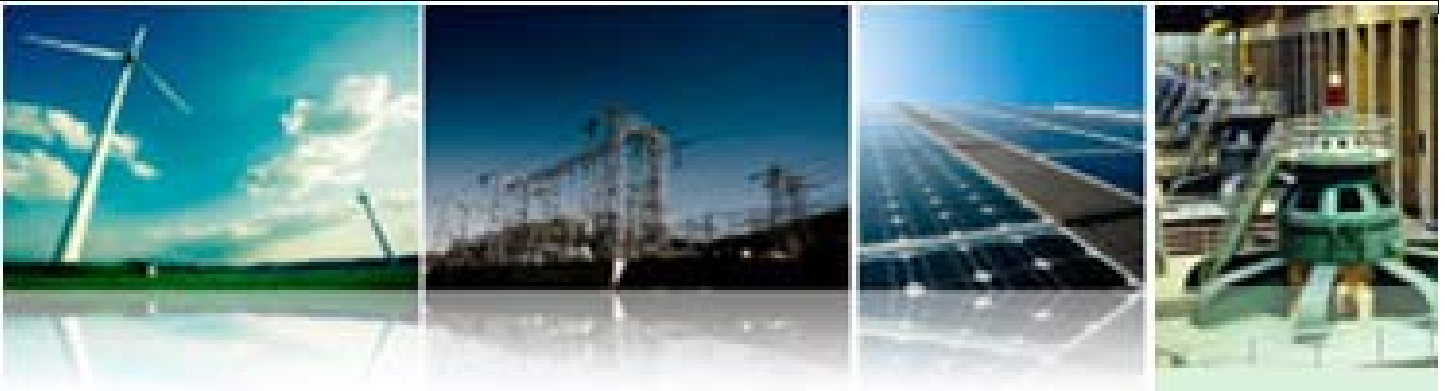


# A Better Way to Secure Utility IT Infrastructure – NERC Compliance for Bulk Power Systems

White  
Paper



Vertical Security Solutions

**FORTINET**®

## 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. This paper outlines a better way to secure Utility Information Technology (IT) Infrastructure by leveraging a Unified Threat Management (UTM) approach and Vulnerability Assessment (VA) strategy 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. In addition to issues for operational data, there may also be database vulnerabilities in customer information, billing and financial systems.

### *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." Also, the intrusion detection system had significant limitations, some workstations on the corporate network had had inadequate security settings or were missing key software patches, and a number of network infrastructure devices had limited or ineffective security configurations.

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. Database vulnerability related issues have grown in importance as well. Idaho Power Co., serving approximately 460,000 customers, got a scare when data from approximately 230 SCSI drives containing customer correspondence and other proprietary information was breached in 2006. Although this breach was a case of physical security policy, database breach costs have risen to nearly \$200/record, with nearly 150 Million database records lost between 2005-07 in the U.S. alone.

### *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	identification and documentation of risk-based assessment methodology used to identify Critical Cyber Assets
NERC CIP-003-1	Security Management Controls	documentation and implementation of Cyber Security Policy reflecting commitment and ability to secure Critical Cyber Assets

NERC CIP-004-1	Personnel and Training	maintenance and documentation of security awareness programs to ensure personnel reinforcement on sound security practices
NERC CIP-005-1	Electronic Security Perimeter(s)	identification of Electronic Security Perimeters surrounding Critical Cyber Assets and all access points therein
NERC CIP-006-1	Physical Security of Critical Cyber Assets	creation and maintenance of a physical security plan, including processes, tools, and procedures to monitor perimeter access
NERC CIP-007-1	Systems Security Management	ensuring that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing Cyber Security Controls
NERC CIP-008-1	Incident Reporting and Response Planning	develop and maintain a Cyber Security Incident response plan that addresses classification, response actions and reporting
NERC CIP-009-1	Recovery Plans for Critical Cyber Assets	creation and review of recovery plans for Critical Cyber Assets

Figure 1: NERC Critical Infrastructure Protection (CIP) Table

Looking at CIPs 002 through 009, CIP-005 Electronic Security Perimeter(s) is most applicable to network security. According to CIP-005, 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 such as Telnet, HTTP, and HTTPS. Similarly, 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. And accountability and auditability are key elements of all NERC requirements. Thus, 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 phased time table sets out NERC compliance milestones based on entity type, with some required to complete the first implementation phase by June 2008, and others by June 2009 or June 2010: Begin Work (phase 1), Substantially Compliant (phase 2), Compliant (phase 3) and Auditably Compliant (phase 4). Although early fines have focused on vegetation issues, e.g., Baltimore Gas & Electric Co. (\$180,000 penalty) and MidAmerican Energy Co. (\$75,000 penalty), cyber security scrutiny is expected to ramp up along with compliance time tables.

## 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
2. **Segmentation** of inside perimeters with **Isolation Technologies**
3. **Antivirus** controls within the network
4. **Intrusion Prevention System (IPS)** within the network
5. **Strong Group-based Authentication** within the perimeter

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. Utilities also 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 eliminating dial-up modems may be appropriate, other times providers need to focus on increasing the security of any dial-up modem based solutions.

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 electrical 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 Utility control systems 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.

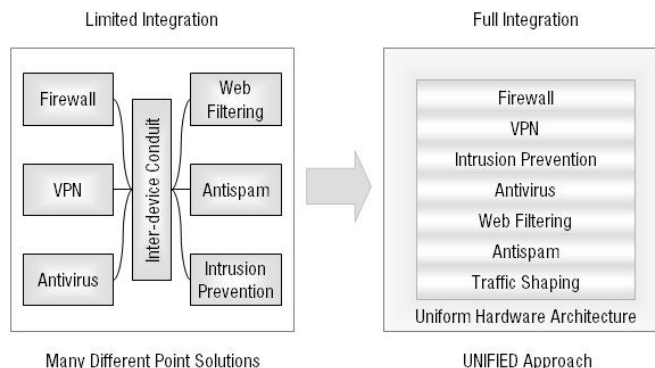


Figure 2: Point solutions vs. Unified threat management

### The Fortinet Solution

Fortinet provides a UTM platform delivering high-performance and best-of-breed network security through intelligent integration in FortiGate™ appliances with custom Application Specific Integrated Circuits (ASIC) based silicon processing hardware for high-speed networks. Fortinet contributes to the effective security and scalable performance provided by a UTM solution with specialized hardware, software, and evolving security content. 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.

ASIC content processors (specifically engineered to perform high-speed comparisons of objects to known threat patterns) implement only scanning logic in hardware, and are not used to store threat pattern data, which continue to be stored by memory. Therefore, updates for evolving threats remain as simple as an update to a software-only solution.

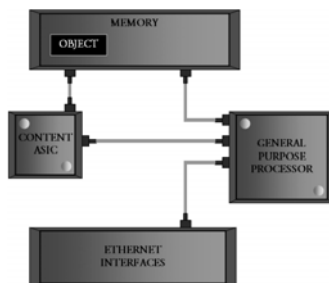


Figure 3: High-Level Architecture of a UTM System with an onboard Content Processor

Moreover, content processors can also contain cryptographic engines that relieve the general purpose processor from the high intensity calculations that take place during encrypted communications. Virtual Private Network (VPN) setup and key maintenance to secure remote connections for daily operations are particularly taxing on a system, making them ideal candidates for hardware acceleration with Fortinet in this manner. It is also important to note that instead of commercially off-the-shelf (COTS) technologies that may expose utilities to further vulnerabilities, the Fortinet approach uses a hardened FortiOS™ operating system for additional protection.

### 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.

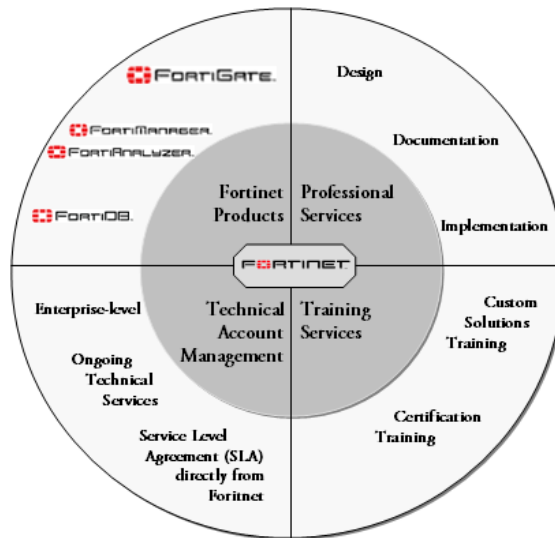


Figure 4: Fortinet custom solutions for NERC compliance

NERC CIPs can be complex, with detailed configurations. Manual implementations without professional assistance can lead to excessive time consumption and error. Fortinet Professional Services 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 (201, 301, FCNSP). Product selection per design includes FortiGate™, FortiManager™, FortiAnalyzer™ and FortiDB™ 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.

NERC CIP SECTION	FORTINET SOLUTION (descriptor)	NERC CIP SECTION	FORTINET SOLUTION (product)
CIP-002	Design architecture / Assessment	CIP-002	Fortinet Professional Services
CIP-003	Database security policy implementation and vulnerability assessment	CIP-005, CIP-006, CIP-007, CIP-008, CIP-009	FortiGate™
CIP-004	Training	CIP-005, CIP-007, CIP-008, CIP-009	FortiManager™ / FortiAnalyzer™ / FortiDB™
CIP-005	Establish electronic security perimeter	CIP-002, CIP-003, CIP-005, CIP-007	FortiDB™
CIP-006	Electronic protection of physical security assets	CIP-004	Fortinet Training Services
CIP-007	Security systems management / Database activity monitoring	CIP-004, CIP-007	Fortinet Technical Account Management
CIP-008	Incident reporting		
CIP-009	Recovery plan and back up		

Figure 5: CIPs addressed by Fortinet custom solutions for NERC compliance

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. FortiDB for database security includes vulnerability assessment, database activity monitoring and audit reporting – adding security for customer information, billing, safety reports and financial data stored in databases. Separate size-appropriate FortiGate UTMs may secure remote offices and regional power facilities.

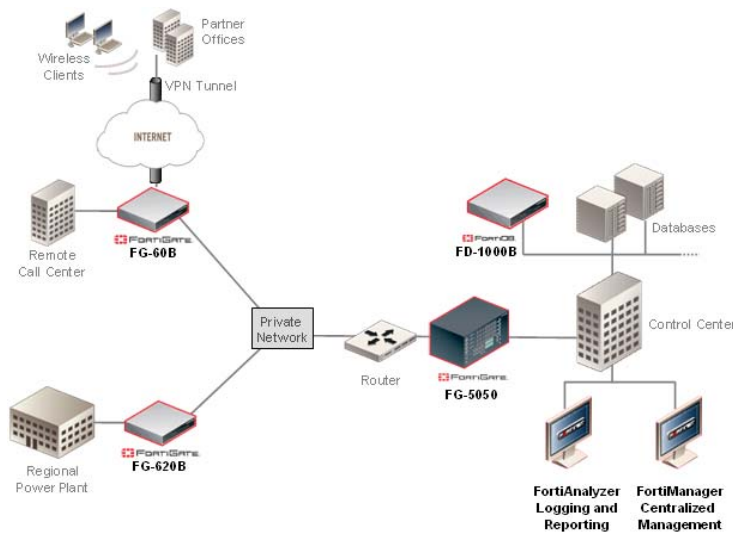


Figure 6: Fortinet deployment scenario

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. FortiDB™ can also help identify database assets using an autodiscovery feature across subnet boundaries.

CIP	Description	Fortinet Solution
✓ CIP-002, R3.1	The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter	Fortinet Professional Services – Designs networking to only use routable protocols to communicate outside the Electronic Security Perimeter
✓ CIP-002, R3.2	The Cyber Asset uses a routable protocol within a control center	Fortinet Professional Services – Designs networking to only use routable protocols to communicate within a Control Center
✓ CIP-002, R3.3	The Cyber Asset is dial-up accessible	Fortinet Professional Services – Eliminates dial-up connections or configures firewall for increased security of any dial-up modem based solutions

Figure 7: CIP-002 addressed by Fortinet custom solutions for NERC compliance

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.

CIP	Description	Fortinet Solution
✓ CIP-005, R1.1	Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s)	FortiGate –Firewall establishes perimeter on all identified Cyber Security Assets; FortiClient – adds an additional layer of protection for end point security by PC or remote devices <ul style="list-style-type: none"> <li>Establish secure out-of-band management</li> <li>Establishes SECURE Access Controls to equipment within Security Perimeter</li> <li>Secures Authenticated Access via SSL</li> <li>Establishes a single point of entry for Contractors and Vendors (suppliers of equipment within security Perimeter) with role based authenticated SECURE access</li> </ul>
✓ CIP-005, R1.2	For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device	Same as CIP-005, R1.1
✓ CIP-005, R1.3	Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s)	FortiGate – Protects Access points into Security Perimeter
✓ CIP-005, R1.4	Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005	FortiGate – Firewall, Physical or Virtual Segmentation with Access Control segments all NON-Critical Cyber Assets from all Critical Cyber Assets

✓ CIP-005, R1.5	Cyber Assets used in the Access Control and Monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009	FortiGate – Firewall protection of FortiManager, FortiAnalyzer, and 2nd Tier authentication servers - Authenticated Secure Access Control of management and logging as per CIP
✓ CIP-005, R2.1	These processes and mechanisms shall use an Access Control model that denies access by default, such that explicit access permissions must be specified	FortiGate – Firewall Access Control, 2nd Tier Authentication, (Secure) RADIUS Authentication, LDAP, Local Database Access Control ; FortiManager – Local Access Control Management
✓ CIP-005, R2.2	At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services	FortiGate – Firewall to Establish Ports and Services via Authentication Method - only allow Ports and Services as they are required by specific users when authenticated; Fall Thru Authentication
✓ CIP-005, R2.3	The Responsible Entity shall maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s)	FortiGate – Establish a single point of entry (dial up access) via SSL solution, Out-of-Band solution (exceptional DR plan)
✓ CIP-005, R2.4	Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible	FortiGate – Single point of access simplifies REPORTING of EXTERNAL ACCESS; Establish Single point of entry (dial up access) via SSL solution with optional 2nd tier authentication; Establish SECURE transport (INTERNAL VPN, Isolation of Remote Access connections to internal devices as specified per authentication of user - Only ALLOW transport to allowed devices)
✓ CIP-005, R2.6	Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner	FortiGate – Firewall authentication control - Header and Footer (appropriate use Banner)
✓ CIP-005, R3	Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week	FortiManager, FortiAnalyzer – Centralized Security Management
✓ CIP-005, R3.1	For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible	FortiManger, FortiAnalyzer – REPORT on Established Single point of entry (dial up access) via SSL solution with optional 2nd tier authentication; DOCUMENTATION on Access control method, report via FortiAnalyzer on all access either Denied or granted
✓ CIP-005, R3.2	Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every 90 calendar days	FortiGate, FortiManager, FortiAnalyzer – FortiGate Authentication failures reported to FortiAnalyzer and FortiManager, logged and set to page IT staff on failed authentication attempts; Intrusion Detection and Prevention on FortiGate intrusion attempts reported to FortiAnalyzer logged and set to page IT staff on Intrusion attempts against critical equipment
✓ CIP-005, R4	Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually	FortiDB – Database security vulnerability assessment
✓ CIP-005, R5.3	The Responsible Entity shall retain electronic access logs for at least 90 calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008	FortiAnalyzer – Retention of Logs depends on log volume and size of FortiAnalyzer - back up to nearline or online storage

Figure 8: CIP-005 addressed by Fortinet custom solutions for NERC compliance

This unified approach to cyber security allows Fortinet to address NERC compliance issues in a comprehensive methodology for substantial mitigation of cyber security risks, without compromising performance.

## 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.

## References

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](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/](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](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](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>

## About Fortinet

Fortinet is the pioneer and leading provider of ASIC-accelerated unified threat management, or UTM, security systems, which are used by enterprises and service providers to increase their security while reducing total operating costs. Fortinet solutions were built from the ground up to integrate multiple levels of security protection--including firewall, antivirus, intrusion prevention, VPN, spyware prevention and antispam -- designed to help customers protect against network and content level threats. Leveraging a custom ASIC and unified interface, Fortinet solutions offer advanced security functionality that scales from remote office to chassis-based solutions with integrated management and reporting. Fortinet solutions have won multiple awards around the world and are the only security products that are certified in six programs by ICSA Labs: Firewall, Antivirus, IPSec VPN, SSL VPN, Network IPS, and Antispam. Fortinet is privately held and based in Sunnyvale, California.

### FORTINET

1090 Kifer Road, Sunnyvale, CA 94086 USA  
Tel +1-408-235-7700  
Fax +1-408-235-7737  
[www.fortinet.com](http://www.fortinet.com)

Copyright© 2009 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, and FortiGuard®, are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance metrics contained herein were attained in internal lab tests under ideal conditions. Network variables, different network environments and other conditions may affect performance results, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding contract with a purchaser that expressly warrants that the identified product will perform according to the performance metrics herein. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any guarantees. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Certain Fortinet products are licensed under U.S. Patent No. 5,623,600.

WPR140-0109-R4