insight.tech
POWERING IoT AND EMBEDDED INNOVATION

Securing the IIoT with Flexible Firewalls

Brandon Lewis

In the IT world, firewalls are one of the most effective tools for protecting sensitive networks. Enterprise firewalls act as gatekeepers between sensitive internal networks and the Internet, applying predefined security rules that prevent unauthorized external traffic from reaching company devices while keeping data on those devices from being exposed to the outside world.

Traditional firewalls are well understood. IT departments generally purchase firewall equipment off the shelf and apply global rules to all devices on an enterprise network. Firewalls required for IIoT networks, on the other hand, are much more complex. This is largely because of the types of devices they protect.

In IT, most systems on a network are equipped with some level of on-device protection, such as antivirus (AV) software that stops malicious code from executing even if it makes it through firewall defenses. Enterprise systems also run operating systems (OSs) that can be updated with the latest software patches whenever a vulnerability is discovered. As a result, firewall administrators can implement baseline levels of security that still allow a wide range of enterprise devices to access the Internet.

But many industrial devices run legacy operating systems (OSs) no longer supported with security patches. Even those with newer OSs often have their software frozen to ensure platform stability. In addition, most industrial systems are severely resource constrained and cannot run local AV technology.

Industrial network firewalls therefore provide the complete security stack for many of these systems. Because security requirements differ from system to system, industrial firewalls are often dedicated to a single production facility or piece of equipment rather than an entire organization, and tuned to their specific needs. They are deployed and maintained by operations engineers or service technicians familiar with the systems that firewalls protect, and support far fewer ports and IP addresses than their enterprise counterparts.

These factors drive several unique design requirements for industrial firewall equipment, including:

- **Flexibility** to meet security requirements of various systems
- **Simplicity** so that operational technologists familiar with industrial systems can deploy and maintain the firewalls
- **Durability** to withstand harsh environments such as a factory floor or inside a large piece of machinery
- **Reliability** to operate efficiently over extended industrial lifecycles
- **Cost** so that multiple firewalls can be used to protect all of the devices on an industrial network

Since each industrial firewall is committed to a small number of devices, there also isn't a need for network processors that provide the highest possible data throughput and compute performance. Instead, the processors that power industrial firewall equipment should emphasize proven technologies and broad market adoption that address the items outlined above.

Flexible Industrial Firewalls on Intel Atom® Processors

Intel Atom® processors E3800 are a family of single- to quad-core systems on chips (SoCs) that have a legacy of deployment in industrial environments, and deliver the performance necessary to meet the demands of most industrial firewall equipment. The processors also include a set of integrated hardware accelerators that support advanced security features, which, if used properly, can significantly reduce the complexity of industrial firewall equipment designs.

For one, Intel® Advanced Encryption Standard–New Instructions (Intel® AES-NI) provide a performance boost for bulk encryption, decryption, and authentication tasks in a hardware block that operates independently of the main CPU cores. This is a key capability for industrial firewalls, as it supplements the primary function of the network processor while also freeing it up for other tasks.

One way industrial firewall designers can take advantage of the extra processor resources provided by Intel AES-NI is through Intel® Virtualization Technology (Intel® VT-x), a capability that allows multiple virtual machines (VMs) to run simultaneously on the same multi-core processor at near-native performance. Also important, these VMs remain securely partitioned from one another, which opens up a range of possibilities for industrial firewall designs.

For instance, firewall functions running in a VM on a discrete security appliance can be separated from other services, such as a Secure File Transfer Protocol (SFTP) server that permits legacy industrial systems to connect to the Internet without the need for additional hardware. Alternatively, industrial firewalls integrated into an existing piece of machinery could partition security applications from control functions, ensuring that technicians can service one subsystem without affecting the other.

While these two technologies address the flexibility and simplicity requirements of industrial firewall equipment, Intel Atom processors E3800 are also architected to withstand harsh industrial environments. The SoCs are available in extended temperature variants capable of -40 °C to 110 °C operation, and their low 3 to 10 W thermal design power (TDP) reduces the need for fan cooling that can cause reliability issues in industrial settings.

Solution Frameworks for Flexible Industrial Firewalls

To aid in the development of customizable industrial firewalls, OEMs are bringing E3800-based solutions to market that leverage many of the features described previously. For instance, the MBox-V from TQ-Group is a flexible, passively cooled box PC that can be deployed as a desktop device or integrated directly into cabinets with DIN rail mounting **(Figure 1)**. All of the device's internal electronics use conformal coating, helping them withstand humidity, gas, dirt, and other irritants often found on the factory floor.

Figure 1. The MBox-V from TQ-Group supports flexible industrial firewalls. (Source: TQ-Group)

By default, the MBox-V includes two Gigabit Ethernet ports, two USB ports, and two Mini DisplayPorts in a 100 mm x 100 mm x 23 mm hardware kit. But the system is completely configurable, and additional interfaces and features can be integrated through internal Mini PCIe add-in cards. The

system also supports an optional trusted platform module (TPM) for added security.

From a software perspective, the MBox-V can be preloaded with a standard industrial firewall stack based on IP tables and a hardened version of Linux. Regular penetration testing by TQ-Group quickly reveals any vulnerabilities in the stack so that patches can be delivered in a timely manner.

TQ's stack offering also supports protocol conversion (FTP to SFTP); network interface, certificate, and key management; as well as "stealth mode" operation, which allows only communications paths to be established between white-listed ports and IP addresses. Audit and error logging round out the feature set.

While the MBox-V supports additional capabilities such as advanced packet filtering, intrusion detection/prevention, and gateway services, it is also designed for users to upload their own custom firewall software. According to TQ-Group, several security companies are already using the MBox-V as the starting point for their industrial firewall designs, and building additional capabilities on top of it in software.

Flexibility Without the Learning Curve

Network firewalls of all types are designed to do one thing: prevent malicious activity on sensitive networks and devices. But industrial networks and the devices they connect come with unique security requirements that demand flexible, reliable, and durable firewall equipment.

Solutions like the MBox-V meet these needs with an architecture familiar to industrial engineers and IT staff alike. These little boxes are a great way to implement secure IIoT networks with little-to-no learning curve.