Data Sheet

iSID

Industrial Cyber Security & Intrusion Detection

SCADA Intrusion Detection

- ▶ Automatic learning of topology and operational behavior
- ▶ Network traffic analysis based on DPI protocols for SCADA
- ▶ Supervision over configuration changes in PLCs
- ▶ Model-based anomaly detection analytics
- ▶ Signature-based detection of known vulnerabilities
- ▶ Non-intrusive network operation
- ▶ Central or distributed deployment
- ▶ Low false alarm rate

radiflow
Secure Your Assets

General

ICS/SCADA systems are used for controlling and monitoring remote operations in a variety of industries and infrastructures, including power utilities, oil and gas production.

Cyber threats to SCADA systems, originating from both external sources and internal activity, have in recent years been on the rise. Deploying an IDS in the SCADA network enables the operator to monitor the distributed network for any changes in the application's behavior, without disrupting normal operation.

Radiflow iSID includes six security packages for protect the Operational Technology (OT) network. Each package has a unique capability to detect suspicious traffic within the network in order to protect the process.

Functional Description

NETWORK VISIBILITY

Radiflow's iSID is able to automatically learn the traffic within the OT network by means of passive network scanning. To do this, the iSID receives data from all devices across the entire network (using port mirroring.) During the learning stage the data is used to construct a network model for all devices, protocols and sessions, which is displayed on a GUI at the end of the learning stage.

The visual network model helps to understand the processes that take place across the OT network, including security events. The visual network model map is also used to manually edit the network model itself, e.g. add a client PC at one of the remote sites, that was not detected during the learning stage.

Following the learning stage, any detected change in the network topology, such as new devices or new sessions, will trigger an alert, compelling the operator to evaluate the underlying event.

CYBER ATTACK

The Cyber Attack package handles known threats designed to exploit vulnerabilities in the SCADA network, including threats to PLCs, RTUs and industrial protocols.

The vulnerability signatures used by the Cyber Attack package are based on public data sources (research labs) as well as Radiflow Labs' own research. The signature database is continuously updated and made available to respond to emerging threats.

POLICY MONITORING

The Policy Monitoring package allows defining policies for each link on the SCADA network. These rules, based on Deep Packet Inspection (DPI) for SCADA protocols, allow the validation of specific commands (e.g. "write to controller") and operational parameter ranges (e.g. the technician should not change the RPM parameter of a turbine outside the 600-800 rpm range.) If a violation occurs, these rules will generate an alert at the control center.

The Policy Monitor also allows editing firewall rules suggested by the iSID after the learning period, and/or easily creating rules manually.

MAINTENANCE MANAGEMENT

Maintenance operations pose innate complexity and risk, since the operator is required to grant network access to the maintenance technician, thus exposing the network during maintenance. The current situation in most SCADA-based systems is that once the technician is granted access, there is no way for the operator to know what's happening on the network, unless a problem arises.

Radiflow's iSID offers a dedicated Maintenance Package to handle maintenance processes. The Maintenance Package provides the option to easily create work orders for specific devices at set time windows through a centralized tool. During maintenance, the iSID offers two monitoring modes: pause monitoring for the maintained zone during the defined time period, to prevent many false alarms; or close monitoring of the maintenance process, and generating an alert for each unauthorized command executed outside the defined work order.

For example, a maintenance work order can be defined to allow access to a specific device, and only between 8:00AM and 10:00AM on a certain day. Outside of this time period, any command would be unauthorized.

At the end of the maintenance period, a log report of all activities during the maintenance session is issued by the iSID.

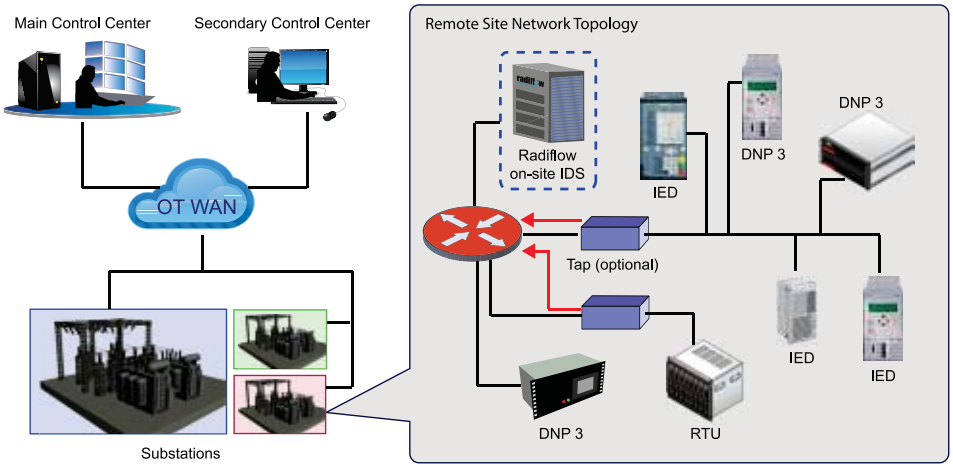

Diagram #1: iSID installed at remote site

ANOMALY DETECTION

The Anomaly Detection package learns the behavior of the OT network. It creates a network model using multiple parameters, including device sequence sampling time, frequency of operational values and more. Once the model is created and approved, the package will detect any abnormal behavior within the OT based on comparison between the monitored packet stream and the learned model.

OPERATIONAL BEHAVIOR

The Operational Behavior package enables the monitoring and auditing of the management of devices (PLC, RTU and IED) at remote sites. Any firmware changes or configuration modifications (e.g. software updates or turning edge devices on or off) will trigger an alert at the control room. In addition to alerting, the iSID will also present a full activity log.

Implementation

While the implementation of devices—especially security devices—on SCADA networks is typically far from simple, installing Radiflow's iSID is very easy and quick, and does not require making changes to the OT network traffic.

LEARNING STAGE

As mentioned, once installed, the iSID enters the Learning Stage in which it collects information about the network. During this stage, a copy of the network traffic is streamed to the iSID with no network intervention, using port mirroring. The iSID's DPI (Deep Packet Inspection) capability is used to extract valuable data such as device ID, links, time, protocol, rules and sample time, which are all necessary to learn the overall network behavior.

The data collected is used to build a complete network model, which in effect assigns a virtual fingerprint to each session between any two devices on the OT network. The network model is then translated into a privileges list, which will trigger an alert on every non-baseline activity. Besides assigning a unique identifier for each session, the iSID will graphically lay out the network topology on its GUI, allowing the investigation of processes and providing insight into the network's inner workings.

OPERATION DETECTION STAGE

At the end of the Learning Stage the iSID transitions to the Detection Stage. In this stage the iSID provides continuous network monitoring and uses its six engines to detect various cyber threats on the SCADA network.

The iSID's dashboard displays a dynamic security event log, as well as a set of aggregate statistics including the number of security breaches detected by each engine and the cyber-health of each sub-network. Alongside the statistics, by drilling down to specific devices the operator is able to edit each device's Policy Monitor rules. This provides operators great flexibility in managing individual devices.

Once the iSID detects an unauthorized activity in the network it will issue an alert on the IDS (or sends Syslog messages to the Syslog server). The operator assigned to investigate the alert has the option to extract the PCAP file from the iSID to expedite the response to the incident.

In addition, the various reports generated by the iSID help improve compliance with regulatory requirements such as NERC CIP.

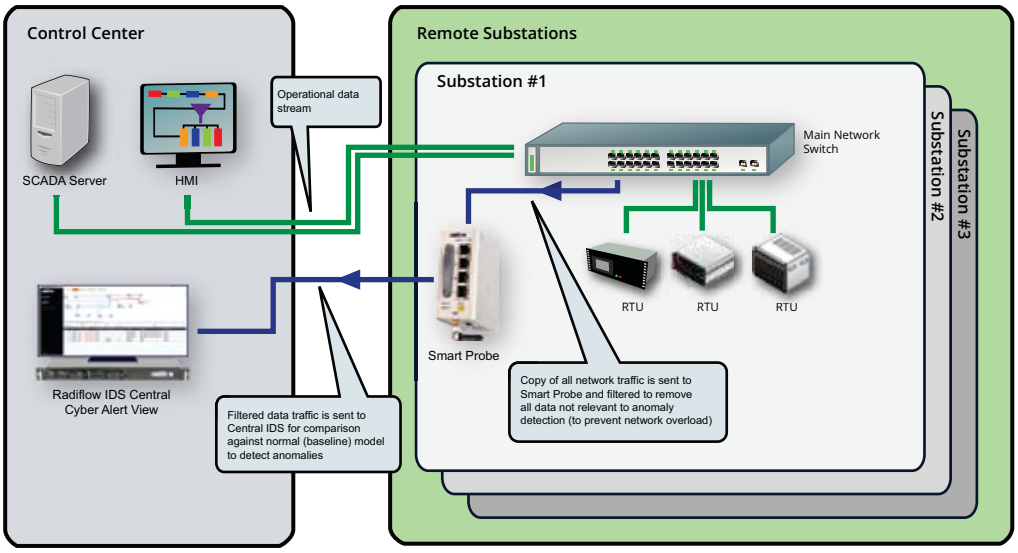

Diagram #2: iSID installed at central location

THE SMART PROBE

Typically, IDSs are implemented as local systems, usually at large sites. Radiflow's Smart Probe enables implementing an IDS at a central location, for the purpose of monitoring multiple small remote sites.

This type of implementation would typically create a network overload problem, caused by the collection and sending of large volumes of data to the Central IDS. Radiflow's complimentary Smart Probe solves this problem: installed at each site, receives all LAN traffic from the local switch, using port mirroring. It then filters out much of the general traffic data, leaving intact the SCADA traffic (e.g. ModBus data).

To further prevent network overload, the Smart Probe compresses the data, and the compressed, filtered traffic is sent to the central iSID over VPN tunnels.

Use Cases	Functions
Technician on-site: an authorized technician connects to the ICS on-site network, to perform scheduled maintenance and PLC firmware upgrade.	• iSID is configured to recognize technician's activities during the predefined operations time window, for the devices under technician's operation. • No false alarms will raise during the technician's operation period, while operations outside of the maintenance boundaries will raise an alert.
Black energy (BE) Malware: Black Energy is an APT malware, with SCADA plugins. Active worldwide, it causes widespread electric grid disruption and power outages.	• iSID will explicitly identify and alert upon BE, based on its communication signature • iSID will detects any unauthorized SCADA commands issues by BE SCADA plugins • iSID will detect anomalies in the industrial process, caused by changes to authorized SCADA commands made by BE. • iSID will facilitate the identification of equipment infected by BE.
Unauthorized PLC configuration changes	• iSID will detect known protocol commands which affect PLC configuration • iSID will detect unknown commands outside of the boundaries of the allowed industrial model
SCADA server attack: the manipulation of a SCADA server's behavior by an outside attacker.	• iSID will detect and alerts upon changes in the industrial model, as implemented in the local network SCADA server. Such changes include anomalies in the sequence of SCADA commands set to the controllers, anomalies in the commands' timing and more.
Spyware: network scanning aimed at gaining information prior to executing an attack.	• iSID will detect attempts by spying malware to scan the network for SCADA devices such as PLCs and RTUs.
Man-in-the-Middle	• iSID will detect and alert upon rogue devices in the network impersonating a valid server, workstation or SCADA controller, by means of Mac or IP address theft.

Ordering Information

- RF–SEC-SERVER/100 – Standard license for 100 devices
- RF–SEC-SERVER/500 – Standard license for 500 devices
- RF–SEC-SERVER/1000 – Standard license for 1000 devices
- RF–SEC-A-SERVER/100 – Advanced license for 100 devices
- RF–SEC-A-SERVER/500 – Advanced license for 500 devices
- RF–SEC-A-SERVER/1000 – Advanced license for 1000 devices
- RF-2120T/48/ET11 - Smart Probe

Minimal Hardware Requirements

- CPU: Intel i7 Quad-Core
- RAM: 16GB DDR4
- Hard Drive: 512GB
- 3 x Network Interface Cards (NIC), preferably supporting DPDK technology.
- Operating System: CentOS

The Standard license includes the following packages: Network Visibility, Cyber Attacks and Policy Monitoring.

The Advanced licenses add-on top of the standard license the following packages: Maintenance Management, Anomaly Detection and Operational Behavior.

Note: The Operational Behavior package will be officially released by December 2016.

Headquarters:
31 HaBarzel St.
Tel Aviv 6971045, Israel

North America:
900 Corporate Dr
Mahwah, NJ 07430

info@radiflow.com
www.radiflow.com

radiflow
Secure Your Assets