Application Note

Secure Substation Automation

Radiflow Security Gateway for Substations

Synopsis: Radiflow 3180 enables the secure access to substation automation devices for remote maintenance. By using this solution the operation of the substation becomes NERC CIP V5 compliant without depredating the operational efficiency.

In recent years, energy suppliers have become a prime target for cyber-attacks by a variety of hostile organizations and governments. To assure safe, reliable and efficient operation, new measures and methods had to be introduced to protect energy facilities.

High Voltage to Medium Voltage **(HV/MV)** substations are typically located in remote, sparsely populated regions, and spread across a wide geographical area. This makes them vulnerable to cyber-attacks, both internal, committed by insiders who have gained unauthorized access, and from the outside, via the substation's network links. The targets within the substation are often the devices that regulate its operation, including Remote Terminal Units **(RTU)** and Intelligent Electronic Systems **(IED)**, which control the substation operation coordinated with the Distribution Management System **(DMS)**. Cyber defense solutions are deployed on-site to maximize the protection of the substation itself.

The North American Electric Reliability Corporation's Critical Infrastructure Protection **(NERC CIP)** standards were introduced to assure the reliable and secure operation of power delivery systems in North America. Version 5 of the standard focuses on Bulk Electric Systems **(BES)** operating at over 100kV, however upgrading a substation's cyber defense system is important also for smaller substations (e.g. **69kV/11kV)** which are often even more vulnerable.

According to security experts the most critical risk to the substations is the human interactions such as maintenance. Radiflow 3180 security gateways are used to secure the substation's network during the maintenance process. The 3180 gateway enforces the policy of the operator's work order in the field with Authentication Proxy Access (APA). The APA lets the operator define a restricted time-window to access a specific device for maintenance operations such as software upgrade without exposing the entire substation to the technician. The APA is using the 3180 DPI engine to validate the data and protect from unauthorized operations. At the end of each operation, the operator gets an activity log report.

Most of the traffic within the SCADA network is generated by machines. Machine-to-Machine (M2M) sessions are automatic without human intervention. As such M2M traffic is predictable and the operator is able to create firewall rules in order to block unexpected traffic. The 3180 validates these SCADA activity rules using its DPI engine for both Ethernet and Serial traffic.

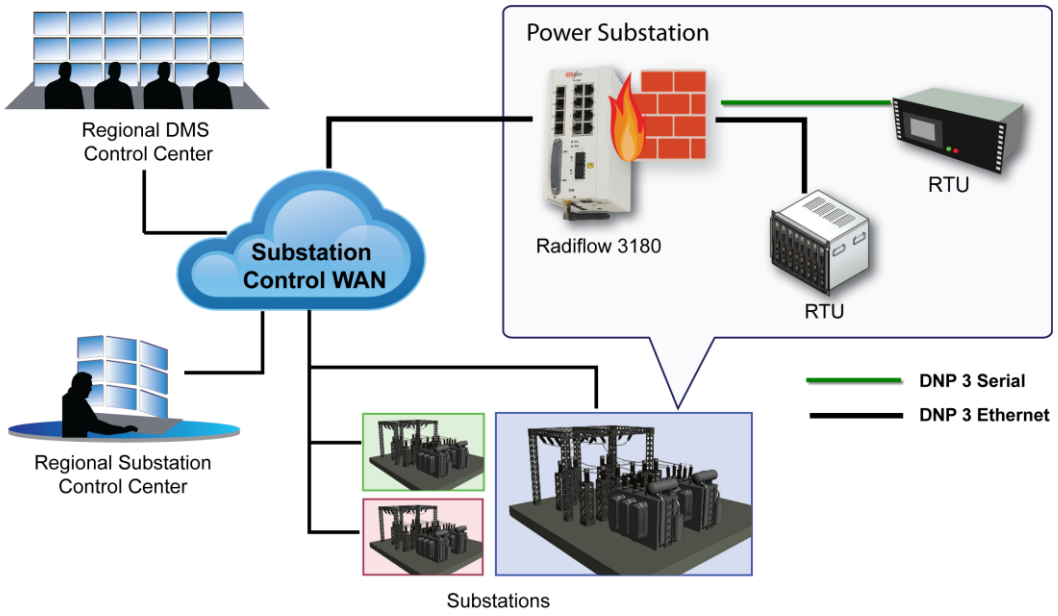
Radiflow secure gateway can integrate with other security tools such as the Radiflow Intrusion Detection System **(IDS)**, Physical security for user identity and Security Information and Event Management **(SIEM)**. This integration provides a comprehensive security solution to the distributed assets of the power utilities.

radiflow
Secure your Assets

Application Note

Secure Substation Automation

Radiflow Security Gateway for Substations



Radiflow Security Benefits

- *Secure access from one substation to another by authorized engineers for performing remote maintenance on devices located within the Electronic Secured perimeter **(ESP).***
- *Authentication Proxy Access **(APA)** provides preconfigured task-based access*
- *Detailed log of all user activity within a remote access session for compliance and audit.*
- *Validation of each user's SCADA behavior using a per-port Deep Packet Inspection **(DPI)** firewall.*
- *Automatic learning of the SCADA process behavior for setting the baseline of the DPI firewall rules.*
- *End-to-end IPsec Layer-3 VPN for secure inter-site connectivity between substations and **EMS/DMS** control centers, to prevent Man-in-the-Middle **(MitM)** attacks.*
- *Support for Ethernet and Serial interfaces, for connecting modern and legacy devices, including protocol gateway functionality.*
- *Reliable WAN interface over Ethernet utilizing copper and fiber, as well as private wireless and cellular (3G/4G) connectivity as a backup link.*
- *Ruggedized security gateway hardware is compliant to IEC 61850-3/IEEE 1613 requirements for operation in harsh environments such as HV/MV substations.*

radiflow
Secure your Assets