Title: Embracing Zero Trust (Part 3 of 7): Logical and Physical Segmentation

Author
Alberto Menéndez
Director, Global Infrastructure Security, Schneider Electric

As part of an ongoing series that discusses the seven principles in our Zero Trust model, this blog focuses on our third principle, **Logical and Physical Segmentation**, and how we apply it within our company.

In the IT and OT world, cybersecurity threats, threat actors techniques and tactics are evolving exponentially every day. The convergence of IT computing and OT environments, which can be difficult to secure, is increasing the cybersecurity risks in many companies, especially industrial ones.

Logical and physical segmentation of networks can help mitigate these risks as it embodies the zero-trust philosophy of "never trust, always verify" by assuming that traffic on any type of network may pose a threat.

What is network segmentation?

Here is a brief overview of network segmentation, including the difference between logical and physical segmentation, as well as micro-segmentation.

In a typical environment, network segmentation involves splitting a network into a number of sub-networks based on criteria such as geographic location, functionality, criticality, risk, and security levels. Companies use network segmentation to better control and monitor traffic using policies that are enabled not only for security purposes, but also to improve network performance. From a security perspective, segmentation can help control access to sensitive systems and, with sub-networks, it helps to reduce the attack surface, isolate breaches, and minimize the blast radius during an attack.

Diving in a bit deeper, logical segmentation is software-based and often uses a virtual local area network (VLAN), while physical segmentation uses hardware to create smaller physical networks that are separated by physical firewalls. Micro-segmentation is a specific software-based technique used for cybersecurity that allows a more granular separation of access to the networks. For instance, it can segment people by their roles as well as the applications and devices they use.

How Schneider Electric applies this principle

As mentioned earlier, network segmentation is particularly important in the industrial world. Traditionally, IT networks, which support applications and computing, were separate from OT networks, which help companies connect, monitor, manage, and secure industrial operations. Today, however, IT and OT networks are converging, especially through technologies like the Internet of Things (IoT), which are essential to OT environments.

We believe it's a good practice to separate critical IT and OT networks from each other, as there are usually inherent risks in each area that need different types of controls and security. As an example, a cyber risk on someone's device that is connected to one of our IT networks is very different than a cyber incident on a security camera that can lead to the sabotage of an OT-connected asset in an industrial area. Segmentation is also helpful in areas with geopolitical issues where there is a greater risk of a cybersecurity attack.

At Schneider Electric, we use VLANs to help limit nefarious traffic flow and prevent data-gathering that may occur through a cyber threat. We use firewalls to protect valuable "crown jewel" assets, and also to protect specific sites. We have next-generation machine learning and AI tools that help us monitor and analyze our network traffic to continually validate our segmentation rules. This helps us identify which traffic is necessary, which is associated with a risky or insecure port or protocol, and what mandatory ports must always be secured.

We also use micro-segmentation, which allows us to enhance our zero-trust capabilities by managing networks with more granular security policies than other segmentation types. Similar to our least-access privilege processes, micro-segmentation can help reduce the risk of cyberattacks by improving security of applications, users, devices, and other areas where more granular security governance is needed.

We believe segmentation is critical in helping to stop the lateral movement and spread of malware from threat actors that can get in our networks, as well as helping us avoid exfiltration of critical data. We also believe that for the most important assets of a company, actual physical security, with cameras and the restriction of certain areas, is essential as well.

Regardless of the type, segmentation is critical today

Both logical and physical segmentation each have their own benefits. Logical segmentation can be automated and typically does not involve new hardware, making it more flexible and less expensive. Physical segmentation can be implemented and managed easier.

While in the past network segmentation might have been used primarily for monitoring networks, today it is a critical necessity for companies that take cybersecurity seriously.