thalesgroup.com

THALES

Building a future we can all trust

IT + OT cybersecurity – both complement and protect each other

IT + OT cybersecurity – both complement and protect each other

When considering cybersecurity solutions, we often focus on IT whilst OT, or operational technology, is overlooked. Understanding the difference between IT and OT is essential. The importance of security measures covering both IT and OT must be a part of any comprehensive plan. They are both crucial to the growing Industrial Internet of Things (IIoT) but the distinction between the two may be blurry with increasing convergence. This document aims to clarify how poorly protected connected devices in the OT domain are very likely to be a threat to the broader IT domain of an enterprise.

Information Technology (IT) networks have been well known for decades by technology experts and novices alike whatever the industry or size of the company. IT covers hardware such as computers and servers, as well as software such as operating systems, and peripherals, all are used to manage computer systems and data. It is usually an aperture to the external world (e.g., website, ftp, etc.). This expanding, connected world brings the need for an IT system to include a variety of protection mechanisms, e.g., firewall, anti-virus, proxy, threat detection, identity and authentication, to name a few.

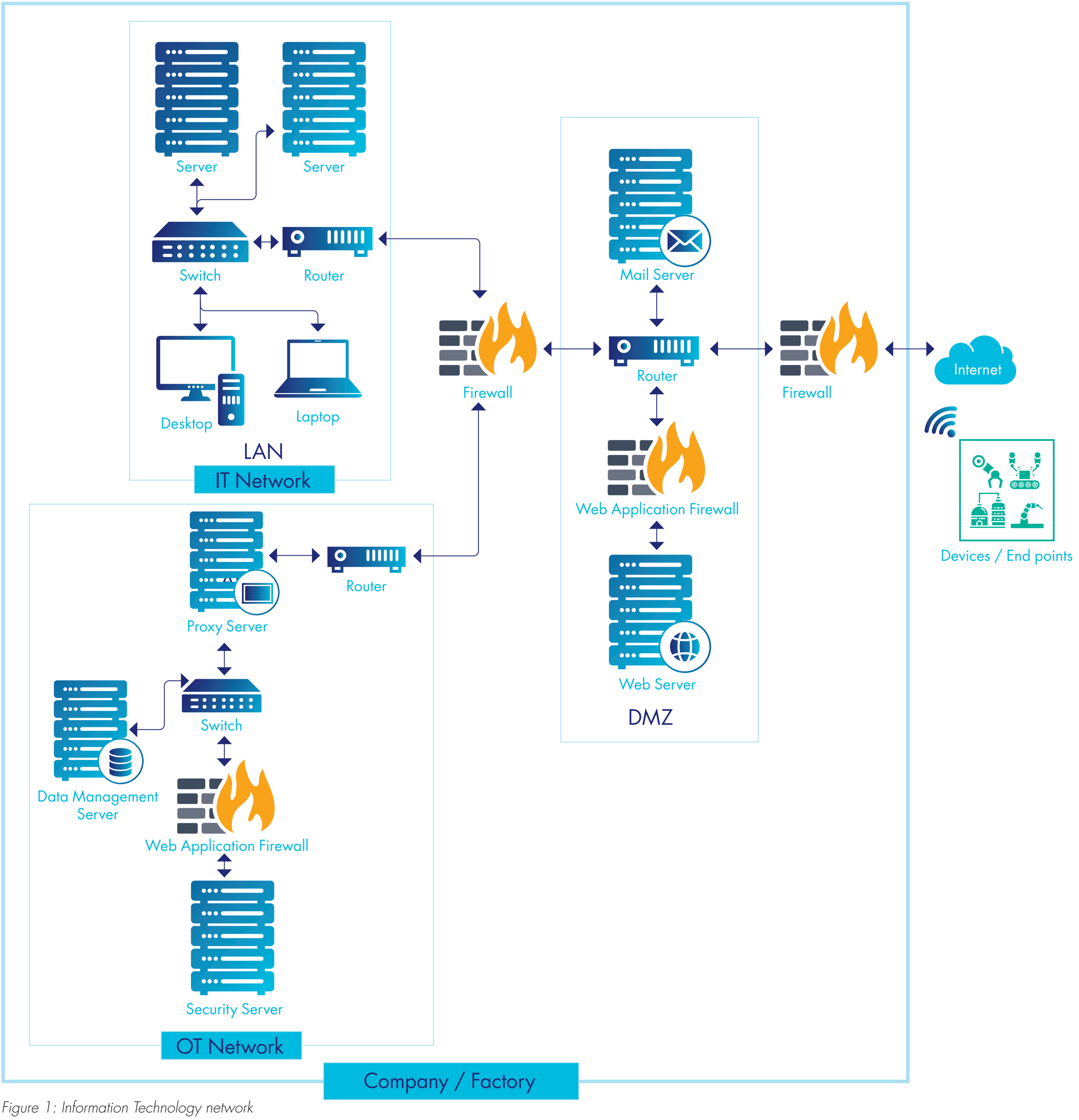

Figure 1: Information Technology network

In some cases, an entity interacts with devices (machines, sensors, actuators, etc.). Sensors collect data and take an active part in physical processes (actuators), such as controlling a pump/valve, a machine, or a smart meter. Collected information is processed by a Data Management System, which is part of the **Operational Technology (OT)** network.

But there's a further use case for a network in which the data is exchanged with the real world. Actuators (valves, pumps, lighting etc.), industrial sensors and even smart meters require bi-directional data exchange and processing in the Data Management System. This forms part of the **Operational Technology (OT)** network. The data exchange between the Data Management System and the physical device could be relatively local, such as within the same building or site, or separated by large distances.

The example on figure 1 above shows a typical IT network interfaced to an external OT network via an external firewall, however other configurations could be considered. The entire OT network could be contained and managed within an organisation's premises.

In any case, every device on the OT network offers a potential point of entry to an organisation's OT or IT infrastructure if not adequately protected.

If these devices are not externally 'visible', say using some wired connection to the rest of the internal network, then the traditional IT cybersecurity can still be considered an adequate level of protection, assuming the assessed levels of threat allow it.

However, there are two important things to consider.

- IT and OT are rapidly converging.
- Devices are often located at some distance from the Data Management System and require Wide Area Networking, usually via wireless communication. In this scenario, the remote assets could be widely spread geographically as is the case with Smart Meters.

Multiple wireless connected devices significantly increase the attack surface, calling for dedicated cybersecurity solutions. The following list provides a good overview of the main points to consider when looking at protecting the OT side:

Key points to consider when securing an OT network:

- Connected devices (e.g., smart meters) must have a solidly protected identity
- All data generated must be cyphered (in motion and at rest)
- Data integrity is crucial. Tampered, manipulated data can lead to false business decisions with significant consequences. For example, the demand/response of a smart grid could be mismanaged based on incorrect data, leading to service interruptions
- Digitally signed remote file/firmware updates are essential to ensure authenticity. Firmware over-the-air updates are likely to be required when considering the potentially long lifespan of a device

Protect both IT & OT for a comprehensive security plan

With an ever-increasing number of connections worldwide leading to larger attack surfaces, cyber criminals are turning their focus to Operational Technology (OT). A successful OT attack on vulnerable end-points, such as remote smart meters, can wreak havoc on businesses and propagate through to the IT infrastructure. The IT cybersecurity budget is usually well accepted and understood, less so for the OT infrastructure. Cyber security expertise is critical to protect against IT and OT attacks as our connected world expands.

A dedicated Security Manager is required to protect the OT and in turn, keep the IT protected. With their increasing convergence, one cannot be cyber safe without protecting the other.

Log on to our cybersecurity page, to learn more about Thales´s solutions to protect your critical end points.

THALES

Building a future we can all trust

> Thalesgroup.com <