Server Technology, Inc.

Joint Interoperability Test Command (JITC):

JITC Tested; Cabinet Power Distribution Units for DOD Information Technology & National Security System Applications

White Paper STI-100-002

Server Technology, Inc.
1040 Sandhill Drive
Reno, NV 89521
+1 (775) 284-2000
www.servertech.com

JITC Tested Cabinet Power Distribution Units

INTRODUCTION

The Joint Interoperability Test Command (JITC) is an independent evaluator of information systems deployed within the Department of Defense (DOD) and is one of the responsible organizations that conducts Information Assurance (IA) and Interoperability (IOP) testing of network devices that will be connected to the Global Information Grid (GIG).

Server Technology provides Power (Cabinet) Distribution Units (CDU's) across a wide range of data center applications. The family of products include Basic, Metered, Smart, Switched, -48 VDC, and Fail Safe Transfer Switches. The products tested feature intelligent IP addressable power distribution, remote management for rebooting connected devices, input current monitoring, environmental monitoring for temperature and humidity, and serial port console access. This testing was conducted to verify Server Technologies security protocols and viability to operate on government computing and networking environments such as the GIG. As well as having these products incorporated into the DOD network environment and/or future DOD acquisition programs by meeting the standards of DOD Directives 8500.1 and 8500.2.

JITC testing was done for commonly known vulnerabilities and to assess its capability for resisting attacker exploits. This paper will address the types of testing that was performed and the specific test results. The Sentry PTXL is the only CDU family on the market to have undergone JITC testing.

TESTING SCOPE AND METHODOLOGY

The Server Technology Sentry PTXL products are designed to provide System Administrators (SA), network operations personnel, and supporting staff with the ability to remotely monitor, manage and control individual or groups of power outlets. This provides the means to control or reboot devices for mission critical applications in locations that might otherwise be deemed inaccessible or cost-prohibitive to organizations operating in a 7 x 24 environment. By incorporating additional features, such as console control ports, the Sentry PTXL also enables responsible personnel to connect to local management access interfaces from remote locations.

All Automated Information Systems (AIS) equipment acquired by the Department of Defense (DOD) is required to undergo both Information Assurance (IA) and Interoperability (IOP) testing/assessments. These requirements enable the DOD to verify the devices capabilities for availability, integrity, authentication, and non-repudiation.

The specific goals of the tests performed on the Sentry PTXL were to confirm:

- Protocol standard conformance
- Resistance to commonly known vulnerabilities
- Adoption of DOD and industry best practices
- System availability

JITC executed testing of the Server Technology, Inc. Sentry PTXL device in accordance with the JITC document number 3B03.001. The assessment was performed at the JITC Indian Head, Maryland test facility. To facilitate the execution of the test plan, a test network configuration was established as depicted in Figure 1.

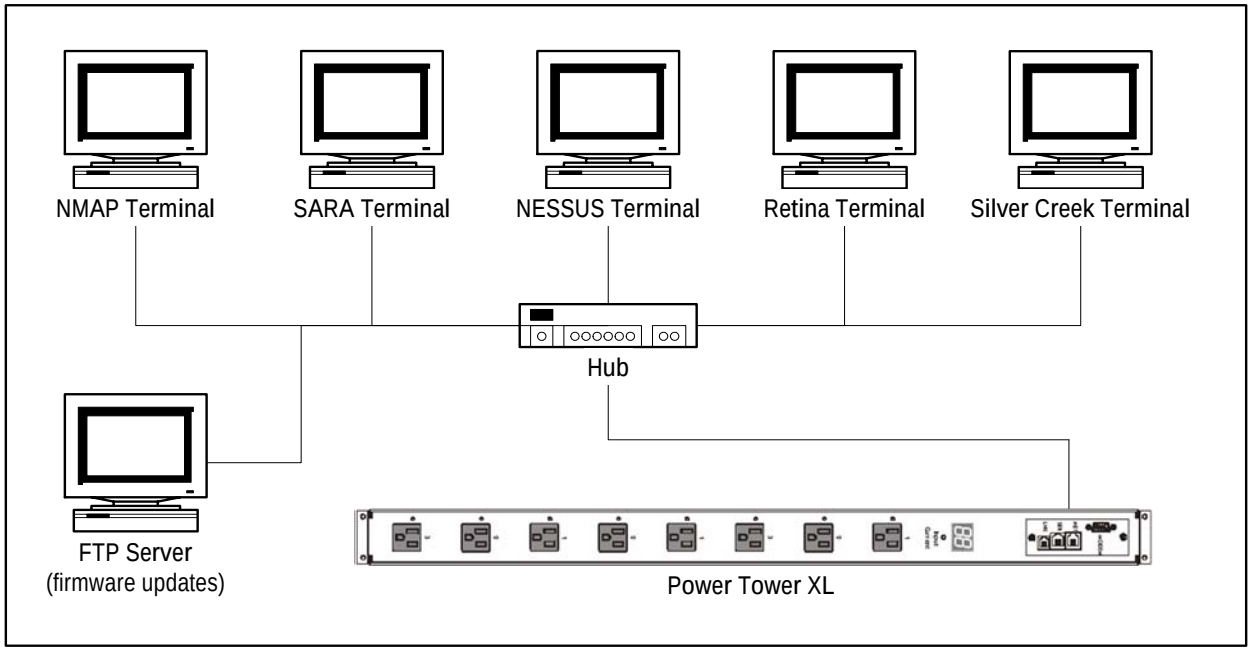

Figure 1: Test Network Configuration

TESTING REQUIREMENTS

The DOD does not currently have network device-specific IA requirements identified for devices such as the Server Technology's Sentry PTXL. The test cases and test procedures were based on IA requirements derived from the following DOD IA standards and industry sources:

- Department of Defense (DOD) Directives (DODDs) 8500.1 and 8500.2
- DOD Instruction (DODI) 8551.1
- Chairman, Joint Chiefs of Staff Manual (CJCSM) 6510.01
- CJCS Instruction (CJCSI) 6510.01
- Industry-recommended IA best practices documentation:
  - SysAdmin, Auditing, Networking and Security (SANS) Institute's "Top 20 Vulnerabilities"
  - Mitre's "Common Vulnerabilities and Exposures (CVE)"

TEST RESULTS AND ANALYSIS

Table 1: Below summarizes the Sentry PTXL device test findings as they relate to specific test cases in the test plan.

Test Case	Title	Score	Comments
1	Transmission Control Protocol/Internet Protocol (TCP/IP) Network Port Scanning	Pass	None
2	Commonly Known Vulnerability Assessment (NESSUS)	Pass	None
3	Commonly Known Vulnerability Assessment (SARA)	Pass	None
4	Commonly Known Vulnerability Assessment (Retina)	Pass	None
5	Simple Network Management Protocol (SNMP) Vulnerability Assessment	Pass	Standards conformant implementation with no identified vulnerabilities.

6	Password Format Policy ("Non-Technical") Assessment	Pass	Present and states DOD compliant policy.
7	Password Format Policy (Technical) Assessment	Pass	**Enforces DOD policy, not just simply being compatible with it. ***
8	Service Provider Module Operating State Change Assessment	Pass	All services can be enabled or disabled via both management interfaces.
9	Audit Log Verification Assessment	Pass	No internal device storage of audit was present however external audit notification is available and accurate.**
10	Network Interface Statistics Assessment	Pass	None
11	Authentication System Assessment	Pass	None

***-** Note per the test report "It appears a great deal of effort from the vendor was undertaken to ensure the Sentry PTXL device not only is compatible with DOD policies and best practices but, to some extent, even enforces those policies through technology.

****-** To provide permanent storage the BSD Syslog Protocol is used. Via this external log interface, all the required audit entries were made available and were tested accurate.

For more information on the test cases see Appendix B. For complete information a copy of the JITC assessment report must be obtained.

CONCLUSION

The Server Technology Sentry PTXL device performed very well and passed all of the specific test cases without any vulnerabilities. Also the Server Technology product showed no noticeable signs of Interoperability problems when installed in a microcosm of the DID GIG.

Currently there are no other CDU's that have been tested to these standards. Meeting these standards shows a commitment to product interoperability, integrity and security ensuring Server Technology products can inter-operate in a joint, combined or coalition team environment.

APPENDIX A:

ACRONYMS

AIS	Automated Information Systems
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJCSM	Chairman of the Joint Chiefs of Staff Manual
CVE	Common Vulnerabilities and Exposures (Mitre)
DOD	Department of Defense
DODD	Department of Defense Directive
DODI	Department of Defense Instruction
GIG	Global Information Grid
IA	Information Assurance
IOP	Interoperability
IP	Internet Protocol
JITC	Joint Interoperability Test Command
MIB	Management Information Base
Sentry PTXL	Power Tower XL
SA	System Administrator
SANS	SysAdmin, Audit, Network, and Security Institute
SARA	Security Auditor's Research Assistant
SATAN	Security Administrator Tool for Analyzing Networks
SNMP	Simple Network Management Protocol
SSL	Secure Socket Layer
SSH	Secure Shell
TCP	Transmission Control Protocol

APPENDIX B:

Test Case Summary

Test Case 1 – Transmission Control Protocol/Internet Protocol (TCP/IP) Network Port Scanning

The objective of this test was to examine the (Sentry PTXL) device to identify all listening TCP/IP network ports and compare them with the list that the device is reporting and enabled. This test was also developed to verify all listening ports have an assigned assurance category as required in Department of Defense (DOD) Instruction (DODI) 8551.1, "Ports, Protocols, and Services Management (PPS)," dated 08/13/2004.

Table B-1 Identified Ports and Services

TCP/IP Port Number	Service
21	Telnet
23	Secure Shell (SSH)
80	Hypertext Transfer Protocol (HTTP)- Management Web Interface Service
443	HTTP over Secure Socket Layer (SSL)-Secured Management Web Interface Service

Test Case 2 – Commonly Known Vulnerability Assessment (NESSUS)

The objective of this test was to examine the Sentry PTXL device to discover if its service provider modules are susceptible to any commonly known vulnerability. This test only inspected service provider modules that are accessed via TCP/IP.

Test Case 3 – Commonly Known Vulnerability Assessment (SARA)

The objective of this test was to examine the Sentry PTXL device to discover if its service provider modules are susceptible to any commonly known vulnerability. This test only inspected service provider modules that are accessed via TCP/IP.

Test Case 4 – Commonly Known Vulnerability Assessment (Retina)

The objective of this test was to examine the Sentry PTXL device to discover if its service provider modules are susceptible to any commonly known vulnerability. This test only inspected service provider modules that are accessed via TCP/IP.

Test Case 5 – Simple Network Management Protocol (SNMP) Vulnerability Assessment

The objective of this test was to examine the Sentry PTXL device to discover if its implemented SNMP service provider module was susceptible to any known vulnerabilities, capable of withstanding a rather aggressive request load, and is standards compliant to all applicable protocol specifications. In performing this test, the accuracy and completeness of the Sentry PTXL SNMP Management Information Base (MIB) was also tested.

Test Case 6 – Password Format Policy ("Non-Technical") Assessment

The objective of this test was to examine the Sentry PTXL devices documentation to identify and assess the implemented password formatting policy. This was to ensure that the device is capable of supporting passwords that meet DOD password formatting requirements for network devices. A review of all supplied user manuals, product documentation, and technical white papers was performed and the appropriate documentation sections were extracted and analyzed.

Test Case 7 – Password Format Policy (Technical) Assessment

The objective of this test was to examine the Sentry PTXL devices implemented password format policy to ensure it is compatible with DOD password formatting requirements as well as the device's documented password format policy.

Test Case 8 – Service Provider Module Operating State Change Assessment

The objective of this test was to examine the Service Provider Modules on the Sentry PTXL device to determine whether they can each have their operating states independently toggled (enabled/disabled).

Service Provider Module	Score
HTTP	Pass
HTTPS	Pass
SNMP	Pass
SSH	Pass
Telnet	Pass

Test Case 9 – Audit Log Verification Assessment

The objective of this test was to examine the Sentry PTXL device and determine whether or not it creates and retains an audit log of all access attempts to each management interface and whenever configuration changes were applied.

Test Case 10 – Network Interface Statistics Assessment

The objective of this test was to examine the Sentry PTXL device to determine if it maintains accurate network interface statistics.

Test Case 11 – Authentication System Assessment

The objective of this test was to examine the Sentry PTXL device to determine if it has implemented an authentication system that allows for the explicit restriction of privileges on a per-account basis.