FORTINET

WHITE PAPER

Securing ICS Infrastructure for NERC Compliance and beyond

The Fortinet Security Solution for ICS

Table of Contents

Introduction

System downtime, data loss, and facility control breakdowns quickly become business critical issues for Utilities and their customers. The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Cyber Security Standards (CIP 002 through 009) define reliability requirements to help address these Cyber Security Vulnerability issues for Bulk Power System owners, operators and users in North America and Canada. NERC violations may lead to costly sanctions and remedial action directives that must be immediately addressed. Moreover, NERC can assess fines of up to a million dollars a day per violation. With oversight by the U.S. Federal Energy Regulatory Commission (FERC) and Canada's National Energy Board (NEB), cyber security standard compliance has become an increasing priority for the power utility industry.

FERC enforcement of the NERC guidelines also apply to Canadian power generators wishing to export power to the US.

A few strategic cyber security investments at the network and application layers can significantly simplify NERC compliance while bringing more security to the environment. This paper outlines a better way to secure ICS Infrastructure by leveraging a Unified Threat Management (UTM) approach that supports critical NERC compliance criteria, while maintaining high performance metrics – without calling for replacement of the entire infrastructure.

Network Security Challenges for Bulk Power Systems

The challenge for Bulk Power Systems is to meet or exceed security compliance standards to thwart potential attacks on the network, thereby contributing to grid reliability, while balancing performance and total cost of ownership (TCO) interests. Today's Utilities need to be vigilant against both intentional and unintentional insider threats from current and former employees and contractors, as well as outsider threats from hackers and cyber terrorists.

Real-World Security Vulnerabilities

The need for effective network and application security has been underscored by real-world industry assessments. To help raise visibility to this important issue, the U. S. General Accountability Office (GAO) issued a related report in May 2008 in partnership with Tennessee Valley Authority (TVA), a wholly owned government corporation which supplies power to 8.7 million US residents in seven states. The report found: "On control systems networks, firewalls reviewed were either inadequately configured or had been bypassed, passwords were not effectively implemented, logging of certain activity was limited, configuration management policies for control systems software were inconsistently implemented, and servers and workstations lacked key patches and effective virus protection."

Similarly, a replica power plant control system was hacked causing a power generator to self-destruct in the "Aurora" experimental cyber attack conducted in March 2007 at the Department of Energy's Idaho Lab. Some experts suggested that such an attack done on a broader scale could have taken months to repair.

End point security is also relevant. In one case the Nuclear and Industrial Safety Agency reported that data leaked from an employee's PC, from a virus likely contracted via peer-to-peer file-sharing, exposed reports on safety inspections and sensitive data on the operational status of nuclear plants in Fukui, Niigata, Shizuoka and Kagoshima prefectures.

Managing Compliance for NERC CIP Audits

NERC offers a consistent framework for security control perimeters and access management with incident reporting and recovery for Critical Cyber Assets (CCAs). A CCA is most simply defined as a device that connects to a control center or other facility outside the substation perimeter using non-dedicated IP-based resources. Approaching network security requirements for these Critical Cyber Asset's with a unified threat management approach can save time and reduce complexity.

CIP	DESCRIPTION	SUMMARY
NERC CIP-002-1	Critical Cyber Asset Identification	Requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System
NERC CIP-003-1	Security Management Controls	Requires that responsible entities have minimum security management controls in place to protect Critical Cyber Assets
NERC CIP-004-1	Personnel and Training	Requires that personnel with authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness.
NERC CIP-005-1	Electronic Security Perimeter(s)	Requires the identification and protection of the Electronic Security Perimeters inside which all Critical Cyber Assets reside, as well as all access points on the perimeter
NERC CIP-006-1	Physical Security of Critical Cyber Assets	Addresses implementation of a physical security program for the protection of Critical Cyber Assets
NERC CIP-007-1	Systems Security Management	Requires responsible entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeters
NERC CIP-008-1	Incident Reporting and Response Planning	Ensures the identification, classification, response, and reporting of cyber-security incidents related to Critical Cyber Assets
NERC CIP-009-1	Recovery Plans for Critical Cyber Assets	Ensures that recovery plans are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices

Section CIP-005 is most applicable to network security. Accordingly, at a minimum all network connections across the perimeter must have a firewall properly configured so only authorized traffic and connections are permitted within the secured zone. This requirement includes IP address-based packet filtering, TCP and UDP transport layer inspection, and review of application layer traffic. Also, Bulk Power System providers and related entities must identify and secure physical and software-defined ports to devices and applications within the electronic perimeter of their networks, and authenticate based on defined groups to only required ports and services. Encrypted virtual private network (VPN) connections may also be required when public or shared IP services are used. It also call for detecting known or suspected malicious communications.

Accountability and auditability are key elements of all NERC requirements. Specifically for NERC CIP-008-1, network security reporting and monitoring at multiple layers and on an end-to-end basis are important components of any compliancy program, e.g., logging and alerting for periodic audits or real-time analysis – especially when IP protocols are at issue.

A Unified Threat Management Approach

To meet NERC compliance guidelines and protect control systems, Utilities need 5 key network security components.

1. Firewall to establish a secure perimeter and to Segment internal networks
2. Secure remote access using VPN
3. Antivirus protection within the network
4. Intrusion Prevention System (IPS) within the network
5. Strong Group-based Authentication capabilities

Organizations need to put in mitigating controls by isolating hosts away from one another or from operator PCs, for instance, by applying segmentation of inside perimeters with isolation technologies. Additionally, since some facilities are in extremely remote locations with little or no permanent staff, out-of-band access is required to resolve problems when in-band access has failed. While in some instances use of a firewall to completely elminating dial-up modems may be appropriate, other times providers need to focus on increasing the security of any dial-up modem based solutions. NERC CIPs also consider scenarios in which antivirus cannot be implemented within a host. Risks often cannot be mitigated by installing protection on the host devices themselves. Even if they could, some of the host system Operating Systems may no longer be supported by the host based security solutions. For instance, end point solutions like some Supervisory Control And Data Acquisition (SCADA) programmable logic controllers (PLCs), commonly used by Utilities to automatically control various industrial processes, will not allow antivirus to run within the host. Instead antivirus must be applied within the network.

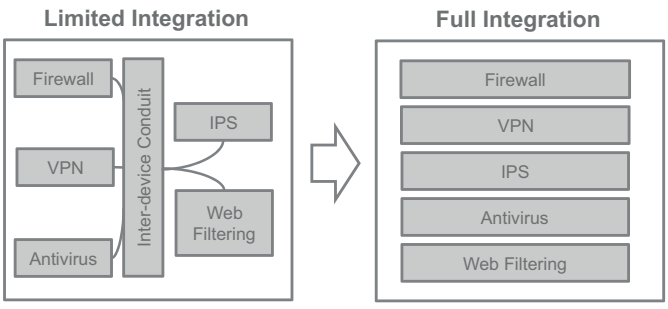

FIGURE 1: COMPARING SOLUTIONS

It is clear that CIPs call for a firewall to establish security perimeters, network segmentation and group-based authentication, as well as implementation of antivirus controls and intrusion prevention systems (IPS). The deployment of these types of technologies in single point products may amount to six or more separate security devices, which may prove cost prohibitive to the utility producer. Point product solutions can be difficult to manage, requiring multiple management interfaces, with no integration between vendors, and no single vendor for issue resolution. Point products are expensive to deploy and maintain with multiple vendor contracts and renewal schedules, costly support licensing, data resource allocation (power, rack space, cooling), and multiple inspection steps that may tax network performance. Furthermore, lack of integration may lead to reduced security. Since ICS need to be readily available at all times, availability of these systems is one of the most critical aspects of any secure network architecture. Therefore, the deployed solutions in most circumstances would be configured in a high-availability scenario, further increasing complexity and costs.

Unified Threat Management (UTM) platforms, also called "Next Generation Firewalls," expand on traditional firewalls to incorporate these additional complementary security technologies. UTM platforms are defined by International Data Corporation (IDC) to minimally include firewall, VPN, intrusion prevention and antivirus features. While it is difficult to manage six or more different point product security devices with limited integration in a network that has to be highly available, a streamlined UTM platform running in high availability mode protects control systems more efficiently – while covering those 5 key network security components necessary for NERC compliance. A UTM approach reduces the number of vendors and appliances, provides comprehensive security, minimizes down-time from individual threats, simplifies security management, improves detection capabilities, and coordinates security alerting, logging, and reporting.

The Fortinet Solution

Fortinet provides UTM platforms that deliver high-performance and best-of-breed network security through FortiGate™ appliances. The appliances come in different capacity and form factors yet run on a consistent OS which provide similar features and management UI. This allows customer the ability to enjoy the flexibility of deploy appropriate systems according to their needs while at the same time, reduces cost and complexities managing them.

FortiGate Rugged-Series is an cost effective UTM solution with

specialized hardware that meets the demanding environmental conditions in remote premises while larger high performance FortiGates, powered by unique ACISs are most suitable for aggregating VPN connectivity at the centralized data center. FortiASIC content and network processors offloads CPU from heavy computations such as cryptographic activities and traffic matching.

FortiOS provides well-proven security functions in the system. Fortinet's strong commitment to independent certification helps to ensure validated security functionality. The unified approach allows for comprehensive security reporting with output log/report information in a common format – a core component for any large organization.

NERC Compliance with Fortinet

Fortinet completes a thorough assessment of a Bulk Power Systems provider's current NERC compliance network security implementations, and then proposes a streamlined solution specific to customer need with a clear estimation of products and services for the project. The Fortinet Enterprise Solution for NERC Compliance consists of a complete package of products, professional services, technical account management and custom solutions training services.

NERC CIP SECTION	FORTINET SOLUTION (descriptor)	FORTINET SOLUTION (product)
CIP-002	Design architecture / Assessment	Fortinet Professional Services
CIP-003	Device and configuration management, workflow controls	FortiManager
CIP-004	Training	Fortinet Training Services
CIP-005	Establish electronic security perimeter	FortiGate with Optional FortiAP, FortiSwitch and FortiClient
CIP-006	Electronic protection of physical security assets	FortiRecorder and FortiCamera
CIP-007	Security systems management	Fortinet Technical Account Management
CIP-008	Monitoring & Incident reporting	FortiManager / FortiAnalyzer
CIP-009	Recovery plan and back up	FortiManager

NERC CIPs can be complex, with detailed configurations. Manual implementations without professional assistance can lead to excessive time consumption and error.

Fortinet Professional Services also provide a better way to secure Utility IT Infrastructures with the Design, Documentation, Implementation, and hands on education of an effective NERC compliance solution for network security, including Training Services Professional services and Custom Solutions Training and Certification Training. Product selection per design includes FortiGate, FortiManager and FortiAnalyzer to help automate the network security requirements and sub-requirements. Enterprise Technical Account Management and ongoing Technical Services – with a Service Level Agreement (SLA) directly from Fortinet – complete the package.

A typical Fortinet deployment scenario would include a FortiGate UTM platform set to high availability mode in the control center with FortiAnalyzer for logging and reporting, and FortiManager for centralized management. Separate size-appropriate FortiGate UTMs may secure remote offices and regional power facilities.

Fortinet addresses CIP-002 Critical Cyber Asset Identification in terms of design architecture and assessment. Specifically, Fortinet professional services designs or redesigns the networking solution with customer to only use routable protocols to communicate outside the Electronic Security Perimeter (R3.1) or within a control center (R3.2), e.g., OSPF, BGP, RIP, and PIM routable

protocols. This can also involve establishment of a routed design, elimination or increases security of dial-up connections (R3.3), and Access Control based on internal or contractor status, for instance.

FortiGate™ addresses CIP-005 by establishing an electronic perimeter around all identified Critical Cyber Assets. Key individual CIP sub- requirements including Access Control, Secure Authentication, Single Point of Entry issues, reporting and documentation are also satisfied.

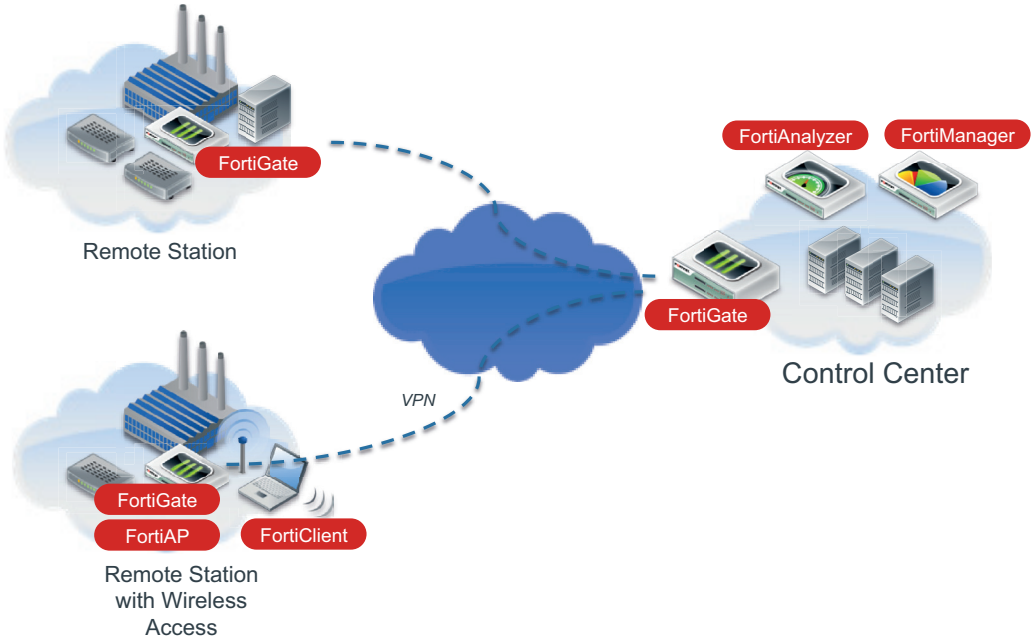

FIGURE 2: FORTINET SOLUTION FOR ICS

Going beyond Compliance Requirements

Fortinet Solution for ICS security goes beyond providing standard security capabilities and services. The unique FortiGate not only serves wired networks but also has wireless and endpoint controller capabilities. This bring huge security and cost benefits as no additional disjointed systems are required to provide wireless connectivity and onsite/remote user access. The FortiGate can connect to multiple rugged FortiAP access points that connect wireless equipment securely. Field engineers may also connect through the wireless networks while the FortiGate ensures that appropriate terminals with FortiClient operating and correct user credentials are allowed access.

Summary

Achieving NERC compliance for Bulk Power Systems' control and monitoring systems delivers increases in the reliable generation and distribution of energy. UTM solutions like FortiGate™ that employ custom ASIC-based processing hardware are now able to accommodate high-speed networks, such as internal network segments, and are able to secure and process traffic as close to line rate as possible. In order to achieve the most benefit and offer the highest levels of security effectiveness and efficiency, complete integration of specialized hardware with the software and security content is essential. Fortinet simplifies network security compliance without sacrificing performance. Moreover, with FortiGate's extended wireless and endpoint solutions, utility providers will gain further cost and security benefits.

Reference:

Barbara A. Connors, B. (2007). Commission approves NERC's assignment of violation risk factors associated with approved reliability standards. FERC Docket Nos: RR07-9-000 and RR07-10-000. Retrieved November 6, 2008, from http://www.ferc.gov/news/news-releases/2007/2007-2/05-17-07-E-8.asp

"Report to Congressional Requesters: TVA Needs to Address Weaknesses in Control Systems and Networks" (May 2008). Document GAO-08-526. U.S. Government Accountability Office. Retrieved November 6, 2008, from http://www.gao.gov/new.items/d08526.pdf

Jeanne Meserve, "Mouse click could plunge city into darkness, experts say" (September 2007). CNN. Available at http://www.cnn.com/2007/US/09/27/power.at.risk/index.html?eref=rss_topstories (last visited November 6, 2008).

"Nuclear Power Plant Data Leaked Via Virus-Infected PC, Posted on Net" (2005). Kyodo News International (RedOrbit). Retrieved November 6, 2008, from http://www.redorbit.com/news/science/183189/nuclear_power_plant_data_leaked_via_virusinfected_pc_posted_on/

Bernard Woodall (2008). "U.S. electricity watchdog issues first violations" (June 2008). Reuters. Retrieved on November 13, 2008, from http://uk.reuters.com/article/rbssIndustryMaterialsUtilitiesNews/idUKN0431655020080604

"Idaho utility hard drives -- and data -- turn up on eBay" (2006). Computerworld. Retried on November 17, 2008, from http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=Energy/Utilities&articleId=111148&taxonomyId=129&intsrc= kc_li_story

"Ponemon Report Shows Sharp Rise in the Cost of Data Breaches" (2006). Ponemon Institute. Retrieved on November 17, 2008, from http://www.ponemon.org/press/Ponemon_2006%20Data%20Breach%20Cost_FINAL.pdf

Metz, C. (1998). IP Routers: New Tool for Gigabit Networking. IEEE Internet Computing, 2(6), 14-18. IEEE (1997). Firewalls: An Expert Roundtable. IEEE Software, 14(5), 60-66.

Gleeson, B., Lin, A., Heinanen, J., Armitage, G., Malis. A. (2000). A Framework for IP Based Virtual Private Networks. Networking Working Group. Retrieved April 23, 2008, from http://www.ietf.org/rfc rfc2764.txt

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA SALES OFFICE
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480