



DEFENSE INFORMATION SYSTEMS AGENCY

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

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

25 Mar 09

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Special Interoperability Test Certification of the TippingPoint 2500N Intrusion Prevention System Running the TippingPoint Operating System Version 3.0.1.1110 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 6212.01E, "Interoperability and Supportability of Information Technology and National Security Systems," 15 December 2008
(c) through (i) 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 TippingPoint 2500N Intrusion Prevention System (IPS) running the TippingPoint Operating System (TOS) Version 3.0.1.1110 met the Internet Protocol (IP) Version 6 (IPv6) Capable interoperability requirements of the Information Assurance (IA) product class 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 TippingPoint 2500N IPS running the TOS Version 3.0.1.1110 successfully completed the related IPv6 Interoperability portions of the "DoD IPv6 Generic Test Plan (GTP) Version 3," August 2007, reference (d), and is certified for listing on the Unified Capabilities (UC) Approved Products List (APL) as IPv6 Capable. This certification expires upon changes that could affect interoperability, but no later than 4 years from the date of this memorandum.

The TippingPoint 2500N IPS was also tested against the recommended requirements of an IA device from the National Security Agency's Draft "IPv6 Information Assurance Test Plan" (ITP) 2008, reference (e).

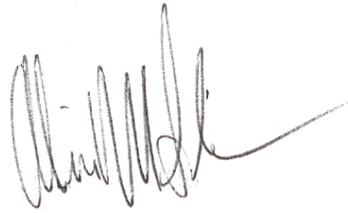
3. This special certification is based on IPv6 Capable Interoperability testing conducted by JITC at Fort Huachuca, Arizona, and the vendor's Letter of Conformance (LoC) dated 23 January 2009. Interoperability testing was conducted from 17 through 27 February 2009 at JITC's Advanced IP Technology Capability. Conformance testing was confirmed by TippingPoint and was verified in the LoC provided. Enclosure 2 documents summary test results from both the GTP and ITP, and describes the devices. Users should verify interoperability before deploying the devices in an environment that varies significantly from that described.

4. The device's interoperability status summary is in Table 1, and Table 2 contains the equipment listing.

JITC Memo, JTE, Special Interoperability Test Certification of the TippingPoint 2500N Intrusion Prevention System Running the TippingPoint Operating System Version 3.0.1.1110 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:



for RICHARD A. MEADOR
Chief
Battlespace Communications Portfolio

2 Enclosures a/s

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

TippingPoint Technologies Inc., Attn: Mr. James Collinge, CISSP, 7501 Capital of Texas Highway, Austin, TX 78731

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) National Security Agency, "Internet Protocol Version Six Information Assurance Test Plan," Draft, 2008
- (f) DoD Chief Information Officer (CIO) Memorandum, "IPv6," 9 June 2003
- (g) DoD CIO Memorandum, "IPv6 Interim Transition Guidance," 29 September 2003
- (h) DoD IPv6 Transition Office, "DoD IPv6 Master Test Plan, Version 2," September 2006
- (i) 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.** The TippingPoint 2500N Intrusion Prevention System (IPS) running the TippingPoint Operating System (TOS) Version 3.0.1.1110, hereafter referred to as the device under test (DUT).
- 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 DUT was an Application Specific Integrated Circuit (ASIC) based Threat Suppression Engine (TSE) designed by TippingPoint to be able to perform thousands of checks on each packet flow simultaneously, with a TSE architecture that utilizes custom ASICs, a 20 Gigabit per second backplane and high performance network processors to perform total packet flow inspection at Layers 2 through 7.
- 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) product class profile requirements for conformance and interoperability are in Table 2-1. Table 2-2 lists the National Security Agency (NSA) recommended requirements test cases used to verify IA status according to the NSA's Draft "IPv6 Information Assurance Test Plan" (ITP).

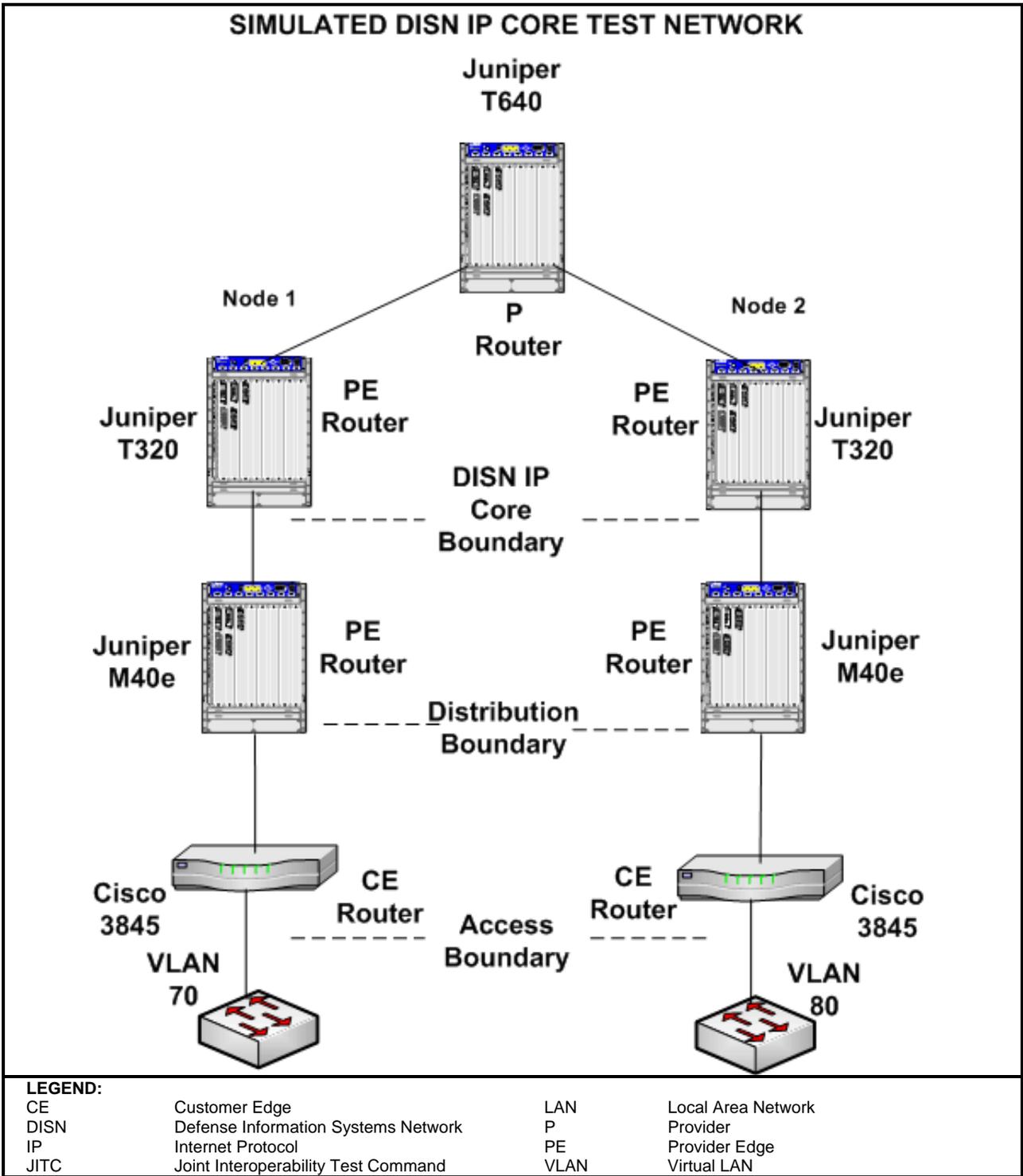


Figure 2-1. JITC Simulated DISN IP Core Network

Table 2-1. IPv6 Capability Requirements and Status

TippingPoint 2500N IPS							
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	
5095	Deprecation of Type 0 Routing Headers in IPv6	Stated in LoC	Yes	M	Met	Yes	
2463	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	Stated in LoC	Yes	M	Met	Yes	Note 1
2461	Neighbor Discovery for IP version 6 (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	S	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	Not Stated	Not Tested	O	Not Tested	No	
2710	Multicast Listener Discovery (MLD)	Stated in LoC	Yes	M	Met	Yes	
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	Note 2
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	
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	
4306	Internet Key Exchange (IKEv2) Protocol	Not Stated	Not Tested	CM	Not Tested	No	
4307	Cryptographic Algorithms for Internet Key Exchange Version 2 (IKEv2)	Not Stated	Not Tested	CM	Not Tested	No	

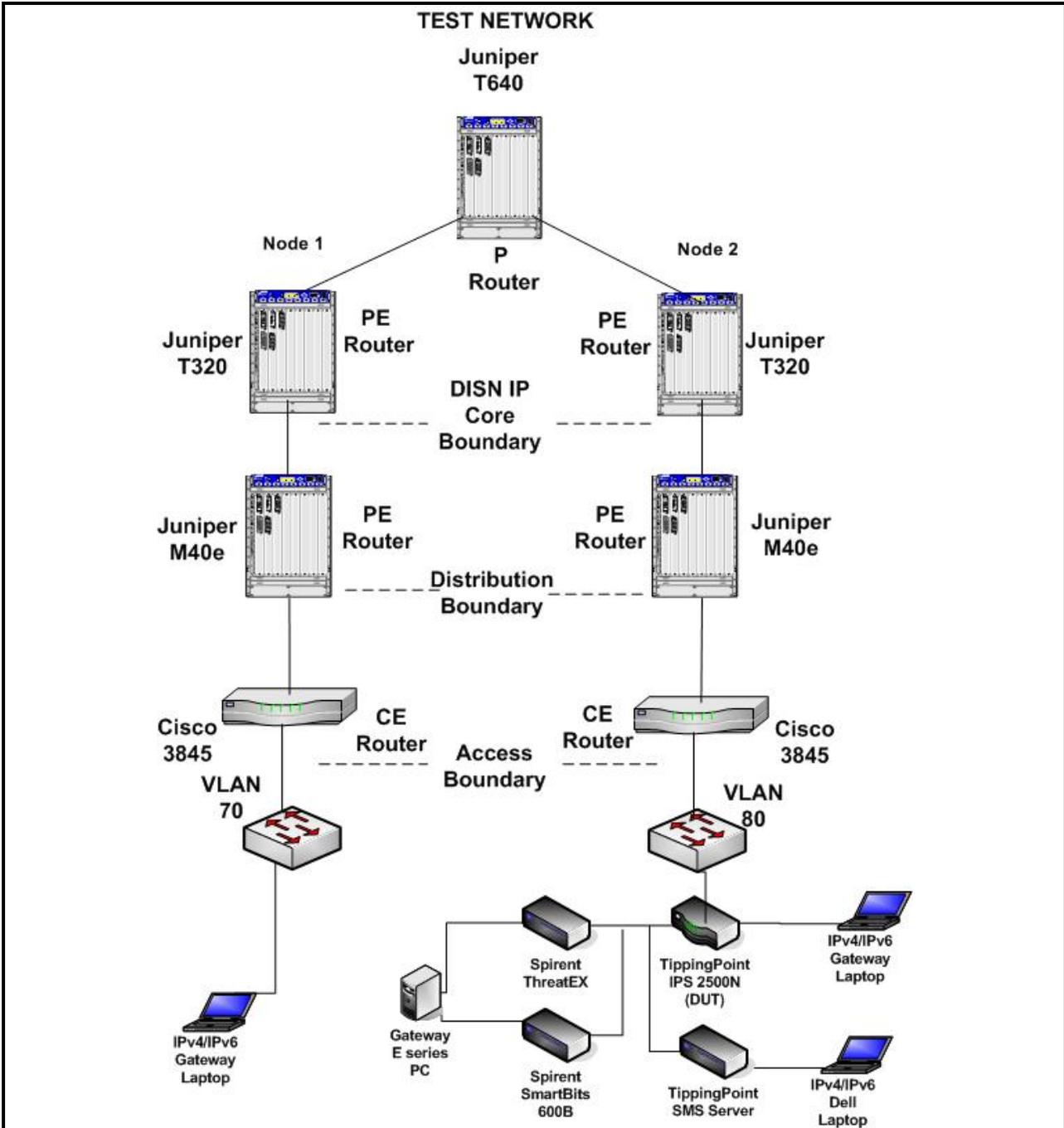
Table 2-1. IPv6 Capability Requirements and Status (continued)

TippingPoint 2500N IPS							
RFC	RFC Title	Testing Completed		IA Device		Implemented	Comments
		Conformance	Interoperability	Requirement	Met/Not Met		
Transition Mechanisms							
4213	Transition Mechanisms for IPv6 Host and Routers	Not Stated	Not Tested	S	Not Tested	No	
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	
IA Device							
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		LoC		Letter of Conformance		
CCM	CBC MAC Mode		M		Must		
CM	Conditional Must		MAC		Message Authentication Code		
CS	Conditional Should		MIB		Management Information Base		
CS+	Conditional Should+		N/R		No Requirement		
DHCPv6	Dynamic Host Configuration Protocol Version 6		NAT		Network Address Translation		
DISR	DoD Information Technology Standards Registry		O		Optional (May)		
DNS	Domain Name Service		OSPF		Open Shortest Path First		
DoD	Department of Defense		PPP		Point-to-Point Protocol		
FTP	File Transfer Protocol		QoS		Quality of Service		
HMC	Hardware Management Console		RFC		Request for Comment		
IETF	Internet Engineering Task Force		RoHC		Robust Header Compression		
IKEv2	Internet Key Exchange Version 2		RSVP		Resource ReSerVation Protocol		
IA	Information Assurance		RTP		Real-Time Transport Protocol		
IP	Internet Protocol		S		Should		
IPS	Intrusion Prevention System		SLAAC		Stateless Address Auto-configuration		
IPSec	Internet Protocol Security		SN		Should Not		
IPv4	Internet Protocol Version 4		S+		Should+		
IPv6	Internet Protocol Version 6		UDP		User Datagram Protocol		
NOTES:							
1. Per DISR Waiver, allowed to meet requirements of RFC 2463 instead of 4443.							
2. The device must be conformant to at least one of the Connection Technologies protocols							
3. 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.							

Table 2-2. NSA Test Case Status

TippingPoint 2500N IPS		
Test Case	Critical	Status
Test 2.1.01: Role Separation	Moderate	Met
Test 2.1.02: Role Revocation	Moderate	Met
Test 2.1.03: Pre-Authentication Advisory Notice	Moderate	Not Met
Test 2.1.04: Post-Authentication Advisory Notice	Moderate	Met
Test 2.1.05: User Session Access	Low	Partial
Test 2.1.06: Authentication Policy	Low	Partial
Test 2.1.07: Local and Remote Administration	Critical	Met
Test 2.1.08: Basic: Inactivity Guard	Low	Partial
Test 2.2.04: Basic: TCP Traffic Enforcement	Critical	Met
Test 2.2.06: Basic: Stateful Inspection	Critical	Met
Test 2.3.01: Advanced: Trusted Computing Base	Critical	Met
Test 2.3.02: Advanced: Environmental Variables	Low	Partial
Test 2.3.08: Advanced: Configuration Surety	Moderate	Partial
Test 2.4.01: Audit Inspection	Moderate	Met
Test 2.4.03: Discretionary Access Control	Low	Partial
Test 2.4.04: Mandatory Access Control	Low	Not Met
Test 2.5.01: ICMPv6 Control Traffic	Critical	Met
Test 2.5.05: IPSec Verification	Critical – if supported	Not Supported
Test 2.5.06: Address Autoconfiguration	Moderate	Met
Test 2.5.07: Transition Mechanism Blocking	Critical – if supported	Not Supported
Test 2.6.01: Attacks: Denial of Service	Critical	Met
Test 2.6.03: Attacks: Common Vulnerabilities and Exploits	Critical	Met
Test 2.6.04: Attacks: Penetration Test	Critical	Met
Test 2.6.05: Attacks: Startup/Shutdown Vulnerabilities	Moderate	Met
Test 2.6.06: Attacks: Tiny Fragments for IPv4 and IPv6	Moderate	Met
Test 2.7.01: Documentation: IPS Developer	Low	Not Met
Test 2.7.02: Documentation: Developer Pre-Coverage	Low	Not Met
Test 2.7.03: Documentation: Strength of IPS	Low	Not Met
Test 2.7.04: Documentation: Development Processes	Low	Not Met
Test 2.7.05: Documentation: Configuration Management	Low	Not Met
Test 2.7.06: Documentation: Delivery Processes	Low	Not Met
Test 2.7.07: Documentation: Administrator/User Guidance	Low	Met
Test 2.7.08: Documentation: Vulnerability Analysis	Low	Not Met
Test 2.7.09: Documentation: Software Design	Low	Not Met
Test 2.7.10: Documentation: Cryptography	Low	Not Met
Test 2.7.11: Documentation: Software Design Test	Low	Not Met
Test 3.1.01: Performance Test	Moderate	Met
LEGEND:		
ICMPv6	Internet Control Message Protocol for IPv6	IPv6
IPSec	Internet Protocol Security	TCP
IPV4	Internet Protocol Version 4	Internet Protocol Version 6
IPS	Intrusion Prevention System	NSA
		National Security Agency
		Transmission Control Protocol

8. TEST NETWORK DESCRIPTION. The DUT was 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.



LEGEND:			
CE	Customer Edge	LAN	Local Area Network
DISN	Defense Information Systems Network	P	Provider
DUT	Device Under Test	PC	Personal Computer
IP	Internet Protocol	PE	Provider Edge
IPS	Intrusion Prevention System	SMS	Security Management System
IPv4	Internet Protocol Version 4	VLAN	Virtual LAN
IPv6	Internet Protocol Version 6		

Figure 2-2. TippingPoint Test Network

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

Table 2-3. TippingPoint Test Configuration Hardware and Software

Equipment Name	Model Number	IOS/OS/Version(s)	
Hardware			
TippingPoint IPS - DUT	2500N	V 3.0.1.1110	
TippingPoint SMS	Dell PowerEdge 1950	Fedora Core 5/V 3.0.0.7063	
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	
Spirent	ThreatEX	V 3.32.62	
Spirent	SmartBits 600B	V 7.56	
2 Gateway Notebook	450ROG	MS Windows XP Professional	
Dell Notebook	8100	MS Windows XP Professional	
Gateway PC	E Series	MS Windows XP Professional	
Software			
Fedora Core 5	N/A	Linux V 2-6-15	
Avalanche	N/A	V 7.56 Build 45385	
MS Windows XP Professional	N/A	Build 5.1.2600 SP3	
VLC Media Player	N/A	V 0.8.6i	
Wireshark	N/A	V 1.0.5 (SVN Rev 26954)	
LEGEND:			
DUT	Device Under Test	R	Release
IOS	Internetworking Operating System	Rev	Revision
IPS	Intrusion Prevention System	SMS	Security Management System
LAN	Local Area Network	SP	Service Pack
MS	Microsoft	SVN	Software Version Number
N/A	Not Applicable	T	New Technology
OS	Operating System	V	Version
PC	Personal Computer	VLC	VideoLAN 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 TippingPoint 2500N IPS met the test requirement.

Test Case Not Applicable . The RFC 5095, Deprecation of Type 0 Routing Headers, specifies that all IPv6 nodes MUST NOT initiate or propagate IPv6 packets containing Type 0 Routing Headers. Any IPv6 node that receives a packet with a destination address assigned to it that contains an RH0 extension header MUST NOT execute traffic-forwarding algorithms. The TippingPoint 2500N IPS met the test requirement.

Test Case C.1.14. The RFC 2463 identifies Internet Control Message Protocol messages for the IPv6 protocol. It includes message format and identifies two types of messages: error and informational. The TippingPoint 2500N IPS 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 TippingPoint 2500N IPS 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 Duplicate Address Detection. The TippingPoint 2500N IPS met the test requirement.

Test Case C.1.1. The RFC 1981 Path Maximum Transmission Unit Discovery for IPv6 is necessary for proper IPv6 implementations. It acts as a mechanism to determine the maximum size of packets to traverse the network without fragmentation. The TippingPoint 2500N IPS 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 TippingPoint 2500N IPS 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 TippingPoint 2500N IPS met the test requirement.

Test Case C.1.8. The RFC 2710 Multicast Listener Discovery (MLD) 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 TippingPoint 2500N IPS 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 TippingPoint 2500N IPS met the test requirement.

b. Conclusion. The TippingPoint 2500N IPS met all the required RFCs.

12. TEST AND ANALYSIS REPORT. 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/>.