



DEFENSE INFORMATION SYSTEMS AGENCY

P. O. BOX 4502
ARLINGTON, VIRGINIA 22204-4502

IN REPLY
REFER TO: Joint Interoperability Test Command (JTE)

20 Jan 09

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Special Interoperability Test Certification of the Secure Computing 1100 and 2150 Sidewinder Family of Firewalls Running Software Version 7.0.1.00 for Internet Protocol Version 6 Capability

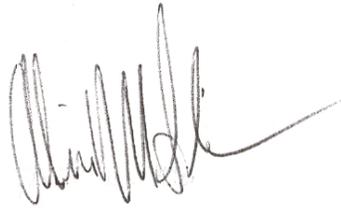
References: (a) DoDD 4630.5, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," 5 May 2004
(b) CJCSI 6212.01D, "Interoperability and Supportability of Information Technology and National Security Systems," 8 March 2006
(c) through (h), see Enclosure 1

1. References (a) and (b) establish the Joint Interoperability Test Command (JITC), as the responsible organization for interoperability test certification.
2. The Secure Computing 1100 and 2150 Sidewinder firewalls running Software Version 7.0.1.00 have met the Internet Protocol (IP) Version 6 (IPv6) Capable interoperability requirements of an Information Assurance (IA) device as described in the Department of Defense (DoD) Information Technology Standards Registry, "DoD IPv6 Standard Profiles for IPv6 Capable Products Version 3.0," July 2008, reference (c). The Secure Computing 1100 and 2150 Sidewinder firewalls running Software Version 7.0.1.00 have successfully completed the related IPv6 Interoperability portions of the "DoD IPv6 Generic Test Plan (GTP) Version 3," August 2007, reference (d), and are certified for listing on the Unified Capabilities (UC) Approved Products List (APL) as IPv6 Capable. The Secure Computing 1100 and 2150 Sidewinder Firewalls are part of a family of firewalls including the Secure Computing 110, 210, 310, 315, 410, 415, 510, 515, 1150, 2100, 4150, RL100, and RM700 Sidewinder Firewalls running Software Version 7.0.1.00 that were not tested. JITC analysis has determined that all devices within this family are functionally identical for certification purposes and are all certified as IPv6 capable. This certification expires upon changes that could affect interoperability, but no later than 3 years from the date of this memorandum.
3. This special certification is based on IPv6 Capable Interoperability testing conducted by JITC at Fort Huachuca, Arizona, and the vendor's Letter of Conformance (LoC) dated 12 December 2008. Interoperability testing was conducted from 10 through 21 November 2008, at JITC's Advanced IP Technology Capability. Conformance testing was confirmed by Secure Computing and was verified in the LoC provided. Enclosure 2 documents the summary test results and describes the devices. Users should verify interoperability before deploying the devices in an environment that varies significantly from that described.

JITC Memo, JTE, Special Interoperability Test Certification of the Secure Computing 1100 and 2150 Sidewinder Family of Firewalls Running Software Version 7.0.1.00 for Internet Protocol Version 6 Capability

6. The JITC point of contact is Donald L. Hann, DSN 879-5130, commercial (520) 538-5130, or e-mail don.hann@disa.mil.

FOR THE COMMANDER:



2 Enclosures a/s

for RICHARD A. MEADOR
Chief
Battlespace Communications Portfolio

Distribution (electronic mail):

Joint Staff J-6

Joint Interoperability Test Command, Liaison, TE3/JT1

Office of Chief of Naval Operations, CNO N6F2

Headquarters U.S. Air Force, Office of Warfighting Integration & CIO, AF/XCIN (A6N)

Department of the Army, Office of the Secretary of the Army, DA-OSA CIO/G-6 ASA (ALT), SAIS-IOQ

U.S. Marine Corps MARCORSSYSCOM, SIAT, MJI Division I

DOT&E, Net-Centric Systems and Naval Warfare

U.S. Coast Guard, CG-64

Defense Intelligence Agency

National Security Agency, DT

Defense Information Systems Agency, TEMC

Office of Assistant Secretary of Defense (NII)/DOD CIO

U.S. Joint Forces Command, Net-Centric Integration, Communication, and Capabilities Division, J68

DITO, Defense Information Systems Agency (DISA), Attn: GE36, P.O. Box 4502, Arlington, VA 22204-4502

Secure Computing Corporation, Attn: Tony Williams, 2340 Energy Park Drive, St. Paul, MN 55108

ADDITIONAL REFERENCES

- (c) Department of Defense (DoD) Information Technology Standards Registry (DISR), "DoD Internet Protocol Version 6 (IPv6) Standard Profiles for IPv6 Capable Products Version 3.0," July 2008
- (d) Defense Information Systems Agency, Joint Interoperability Test Command, "DoD IPv6 Generic Test Plan Version 3," August 2007
- (e) DoD Chief Information Officer (CIO) Memorandum, "IPv6," 9 June 2003
- (f) DoD CIO Memorandum, "IPv6 Interim Transition Guidance," 29 September 2003
- (g) DoD IPv6 Transition Office, "DoD IPv6 Master Test Plan, Version 2," September 2006
- (h) DoD, "DISR Global Information Grid (GIG) Convergence Master Plan (GCMP), Version 5.25," 29 March 2006

INTERNET PROTOCOL VERSION 6 CAPABLE TESTING SUMMARY

1. **SYSTEM TITLE.** Secure Computing 1100 and 2150 Sidewinder Firewalls running Software Version (V) 7.0.1.00, hereafter referred to as the devices under test (DUTs).
2. **PROPONENT.** Department of Defense (DoD) Internet Protocol (IP) Version 6 (IPv6) Transition Office (DITO).
3. **PROGRAM MANAGER/USER POC.** DITO, Defense Information Systems Agency (DISA), Attn: GE36 Sam Assi, P.O. Box 4502, Arlington, VA 22204-4502, (703) 882-0241, e-mail: sam.assi@disa.mil.
4. **TESTER.** Donald L. Hann, Joint Interoperability Test Command (JITC), P.O. Box 12798, Fort Huachuca, AZ 85670-2798, DSN: 879-5130, commercial: (520) 538-5130, e-mail: don.hann@disa.mil.
5. **DEVICE UNDER TEST DESCRIPTION.** The DUTs were Secure Computing Sidewinder Firewalls, designed by Secure Computing for high network performance and global visibility of dynamic threats in order to block attacks such as viruses, worms, Trojans, intrusion attempts, spam and phishing tactics, cross-site scripting, Structured Query Language (SQL) injections, denial-of-service, and attacks hiding in encrypted protocols.
6. **OPERATIONAL ARCHITECTURE.** The operational architecture was the JITC simulated Defense Information Systems Network (DISN) IP Core Network as depicted in Figure 2-1.
7. **REQUIRED DEVICE INTERFACES.** All IPv6-capable products to be included on the Unified Capabilities Approved Product List must meet the requirements of the DoD Information Technology Standards Registry (DISR), "DoD IPv6 Standard Profiles for IPv6 Capable Products Version 3.0," July 2008. Product testing conducted against these requirements is in accordance with the "DoD IPv6 Generic Test Plan (GTP) Version 3," August 2007. The IPv6 Information Assurance (IA) device profile requirements for conformance and interoperability are in Table 2-1.

Table 2-1. IPv6 Capability Requirements and Status

Secure Computing 1100 and 2150 Sidewinder Firewalls							
RFC	RFC Title	Testing Completed		IA Device		Implemented	Comments
		Conformance	Interoperability	Requirement	Met/Not Met		
IPv6 Base							
2460	Internet Protocol version 6 (IPv6) Specification	Stated in LoC	Yes	M	Met	Yes	
4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	Stated in LoC	Yes	M	Met	Yes	
2461	Neighbor Discovery for IPv6	Stated in LoC	Yes	M	Met	Yes	
2462	IPv6 Stateless Address Auto configuration	Stated in LoC	Yes	M	Met	Yes	
1981	Path Maximum Transmission Unit Discovery for IPv6	Stated in LoC	Yes	M	Met	Yes	
4291	IPv6 Addressing Architecture	Stated in LoC	Yes	M	Met	Yes	
4007	IPv6 Scoped Address Architecture	Stated in LoC	Yes	M	Met	Yes	
4193	Unique Local IPv6 Unicast Addresses	Stated in LoC	Yes	O	Met	Yes	
2710	Multicast Listener Discovery (MLD)	Stated in LoC	Yes	M	Met	Yea	
3810	Multicast Listener Discovery Version 2 (MLDv2) for IPv6	Not Stated	Not Tested	S+	Not Tested	No	
2464	Transmission of IPv6 Packets over Ethernet Networks	Stated in LoC	Yes	CM	Met	Yes	
IPSec							
4301	Security Architecture for the Internet Protocol	Not Stated	Not Tested	CM	Not Tested	No	
4302	IP Authentication Header	Not Stated	Not Tested	CS	Not Tested	No	
4303	IP Encapsulating Security Payload (ESP)	Not Stated	Not Tested	CM	Not Tested	No	
4308	Cryptographic Suites for IPsec	Not Stated	Not Tested	CM	Not Tested	No	
4305	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)	Not Stated	Not Tested	CM	Not Tested	No	
4869	Suite B Cryptographic Suites for IPsec	Not Stated	Not Tested	CM	Not Tested	No	
4309	Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP)	Not Stated	Not Tested	CS	Not Tested	No	
3971	Secure Neighbor Discovery	Not Stated	Not Tested	S	Not Tested	No	
3972	Cryptographically Generated Addresses	Not Stated	Not Tested	S	Not Tested	No	
3041	Privacy Extensions for Stateless Address Auto configuration in IPv6	Not Stated	Not Tested	S	Not Tested	No	

Table 2-1. IPv6 Capability Requirements and Status (continued)

Secure Computing 1100 and 2150 Sidewinder Firewalls							
RFC	RFC Title	Testing Completed		IA Device		Implemented	Comments
		Conformance	Interoperability	Requirement	Met/Not Met		
2407	The Internet IP Security Domain of Interpretation for ISAKMP	Stated in LoC	Yes	CM	Met	Yes	
2408	Internet Security Association and Key Management Protocol	Stated in LoC	Yes	CM	Met	Yes	
2409	The Internet Key Exchange (IKE)	Stated in LoC	Yes	CM	Met	Yes	
4109	Internet Key Exchange (IKEv1) Protocol	Stated in LoC	Yes	CM	Met	Yes	
4304	Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP)	Not Stated	Not Tested	CS	Not Tested	No	
Transition Mechanisms							
4213	Transition Mechanisms for IPv6 Host and Routers	Stated in LoC	Yes	S	Met	Yes	
2766	Network Address Translation – Protocol Translation (NAT-PT)	Not Stated	Not Tested	SN	Not Tested	No	
Server							
3162	RADIUS (Remote Authentication dial-In User Service) and IPv6	Not Stated	Not Tested	CM	Not Tested	No	
Information Assurance							
3585	IPsec Configuration Policy Information Model	Not Stated	Not Tested	CS+	Not Tested	No	
3586	IP Security Policy Requirements	Not Stated	Not Tested	CS+	Not Tested	No	
LEGEND:							
CBC	Cipher Block Chaining		ISAKMP		Internet Security Association and Key Management Protocol		
CCM	CBC MAC Mode		IPv6		Internet Protocol Version 6		
CM	Conditional Must		LoC		Letter of Conformance		
CS	Conditional Should		M		Must		
CS+	Conditional Should+		MAC		Message Authentication Code		
DHCPv6	Dynamic Host Configuration Protocol Version 6		O		Optional		
DoD	Department of Defense		RFC		Request for Comment		
IA	Information Assurance		S		Should		
IETF	Internet Engineering Task Force		S+		Should Plus		
IKEv2	Internet Key Exchange Version 2		SLAAC		Stateless Address Auto-configuration		
IP	Internet Protocol		SN		Should Not		
IPSec	Internet Protocol Security						
NOTE: The terms Must, Conditional Must, Should, Should+, Conditional Should, Conditional Should +, Should Not, and Optional are used to reference specific required RFCs from the IETF, the DoD Information Technology Standards Registry, and the DoD IPv6 Generic Test Plan.							

8. TEST NETWORK DESCRIPTION. The DUTs were tested as part of the JITC simulated DISN IP Core Network managed by the Advanced IP Technology Capability, and configured as shown in Figure 2-2.

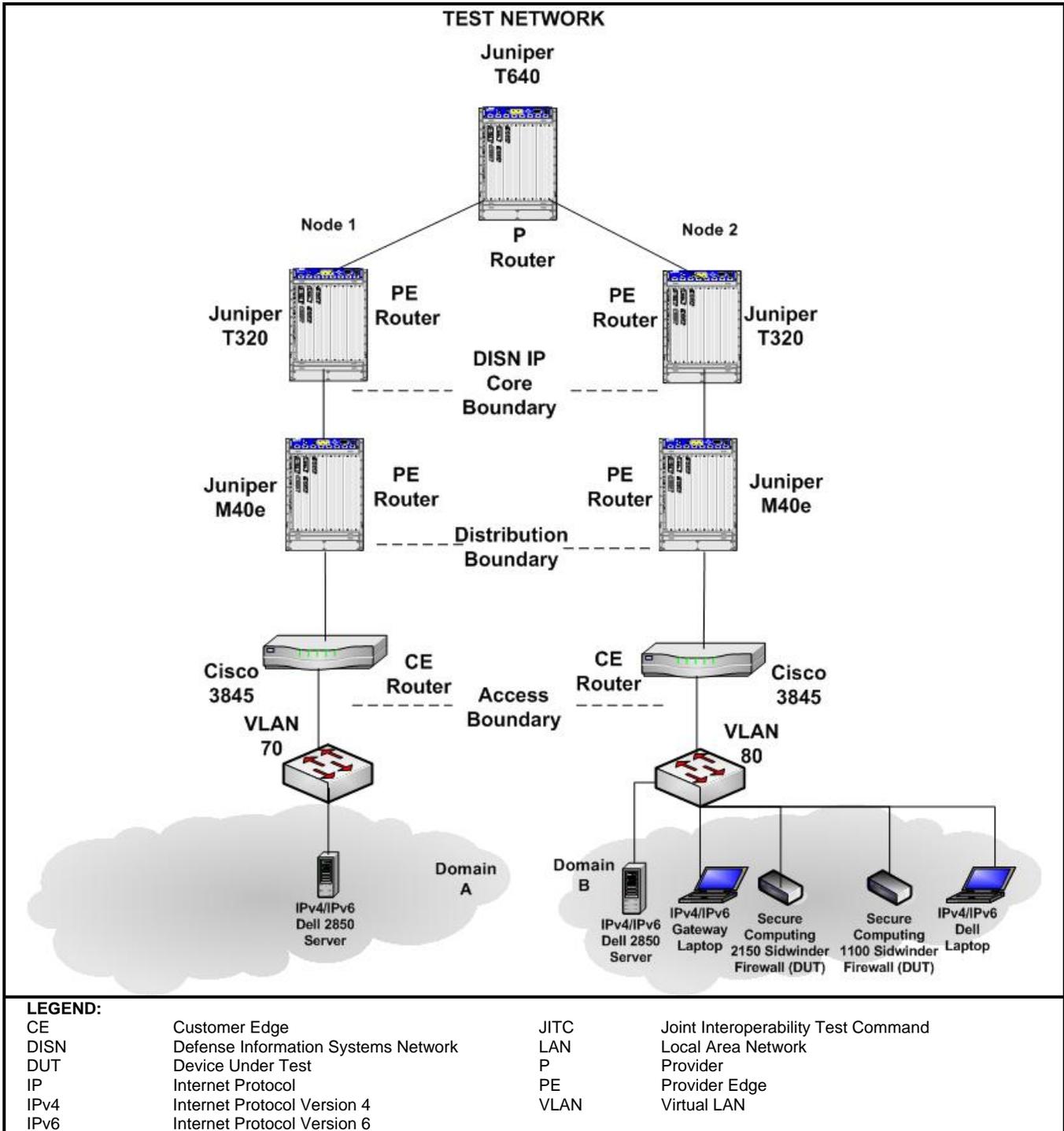


Figure 2-2. Test Network

9. DEVICE CONFIGURATIONS. Table 2-2 provides hardware and software components used in the test network.

Table 2-2. Test Configuration Hardware and Software

Equipment Name	Model Number	IOS/OS/Version(s)
Hardware		
Secure Computing Firewall - DUT	1100	7.0.1.00
Secure Computing Firewall - DUT	2150	7.0.1.00
2 Cisco Routers	Cisco 3845	12.4(11)T
2 Juniper Routers	Juniper M40e	V 7.6R3.6
2 Juniper Routers	Juniper T320	V 7.5R4.4
Juniper Router	Juniper T640	V 7.5R4.4
2 Dell Power Edge Servers	2850	MS 2003 Server
Dell Latitude Notebook	C810	Windows XP Professional
Gateway Notebook	450ROG	Windows XP Professional
Software		
Windows XP Professional	N/A	Build 5.1.2600 SP 3
Windows Server 2003	N/A	Build 5.2.3790 SP 2
VLC media player	N/A	V 0.8.6d
Xlight FTP Server	N/A	V 2.86
Wireshark	N/A	V 1.0.4 (SVN Rev 26501)
LEGEND:		
DUT	Device Under Test	R Release
FTP	File Transfer Protocol	Rev Revision
IOS	Internetworking Operating System	SP Service Pack
LAN	Local Area Network	SVN Software Version Number
MS	Microsoft	T New Technology
N/A	Not Applicable	V Version
OS	Operating System	VLC Video LAN Client

10. TEST LIMITATIONS. None.

11. TEST RESULTS .

a. IPv6 Base.

Test Case C.1.2. The Request for Comments (RFC) 2460 IPv6 Specification is the base specification of the IPv6 protocol. It specifies a number of parameters that enable successful completion of IPv6 traffic addressing and control. The Secure Computing 1100 and 2150 Sidewinder Firewalls running Software V 7.0.1.00 met the test requirement.

Test Case C.1.14. The RFC 4443 Internet Control Message Protocol (ICMP) for the IPv6 specification identifies ICMP messages for the IPv6 protocol. It includes message format and identifies two types of messages: error and informational. The Secure Computing 1100 and 2150 Sidewinder Firewalls running Software V 7.0.1.00 met the test requirement.

Test Case C.1.3. The RFC 2461 Neighbor Discovery for IPv6 specifies the neighbor discovery function that is similar to address resolution protocol in IP Version 4 (IPv4). It is necessary for implementing neighbor solicitations and neighbor advertisements within IPv6. The Secure Computing 1100 and 2150 Sidewinder Firewalls running Software V 7.0.1.00 met the test requirement.

Test Case C.1.4. The RFC 2462 IPv6 Stateless Address Auto-configuration specifies how a host auto-configures its interfaces in IPv6. These steps include determining whether the source addressing should be stateless or stateful, whether the information obtained should be solely the address or include other information, and whether Duplicate Address Detection identifies duplicate addresses on the network, and then issues a new address accordingly. The Secure Computing 1100 and 2150 Sidewinder Firewalls running Software V 7.0.1.00 met the test requirement.

Test Case C.1.13. The RFC 4291 IPv6 Addressing Architecture defines the specifications for the addressing architecture of the IPv6 protocol. The definitions cover unicast addresses, anycast addresses, and multicast addresses. The Secure Computing 1100 and 2150 Sidewinder Firewalls running Software V 7.0.1.00 met the test requirement.

Test Case C.1.11. The RFC 4007 IPv6 Scoped Address Architecture defines the nature and characteristics for the usage of IPv6 addresses of different scopes. The Secure Computing 1100 and 2150 Sidewinder Firewalls running Software V 7.0.1.00 met the test requirement.

Test Case C.1.12. The RFC 4193 Unique Local IPv6 Unicast Addresses defines globally unique local addresses. Local IPv6 unicast addressing is intended to be used for local communications and is not expected to be routed to the Internet. The Secure Computing 1100 and 2150 Sidewinder Firewalls running Software V 7.0.1.00 met the test requirement.

Test Case C.1.8. The RFC 2710 Multicast Listener Discovery for IPv6 specifies the protocol used by an IPv6 router to discover the presence of multicast listeners (i.e., nodes wishing to receive multicast packets) on its directly attached links, and to discover specifically which multicast addresses are of interest to those neighboring nodes. The Secure Computing 1100 and 2150 Sidewinder Firewalls running Software V 7.0.1.00 met the test requirement.

Test Case C.1.5. The RFC 2464 Transmission of IPv6 Packets over Ethernet Networks specifies the frame format for transmission of IPv6 link-local addresses and statelessly auto-configured addresses on Ethernet networks. The Secure Computing 1100 and 2150 Sidewinder Firewalls running Software V 7.0.1.00 met the test requirement.

b. Transition Mechanisms.

Test Case C.3.18. The RFC 4213 Transition Mechanisms for IPv6 Host and Routers specifies IPv4 co-existence mechanisms that can be implemented by IPv6 devices. The Secure Computing 1100 and 2150 Sidewinder Firewalls running Software V 7.0.1.00 met the test requirement.

c. Conclusion. The Secure Computing 1100 and 2150 Sidewinder Firewalls running Software V 7.0.1.00 met all the required RFCs.

12. TEST AND ANALYSIS REPORT. No detailed test report was written in accordance with guidance from the Assistant Secretary of Defense (Networks & Information Integration). All test data is maintained in the Advanced IP Technology Capability and is available upon request. This certification is available on the Joint Interoperability Tool (JIT). The JIT homepage is <http://jit.fhu.disa.mil> (NIPRNet), or <http://199.208.204.125/> (SIPRNet). The JIT has links to JITC interoperability documents to provide the DoD community, including the warfighter in the field, easy access to the latest interoperability information. System interoperability status information is available via the JITC System Tracking Program (STP). The STP is accessible by .mil/.gov users on the NIPRNet at: <https://stp.fhu.disa.mil/>.