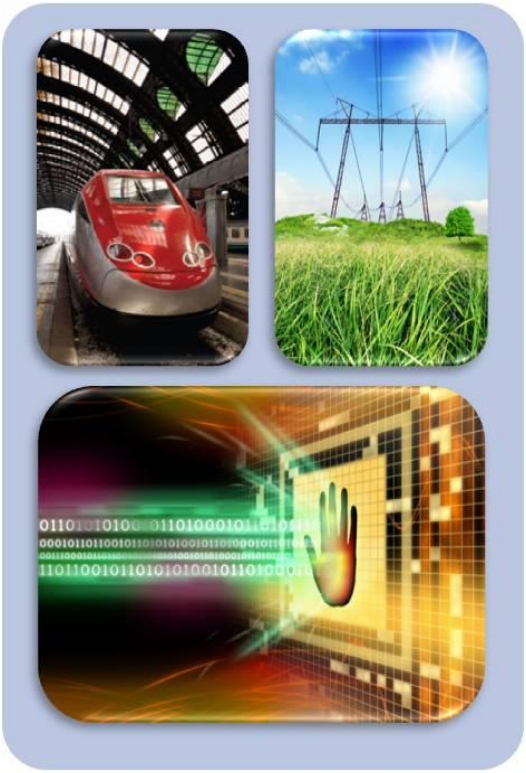
radiflow
Secure your Assets

Secure Networking for Critical Infrastructure

Using Service-aware switches for Defense-in-Depth deployment



June, 2012

radiflow
Secure your Assets

Introduction

The proliferation of Ethernet as the main infrastructure for mission-critical SCADA applications is raising the concerns about the vulnerability of these networks to cyber security threats.

The case of the Stuxnet malware, initially reported in July 2010, was the first known malware specifically designed to damage industrial automation equipment. The Stuxnet malware was infecting computers with Siemens Step7 industrial control systems (ICS) via the USB memory device and via the network. Once infecting such a computer the malware was targeting Simatic programmable logic controllers (PLC) to modify their software in a way that damaged the overall production-line operation in a discrete way over time.

The Stuxnet case raised the awareness for the vulnerability of industrial control systems (ICS) to cyber attacks in general. An area of major concern in this respect are the nation-wide critical infrastructure applications that deploy SCADA systems over distributed Ethernet networks.

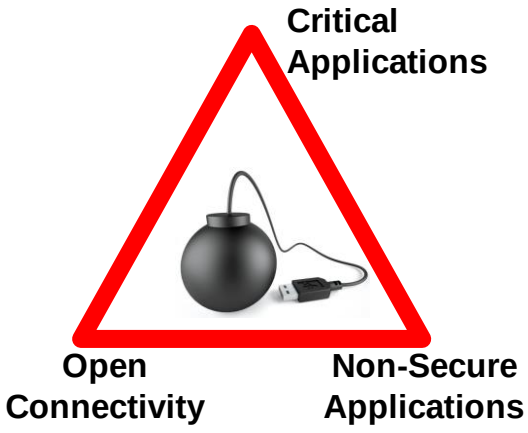
According to a report from 2009 in the Wall Street Journal, US intelligence officials stated that cyber-spies repeatedly gained access to the national electrical grid and left behind software programs that can be later used to disrupt the system. Furthermore an experiment from 2007 showed hacking into the replica of a power plant control system causing the generator to self-destruct due to changes made in its operating cycle.

A real-life example happened in Maroochy Shire Council's sewerage system in Australia in 2000. A dissatisfied sub-contractor engineer accessed the Maroochy Sewerage SCADA System remotely with a radio equipment and modified the operation of the sewerage pumping stations. The sub-contractor accessed the system multiple times over 3 months causing 800,000 liters of raw sewage to spill out into local parks and rivers.

The migration of the SCADA applications from proprietary local connectivity to an open standard network introduces new cyber security vulnerabilities and significantly increases the risk for a cyber attack. Recently it has become clear that such cyber security vulnerabilities in the critical services of the country are turning into high-profile targets for hostile organizations. The result is a new area in cyber security named APT (Advanced Persistent Threats) which handles long-term penetration attempts by resourceful organized groups or nations.

The common network security concept for utilities is based on the setup of a private network which is not connected to the Enterprise network or to the Internet. The access of the end-devices to this private network is controlled using device authentication methods from the enterprise world (MAC address, IP address or IEEE802.1x certificate).

However the deployment of simple end-devices using non-secure SCADA protocols in small unmanned sites, creates the risk of a physical penetration to such a remote site followed by the activation of a malware that damages the operation of other remote devices over the network.



In view of the above situation analysis, it's clear that new specific utility-oriented security solutions need to be defined and implemented in such deployments.

Distributed SCADA security

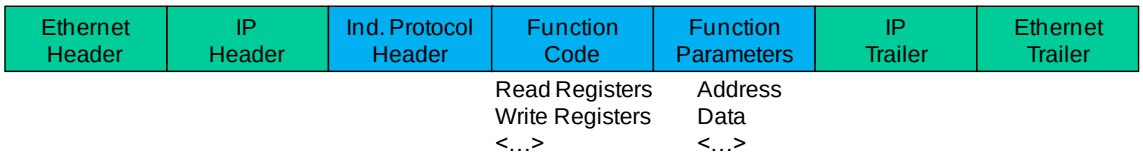
The best solution would be the migration in all the end-points to a secure SCADA protocol with strict authentication and authorization mechanisms that verifies the validity of the commands received by each device from its remote peers. Unfortunately the development of such a solution and even further the migration of all installations to use it is a long-term process.

In view of the critical nature of the SCADA applications an alternative network-based security solution should be deployed protecting the end-devices from an insider attack. Such as equivalent alternative is to deploy a personal SCADA firewall next to each end-device that will monitor the detailed SCADA communication flow. The resulting network-wide distributed IPS (Intrusion Prevention System) deployment will monitor all the critical SCADA traffic in the network and detect any abnormal behavior compared to the valid application logic.

Radiflow offers a unique patent-pending solution for such a distributed service-aware deployment in SCADA networks using its service-aware ruggedized switches. ***Radiflow*** switches contain a powerful co-processor dedicated for the processing of SCADA protocols with an optimized internal link to the system traffic switching core so that selected traffic can be re-directed to the co-processor for further processing.

Using such built-in protocol processing capabilities in the ***Radiflow*** switch in every utility site, **a SCADA firewall is automatically deployed next to each end-device.**

Furthermore the ***Radiflow*** switches support both Ethernet and Serial-based interfaces so that legacy devices can be connected to the network as well. For such serial-based traffic flows the same SCADA firewall processing is performed so that **serial-based SCADA sessions carried over Ethernet tunnels are also protected against such insider attacks.**



The service-aware firewall checks each packet in details including:

- ☑ Protocol validity – Check that the packet structure and all its control fields comply to the standard and that the session flow follows the expected logic (i.e. session initiated by master, response matches request, session setup sequence, etc.).
- ☑ Application logic – Per each pair of source and destination devices verify that only the allowed communication is performed by checking the function code and the command parameters according to the operator defined values.
- ☑ Abnormal patterns – Monitor the communication per devices searching for abnormal application behavior such as repetitive usage of specific sensitive commands (reset, clear history, etc.), burst of traffic beyond a reasonable threshold, etc.
- ☑ Violation processing – Once an abnormal behavior is detected the operator will be notified and the violating packet can be optionally dropped.

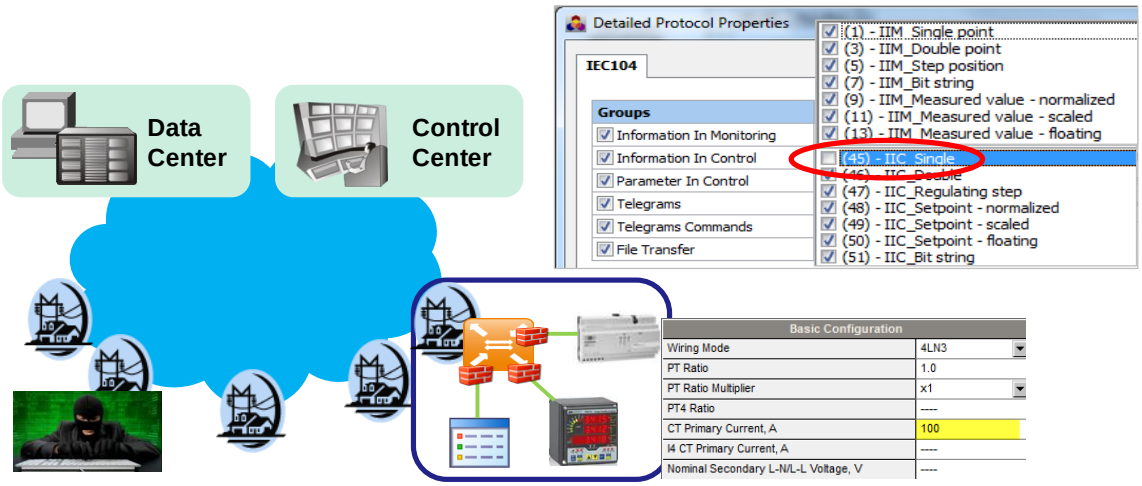
When deploying such a detailed network-wide security solution the provisioning task is becoming quite tedious and error-prone. To address this issue the distributed SCADA firewalls in the switches are complemented with a service-management tool named iSIM, that enables the **intuitive provisioning of the network-wide valid application logic and automatically translates it to the specific firewall rules for each switch.**

This security events log in the management tool also assists the operator with an **auto-learning process of the actual service flows in the network** by presenting all the security violation packets with a proposal how to resolve each violation with a new security rule that will be added to the valid security configuration.

The integrated security mechanism in the *Radiflow* switches and the iSIM management tool enables the efficient deployment of a distributed SCADA security solution in the network.

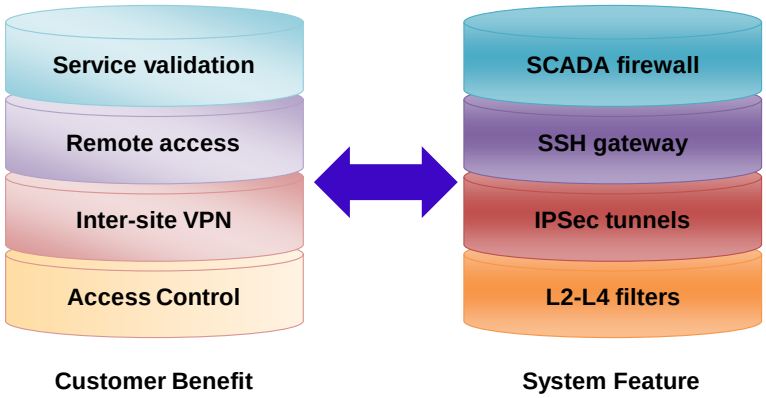
The example is the drawing below shows a smart-grid site with a power measurement device which is controlled using IEC104 protocol. Using the ***Radiflow*** distributed SCADA firewall The IEC104 sessions from other remote sites are limited only to monitoring commands while the control center can also issue configuration commands.

As a result when an attacker that penetrates a remote site and tries to re-configure the SCADA devices in other sites, the abnormal behavior is detected by the firewall and the attack is blocked.



Radiflow Defense-in-Depth tool-set

In addition to the SCADA firewall, ***Radiflow*** switches provide a comprehensive security tool-set so that a complete defense-in-depth solution can be deployed in the network without adding dedicated security appliances on-top of the Ethernet infrastructure.



Network Access Control

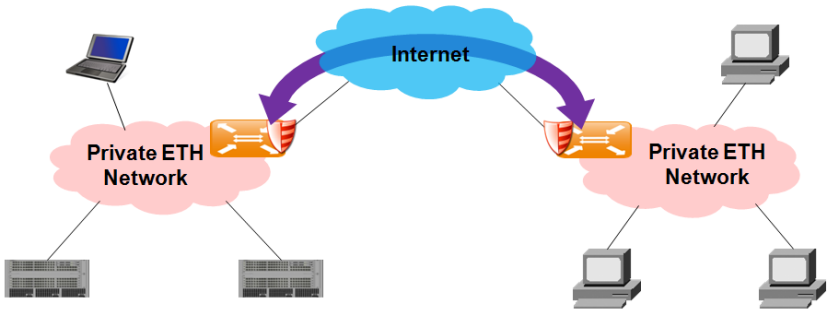
The connection of the end-devices to the network is controlled based on their physical authentication so that per network port only specific devices can be connected. This basic level of security is achieved by authentication of the entities connected to the ***Radiflow*** switches in 2 possible ways:

- ☑ The configuration of ACL (Access List) rules per port to allow only devices with specific MAC addresses or IP addresses to be connected to this port.
- ☑ User authentication using IEEE 802.1x protocol in which the switch passes the authentication request from the end-device to a central RADIUS server to verify it's access rights before opening this port for regular traffic.

Inter-site VPN

In some cases a distributed utility network uses public transport links to connect between the sites. For example in case of a smart-grid application some of the transformation sites connect using cellular modems.

When the inter-site connectivity uses such a public infrastructure, the traffic must be encrypted to ensure its confidentiality and its integrity against potential man-in-the-middle attacks.



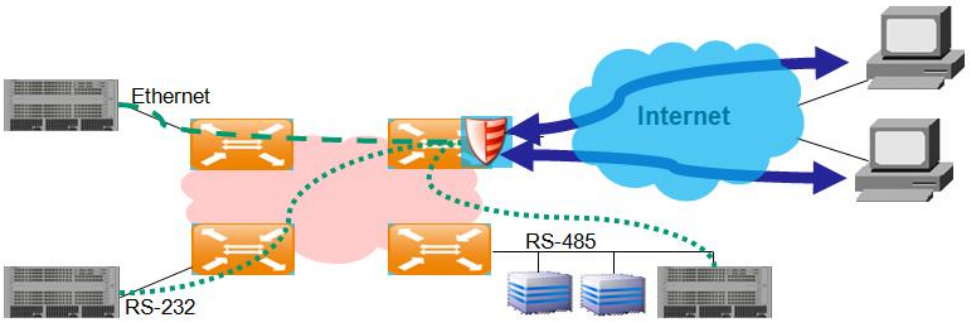
Such a VPN (Virtual Private Network) connection is supported by the ***Radiflow*** switches using GRE tunnels over an IPSec encrypted link. The GRE tunnels can be used in transparent Ethernet mode to create a L2 VPN or in DMVPN mode to create a L3VPN. For example when the network used VLANs to identify the services the L2 GRE tunnel preserves the VLAN information while a L3 VPN tunnel would strip the VLAN information and pass only the IP data.

Secure Remote Access

When a remote user needs to access a secure network for operational or maintenance tasks, it's critical to ensure that only the limited set of authorized activities are enabled and are performed in a strict secure manner. Since this remote access is done by an individual from an unknown location a VPN connection as described above it too risky and a more controlled tunnel with limited access rights should be used.

The ***Radiflow*** switches contain a SSH server to enable such limited remote access for operation and maintenance. As such the communication channel between the remote user and the switch is SSH-encrypted. Furthermore for strict security sites the SSH session can also be limited to be initiated by the server from the secure site outbound using reverse-SSH. After the SSH tunnel is created, the access is controlled per user login authentication and specific access authorizations which are configured either locally in the switch or retrieved from a central RADIUS server.

Originally SSH was planned as a secure terminal but it's now used as a secure transport for any IP-based session. As a result the SSH gateway is used for secure remote access for any protocol with a simple re-route of the traffic in the remote computer to a local-host that is encapsulated over the secure SSH tunnel to the secure network. In this setup the switch acts as a proxy in the session so that the local network structure in the secure site is not exposed externally and further on-line security checks are performed similar to the functionality of the SCADA firewall.



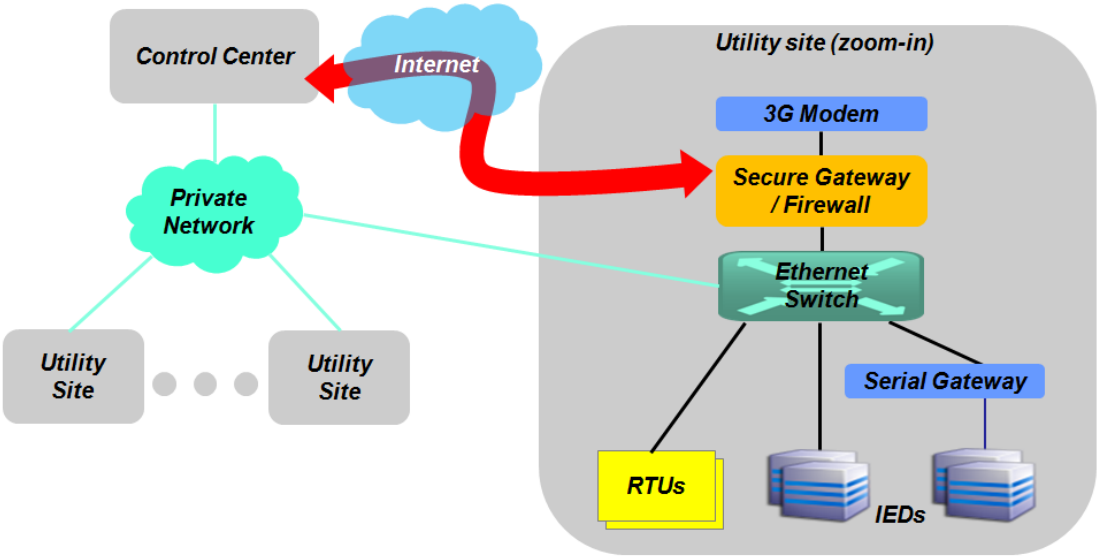
SCADA Firewall

As described above ***Radiflow*** switches contain an integrated firewall on each port, providing a network-based distributed security solution equivalent to the use of personal firewalls on all the SCADA devices in the network.

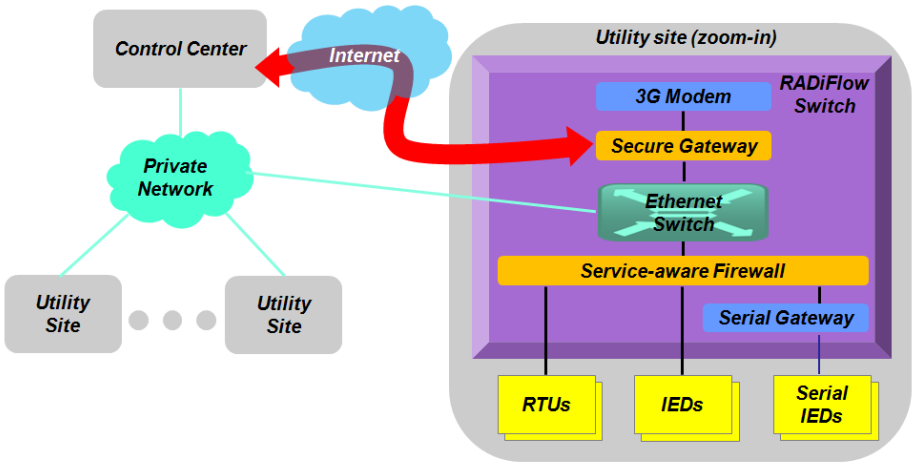
Such a distributed deployment of service-aware firewalls is used to validate the application logic as it's represented in the communication flow between all devices in the network.

Application example

The *Radiflow* service-aware Industrial Ethernet switches provide an extensive feature-set to enable deployment of a simple yet secure network solution for a wide variety of SCADA application topologies.
A nation-wide utility has many distributed sites which needs to be inter-connected. Such a typical site would include an Ethernet switch, Serial gateways to connect the legacy devices and optionally a 3G cellular modem in case of a remote site outside the reach of the utility private network. Furthermore as discussed above for a proper security solution an SCADA firewall should monitor all the traffic to the devices and a secure VPN gateway should encrypt the data flowing over the public cellular network.



Using the ***Radiflow*** service-aware switch this site can be greatly simplified using the integrated functions of the switch including the serial gateway, service-aware firewall, IPSec VPN gateway and a 3G modem.

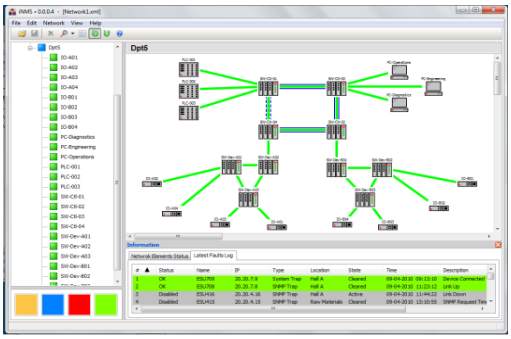


Conclusion: Why Radiflow?

The increasing usage of distributed Ethernet networks in critical infrastructure applications raises the concern from cyber security threats that can damage basic national services. As a result there is a clear need for a comprehensive defense-in-depth solution dedicated for the SCADA networks while keeping the overall network design simple.

Radiflow provides a unique solution with a SCADA firewall engine integrated in its Industrial-Ethernet switches which is the basis for an easy deployment of strict security measures throughout the internal communication network.

Furthermore the ***Radiflow*** portfolio offers switches in several form factors with a modular multi-service architecture that supports the evolution of the network with legacy serial-based and Ethernet device and a growing need of Ethernet ports and bandwidth.
The complete ***Radiflow*** solution is complemented by the iSIM service management tool to support the easy operation and maintenance of the network.



The resulting network design is a secure yet cost-effective solution that enables the deployment of Ethernet networks as the basis for critical infrastructure applications.

For more information about ***Radiflow*** products

email: info@radiflow.com

web: http://www.radiflow.com