Solution Brochure

Radiflow OT Security

Optimized Security approach for SCADA Networks

Radiflow OT Security

- IDS & IPS with multiple deployment models
- DPI of IP & Serial SCADA protocols
- Model-based analytics for M2M sessions
- Self-learning of application behavioral model
- Signature Based detection of known vulnerabilities
- Task-based validation of H2M sessions
- Integration with physical security
- Authentication Proxy for access to end-devices
- Encrypted VPN tunnels for inter-site connectivity

radiflow
Secure your Assets

General

Supervisory Control and Data Acquisition (SCADA) systems are used for controlling and monitoring remote operations in a variety of industries and infrastructures, including power utilities, oil and gas production and many more.

SCADA systems include automation devices distributed across multiple remote sites controlled from control centers where all data is clearly presented using an intuitive HMI (Human Machine Interface).

Cyber threats to SCADA systems have in recent years been on the rise. Terrorists and criminals have set their sights on critical infrastructure that utilize SCADA systems due to vulnerabilities and the huge potential to disrupt civilian life.

The Challenge

Most SCADA applications utilize a dedicated operational network (OT Network) which is separated from the IT networks (the Enterprise network and the Internet). However, once an attacker gains access to the OT network from any location, there are no security measures that would prevent him from accessing the entire network and inflicting damage to any connected assets locally or at remote sites.

In many utilities, the weakest links, in terms of security, are the remote substations which are located in sparsely populated areas with limited physical security. Connecting to the network in such a remote site provides unlimited access locally and to other sites.

The SCADA networks to such remote sites suffer from several types of security problems. First, Industrial protocols were not planned with security built-in. Therefore there are no authentication methods in the protocols. Once an attacker enters the network, he can send commands to every device that he finds at the network. Another problem is the visibility of the network. In the IT network there are various monitoring tools which assist in detecting security incidents. However, these solutions fail when it comes to the OT network. OT networks have different protocols, different behavior, and even small amount of commands can cause a lot of damage.

Furthermore SCADA systems handle two different types of network traffic that should be protected in different ways: M2M (Machine to Machine) for the automation processes and H2M (Human to Machine) generated by a person inside the SCADA network, usually for maintenance, either physical (on-site) or remote.

The Security Tool-Set

ANOMALY DETECTION

To protect against various cyber-attacks one needs a good firewall to detect unauthorized traffic even when the attacker gained access to the network. Today there are a few levels of firewalls in the critical infrastructure space - a simple firewall can prevent unauthorized traffic by validating devices at IP level, while other firewalls are analyzing the traffic with DPI (Deep-Packet-Inspection) engines that are validating the SCADA commands in depth.

In light of the predictable nature of the M2M traffic in the SCADA networks, the traffic validation can be further enhanced with behavioral analysis algorithms deployed either in-line throughout the network (IPS – Intrusion-Prevention-System) or in a central monitoring system (IDS – Intrusion-Detection-System).

IDENTITY MANAGEMENT

According to NERC CIP, before granting a physical or remote access to the network the users have to be validated. In order to verify the users there are several authentications methods, from physical authentication such as facial recognition and a magnetic card, as well as logical authentication like username and password with smart passwords management. Usually after the user authenticated he gets access to the network and each operation is recorded in a log file.

It is recommended that the access granted to the user would be limited in scope according to the specific task that he has to perform.

INTER SITE CONNECTIVITY

Encrypted VPN tunnels provide secure inter-site connectivity against man-in-the-middle attacks. Such VPNs are used when trusted links, such as dedicated fibers, are not available to connect all the remote sites of the utility. There are multiple VPN methods therefore it is important to ensure its fit to the operator needs in aspects such as scalability, interoperability.

On the security plane the important aspects of the VPN are the algorithm types, key length and keys management as defined for example in the FIPS guidelines. Special care should be given to the key management of large-scale distributed VPNs - Pre-shard key is an easy and common key management but it would be better to manage keys with certificates, where the device gets the key from a central server that ensures the device is approved.

How to secure common SCADA operations

Operation use case	Security risk	Authentication	DPI Monitoring	DPI Enforcing	VPN
SCADA sever → devices	Medium		✓		
Physical access	High	✓		✓	
Remote access	High	✓		✓	✓
Connection between remote sites	High		✓		✓

Radiflow Solution

Radiflow's security solutions were developed especially for the critical infrastructure based on three underlying assumptions:

1. Vulnerabilities exist, whether in the end-devices or the control systems, in the network or in the SCADA protocols used.
2. Attackers will eventually find a way to penetrate even the most isolated network, as demonstrated in recent years.
3. The potential damage caused by attacking an infrastructure is immense, and detection time is critical.

Radiflow provides components that identify network threats, isolate malicious activities, and prevent threats from spreading across the network. These solutions are handling both the M2M and the H2M traffic sessions, each with specific tools.

These security solutions were developed using the expertise and experience of our security experts and refined in close interaction with leading SCADA vendors and operators since 2009.
These solutions were further validated and endorsed by leading research labs in the U.S and are continuously enhanced based on close cooperation with the academy on new security technologies.

ANOMALY DETECTION

In order to achieve maximum protection against cyber threats, Radiflow developed two types of products both utilizing the same SCADA DPI capabilities:

1. Secure ruggedized router - located in the remote sites and includes a built-in per port SCADA DPI firewall.
2. IDS – A central server that monitors the whole network and can detect sophisticated attacks within the SCADA network.

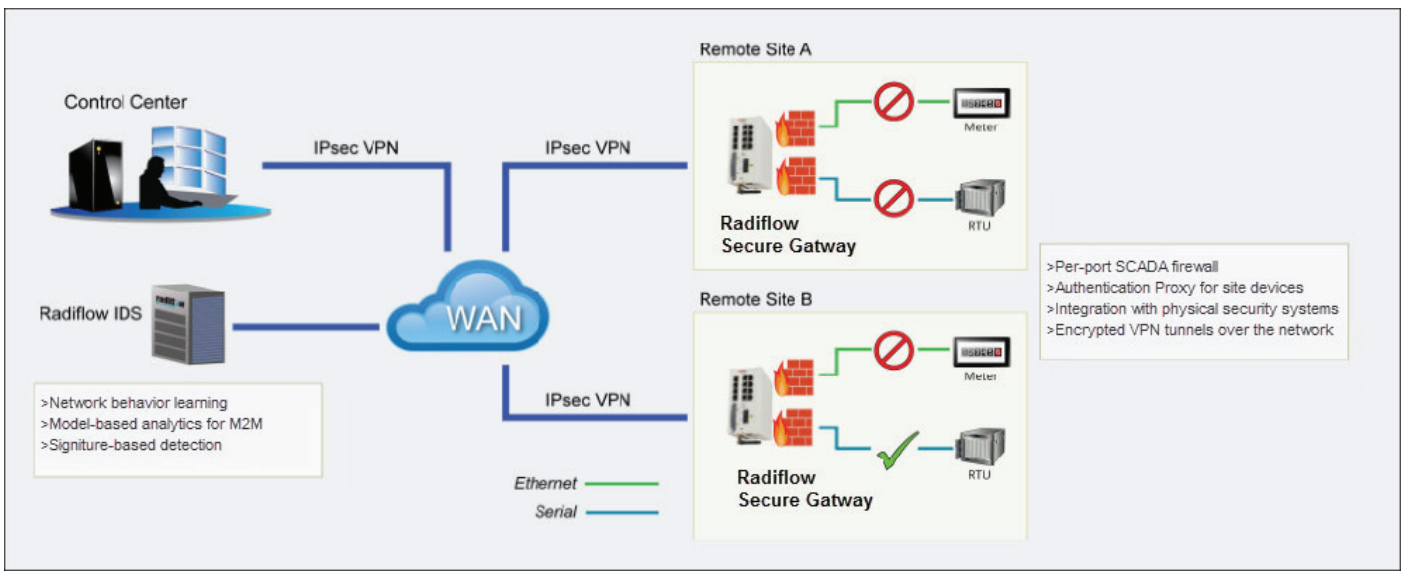
DISTRIBUTED DPI FIREWALL

To achieve airtight protection, Radiflow developed its DPI Firewall engine for SCADA protocols (DNP3, IEC 101/104/61850, ModBus) that is implemented in distributed ruggedized routers. The distributed DPI firewall ensures that the operator has full control over the network traffic for both M2M and H2M sessions. The whitelist-based firewall is installed at every port for both Serial and IP traffic, meaning that every access point is firewalled and each SCADA protocol packet is validated up to its function code and the command content.

Once deployed, Radiflow's devices starts learning the network, including its topology, devices (IP, unit-ID/ASDU), p rotocols, links and valid range parameters. At the end of the learning process, the NMS (network management system) tool displays the network and application topology and suggests a whitelist based on a traffic modeling algorithm. The operator is able to choose and edit which policies to monitor or enforce in each location. The distributed firewall enables the prevention of unauthorized traffic that does not correlate with the whitelist in order to validate M2M sessions and task-based H2M sessions. The firewall is also loaded with signatures for known vulnerabilities of the network devices (e.g. Shellshock).

IDS

On top of the distributed DPI deployment, Radiflow offers a complementary IDS server that monitors the network from a central location. The IDS gathers information from the entire network and uses its DPI engine to model the network and application behavior and display its structure (topology, devices, links and SCADA sessions) on an interactive map. This SCADA analysis tool creates a model which characterizes the normal behavior of the distributed SCADA application such as process sequence and device sampling time. Once the model of the normal application is learnt it is presented to the operator for approval. Once approved the network monitoring starts and the model-based IDS tool is able to detect network scanning, out of range commands and parameters and other abnormal activities.
Radiflow IDS also includes has a signature based detection engine, a network traffic that correlates to a known vulnerability in one of the protocols or devices (PLC, RTU, etc.), will be detected. Once a deviation is detected an alert is reported to the operator and optionally a Syslog message is sent to a SIEM tool. The user can also drill-down into the traffic that caused the alert and decide if the baseline model should be updated to include such a network activity.



Cyber security solution for substation automation

IDENTITY MANAGEMENT

To protect H2M processes, one of the most important requirements in NERC CIP V.5 for protecting remote sites is the capability to identify the user and create specific network privileges per identified user, prior to granting the user access to the network.

Radiflow's device includes a built-in APA (Authentic ation Proxy Access) with smart passwords management system. Prior to granting a user network access, the user needs to log in to Radiflow's internal authentication engine. After validating the user's profile, specific access is granted to predefined devices and functions, and each operation is logged.

For physical access at remote sites, the Radiflow system integrates with physical identity server systems (e.g. magnetic card access control systems) and dynamically activates a set of cyber-security rules according to the user that entered the site. This adds a layer of authentication to physical (on-site) access to the network. Furthermore the solution is also integrated with video management systems using video analytics for the user authentication and for tuning of the CCTV systems based on the activities detected in the cyber space (technician connected to a specific network port, etc.)

VPN

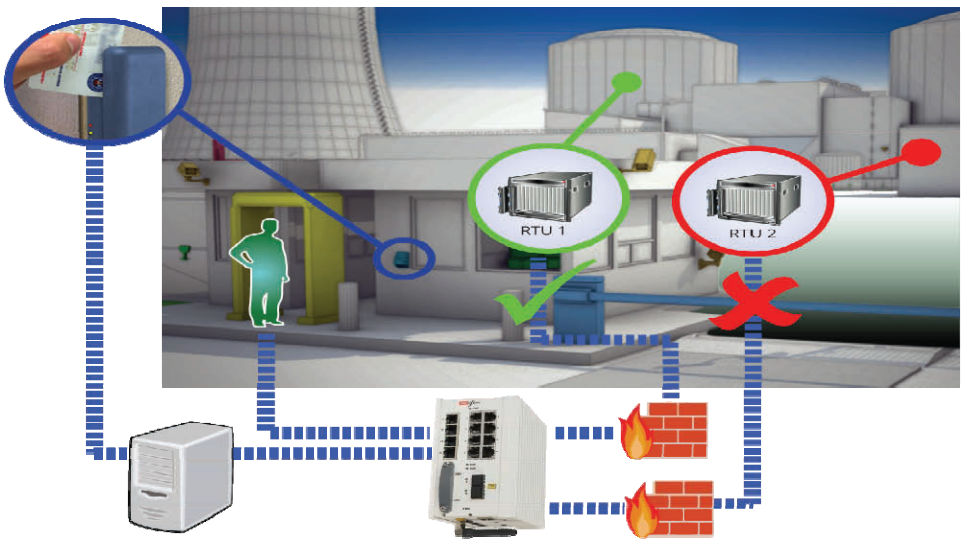
Radiflow routers ensure inter-sites secure connectivity by using L2/L3 VPN. Although there are many VPNs modes such as IPsec, DMVPN and mGRE tunnels, Radiflow routers support interoperability with most leading VPN routers for ensuring a smooth deployment.

Radiflow devices are compliant with FIPS guidelines for cryptography modules, by using recommended algorithms such as 3DES, key length of 256 bits and key management such as X.509 certificates with SCEP enrollment that authenticates the network devices with a central server before initiating the encrypted tunnel.

EASY DEPLOYMENT

Radiflow provides a comprehensive SCADA security tool-set. However since security adoption in OT networks is a delicate process, special emphasis is also given to the ease of deployment:

1. Radiflow security routers combine an extensive communication feature-set (i.e. Ethernet, PoE, Serial and Cellular interfaces) with the security capabilities for easy deployment in remote sites.
2. For the anomaly detection the normal network behavior is learnt automatically and presented to the user for approval before being deployed.
3. All the security features are managed via a central GUI tool that presents the distributed application deployment, its normal behavior baseline and any deviation that is detected.
4. Radiflow security tools provide interfaces for easy integration with other complementary security suites such as syslog reporting to SIEM tools, identity information from physical security servers, etc.



Integrated with physical authentication solutions

Headquarters:
31 HaBarzel
Tel Aviv, 6971045

North America:
900 Corporate Dr
Mahwah, NJ 07430

E-mail info@radiflow.com
www.radiflow.com

radiflow
Secure your Assets