U.S. DEPARTMENT OF
ENERGY

PNNL-18295

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Control System Applicable Use Assessment of the Secure Computing Corporation - Secure Firewall (*Sidewinder*)

MD Hadley
SL Clements

January 2009

Pacific Northwest
NATIONAL LABORATORY

DISCLAIMER

Neither the United States Government nor any agency thereof, nor Battelle Memorial Institute, nor any of their employees, makes **any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights**. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof, or Battelle Memorial Institute. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401, fax: (865) 576-5728
email: reports@adonis.osti.gov

Available to the public from the National Technical Information Service,
U.S. Department of Commerce, 5285 Port Royal Rd., Springfield, VA 22161
ph: (800) 553-6847, fax: (703) 605-6900
email: orders@ntis.fedworld.gov
online ordering: http://www.ntis.gov/ordering.htm

♲ This document was printed on recycled paper.

PNNL-18295

Control System Applicable Use Assessment of Secure Computing Corporation – Secure Firewall (Sidewinder)

MD Hadley
SL Clements

Contributors:
TW Edgar
MP Allen
PA Craig

January 2009

Prepared for
Secure Computing Corporation
Under a Related Services Agreement
With the U.S. Department of Energy
Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99352

Summary

Battelle's National Security & Defense objective is, *"applying unmatched expertise and unique facilities to deliver homeland security solutions. From detection and protection against weapons of mass destruction to emergency preparedness/response and protection of critical infrastructure, we are working with industry and government to integrate policy, operational, technological, and logistical parameters that will secure a safe future"*. In an ongoing effort to meet this mission, engagements with industry that are intended to improve operational and technical attributes of commercial solutions that are related to national security initiatives are necessary. This necessity will ensure that capabilities for protecting critical infrastructure assets are considered by commercial entities in their development, design, and deployment lifecycles thus addressing the alignment of identified deficiencies and improvements needed to support national cyber security initiatives.

The Secure Firewall (*Sidewinder*) appliance by Secure Computing was assessed for applicable use in critical infrastructure control system environments, such as electric power, nuclear and other facilities containing critical systems that require augmented protection from cyber threat. The testing was performed in the Pacific Northwest National Laboratory's (PNNL) Electric Infrastructure Operations Center (EIOC). The Secure Firewall was tested in a network configuration that emulates a typical control center network and then evaluated. A number of observations and recommendations are included in this report relating to features currently included in the Secure Firewall that support critical infrastructure security needs.

The Secure Firewall's proprietary design, functionality and real-time intelligence enable it to provide solid protection to critical systems.

This report also includes recommendations intended to identify attributes related to publically available cyber security initiatives to consider for improving the Secure Firewall (*Sidewinder*) appliance and identify additional attributes for the product roadmap. Additionally, these recommendations should assist in planning for the implementation of future features that may make the Secure Firewall (*Sidewinder*) more effective and adaptable to securing critical infrastructure assets.

Overall the Secure Firewall was a qualified tool that could be applied to the protection of critical infrastructure and resiliency. Each of the categories listed below are expanded in the text of this report that together comprise a set of criteria for a firewall appliance that is well suited for to protect critical infrastructure assets.

- Defense in depth
- Principle of least privilege
- Proxy agents
- Intrusion Detection/Prevention Systems
- Remote access
- Interface communication
- Port Communication
- Redundancy

Contents

SUMMARY .... **III**

OVERVIEW **1**

FEATURES THAT SUPPORT CRITICAL INFRASTRUCTURE SECURITY **2**

Defense in depth *2*
Principle of least privilege *2*
Proxy Agents *2*
IDS / IPS *3*
Remote access *3*
Interface communication *3*
Port Communication *3*
Redundancy *3*

TEST ENVIRONMENT **4**

ROUTING BETWEEN ZONES (CALLED "BURBS") 7
Business to/from DMZ *7*
DMZ to/ from Control Center *7*
Control Center to/from the Process Control Network (PCN) *7*
Phasor Measurement Unit (PMU) to/from PCN *8*
TESTING NOTES 8
Secure DNP: *8*
Phasor Data: *8*

OBSERVATIONS **9**

Graphical User Interface *9*
Initial Use *9*
Viewing Rules *9*
VPN Configuration *9*

SUGGESTED PRODUCT ROADMAP FEATURES FOR FUTURE CIP CAPABILITIES **10**

Enhanced Anomaly Detection *10*
Enhanced Rule Views *10*
Support for Phasor Data *10*
Support for MPLS *10*
Support for Serial Communications *10*
Expanded Filters/Proxies *10*
Control System Specific Service Rules and Signature Groups *10*
Emphasis on Reliable Operations *11*

CONCLUSIONS **12**

GLOSSARY **13**

Overview

The purpose of this assessment was to assess the proprietary capabilities of the Secure Firewall (*Sidewinder*) appliance associated with control system environments. The assessment was conducted in the Electric Infrastructure Operations Center (EIOC) at the Pacific Northwest National Laboratory. The EIOC contains multiple live data feeds from industry as well as an operational Energy Management System (EMS). The EIOC provided both live and replayed data for the assessment.

The goals of the assessment were five fold:

- Identify performance impacts
- Identify features that directly support control system security requirements
- Identify capabilities that could be customized to better support control system security requirements
- Identify where the technology could be used in a control system network
- Provide recommendations for technology enhancement

The primary project deliverables include this technical report and participation in future Webinars intended to describe the activities that supported the evaluation of the Secure Firewall.

Features That Support Critical Infrastructure Security

The age and operational requirements of control system and IT networks differ in significant ways. The business network will often replace most of their systems every 3-5 years where control system networks are on a 20-30 year replacement cycle. The control system often requires 24x7x365 reliability where the business systems are typically more able to accommodate short outages. Control systems also operate on implicit trust e.g. if a device receives a valid command it will execute it whether or not it came from a valid operator, where traditional IT networks provide methods for authentication before execution. These fundamental differences and a multitude of others make critical infrastructure security challenging. In today's deregulated bulk electricity environment companies are constantly seeking economical advantages. This has lead to more frequent connections between the once isolated business and the control system networks. In turn this has significantly redefined and increased the threats on control system networks.

Regulatory standards for critical infrastructure systems have/are being developed to help mitigate these threats but they are in their infancy and are expected to change even as of the writing of this assessment. The most complete and thorough set of standards come from the National Institute of Standards and Technology (NIST). Specific NIST standards applicable to critical infrastructure systems are NIST 800-53 (see industrial control system supplemental guidance information) and SP 800-82 (expected to become a published document in 2009).

The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection group of standards (CIP-002 through CIP-009) were written to protect the bulk electric system from cyber events. Pertinent requirements address the monitoring and control of the NERC defined *electronic security perimeter* (ESP).

The following topics describe Secure Firewall (*Sidewinder*) features that address current issues pertaining to critical infrastructure protection requirements. Recommendations to expand current capabilities are contained in the Suggested Product *Roadmap* section.

Defense in depth

Just as there is not a single medicine to heal all ailments there is not one security technique that mitigates all threats. The Secure Firewall that was assessed provides multiple layers of security employing techniques to detect and mitigate security threats. These include an Intrusion Prevention System (IPS), Virus Scanning (add-on), TrustedSource™ (reputation service), Geo-Location, and SmartFilter™ to control users' access to the Internet.

Principle of least privilege

The principle of least privilege is to give users/processes the rights necessary to do their work but no more. The Secure Firewall uses a patented technology called Type Enforcement™ that limits each user/process to a specific domain. If that domain were compromised the other domains would still be safe, e.g. if email were compromised the web server would still be secure. The Secure Firewall also by default restricts communication between zones putting the onus on the system administrator to allow necessary communication.

Proxy Agents

Proxies provide more granular control of network traffic. Proxy agents are defined to force network traffic to comply with protocol standards. The Secure Firewall currently has proxy agents for a number of protocols including DNS, FTP, H323, HTTP and HTTPS, which are becoming more prevalent in control system networks.

IDS / IPS

Intrusion Detection and Protection systems are common place in today's IT networks but they are still nascent in the control systems world. In recent years a small number of signatures have been written to look for specific vulnerabilities in control systems. The Secure Firewall provides signature and anomaly based intrusion detection and has a configurable response mechanism. Currently there are 28 signatures defined that support SCADA protocols (MODBUS/TCP, DNP3/TCP, and ICCP/TCP).

Remote access

Control systems in the electric power industry and many other critical infrastructure areas are typically very geographically dispersed and require remote access to the system. Many commercially available products allow VPN connections granting a user access to the remote network. The Secure Firewall *adds* the ability to enforce firewall rules specific to individual VPN connections.

Interface communication

There significant business drivers creating the need to get data from the control network to business network. The ability to do this in an intrinsically secure manner is still quite difficult. One very important feature of the Secure Firewall is the ability to set interfaces to transmit and/or receive only, or any combination. This functionality could be very useful for creating a secure data transfer path for communication flowing from a high security network (e.g. a control center) and a lower secure network (e.g. the corporate network). More information on the ability of the Secure Firewall to function as a logical *data diode* is requested.

Port Communication

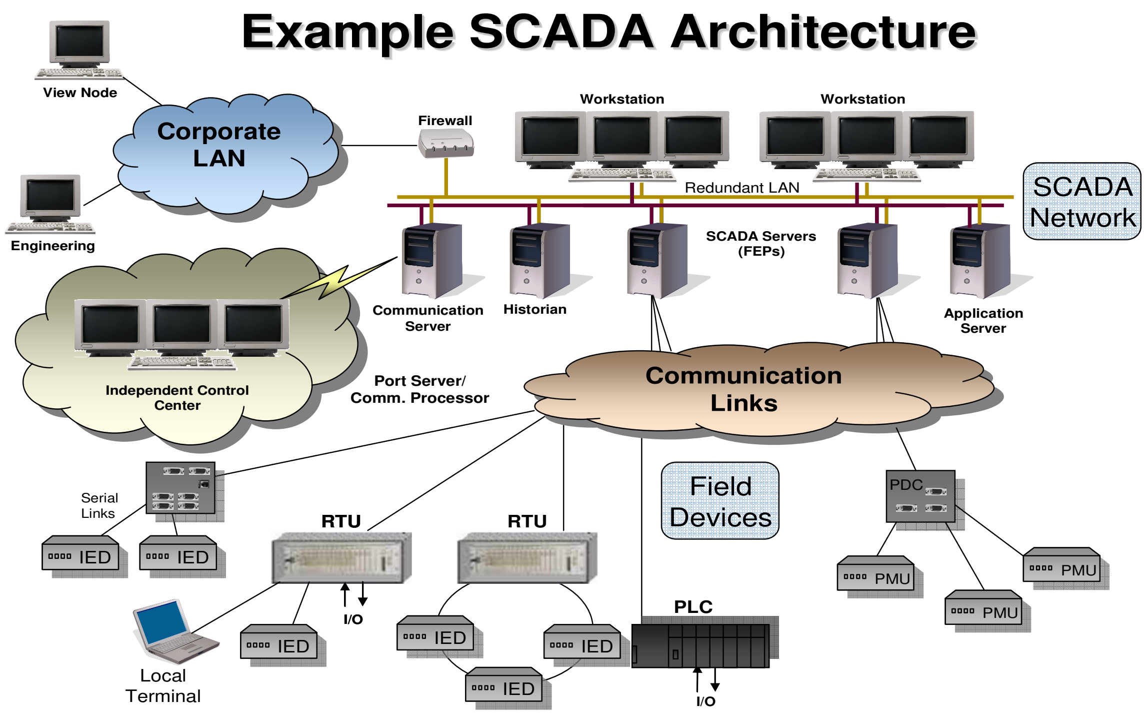
As stated above current control systems operate on *implicit trust*. The Secure Firewall provides authentication mechanisms to prohibit allowed traffic until authentication occurs. This helps assure that communications are valid and aids operators in defining and enforcing their security perimeter which is a requirement for the NERC CIP standards.

Redundancy

The Secure Firewall supports the industry's requirement of high availability for controls systems by providing firewall load sharing and redundant *high availability* (HA) failover capabilities.

Test Environment

A typical control system network contains numerous connections to other networks, organizations, and remote facilities. The number of connections can literally be in the thousands, making securing such an environment a significant challenge. The connections may utilize serial and/or routable protocols, a variety of communication mediums, and often require redundant communication pathways. The following diagram depicts an example of a complicated network design typical of an environment where the Secure Firewall would be deployed.



A brief discussion on data acquisition schemes, also known as telemetry, is required to fully understand the predictable nature of control system communication. Telemetry is the method SCADA servers use to retrieve information from field devices. This communication is extremely predictable, and deviation from the communication pattern highly discernable. For each field device, a SCADA server will request known data types. For example, the status of breakers and the frequency and voltage of the electric grid, are requested at regular intervals. Below is a diagram depicting a minute broken into two-second time slices. Every two seconds, the status of breakers is requested. Once a minute frequency and voltage are requested. Note that more than one request can be made during a time slice.

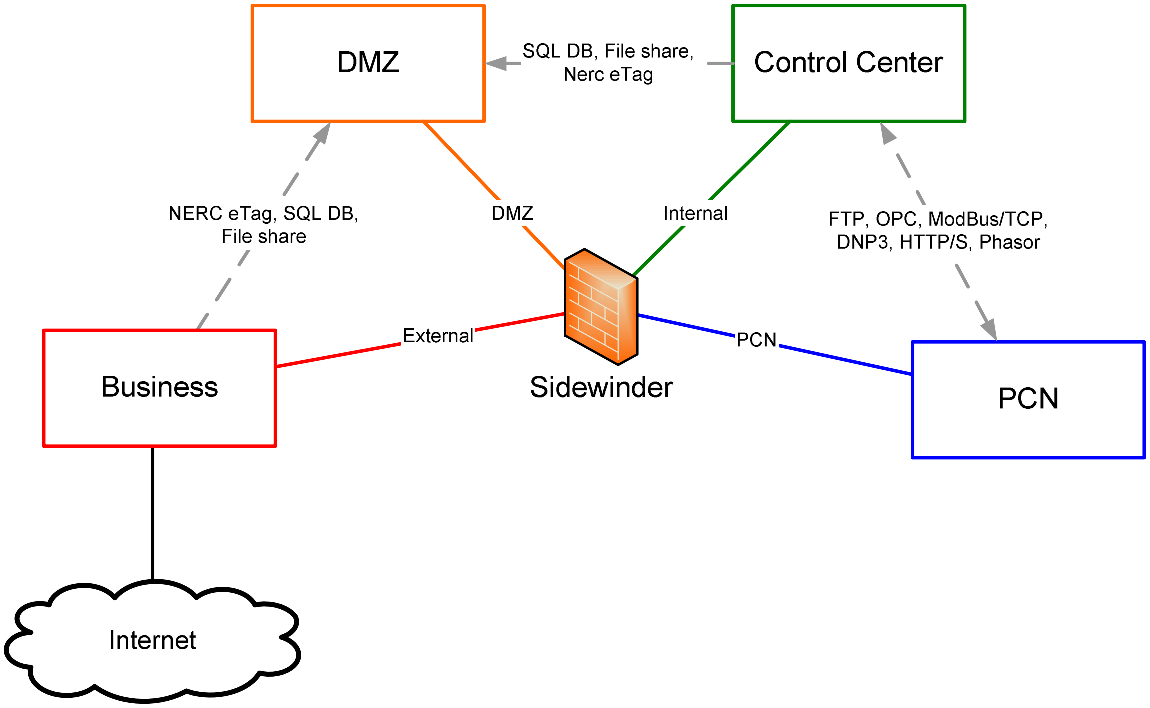
Relative Timing of Telemetry Requests

	Time Slice																													
Data Type	0	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48	50	52	54	56	58
Status	X		X		X		X		X		X		X		X		X		X		X		X		X		X		X	
Frequency																									X					
Voltage															X															

A control system network utilizes a variety of data types to ensure reliable operations of the infrastructure environment. The following table identifies the data types, their purpose within a control system, and data timing requirements.

Data Type	Use	Protocol	Timing Requirements	Notes
Synchro Phasor Data	Provides better situational awareness and is an indicator of the rate of change. Typically used at critical point in the monitored infrastructure.	BPA Stream Reader	Typically, 30 samples are taken per second from each remote location. The data rate may be as high as 60 or 120 samples per second.	Passing broadcast traffic between zones is prohibited by the Secure Firewall therefore tests were run with directed UDP traffic.
Data Transfer Tests	To pass data between a control center network and a business system.	SQL and Windows File Shares are common methods used for this function.	10 minute time frame.	A DMZ zone was used for this test.
SCADA Protocols	Used for the monitoring and control of the power grid, distribution systems, and generation.	DNP and Modbus	Varies by data type from a request every 2 seconds to once per minute.	We tested with routable versions of these protocols. However, the majority of infrastructure utilizes the serial versions.
IT Protocols	HTTP and XML data formats are becoming more popular for device configuration and communication, respectively.	NERC e-tag XML format; FTP	Widely varied.	Vendors are including IT protocols in control system products at an increasing rate.
Operator Console	Used to communicate between the console computer(s) and either the SCADA server or communications server.	Varies by implementation. Can be OPC, proprietary, or the SCADA protocol.	Real time or near real time data requirements.	Our testing utilized OPC; DNP and Modbus were tested under SCADA protocols.

A single Secure Firewall configured with four zones was used for the assessment. The protocols and zone configuration are shown in the following diagram:


DMZ
SQL DB, File share, Nerc eTag
Control Center
NERC eTag, SQL DB, File share
DMZ
Internal
FTP, OPC, ModBus/TCP, DNP3, HTTP/S, Phasor
External
PCN
Business
Sidewinder
PCN
Internet

Routing between Zones (called "Burbs")

This section describes the firewall rules for routing between zones.

Business to/from DMZ

The business zone is also the Internet/External zone. There is a need for business systems to gather information from the process control network for billing, scheduling, and other business needs. For the purpose of the assessment there were three rules created. The first allows for read only access to a file share in the DMZ, the second used pre-existing rules to allow MS-SQL queries to be made to a database, and the third rule allows NERC eTag (XML/HTTP) traffic to flow to a single device in the DMZ.

DMZ to/ from Control Center

The control center is the final destination for much of the traffic on the process control network. The data that is needed for business reasons in the business network is pushed to the DMZ from the Control Center/Internal zone. This includes the three data streams in the previous section, MS-SQL, File share, and NERC eTags.

Control Center to/from the Process Control Network (PCN)

Devices on the process control network (PCN) use many different protocols. Many rules were necessary to support these protocols and to allow for proper communications to and from these devices. It would be advised to create a *service group* similar to the Internet Service group that had the necessary services and rules pre-built for process control networks. The most prevalent protocols for process control networks are ModBus and DNP. The Secure Firewall does not currently provide support for monitoring or filtering serial communications, which is the most common control center medium. We tested the routable versions of these protocols. Other important protocols to consider for this service group would be FTP, OPC, Syslog, and HTTP.

Phasor Measurement Unit (PMU) to/from PCN

The best practices recommend tunneling phasor measurement data via a VPN into the PCN. It is recommended that VPNs terminate in a virtual zone and then get routed to the proper destination or endpoint zone. Our network configuration did not allow for this setup and further research needs to be done to determine the best configuration for transferring PMU data.

Testing Notes

The Secure Firewall successfully passed the ModBus-TCP and DNP for IP. It also alerted on these protocols when probed with known malicious traffic. We tested the following protocols in further detail.

Secure DNP:

Secure DNP is a relatively new addition to the DNP protocol. We tested to see how the Secure Firewall would respond fearing that it may alert that it is malicious traffic. Initially the Secure Firewall alerted on "non DNP traffic on DNP Port". After looking into closer detail it was a configuration error on the slave device. Once the devices were configured correctly the alerts stopped and both normal DNP and Secure DNP pass through without alert.

Phasor Data:

Broadcast:
The initial test attempted to capture PMU (i.e., phasor data) that was on the broadcast IP address of one subnet/zone and redirect into another subnet/zone. The Secure Firewall did not allow this to occur. We also attempted to send the phasor data from the phasor measurement device to the broadcast address of another zone without success.

Directed UDP:
Directed UDP traffic was sent from the relay device that generated the data directly to receiving host in another zone and was passed correctly and accurately.

Latency:
Latency is a major concern with real-time systems.. We looked at the latency in phasor data. It is transmitted at up to 120 times per second and must be timely in order to be useful to operators. I tested the processing time on the directed UDP phasor data being transmitted at a typical 30 times per second. I captured traffic entering on both the receiving and the transmitting network interface cards and measured the latency between the two. The Secure Firewall adds latency between .00009 and .00017 seconds between receiving the packet, tearing down the connection, scanning the traffic for matches to the signatures, rebuilding the packet, and finally sending the packet out the destination interface. This latency would be considered insignificant and would not affect the desired near real-time quality of the data desired at the endpoint destination. This was an impressive attribute of the Secure Firewall considering the process that was just described. It should be noted that this capability was assessed on a non-congested link but appears to be more than sufficient for handling phasor data.

Observations

Security includes people as well as technologies. That is, the ability for personnel to interact with technologies deployed within their company's security environments. The perimeter security team at PNNL is familiar with a variety of products that perform security functions commonly employed in multiple and complex computing environments. Their observations and first impressions on ease of use and functionality are included below. This is important as operators in critical infrastructure who are tasked with managing the Secure Firewall, depending on their level of experience or time on the job, may or may not be familiar with such advanced IT or firewall technologies.

Graphical User Interface

The Secure Firewall has a look and feel consistent with similar type products and capabilities. This consistency would be expected of *any* device commonly available on the commercial market. Many IT technologies attempt to ensure a standard look and feel especially where monitoring, maintenance, and responses are required of trained personnel. The management interface/GUI used with the Secure Firewall appliance has many of the same attributes and layouts that are easily recognized by anyone familiar with computer/software user interfaces.

Initial Use

The Secure Firewall is no more difficult to learn than other products. While there are some new terms and a new layout, the Secure Firewall has a learning curve comparable to other firewall products. One can quickly come up to speed and configure the Secure Firewall with a basic knowledge of networking and firewalls.

Viewing Rules

Finding a specific *rule* is easy with the search feature provided in the GUI, however finding a specific 'rule set' is challenging. There is a substantial amount of information required to define a specific rule and displaying all this information would quickly make a display cumbersome and crowded. Yet the ability to view this information when needed is very beneficial. Currently a mechanism to view and/or sort rules by a specific attribute is not provided. We offer two recommendations to improve viewing rules.

1. The ability to filter the rules based on zone or interface. Management of the rules otherwise is more difficult and time consuming. Providing a mechanism to view configuration rules per *interface* or *zone* would be beneficial to operators of the Secure Firewall.
2. Provide mouse over capabilities to see more details to the rules/services. The way that the Secure Firewall defines services and then uses the services to define rules allows for easy reuse and modularity but it also obfuscates exactly what a rule is doing. The rule set only shows the service name not what ports it contains. This could lead to unnecessary rules and unexpected holes in zone communication.

Note: The Secure Firewall may have already undergone some changes in normal product improvement cycles. However, the version that we assessed did not contain such changes.

VPN Configuration

VPNs are frequently used in the control system networks. The Secure Firewall provides a full set of VPN features. It includes the ability to limit VPN connections to specific IP addresses and/or subnets. This is very beneficial when connecting two static locations and commonly desired in control systems environments especially where routable protocols are utilized. We encountered a slight problem when configuring the VPN in *VPN Properties*. First, we had to erase previous work and exit the *VPN Properties* screen to go back to another screen to configure the pools and groups needed in the *VPN Properties* screen. It would be useful if one could configure new pools, groups, etc within the *VPN Properties* screen.

Suggested Product Roadmap Features for Future CIP Capabilities

Enhanced Anomaly Detection

Ensure anomaly detection capabilities support the predictable nature of SCADA communication. Both the communicating devices and the communication patterns are well known and consistent. The ability to detect a device communicating out of turn, too frequently, or not frequently enough, or a new device altogether would be indicative of potential malicious activity. The ability to monitor communications for variations from their predictable patterns would be a very powerful tool, as the content of malicious and non-malicious traffic is often indecipherable.

Enhanced Rule Views

The ability to sort firewall rules by zone would assist in maintenance. There is at times an animosity between control system and IT staff at a utility. Call it distrust or lack of appreciation for the other's environment. In short, these products may be deployed and maintained by staff whose primary purpose is not perimeter security. The ability to easily access all rules for a zone would assist in maintenance and limit security holes through mis-configurations.

Support for Phasor Data

Synchro-phasor measurements aid in detecting and mitigating an unstable power grid. The ability to move this data around is very important to the bulk electricity industry. Support for inter-zone broadcast traffic would allow all currently available phase-angle communications to be processed.

Support for MPLS

Support for MPLS is desirable. Utilities are considering MPLS to provide a redundant communication environment. MPLS supports a backup control center located far distant from the primary control center. MPLS allows this to occur without the need for redundant communication media to remote substations.

Support for Serial Communications

The primary method to monitor and control our nation's critical infrastructure is via serial ports and protocols. Our interviews with industry show that serial protocols will be in use for the next 20 to 30 years. To date there has been a dearth of research and development in securing this critical piece to our national infrastructure. Currently the ability to adequately secure serial communication does not exist. Adding serial support to the Secure Firewall and its related technologies (e.g. Trusted Source™, and anomaly detection) would provide the serial community with a security tool that currently is unavailable.

Expanded Filters/Proxies

Develop working relationship with energy management system vendors (e.g. AREVA, Siemens, GE, ABB, Telvent) and develop filters to secure the protocols used to communicate between the operator console and the SCADA/Communications server.

Control System Specific Service Rules and Signature Groups

Anything that can be done to simplify the configuration and deployment will increase security. Two easy enhancements would be to create process control system protocol services rules (e.g. DNP, ModBus, OPC etc) and IPS Signature groups for the SCADA/PCS signatures.

Emphasis on Reliable Operations

The emphasis on *reliable operations* in industry today doesn't effectively address the necessity to identify cyber security vulnerabilities and provide effective mitigation measures. However, the groundwork is well underway for increasing the vigilance necessary to ensure reliable operations in our Nation's critical infrastructure. Recognition at all levels of government, industry, and the public of that one very important component of reliable operations is the assurance that this infrastructure is protected from the damaging effects that can be caused by cyber attacks from far-reaching and well disguised cyber adversaries. To understand, and maintain current with, the vulnerabilities that have been established as a *top ten list*, the U.S. Department of Energy (DOE) National SCADA Test Bed (NSTB) program has provided initial recommended mitigation strategies to this list in the North American Electric Reliability Corporation (NERC) "Top 10 Vulnerabilities of Control Systems and Their Associated Mitigations - 2007"[1]. A presentation of these vulnerabilities, and graded mitigation measures accurately describe the contributing expert's 2007 concerns in the cyber landscape.

Another valuable contribution to the overall mission and goals of providing reliable operations is the comprehensive efforts by the Department of Energy Office of Electricity Delivery & Energy Reliability's "Roadmap to Secure Control Systems in the Energy Sector".[2] This effort captures the effort currently being applied to ensure that short and long term solutions are coordinated within government organizations, national laboratories, industry partners, and vendors to provide consistent, stable, and efficient methods for implementing cyber security.

Many of the attributes of this groundwork are being actively addressed through the foresight of vendors, such as Secure Computing, to ensure their products meet current and future capabilities for securing critical infrastructure assets and infrastructure. The Secure Firewall (*Sidewinder*) product has many of these capabilities and specific features that will effectively support this mission. The features of the Secure Firewall that were reported in this assessment adequately fit the current cyber security needs for securing and protecting critical infrastructure. An example would be the isolation of control system perimeters from corporate or other adjacent networks by an appropriate combination of firewall traffic management and DMZ configurations. This effort effectively meets the need to eliminate weaknesses in control system perimeter protection and increase the difficulty for an external attacker to exploit vulnerabilities. This is simply *one* important example as illustrated in the DOE-NSTB "Lessons Learned From Cyber Security Assessments of SCADA and Energy Management Systems"[3]. Additionally the Secure Firewall (*Sidewinder*) has appropriately addressed the entire set of vendor recommendations provided in this report identified as Actions #1 through #5 (Section 4.2 Recommendations for System Vendors) which remain current actions for the 2009 control system vulnerability environment thus resulting in increased reliability through the Secure Firewall security attributes and features.

[1] NERC Top 10 Vulnerabilities of Control Systems – 2007, is published by NERC offering a non-prioritized list of the top 10 most common vulnerabilities that put control systems in the electricity sector at risk. A copy of this document in full can be attained at: http://www.oe.energy.gov/information_center/reports.htm along with many other valuable contributions to securing our Nation's critical infrastructure.

[2] Department of Energy – Office of Electricity Delivery & Reliability – "Roadmap to Secure Control Systems in the Energy Sector" January 2006. http://www.controlsystemsroadmap.net

[3] DOE-NSTB "Lessons Learned From Cyber Security Assessments of SCADA and Energy Management Systems", September 2006.

Conclusions

Based on the report herein, PNNL's assessment of the Secure Firewall is that it contains the features necessary for a robust CIP CI/KR security program. Some of the most apparent capabilities are the tiered approach to security otherwise known as defense-in-depth, high availability, application of least privilege and providing a strong boundary between IT and control/ICS/SCADA systems.

A number of future modifications could be made to the Secure Firewall to make it even more valuable to the control system industry including enhanced rule sorting, support for MPLS, better configuration for VPNs and customized service rules and signature groups. Adding serial support would be a unique and extremely beneficial feature for this community.

Future modifications, some of which may have already been addressed in subsequent improvements and revisions or planned improvements of the Secure Firewall product, should also continue to be aligned with the overall protection requirements and needs of the control system environments as identified by emerging regulatory expectations and developed standards for acceptable practices.

Finally, there are many other standards and reports that contain cyber security attributes desirable of vendor solutions applied in control system environments. To decrease the challenge of addressing these attributes, the Secure Firewall (*Sidewinder*) appliance could effectively be deployed in many current control system environments. Where recommendations have been made to increase the effectiveness of the Secure Firewall for applicable use in future control system environments, the reviewers are confident that such capabilities could be identified by the vendor's development roadmap and continued interaction with the efforts of government policymakers, the national laboratories, and industry advisory groups.

Glossary

BPA	Bonneville Power Administration: A federal agency under the U.S. Department of Energy that servers the Pacific Northwest through operating an extensive electricity transmission system and marketing wholesale electrical power.
CI/KR	Critical Infrastructure/ Key Resources
CIP 002-009	Critical Infrastructure Protection: A group of standards written by NERC to protect the bulk electric system from cyber events.
Communication Server	A server that translates protocols allowing devices to communicate that otherwise could not do so.
DMZ	De-Militarized Zone: A controlled segment of a network architecture between an organization's private network and the outside public network.
DNP	Distributed Network Protocol: A common communication protocol used in process control systems. It is used in both serial (un-routable) and TCP/IP communications (routable).
DNS	Domain Name Service: this service translates names from human readable form e.g. my.firewall.com to the machine readable form of 192.168.0.1
EIOC	Electricity Infrastructure Operations Center: A laboratory at Pacific Northwest National Laboratory that combines software, real-time grid data, advanced computation, and a fully capable control room to research topics relating to the electric power grid.
ESP	Electronic Security Perimeter: A title defined in the NERC CIP requirements detailing the boundaries of electronic communication systems.
eTag	eTag: a standard information format defined by NERC that is used to communicate supply and demand requirements between different entities in the bulk electric power industry.
FEP	Front End Processor: a computer that handles input and output communications with various end devices.
FTP	File Transfer Protocol: a clear text protocol typically used to transfer large amounts of data.
GUI	Graphical User Interface: an interface that allows people to interact with electronic devices through visual indicators
HMI	Human Machine Interface: The interface between human and machines. In today's control systems this is typically a computer, though it may be levers, buttons, valves or other controls.
H323	A networking protocol used for audio/visual conferencing
Historian	A database system that is optimized for real-time gathering and processing of control system data.
HTTP	Hypertext Transfer Protocol: used for transmitting web pages on the Internet.
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer: used for sending secure web pages over the Internet.
ICCP	Intercontrol Center Communication Protocol: used for communication between two or more control centers.
ICS	Industrial Control Systems
IED	Intelligent Electronic Device: sensors, valves, gates, etc that make up the

	control system
LAN	Local Area Network
Latency	A delay, the period between the initiation of something and its occurrence.
ModBus	A communication protocol commonly found in process control systems
MPLS	Multiprotocol Label Switching: a data packet routing protocol with improved routing speeds
NERC	North American Electric Reliability Corporation
OPC	A series of standards specifications used in process control industries
PCN	Process Control Network
PCS	Process Control System
PDC	Phasor Data Concentrator: Aggregates data from multiple PMUs
PLC	Programmable Logic Controller: a digital computer used for automation of electromechanical processes.
PMU	Phasor Measurement Unit: Measures the phase angle of electrical power
PNNL	Pacific Northwest National Laboratory
RTU	Remote Terminal Unit: a microprocessor that monitors sensors and devices and transmits all the data to a central monitoring station.
SCADA	Supervisory Control and Data Acquisition: hardware and software that gathers real-time data from remote locations in order to control equipment and conditions.
SQL	Structured Query Language: used to query databases
Syslog	A protocol for forwarding log messages on an IP network
UDP	User Datagram Protocol: a unidirectional stateless protocol for sending messages over an IP network. Frequently used for transmitting phasor measurement.
VPN	Virtual Private Network: a technology that creates a secure tunnel through an untrusted network.
XML	Extensible Markup Language: a specification for creating custom data definitions. Current NERC eTags are defined using XML.