LAYERING NETWORK SECURITY THROUGH SEGMENTATION

JANUARY 2022

An effective technique to strengthen security, network segmentation is a physical or virtual architectural approach dividing a network into multiple segments, each acting as its own subnetwork providing additional security and control. Creating boundaries between the operational technology (OT) and information technology (IT) networks reduces many risks associated with the IT network, such as threats caused by phishing attacks. Segmentation limits access to devices, data, and applications and restricts communications between networks. Segmentation also separates and protects OT network layers to ensure industrial and other critical processes function as intended. Properly implemented Demilitarized Zones[1] (DMZs) and firewalls can prevent a malicious actor's attempts to access high-value assets by shielding the network from unauthorized access. Firewalls can be configured to block traffic from network addresses, applications, or ports while allowing necessary data through. Policies and controls should also be used to monitor and regulate system access and the movement of traffic between zones.

The following graphics illustrate the level of effort needed, with yellow representing low effort and red representing high effort, for attackers to breach and navigate an unsegmented network versus a highly segmented network. These depictions are not to be construed as representing an engineering diagram for use in a production environment nor is segmentation the only tool to secure a network.

FIGURE 1: UNSEGMENTED IT AND OT NETWORK

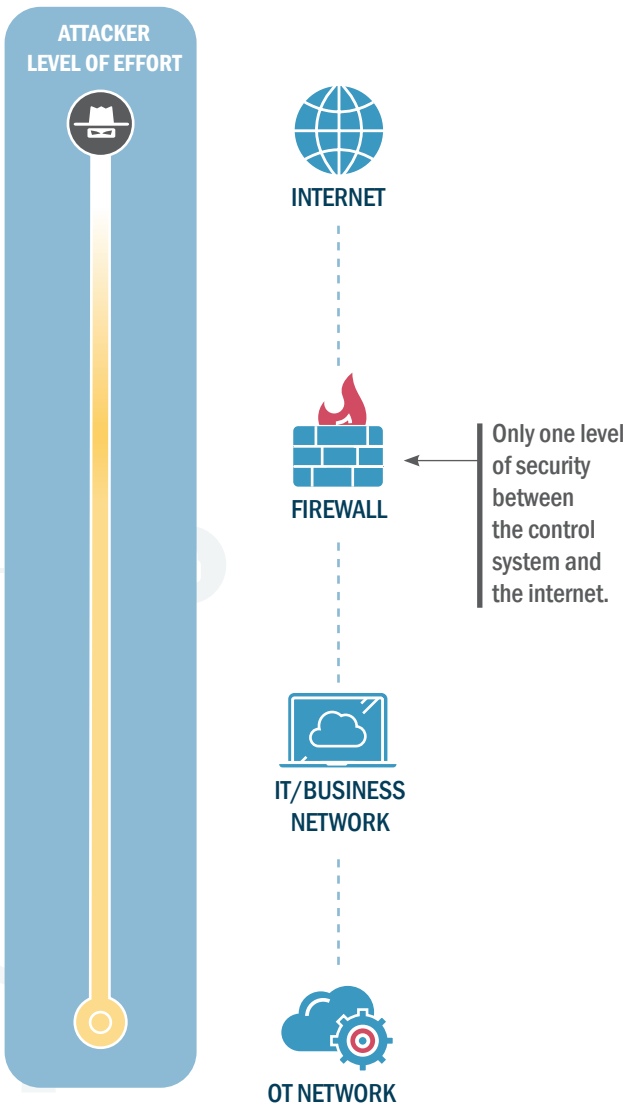
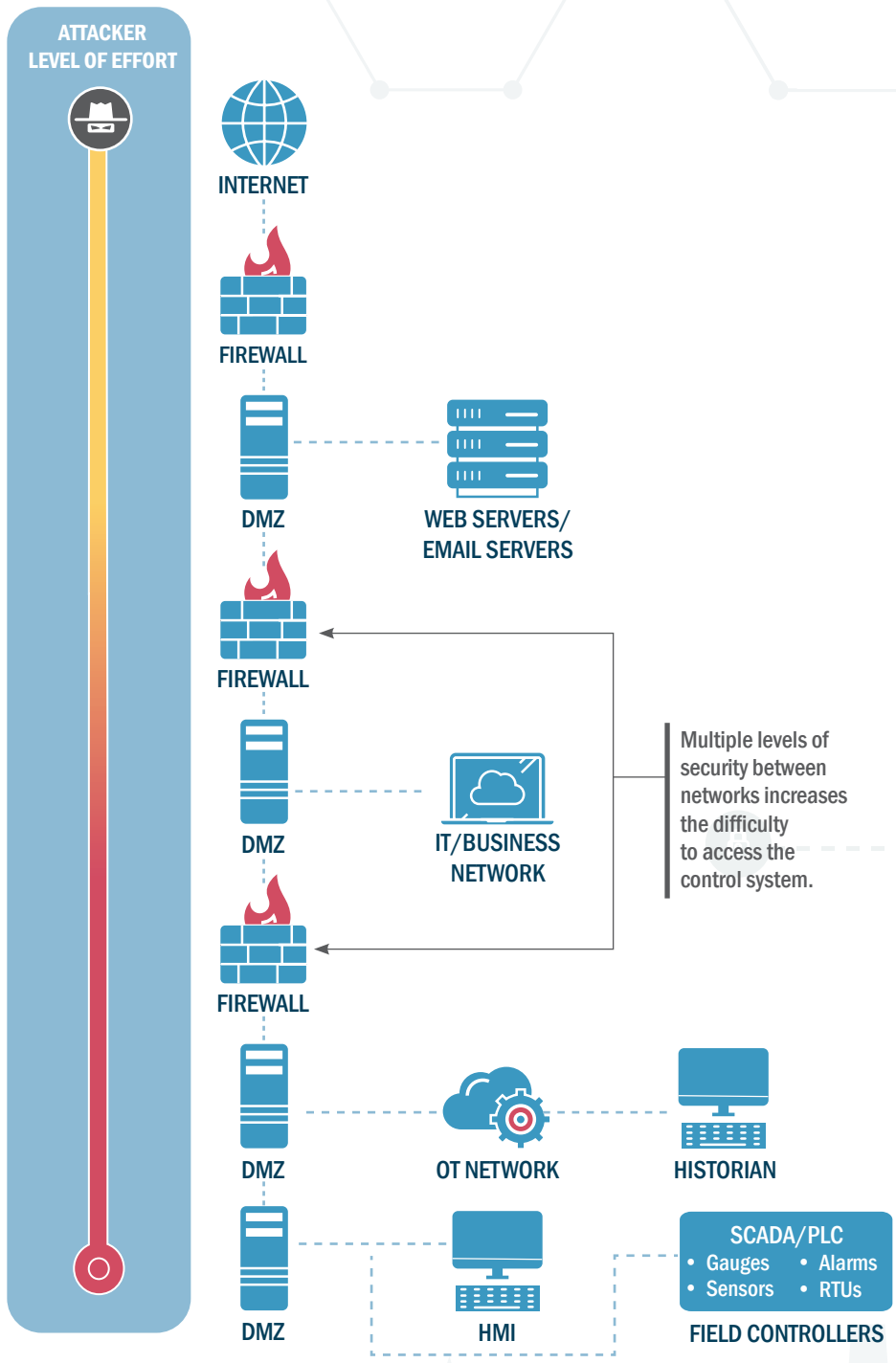


FIGURE 2: A SEGMENTED PURDUE ENTERPRISE REFERENCE ARCHITECTURE (PERA) NETWORK ARCHITECTURE



UNSEGMENTED IT AND OT NETWORKS INCREASE RISK[2]:

- OT networks are exposed to vulnerabilities in connected IT networks.
- Easier for threat actors to move laterally after breaching the IT netwo
- Detecting threat actors is more difficult due to increased volume of network traffic.

BENEFITS OF SEGMENTING BETWEEN IT AND OT NETWORKS:

- Segmented zones isolate and protect high-value assets and data.
- Malicious traffic is easier to detect, prevent, and contain.
- Threat actors must negotiate multiple firewalls and other protocols to access the OT environment.

[1] Demilitarized Zone (DMZ): In networking, a DMZ is a physical or logical subnet that separates a local area network from other untrusted networks.
[2] Since 2015, the Cybersecurity and Infrastructure Security Agency identified boundary protection as the most prevalent discovery in network security architecture assessments across multiple industries. For additional information refer to **NIST Special Publication (SP) 800-53**, System and Communications Protection 7 (SC-7) Boundary Protection.

RECOMMENDATIONS:

- Establish a segmented high security zone for high value assets and/or OT systems components.
- Protect access to devices within this zone by using specific firewall access controls.
- Establish a DMZ for work that must be within the high security zone.
- Allow only specific devices within the DMZ to connect to high value assets, and only through specified connections.
- Allow only specific users/devices to connect remotely to devices in this DMZ to access high value servers.
- Limit data traffic to the IT network with remote access control.