WHITE PAPER

How to Choose the Right Industrial Firewall: The Top 7 Considerations

Li Peng
Product Manager

MOXA®

Defense-in-depth protection made simple with industrial firewalls

Central to industrial control systems, industrial control networks help facilitate efficient and safe operations in vital sectors such as utilities, oil and gas, water, transportation, and manufacturing. A resilient control network relies on a network that can effectively detect and filter unwanted traffic. Traditionally, some industrial control networks are physically isolated or air gapped to ensure network security. However, that may not be the best practice as control systems are increasingly more interconnected to exchange data and to enable smarter automation.

One major concern of converged networks is the emergence of a new class of threats that targets industrial automation systems. Often lacking security measures, legacy networks are particularly vulnerable to malicious network attacks or unintended operations. Once compromised, these legacy networks can become back doors that allow attackers and unauthorized personnel to gain access to corporate networks.

To address the issues of network security for industrial control systems, a clear understanding of the security challenges and effective defensive countermeasures are required. A "defense-in-depth" approach can be applied to industrial control systems and can provide a more flexible and usable framework for improving defenses against network breaches.

In this paper, we present the challenges of implementing network security and network security risk management. We also include information on how to develop mitigation strategies for specific problems and provide directions on how to define a defense-in-depth security program for industrial control networks.

Released on April 24, 2015

Moxa is a leading manufacturer of industrial networking, computing, and automation solutions. With over 25 years of industry experience, Moxa has connected more than 30 million devices worldwide and has a distribution and service network that reaches customers in more than 70 countries. Moxa delivers lasting business value by empowering industry with reliable networks and sincere service for automation systems. Information about Moxa's solutions is available at www.moxa.com.

How to contact Moxa
Tel: 1-714-528-6777
Fax: 1-714-528-6778

Reliable Networks ▲ Sincere Service

Challenges of implementing industrial network security

1. Changes in network topology

Deploying a new firewall into industrial control networks can be a complicated process due to various issues, such as IP address reconfiguration, network topology changes, and compatibility with existing firewalls. The first challenge is to determine the right firewall type for your network.

Generally, a firewall provides two filtering options, routed and transparent (or bridged), to cater to different network topologies. We will briefly examine each of the firewall connectivity options below:

- A **routed firewall** acts as an L3 node and protects networks connected to its two logical interfaces. In the following network topology example, a routed firewall is deployed between the plant network and the enterprise network and at the perimeter of the different network zones. A routed firewall participates in the IP process and can perform tasks such as network address translation (NAT) and port forwarding. Although a routed firewall provides the most capability and flexibility, substantial network configuration may be required.

- A **transparent firewall** is suitable for protecting critical devices or equipment inside a control network where network traffic is exchanged within a single subnet. A transparent firewall does not participate in the IP process and can be installed in the network without having to reconfigure IP subnets.

2. Filtering performance and latency

In most industrial control applications, response time is a critical factor. When firewalls are deployed in a control network, the data filtering processes that are performed create latency. Although many vendors claim maximum performance for their firewalls based on the benchmark of filtering data using one firewall rule, in the real world, hundreds of firewall rules may be activated to filter traffic in a control network, placing doubts on the actual firewall performance.

An industrial firewall should minimize control data interruption and allow as much throughput as possible between controllers and I/O devices. Additionally, the data filtering performance must be consistent for various types and sizes of control traffic packets. In general automation applications, a response time in milliseconds is required to enable real-time applications such as process control, DCS, and data acquisition.

[Video] Performance test of different industrial firewalls: YouTube

3. Firewall event logging and notification

Regardless of the type of industrial firewalls being implemented, event logging is critical to ensure that the firewall rules are implemented and functioning properly. In addition, logs allow administrators to monitor what is happening in the control network. Equally important, a good log file maintenance plan allows the review of any security events or issues, days, weeks, and even months after they occur. Administrators can also review these logs to evaluate the strength of current firewall policies, leading to continuous security enhancements.

According to an IT expert from a major oil company in the US, a firewall must be capable of sending SNMP events with an emergency severity level that require immediate attention. What this means is that an industrial firewall must provide the configuration flexibility that allows administrators to define a severity level for each firewall rule and create a log for each triggered event. On the other hand, to prevent an email inbox from being flooded with notifications for all events, a firewall must offer the option to allow the network administrator to disable automatic notifications for non-critical events.

4. Mass deployment of firewall rules

In industrial applications, there could be up to hundreds or thousands of firewalls installed to control data traffic and protect field equipment from malicious attacks. As the most widely used method, a firewall whitelist allows only specific traffic on a network. This raises the question of how easy it is to change the firewall rules for the many firewalls in the field once a new service is introduced into a control network.

There are two ways to mass deploy firewall rules: batch command (through the command line interface) and centralized firewall management software. Both are easy to use and are effective mass deployment methods. The use of one or the other depends on the preference of the network administrator. An industrial firewall solution should include both options.

5. Industrial protocol filtering

Most industrial protocols use TCP/IP or UDP as the communication base for data transmission. General firewalls can filter data at the IP or MAC layer to prevent any un-authorized access to critical equipment. Traditionally, firewalls deny all inbound traffic and allow only one-way or round-trip traffic with firewall whitelists. However, whitelisting only blocks any un-authorized hosts but grants access to all authorized hosts at the IP or MAC layer. As network complexity increases, whitelisting is inadequate to provide effective network security for industrial applications. While whitelisting protects un-authorized access to industrial devices, it is not effective in filtering control data. What is needed are well-designed firewalls that can allow or deny traffic based on protocols to enable checks on control data in the network. One such solution is Modbus TCP deep packet inspection.

[Video] PacketGuard Security for Modbus TCP Industrial Networks: YouTube

6. **Intuitive configuration interface**

   Configuring and deploying firewalls in an industrial control network requires trained administrators who are capable of designing effective firewall rules. It is important for firewall vendors to provide intuitive and easy-to-use configuration interfaces to automate the configuration process. An industrial firewall should include a command line interface, a graphical user interface, and, preferably, a firewall setup wizard to allow administrators to get firewalls up and running in the field within minutes.

7. **Industrial-grade design for harsh environments**

   In industrial applications, firewalls are often located in cabinets under harsh conditions, such as high temperatures and vibration. In this case, the firewall's rugged design is as important as its performance. A firewall for industrial applications should comply with industry standards, which could include C1D2 (oil and gas), NEMA TS2 (transportation), EN 50121-4 (trackside), and UL (factory automations).

Today, there are many standards and regulations that define network security guidelines for industrial control systems. For example, ISA/IEC 62443 for industrial automation applications and NERC-CIP for power substations. In addition, NIST also published the SP800-82 standard to guide network professionals who oversee industrial control systems and are tasked with firewall deployment to protect critical industrial devices and equipment. With effective and reliable industrial firewalls, deploying industrial firewalls in the field to secure control networks and ensure maximum system uptime has never been easier.