness and resiliency of industrial systems.

Table of Contents

Be certain.
Belden.

Firewalls: An Essential Component of Industrial Network Security

Modern security models adopt a holistic approach, taking into consideration not only technology but also the processes and people involved. This is why it has been a long time since firewalls alone have been promoted as a sufficient or exclusive measure for securing industrial plants and networks. Firewalls are however the core elements in network segmentation and therefore are an essential part of any network security strategy[1].

Over time, the term "firewall" has come to be very widely used and now applies to a broad range of technologies with different methods of operation and objectives. Today, the diverse firewall array includes: stateless and stateful firewalls, transparent firewalls, firewalls at various levels of the network reference architectures, firewalls with deep packet inspection and even firewalls with intrusion detection features. Then, there are additional methods that can control and limit network traffic, such as access control lists. This leaves the system designer with the question of which type of firewall is appropriate for which use case.

General Function of a Firewall

Firewalls are devices that protect networks or network devices, such as industrial PCs, control systems, cameras, and other devices from unauthorized access by preventing network traffic to or from these systems. The first broad distinction here is the difference between host firewalls and network firewalls. The first is installed on a computer (host) or already provided by the operating system as a software feature. Examples of these personal firewalls are the Windows system firewall or the iptables firewall, which is part of most Linux systems.

In contrast to that, network firewalls are specifically developed for use as a firewall and are placed in the network rather than on a PC. These network, or hardware, firewalls are important elements in industrial facilities, especially when they are connected to additional networks (e.g., office networks) or when wired transmissions are combined with wireless technologies. In these situations, a network firewall serves to establish the network boundary as the first line of defense against attacks and only allows 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 the packet corresponds to a desired template for traffic patterns. The firewall then filters (drops or discards) or forwards packets that match these templates. These templates are modeled in the form of rules. A firewall at the boundary of a network can, for example, include rules in the form of "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, e.g. Modbus/TCP, such as "Write-commands for the Modbus/TCP protocol, coil 56, are permitted only from the maintenance terminal."

Because network-based firewalls are of great significance for industrial facilities, this article 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 important components in today's security strategies. Different types of firewalls are used in various locations within the network to provide different types of protection as part of a Defense in Depth2 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, or permit only specified communications between devices to protect not only against malicious attack but also against device or operator error. The concept of precisely limiting communication between participants in internal networks, as well as partitioning of 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 component of a Defense in Depth security strategy.

Defense in Depth is a strategy where multiple layers of defense are implemented, in contrast to just one defense mechanism, a single firewall, for example. The reason why Zones and Conduits and Defense in Depth go together so well is that key elements of both strategies complement 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 add to the resilience of the network in the case 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 is protected. And, because 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 keeping 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 for any culture, you will see that layers of security were built into the castle design – moats, multiple walls, 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[2], since gates are useless without walls. In order to implement these best practices in communication networks, numerous firewalls are used at various locations in the network.

Firewalls at Network Boundaries

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

Firewall in a Small Cell or External Site

Industrial firewalls with router functions are perfect for smaller external sites. This allows, for example, distribution stations or remote work sites to be connected to the rest of the company's control infrastructure via a cellular network. The firewall controls the flow of network traffic out of and into the external site's local network. Because such a firewall represents the border between the company's own network (the external site) and an external network (a provider network or the Internet), the firewall must possess full capabilities for packet filtering and filtering traffic between various networks (see figure 1). Such a firewall is called an IP firewall since it processes Internet Protocol (IP) traffic. Because these firewalls are often installed very near the actual facility, industrial hardening must also be taken into consideration. Extended temperature ranges and/or approval for use in special areas (e.g. energy supply, hazardous location and transportation) are crucial.

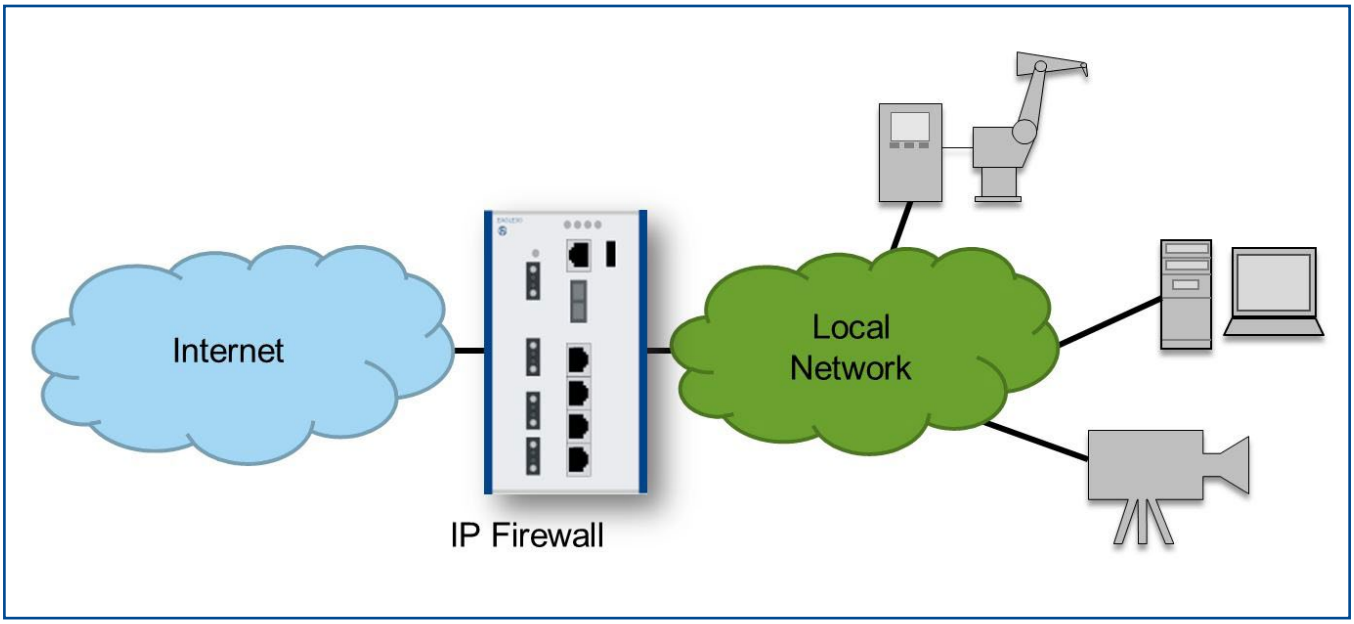

Fig. 1: Firewall between the Internet and the local company network

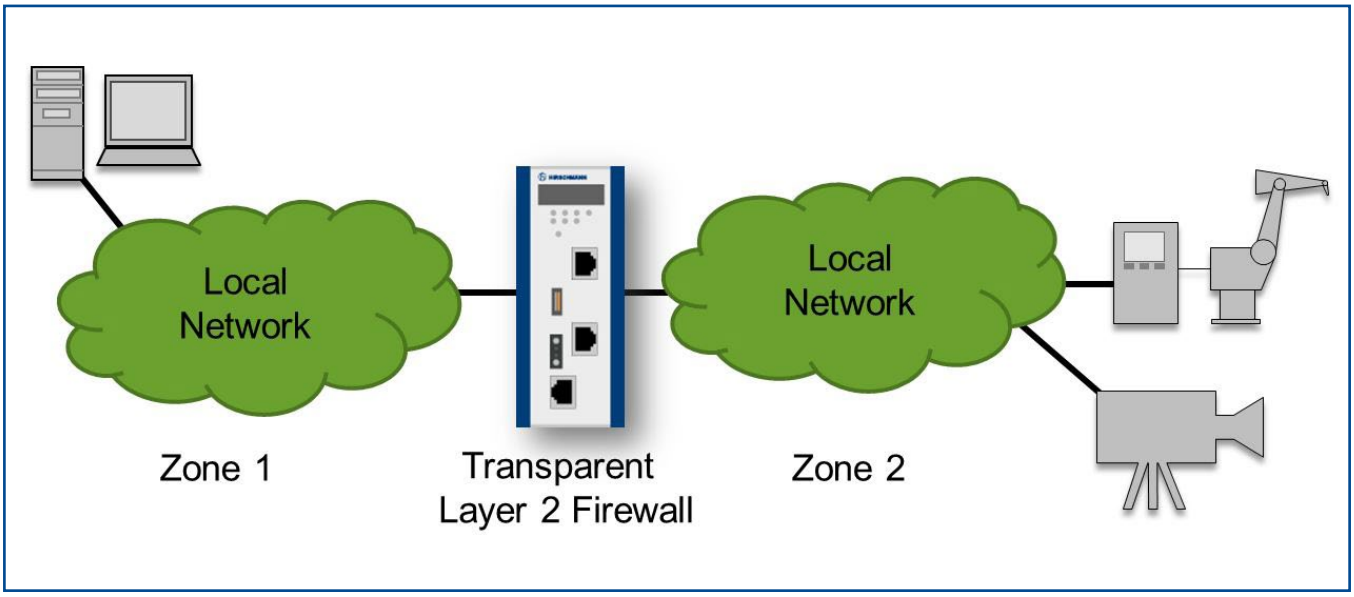

Fig. 2: Firewall within a local network

Firewall at the Field Level

It is rarely sufficient to protect only the external boundaries of the network against attackers. Many threats actually originate inside a network. Industry studies have shown that most "cyber incidents" are not due to intentional external attacks but from software or device failures and human error. In a networked control system, errors and mistakes can quickly propagate within the system unless proper design steps are undertaken to isolate and contain failures. Thus, an effective cybersecurity strategy is not just about security but is also an important component of ensuring the safety, resiliency and reliability of your system.

In this case, firewalls can contribute to the overall resiliency against unintentional errors by limiting communication between different zones of the local network (see figure 2). This requires a firewall that is tailored to fit this particular 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 it prevents other attempts at communication.

The demands put on a firewall in use within a network differ from the demands put on a firewall in use 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. The layer 2 firewall implements filtering functions on local communication, which usually happens on the Ethernet level or "Layer 2" in the Department of Defense (DoD) or ISO-OSI layering model.

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

Due to the fact that these firewalls are usually implemented at the field level, the application parameters (temperature, vibration and other environmental factors), as well as the necessary approvals, must be taken into consideration. This results not only in significant functional differences of these devices, compared to conventional IT firewalls, but also in different outward appearance, device sizes, device housing, cooling (usually, only passive cooling is possible) as well as in supported network media and transceiver technology.

Firewall in a WLAN

Communication from wireless to wired networks can also be controlled by firewalls. If a client is connected to a WLAN, it is possible, in principle, to communicate directly with all other devices in the same network. Thus, an attacker can extend a successful attack on a client that is connected to the WLAN to any other device on the Ethernet network.

This problem can be solved by restricting the forwarding of messages between WLAN clients with a firewall at the WLAN access point. For example, the communication of a tablet that is connected to a device via a WLAN can be limited so that it can only access data through the user interface but not additional subsystems or other devices connected to it.

This is the reason why Belden industrial wireless LAN access points, for example the BAT products from Hirschmann, are all equipped with firewall functionality. In this case, the network also needs a transparent layer 2 firewall that is able to filter communication within a network (directly between the WLAN devices). In order to do this, the firewall must be implemented directly at the access point. Industrially hardened devices are important here as well.

Security in Other Network Infrastructure

As part of Defense in Depth, it is useful to restrict communication to the desired patterns and communication relationships at all other points in the network. Because firewalls introduce transmission latency (delay in transmission) and reduce network throughput, the use of a dedicated firewall may not be feasible throughout all parts of the network. Instead, internal network protection comes from high-quality network switches and routers with powerful stateless filtering rules as further described in the next section. These rules are usually not referred to as firewall rules but rather as Access Control Lists (ACL). ACLs are suited for any situation where rapid filtering must take place within a network.

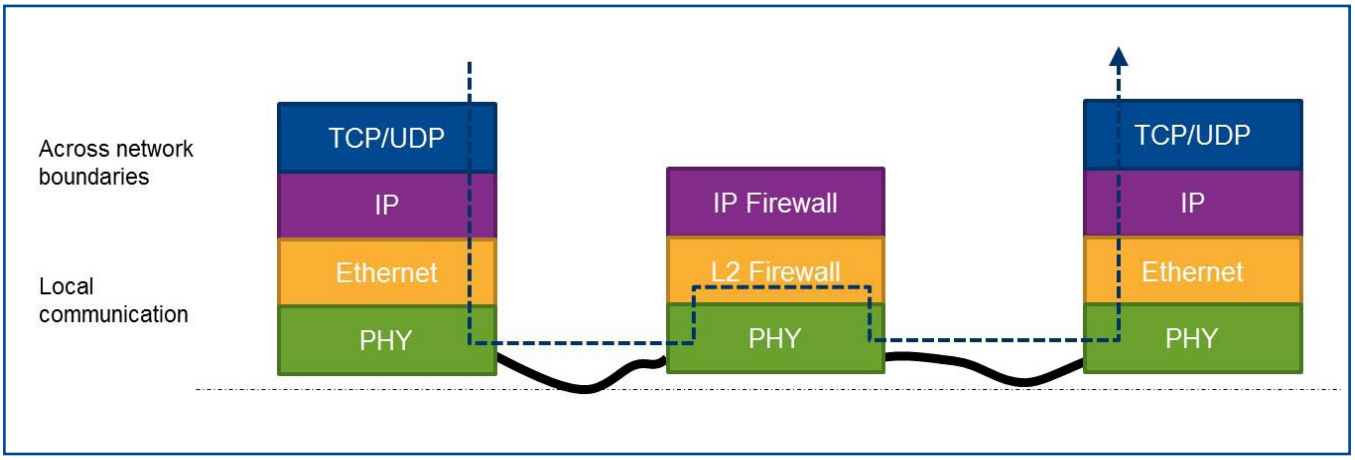

Fig. 3 – Layer 2 transparent firewall

Differences in Filtering

The environment and the placement within the network are not the only factors that determine the requirements of a firewall. Different use cases place different requirements on the filtering mechanisms that are needed. It is important to differentiate how deeply a firewall can observe the communication between different devices. A broad range of solutions is available that covers this aspect. The available spectrum ranges from firewalls that can only perform simple pattern recognition on packets (often called signatures) all the way up to firewalls that understand the functions and procedures in industrial protocols and thus can prevent individual communication templates in a targeted manner.

The simultaneous combination of differing security characteristics, like firewall mechanisms for instance, can ensure additional security when implementing Defense in Depth. Once again, the master builders of the Middle Ages provide the 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. Thus, an attacker had to develop a much more sophisticated strategy in order to overcome not only the wall, but also the moat.

In modern communications 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 may be in various phases (states). For example, the communication relationship is usually initiated in a first phase. Active communication is conducted in a second phase and the connection is ended in a third phase. A concrete example of a protocol that uses this procedure is the Transmission Control Protocol (TCP). TCP is often combined with the Internet Protocol (IP) to form TCP/IP.

As the name implies, stateless firewalls[3] do not react to the state of a communication connection nor do they differentiate between the various phases. Thus, stateless firewalls only determine which individual devices or applications may communicate with one another but cannot determine whether the participants are conducting the communication according to the normal procedure. In particular, a stateless firewall cannot recognize or prevent any attacks resulting from abnormal protocol behavior. This puts especially vulnerable industrial devices with minimal self-defense at risk to be hit by, for example, a so-called denial of service attack. Such an attack can be performed by deliberately flooding the communication interface of an industrial device with traffic and overloading it with forged or erroneous communication requests.

Stateful Firewalls

In contrast to stateless firewalls, stateful (state aware) firewalls monitor the communication process of the participants and use this recorded information, such as the initiation or termination of the connection, as the foundation for the packet filtering. Thus, attacks that attempt to communicate over connections that are already established can be recognized and prevented. Equally, attacks that use a known faulty connection in order to load and overload a system can be prevented.

Deep Packet Inspection

Deep Packet Inspection[3] is an extension of Stateful Packet Inspection. Stateful firewalls normally only examine the header at the beginning of the packet because the header contains all the information needed for the firewall to determine and monitor the communication state such as sequence numbers and the communication flags used by TCP. Deep Packet Inspection goes one step further and allows examination beyond the communication header all the way to the payload (e.g. control protocols of the industrial applications) of a packet. In this way, highly specialized attack patterns, that are hidden deep in the communication flow can be discovered.

To do this, the firewall must be capable of interpreting the respective communication protocol in order to differentiate between a well-formed, “good” packet and a malicious packet or harmful payload. Therefore, Deep Packet Inspection firewalls are often implemented as additional components of a Stateful Packet Inspection firewall and only for select protocols and application purposes, such as industrial protocols.

A Deep Packet Inspection firewall offers a high degree of security, often with a rule set that can be highly individualized and finely configured, but it demands more computing power. Equally necessary is a specialized configuration interface for establishing the firewall rules. Fortunately, leading products have built-in tools, making this process straightforward.

Because of their ability to provide very granular protection for not only which devices communicate with one another but also the ability to understand control protocols and allow only certain types of communications, Deep Packet Inspection firewalls are well suited to secure the conduits between various industrial zones. By carefully deploying them at select points within the network Deep Packet Inspection firewalls significantly harden industrial communications.

Sometimes, the term Deep Packet Inspection is used when describing a very different security mechanism that is implemented using a signature database rather than by fully decoding the application protocol. Signature files provide a very different type of protection. Signature files match the bits with a packet to a set of signatures to identify and block a set of previously identified vulnerabilities. So, while signature files can protect against known vulnerabilities, they do not provide the broad protection against malformed packets that protocol-level DPI provides, nor do they allow the message flow to be tightly configured to only allow messages that make sense in the operation of our specific system.

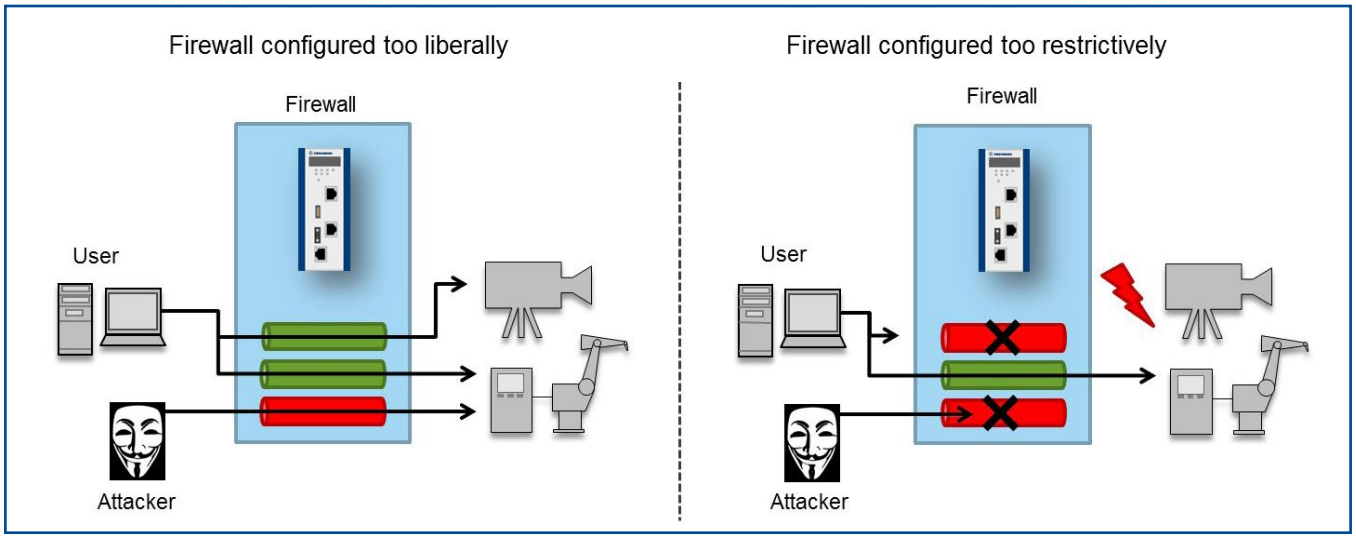

Fig. 4: Integrating a firewall into an existing industrial network may lead to too liberally or too restrictively configured rule sets.

Management of Firewalls

Just as there are differences in the application areas and the capabilities of the packet filter, there are differences in the additional functions of firewalls. An easy-to-use firewall can be the difference between a solution that is feasible for use or a solution that is more of an obstacle than an enabler in the implementation of a security strategy. This can be demonstrated by reviewing two typical management tasks: a) the integration of a new firewall in an existing industrial network and b) the management of multiple firewalls with network management tools.

Learning Firewalls

Deploying a new firewall in an existing industrial network is no trivial matter. In such an application, there are generally numerous communication relationships that are only completely and correctly summarized and documented in the rarest of cases. Since the main function of a firewall is the prevention of unknown network traffic, the initial configuration of these devices is especially difficult. 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 great obstacle to an attacker or protection against misbehaving devices or malware.

If the firewall is configured too restrictively, it blocks the communication of a potential attacker, but it also hinders regular traffic so that the facility no longer operates faultlessly in all situations. This can lead to delays and costly repairs.

Therefore, it is important to configure the firewall properly in order to permit desired communication while simultaneously preventing undesired traffic. Without a complete view of all communication relationships, the integration of a firewall into an existing network can be a nerve-wracking situation (see figure 4).

Thus, modern, high-quality industrial firewalls support employees during commissioning by offering special analysis modes. Such a mode (e.g. a Firewall Learning or Test Mode) enables the firewall to analyze the communication relationships in a network during a learning phase. During this learning phase, the firewall records all communication relationships without restricting any of them. With the help of the connection analysis, an administrator can then detect the desired or undesired communication relationships quickly and easily create a custom configuration of the firewall (semi-) automatically. This saves times and enables a functional and secure configuration without risking downtimes and failures. The duration of the learning period must be freely configurable since the firewall must observe all communication relationships during the learning phase. In particular, in the case of sporadic communication relationships, e.g. during regularly scheduled maintenance, the timeframe must be set accordingly to also capture this sporadic communication.

Management of Multiple Firewalls

The use of firewalls to isolate various devices and facility components from one another is an important aspect of a Defense in Depth strategy. If an attacker has overcome an initial obstacle and penetrated the network, additional firewalls with more specific rules can prevent penetration into additional and more sensitive facility components.

But take note, the use of multiple IP firewalls and transparent layer 2 firewalls requires management and configuration of these devices. Without a powerful management tool for simple (mass) configuration of firewalls, this task can be very time-consuming and error-prone in the case of changes to the network infrastructure. Hence, it is important that the firewalls can be managed and monitored centrally by network management tools to assist this process.

With proper management tools (such as Industrial HiVison), standard configurations can be implemented quickly on newly installed firewalls, and mass configuration changes can likewise be made to adapt to network infrastructure changes. An example of such a change would be on a new log server that can be reached by all devices in the production network. If all firewalls must be configured individually, the IP address and the port of the log server must be set on each firewall. This is time-consuming and subject to errors. With mass-configuration via a network management tool, this task can be simultaneously and reliably performed for all firewalls at once.

Availability of the Technologies Presented

Belden, with its Hirschmann, Tofino Security and GarrettCom products, offers a broad range of firewall solutions. The variety of these solutions can be seen in table 1. The firewalls have differing characteristics depending on the application.

The EAGLE20/30 firewall family has a stateful IP firewall as well as hardware-accelerated ACL filter rules and a DPI filter for deep packet inspection of certain industrial protocols. The EAGLEOne products are transparent layer 2 firewalls for use within a local network. Both EAGLE products have a Firewall Learning Mode in order to create the rules from the network traffic observed. The Tofino DPI firewall is a transparent layer 2 firewall with a high-grade user interface tailored for industrial applications along with a rich set of Deep Packet Inspection options for various popular industrial protocols.

The GarrettCom Magnum 5RX and 10RX secure routers include a built-in stateful firewall as well virtual private network (VPN) security. All Hirschmann WLAN access points have an integrated stateful layer 2 firewall and IP firewall. Many Belden products with firewalls can be monitored and configured effortlessly via the Industrial HiVision management software. Many Hirschmann switches also offer the possibility of configuring high-performance ACL filter rules in order to consistently protect the network against attackers.

Summary

Even though firewalls are just one of many essential parts in modern security practices, they are still a pivotal element that no security model can do without. For implementing important principles from international standards and best practices, firewalls are absolutely essential to operations.

Firewalls are not a single type of device but rather a diverse collection of devices with differing technical characteristics, hardware features and equipment and regulatory and industry approvals that impact the types of industrial environments they can be used in and the use cases they best serve.

It is therefore crucial to choose the correct firewall for each area in the industrial network. To maximize the effectiveness of firewalls, network designs need to follow the rules set forth with the best practices of Zones and Conduits as well as Defense in Depth. By combining different firewall functions in an overall network defense strategy and by positioning the different types of firewalls in the network where they can play to their strengths, it is possible to design networks that are prepared for the future and will stand the test of time.

	Transparent layer 2 firewall	Transparent layer 2 DPI firewall	Stateful layer 3 firewall	WLAN access point with firewall	Router with firewall
Product example	EAGLE One	Tofino Xenon	EAGLE 20/30	OpenBAT	Magnum 10RX Magnum 5RX
Application	Network boundary/ internal network/ field level	Internal network/ field level	Network boundary/ internal network/ field level	Network boundary/ internal network/ field level/ WLAN protection	Edge (5RX) or core (10RX) router
Product Features (excerpt)					
Access Control Lists	MAC	MAC	MAC/IP/ TCP/UDP	MAC/IP/ TCP/UDP	MAC/IP/ TCP/UDP
Layer 2 firewall	✔	✔	—	✔	—
Layer 3 firewall	✔	—	✔	✔	✔
Deep Packet Inspection	—	Modbus, OPC, Ethernet/IP, DNP3, IEC 60870-5-104	Modbus, OPC	—	—
NAT	✔	—	✔	✔	✔
VPN	✔	—	✔	✔	✔
Router/router redundancy	✔/✔	—	✔/✔	✔/✔	✔/✔
WAN & WWAN interfaces	—	—	SHDSL/3G, LTE	3G, LTE (with IP67 version)	T1/E1
Ports	2 FE	2 FE	4 FE, 2 GE	2 GE, 2 WLAN	Configurable up to 10 GE ports (copper or SFP), 16 T1/E1 ports, or 32 serial ports
Firewall Learning/Test Mode	✔	✔	✔	—	—
Configurable with Industrial HiVision	✔	—	✔	✔	Selective features

Table 1: Types of Industrial Firewall Solutions

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 Industrial Control Systems (ICS) Security, 2011

Belden Competence Center

As the complexity of communication and connectivity solutions has increased, so have the requirements for design, implementation and maintenance of these solutions. For users, acquiring and verifying the latest expert knowledge plays a decisive role in this. As a reliable partner for end-to-end solutions, Belden offers expert consulting, design, technical support, as well as technology and product training courses, from a single source: Belden Competence Center. In addition, we offer you the right qualification for every area of expertise through the world's first certification program for industrial networks. Up-to-date manufacturer's expertise, an international service network and access to external specialists guarantee you the best possible support for products.

Irrespective of the technology you use, you can rely on our full support – from implementation to optimization of every aspect of daily operations.

Always Stay Ahead with Belden

In a highly competitive environment, it is crucial to have reliable partners who add value to your business. When it comes to signal transmissions, Belden is the No. 1 solutions provider. We know your business and want to understand your specific challenges and goals to show how effective signal transmission solutions can push you ahead of the competition. By combining the strengths of our five leading brands, Belden, GarrettCom, Hirschmann, Lumberg Automation and Tofino Security, we are able to offer the integrated solution you need. Today, it may be a single cable, switch or connector, to solve a specific issue; tomorrow, it can be a complex range of integrated applications, systems and solutions. With the rise in smart, connected devices brought on by the Industrial Internet of Things (IIoT), together, we can make sure your infrastructure is ready to handle and make sense of the influx of data. Transform your business now with instant access to information, and make your vision a reality. Visit info.belden.com/iiot to learn more.

About Belden

Belden Inc., a global leader in high quality, end-to-end signal transmission solutions, delivers a comprehensive product portfolio designed to meet the mission-critical network infrastructure needs of industrial, enterprise and broadcast markets. With innovative solutions targeted at reliable and secure transmission of rapidly growing amounts of data, audio and video needed for today's applications, Belden is at the center of the global transformation to a connected world. Founded in 1902, the company is headquartered in St. Louis, USA, and has manufacturing capabilities in North and South America, Europe and Asia.

For more information, visit us at www.belden.com and follow us on Twitter @BeldenIND.