CHECK POINT + RAD
ROBUST CYBER SECURITY FOR POWER UTILITIES

Benefits

- Enable compliance with NERC-CIP directives
- Protect OT networks by eliminating RTU and SCADA equipment vulnerabilities
- Deep visibility and control of ICS/SCADA communications
- Secure remote access into OT networks

INSIGHTS

Industrial Control Systems (ICS) and protocols in power utility control networks – also known as operational technology (OT) networks – were primarily designed with operational safety and reliability in mind. Security was not considered a top priority and, at best, any defense employed followed the “Security by Obscurity” philosophy. These days, however, critical infrastructure networks become smarter, automated and more connected – and are more susceptible than ever to cyber threats. They are subjected to hundreds, sometimes thousands of cyber-attacks per day. With so much on the line, even the smallest breach in security could spell disaster. As a result, the security of critical networks is at the center of attention of industry and government regulators alike. The first binding regulation was the set of requirements for critical infrastructure protection (CIP), which was introduced in 2008 by the North American Electric Reliability Council (NERC). Since then, the NERC CIP set of requirements have been constantly evolving to make sure power utilities are well equipped to meet new threats.

BOOST YOUR NERC-CIP COMPLIANCE

Check Point and RAD offer a joint end-to-end cyber security solution that protects any utility OT network by eliminating RTU and SCADA equipment vulnerabilities, as well as defends against cyber-attacks on the network’s control and data planes. The solution meets the following NERC-CIP requirements:

1) Malicious Communications Detection (CIP-005-5, CIP-007-5)
2) Device Connection Control (CIP-007-5)
3) Secure Interactive Remote Access – Intermediate System (CIP-005-5)
4) Patch management (CIP-007-5)
5) ”Man in the Middle” (MITM) attack prevention (expected in NERC-CIP v6)
6) Logging (CIP-007-5)

The solution integrates Check Point’s ICS Security Gateway within RAD’s secure-by-design multiservice networking equipment and consists of various building blocks as described in Figure 1:

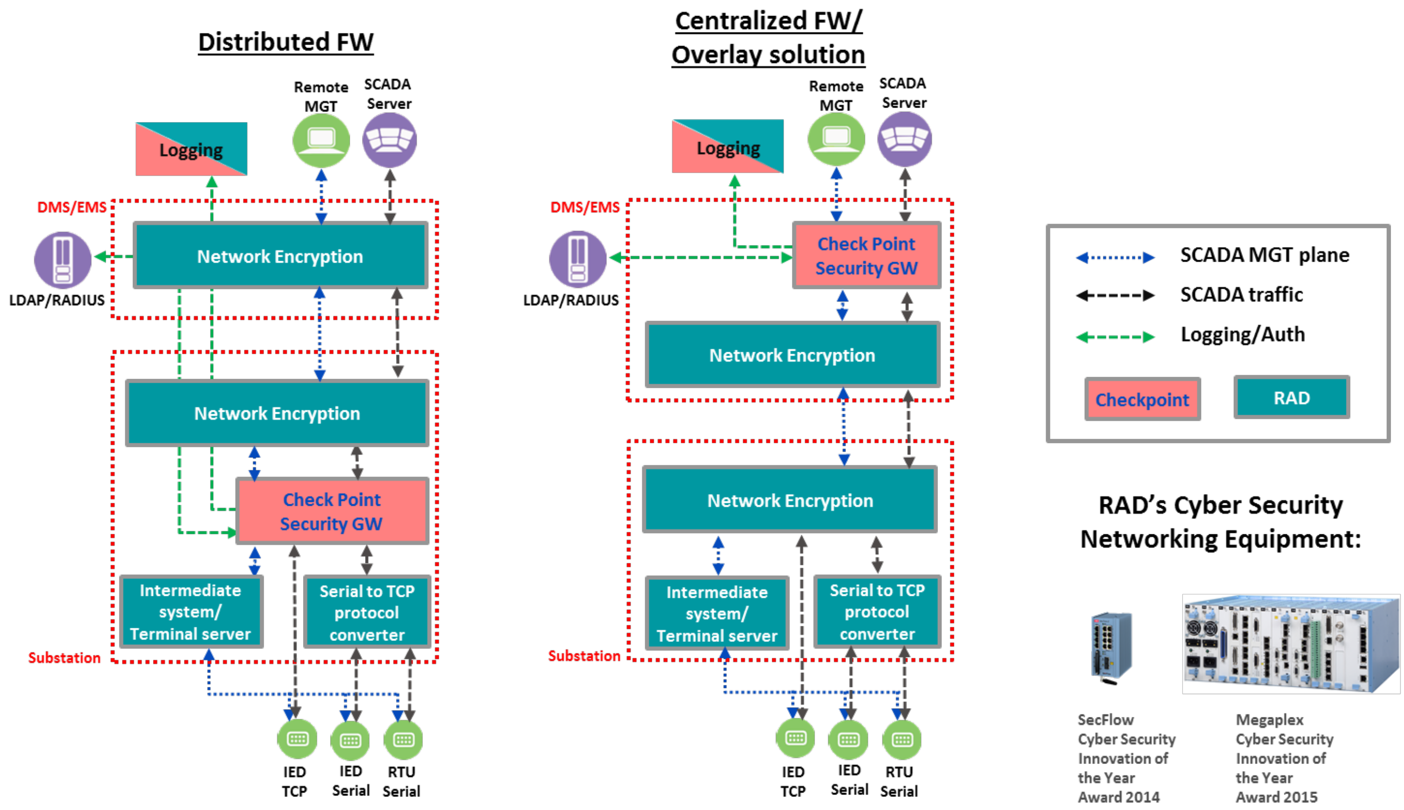

Figure 1: building blocks of the Check Point-RAD cyber security solution

- Overlay solution, adds a cyber security layer (NERC-CIP-compliant) to any existing ICS/SCADA OT network.
- RAD's secure-by design multiservice networking platforms handle various SCADA protocols, serial and TCP-based, from different SCADA devices. Serial to TCP protocol conversion is optional, depending on the utility's current and future topologies and needs. RAD's networking equipment employ Device Connection Control (802.1x) with the option to disable all unused ports to prevent connection of rogue devices or unauthorized users.
- Check Point's ICS Security Gateway software is fully integrated in RAD's Megaplex-4 multiservice platform and can be installed in any substation/"tail site" or control center, in distributed or centralized topologies. The ICS Security Gateway includes firewall, application control (APCL), intrusion prevention (IPS), and VPN software blades and provides deep packet inspection (DPI) for SCADA communications, virtual patching and logging for inbound and outbound traffic.
- An Intermediate System for Interactive Remote Access is uniquely combined with a built-in terminal server, allowing secure control of IP and serial (RS-232/RS-485) SCADA devices. This powerful combination further includes tunneling, data encryption, multi-factor user authentication, and authorization to manage only predefined SCADA devices.
- An integral part of RAD's end-to-end cyber security solution is network encryption, allowing the utility to protect from "Man-in-the-Middle" attacks using IPsec (Layer 3 encryption) and MACsec (Layer 2 encryption) tunnels, depending on the OT network.
- Check Point's logging server (SmartEvent), as well as a Syslog server collect and logs events from the Intermediate System and from the ICS Security Gateway.
- Network management is performed by the RADview and Check Point systems. Management of the security features is separated from that of the networking features, providing discrete administrative authority to technicians and other relevant personnel.

CONCLUSION

The joint Check Point-RAD cyber security solution for power utilities' OT networks provides the ultimate, multi-tier protection to enable optimal compliance with the new NERC-CIP directives. It is strategically located to securely manage all electronic access to the substation's electronic security perimeter (ESP) and to protect the cyber assets within it from external and internal attacks. Power utilities are provided a full suite of cyber security defenses, including encryption, authentication, intrusion prevention, anomaly detection, integrity verification, and more.

ABOUT CHECK POINT

Check Point Software Technologies Ltd. (www.checkpoint.com), is the largest pure-play security vendor globally, provides industry-leading solutions, and protects customers from cyberattacks with an unmatched catch rate of malware and other types of attacks. Check Point offers a complete security architecture defending enterprises' networks to mobile devices, in addition to the most comprehensive and intuitive security management. Check Point protects over 100,000 organizations of all sizes. At Check Point, we secure the future.

ABOUT RAD

RAD (www.rad.com) is a leader in secure communications solutions for the critical infrastructure of power utilities and other segments of the energy industry. Our Service Assured Networking solutions include best-of-breed tools for cyber security and mission-critical communications, as well as for seamless migration to modern packet switched networks and applications. RAD provides field-proven solutions for operational WAN, ruggedized substation LAN, automation backhaul, Tele-protection, wireless PTP/PTMP, and broadband mobility. Founded in 1981, RAD has an installed base of more than 14 million units and is a member of the $1.25 billion RAD Group of companies, a world leader in communications solutions.