Application Note

Substation Security

IDS-Based Cyber Defense by Radiflow

***Synopsis**: IDS (Intrusion Detection System) is a critical element in the protection of SCADA systems. By learning the network topology and creating a comprehensive normal network model, IDS systems enable detecting nuanced anomalies and handling highly complex cyber-attacks. IDS systems provide operators a comprehensive view of the OT network for efficient network management. As important is the IDS passive nature that makes it very easy to deploy, and do not interfere with the operational network traffic.*

Supervisory Control and Data Acquisition **(SCADA)** systems are used for controlling utility operations such as electric power, water and oil. In the case of power utilities the SCADA function is fulfilled by Distribution Management Systems **(DMS)**. These SCADA systems are responsible for controlling highly critical operations, making them, especially over the last decade, a primary target for cyber-attacks.

Cyber defense for SCADA systems in critical infrastructure needs to comply with the NERC-CIP regulations for protecting Bulk Electric Systems **(BES)**.

Intrusion detection systems **(IDS)** are capable of protecting critical infrastructure against cyber-attacks by capturing and logging suspicious traffic and detecting anomalous behavior, such as connection of new devices, topology changes and unusual scanning. This is achieved through real-time analysis of all network traffic, which is validated against a dynamic normal network model.

On-Site IDS Deployment

To comply with cyber defense requirements, the IDS can be installed at a centralized location which supports multiple sites, or deployed on-site at select remote sites. In the case of on-site deployment, all IDS systems are managed from a central location.

Why choose on-site IDS:

- On-site monitoring of all operations
- Simple to deploy and operate
- Does not interfere with local operations
- Interfaces with existing architecture
- Analysis of operational behavior

The consideration whether to deploy the IDS at a central location or on-site depends on the level of criticality of the remote site and its network complexity.

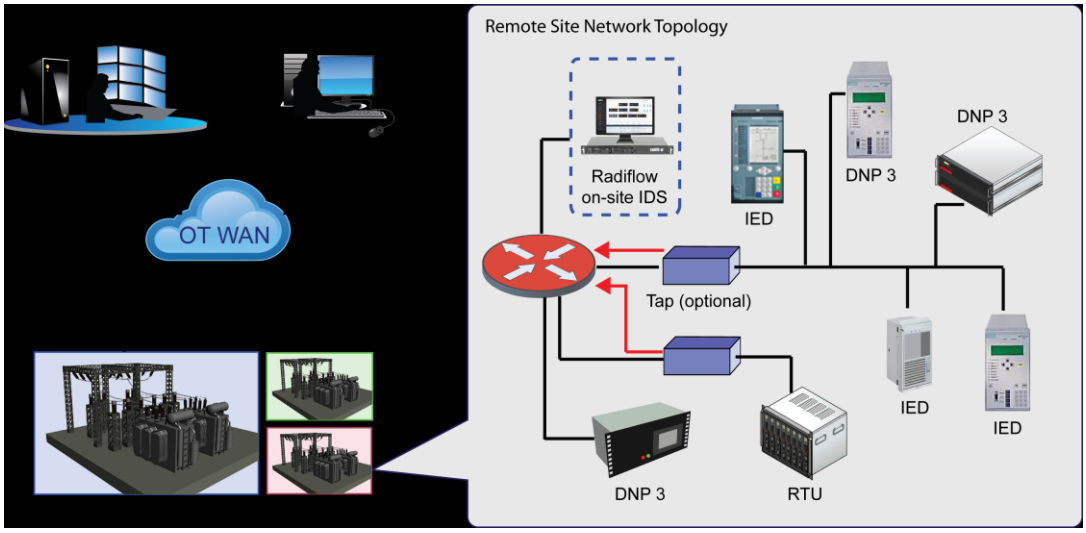
As a rule, the IDS should be installed on-site at critical sites (as defined by the operator), where the complexity of the network exposes it to in-field attacks. This is usually the case in large sites that host a large number of often-unprotected devices, making it extremely difficult to detect the source and the pattern of cyber-attacks.

Contributing to the complexity of the site, and hence its vulnerability, is the inter-communication between devices, which may not be intercepted by on-site firewalls typically designed to handle incoming and outgoing traffic.

Application Note

Substation Security

IDS-Based Cyber Defense by Radiflow



Cyber defense using on-site IDS.

Key Features

The IDS analyzes anomalies such as utilized bandwidth, type of protocols, accessed ports, and unprecedented traffic level between connected devices.

The accurate detection of attacks is very difficult, since the parameters and conditions that qualify normal or abnormal behavior constantly change. While the detection process is always based on a known behavior, it must be constantly fine-tuned through a properly defined self-learning process.

To this end, the IDS simultaneously performs up to six of the following processes:

- **Network Visibility:** Based on self-learning of the SCADA network through passive (and optionally active) scanning of all data transactions.
- **Maintenance management:** An Authenticated Proxy Agent (APA) process for managing maintenance operations at a central place.
- **Signature-based detection:** ongoing detection of attacks that take advantage of PLC vulnerabilities, known protocol vulnerabilities and software signatures.
- **Virtual firewall:** creation of firewall rules on every link, as well as “dynamic firewall rules” that apply only to specific times (e.g. for scheduled maintenance).
- **Anomaly detection:** detection of abnormal activity, including new devices, topology changes, abnormal memory access and firmware change, in comparison to the normal network model created by the IDS.
- **Operational behavior:** detection of abnormal delays in links and abnormal rates of packet dropping and retransmits caused by excess network load.

radiflow
Secure your Assets