Application Note

Production Floor Security

Network Monitoring & Secure Access to the Production Floor

Synopsis: Industrial Control Systems (ICS) used in manufacturing are exposed to a myriad of cyber threats. Protecting ICSs from cyber attacks requires a dedicated solution designed for automated processes, rather than standard IT security solutions. Radiflow's comprehensive solution combines its Secure Gateway and Intrusion Detection System. Together, the integrated solution provides secure access to PLCs while continuously monitoring the network for abnormal behavior that may be indicative of malicious activity.

The manufacturing environment has undergone many changes in recent years, the result of globalization, fluctuations in the price of raw materials and consumers' demand for high quality. To stay competitive, manufacturers increasingly rely on IOT and other "Smart Factory" technologies. These technologies maximize efficiency and quality, and can be controlled from anywhere, 24/7, with real-time updates from the factory floor.

The downside of the Smart Factory is exposure to cyber threats. And though awareness has been developing steadily, most manufacturers that invest in cyber security technologies still purchase IT security solutions, even though such systems won't protect their production processes. Industrial Control Systems (ICS), which run the production floor, are fundamentally different from IT networks; therefore, many attacks on the ICS network would not be detected by IT security solutions. What's needed is a solution designed specifically for ICS networks.

Radiflow's end-to-end solution combines its powerful Secure Gateway and its iSID Intrusion Detection System (IDS). Together they enable the detection of sophisticated cyber-attacks aimed at disrupting production processes.

The Radiflow 3180 Secure Gateway provides access to the production floor, with different access rights for each stakeholder. The Gateway's authentication proxy authenticates each user and restricts the user's access based on role or predefined tasks (e.g. , for a maintenance technician, the Gateway would restrict which PLC to access, during which time slot, the types of commands approved for use, etc.). Furthermore, all sessions are recorded for auditing purposes.

Radiflow's secure gateway enables manufacturers to maximize production line uptime by granting remote access to PLC vendors for monitoring their device's behavior and overall health.

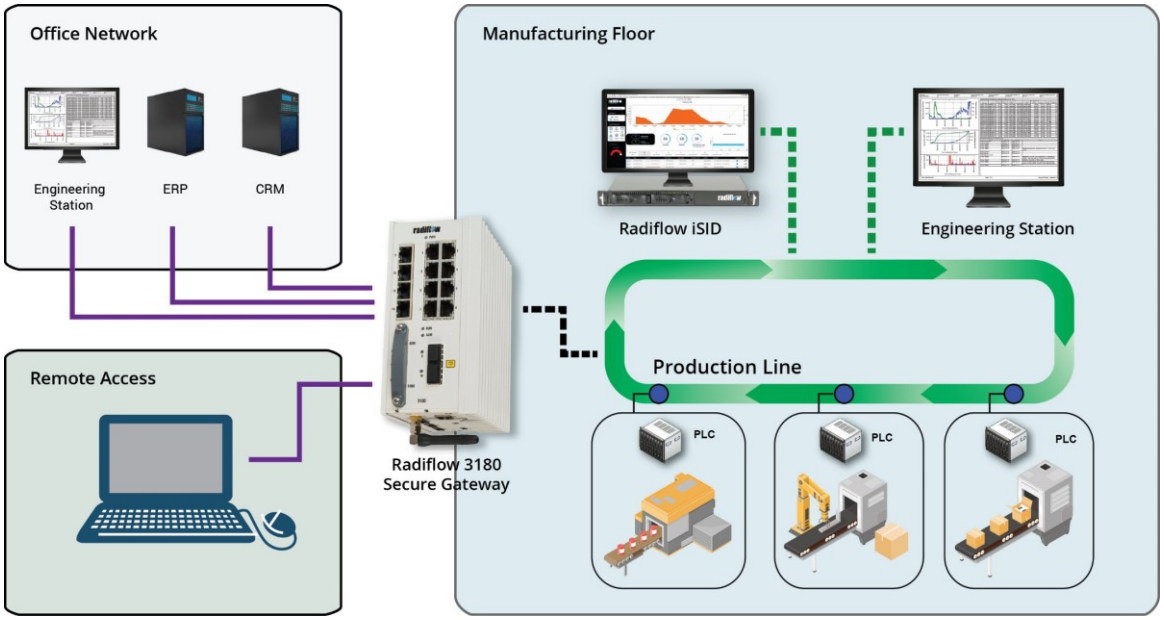
Radiflow's iSID Industrial Intrusion Detection System (IDS) was designed to protect production floor operations by capturing and logging suspicious network traffic and detecting anomalies, such as unusual network scanning and changes in the production process model.

This is achieved through real-time analysis of all network traffic, which is validated against a dynamic baseline network behavior model created by the IDS (using passive network scanning). The IDS will issue alerts for anomalies in the production floor that may indicate an insider attack (e.g. a malware on one of the PLCs).

Application Note

Production Floor Security

Network Monitoring & Secure Access to the Production Floor



Key Features

- **Secure maintenance:** Authentication Proxy Access (APA) is used to validate technician credentials and provide preconfigured task-based access over a built-in IPSec VPN tunnel.
- **Maintenance Logging**: Monitor and record all activities performed during maintenance sessions according to preconfigured policies.
- **Secure data collection from the production floor**: Unidirectional DPI firewall between the corporate network and the production floor.
- **Network Modeling:** Display of all network assets and any changes in connectivity, based on self-learning of the ICS network through passive scanning of all data transactions.
- **Anomaly detection:** Detection of abnormal activity such as changes in the production process sequence, abnormal memory access, based on the normal application behavior model created by the iSID.
- **Policies management:** Defining policies for each session on the ICS network. These rules, based on Deep Packet Inspection (DPI) for industrial protocols, allow the validation of specific commands and operational parameter ranges.
- **Assets management:** Managing, monitoring and auditing the PLCs in the factory. Any firmware changes, configuration or critical command (on/off) will trigger an alert.
- **PLC failures predictive analytics:** iSID's Anomaly Detection function constantly examines the behavior of the PLC. Once a behavioral change is detected the iSID will issue a request for inspecting the PLC.

radiflow
Secure your Assets