Network to Network Protection

Introduction

In late 2014, a steel mill in Germany suffered massive damage as the result of a cyber attack that required advanced hacking skills, applied industrial control knowledge and endurance. No one has claimed responsibility for the attack and the lack of attribution and clear objective emphasize that not only are the threats very real, but anyone can become a target without apparent reason. This incident is only one of many examples of successful cyber attacks of industrial automation and control systems, and together with Stuxnet manifests the reality of cyber threats.

Unless you have experienced a serious security incident first hand, it is easy to believe such attacks only happens to someone else, but not having experienced such an incident however, does not mean you haven't been compromised. In fact, according to a report from KPMG from 2014, it is more likely than not that information is being exfiltrated by malware without your knowledge from your office networks. 14 companies were studied, and data was actively stolen from 10 of them without their knowledge.

The report is yet another strong indication traditional, best-practice defense like anti-virus, perimeter firewalls and network intrusion detection systems based on signatures are easily avoided. It also indicates insufficient organizational readiness as no action was taken even when malicious code was detected.

Westermo present a series of five basic applications assets owners can apply in their own networks to improve the security posture in a sustainable way.

Network to Network Protection

Cyber protections are usually coordinated with physical protection, sometimes referred to as the logical and physical security perimeters or boundaries. If an attacker gains physical access to a cyber asset, that asset should be considered compromised as cyber assets themselves are not designed to withstand physical tampering. Creating physical security boundaries, like 6-wall shell protection with physical access control, therefore becomes important. When two devices in different physical security zones need to communicate, that communication must be protected.

Such protection may be physical in nature, for example making sure the communication media like cables/fiber are protected by steel tubes or similar which is applicable over shorter distances. The protection may also be logical, such as virtual private networks (VPN) that use cryptography to protect the communication.

WeOS powered devices are able to provide VPN, and thereby protect the data in transit between the two VPN end-points which can be either two WeOS devices or one WeOS device and another device or computer that support the same protocols and algorithms.

Protection

A virtual private network (VPN) provides mutual authentication and confidentiality between two communicating IP end-points such that even if an attacker can intercept data, it is not possible to decipher the content or manipulate it. The secure link can be established over any other existing and untrusted IP network such as the Internet.

With WeOS, it is also possible to combine the network-to-network protection link with Network Segregation or Perimeter Protection applications adding an additional layer of protection by enabling the firewall for the link.

Detection

As with intrusion detection in general, network-to-network protection also contribute to the overall intrusion detection architecture as it is possible monitor connection requests, failed/successful authentication, interrupted sessions, etc. Depending on intrusion detection system, it may be possible to profile the normal behavior of a network-to-network protection application and thereby be able to alert on anomalies that may indicate an attack. It may of course also indicate a simple technical failure, which is also good to know about.

Enabling the firewall also improve the intrusion detection possibilities as known bad can be dropped and logged, and previously unknown connection requests can be logged for immediate action using the white, grey and black list (WGB) approach.

Typical applications

When connecting two networks, WeOS works well also for non-industrial environments, but the robustness of our devices makes them perfect for use in the field, for example protecting the communication over a VDSL line between two field cabinets.

Using a trackside control system as example it is a perfect fit for connecting the office network with the operational control system as illustrated in *Figure 1 - Network to network protection*

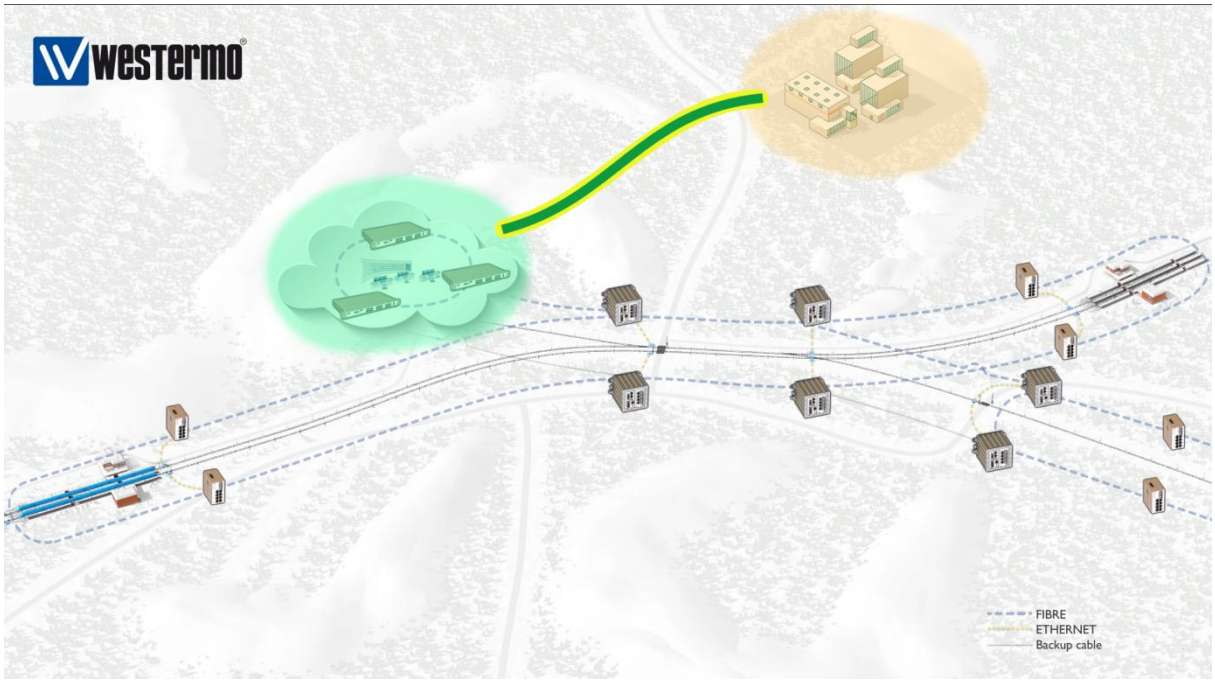

Figure 1 - Network to network protection