



## DEFENSE INFORMATION SYSTEMS AGENCY

P. O. BOX 549  
FORT MEADE, MARYLAND 20755-0549

IN REPLY  
REFER  
TO:

Joint Interoperability Test Command (JITC)

**1 Aug 12**

### MEMORANDUM FOR DISTRIBUTION

**SUBJECT:** Special Interoperability Test Certification of the Sourcefire 3D System Intrusion Protection System and Intrusion Detection System with Software Release 4.10.X

References: (a) DoD Directive 4630.05, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," 5 May 2004  
(b) DoD CIO, Memorandum, "Interim Guidance for Interoperability of Information Technology (IT) and National Security Systems (NSS)," 27 March 2012  
(c) through (f), 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 Sourcefire 3D System Intrusion Protection System (IPS) and Intrusion Detection System (IDS) with Software Release 4.10.X, hereinafter referred to as the System Under Test (SUT), meets all the critical interoperability requirements for an IPS/IDS and is certified for joint use within the Defense Information System Network (DISN). The operational status of the SUT must be verified during deployment. Any new discrepancies that are discovered in the operational environment will be evaluated for impact and adjudicated to the satisfaction of the Defense Information Systems Agency (DISA) via a vendor Plan of Action and Milestones to address the concern(s) within 120 days of identification. JITC conducted testing using IPS/IDS requirements within the Unified Capabilities Requirements (UCR) 2008, Change 2, Reference (c) and IPS/IDS test procedures, Reference (d). JITC does not certify any other configurations, features, or functions, except those cited within this memorandum. This certification expires upon changes that affect interoperability, but no later than four years from the date of this memorandum.

3. This certification is based on interoperability testing conducted by JITC, review of the vendor's Letter of Compliance (LoC), and DISA Information Assurance (IA) Certification Authority (CA) approval of the IA configuration. JITC conducted interoperability testing at the Indian Head, Maryland test facility from 5 through 29 July 2011. The DISA Field Security Operations (FSO) CA has reviewed the IA Findings Report for the SUT, Reference (e), and based on the findings in the report has provided a positive recommendation of the IA configuration on June 15, 2012. The acquiring agency or site will be responsible for the DoD Information Assurance Certification and Accreditation Process (DIACAP) accreditation. The JITC certifies the SUT has met the UCR requirements for IPS/IDS devices. Enclosure 2, documents the test results and describes the test network and system configurations including specified patch releases. Enclosure 3, System Functional and Capability Requirements, lists the IPS/IDS Capability Requirements (CR) and Functional Requirements (FR).

JITC Memo, JTG, Special Interoperability Test Certification of Sourcefire 3D System Intrusion Protection System and Intrusion Detection System with Software Release 4.10.X

4. Section 5.8 of Reference (c) establishes the threshold CRs/FRs used to evaluate the interoperability of the SUT as an IPS/IDS. Tables 1 and 2 list the IPS/IDS interfaces, CRs, FRs, and status of the requirements.

**Table 1. SUT Interface Interoperability Status**

Interface	Critical (See note 1)	UCR Reference (UCR 2008 CH 2)	Threshold CR/FR Requirements (See note 2)	Status	Remarks								
<b>Intrusion Protection System</b>													
10Base-X	No	5.3.2.4/5.3.3.10.1.2	1-4	Met	SUT met requirements for specified interfaces								
100Base-X	No	5.3.2.4/5.3.3.10.1.2	1-4	Met	SUT met requirements for specified interfaces								
1000Base-X	No	5.3.2.4/5.3.3.10.1.2	1-4	Met	SUT met requirements for specified interfaces								
10GBase-X	No	5.3.2.4/5.3.3.10.1.2	1-4	N/A	Not supported by the SUT								
40GBase-X	No	5.3.2.4/5.3.3.10.1.2	1-4	N/A	Not supported by the SUT								
100GBase-X	No	5.3.2.4/5.3.3.10.1.2	1-4	N/A	Not supported by the SUT								
<p><b>NOTES:</b></p> <p>1. UCR did not identify individual interface requirements for security devices. SUT must minimally provide an Ethernet interface (one of the listed).</p> <p>2. CR/FR requirements are contained in Table 2. CR/FR numbers represent a roll-up of UCR requirements. Enclosure 3 provides a list of more detailed requirements for security device products.</p> <p><b>LEGEND:</b></p> <table style="width: 100%; border: none;"> <tr> <td style="width: 50%;">Base-X Ethernet generic designation</td> <td style="width: 50%;">GBaseX Gigabit generic designation</td> </tr> <tr> <td>CH Change</td> <td>N/A Not Applicable</td> </tr> <tr> <td>CR Capability Requirement</td> <td>SUT System Under Test</td> </tr> <tr> <td>FR Functional Requirement</td> <td>UCR Unified Capabilities Requirement</td> </tr> </table>						Base-X Ethernet generic designation	GBaseX Gigabit generic designation	CH Change	N/A Not Applicable	CR Capability Requirement	SUT System Under Test	FR Functional Requirement	UCR Unified Capabilities Requirement
Base-X Ethernet generic designation	GBaseX Gigabit generic designation												
CH Change	N/A Not Applicable												
CR Capability Requirement	SUT System Under Test												
FR Functional Requirement	UCR Unified Capabilities Requirement												

**Table 2. SUT Capability Requirements and Functional Requirements Status**

CR/FR ID	Capability/ Function	Applicability (See note)	UCR Reference (UCR 2008 CH 2)	Status	Remarks																								
1	<b>Conformance Requirements</b>																												
	Conformance Standards	Required	5.8.4.2	Met																									
2	<b>Information Assurance Requirements</b>																												
	General Requirements	Required	5.8.4.3.1	Met																									
	Reserved	N/A	5.8.4.3.2	N/A																									
	Configuration Management	Required	5.8.4.3.3	Met																									
	Alarms & Alerts	Required	5.8.4.3.4	Met	See the Information Assurance Findings and Mitigations Summary Report.																								
	Audit and Logging	Required	5.8.4.3.5	Met	See the Information Assurance Findings and Mitigations Summary Report.																								
	Reserved	N/A	5.8.4.3.6	N/A																									
	Documentation	Required	5.8.4.3.7	Met	See the Information Assurance Findings and Mitigations Summary Report.																								
	Cryptography	Required	5.8.4.3.8	N/A	Cryptography is optional with the exception that all outgoing communications are encrypted.																								
	Security Measures	Required	5.8.4.3.9	Met																									
	System and Communication Protection	Required	5.8.4.3.10	Met																									
	Other Requirements	Required	5.8.4.3.11	Met																									
Performance	Required	5.8.4.3.12	Met																										
3	<b>Functionality</b>																												
	Policy	Required	5.8.4.4.1	N/A	FW & VPN Only																								
	Filtering	Required	5.8.4.4.2	N/A	FW Only																								
4	<b>IPS Functionality</b>																												
	IPS Security Device Requirements	Required	5.8.4.5	Met	IDS/IPS Only																								
<p><b>NOTE:</b> Criticality represents high level roll-up of the CR/FR area. Table 3-1 of Enclosure 3 provides detailed CR/FR for each security device product (FW, IPS/IDS, VPN component).</p> <p><b>LEGEND:</b></p> <table> <tr> <td>CH</td> <td>Change</td> <td>IP</td> <td>Internet Protocol</td> </tr> <tr> <td>CR</td> <td>Capability Requirement</td> <td>IPS</td> <td>Intrusion Prevention System</td> </tr> <tr> <td>FR</td> <td>Functional Requirement</td> <td>N/A</td> <td>Not Applicable</td> </tr> <tr> <td>FW</td> <td>Firewall</td> <td>UCR</td> <td>Unified Capabilities Requirements</td> </tr> <tr> <td>ID</td> <td>Identification</td> <td>VPN</td> <td>Virtual Private Network</td> </tr> <tr> <td>IDS</td> <td>Intrusion Detection System</td> <td></td> <td></td> </tr> </table>						CH	Change	IP	Internet Protocol	CR	Capability Requirement	IPS	Intrusion Prevention System	FR	Functional Requirement	N/A	Not Applicable	FW	Firewall	UCR	Unified Capabilities Requirements	ID	Identification	VPN	Virtual Private Network	IDS	Intrusion Detection System		
CH	Change	IP	Internet Protocol																										
CR	Capability Requirement	IPS	Intrusion Prevention System																										
FR	Functional Requirement	N/A	Not Applicable																										
FW	Firewall	UCR	Unified Capabilities Requirements																										
ID	Identification	VPN	Virtual Private Network																										
IDS	Intrusion Detection System																												

JITC Memo, JTG, Special Interoperability Test Certification of Sourcefire 3D System Intrusion Protection System and Intrusion Detection System with Software Release 4.10.X

5. In accordance with the Program Manager's request, JITC did not develop a detailed test report. JITC distributes interoperability information via the JITC Electronic Report Distribution system, which uses Non-secure Internet Protocol Router Network (NIPRNet) e-mail. More comprehensive interoperability status information is available via the JITC System Tracking Program (STP), which .mil/.gov users can access on the NIPRNet at <https://stp.fhu.disa.mil>. Test reports, lessons learned, and related testing documents and references are on the JITC Joint Interoperability Tool at <http://jit.fhu.disa.mil> (NIPRNet). Information related to Defense Switched Network (DSN) testing is on the Telecommunications Switched Services Interoperability website at <http://jitc.fhu.disa.mil/tssi>. All associated data is available on the DISA Unified Capabilities Certification Office (UCCO) website located at <https://aplots.disa.mil>.

6. The JITC testing point of contact is Mr. Keith Watson, commercial (301) 743-4305. His e-mail address is [keith.d.watson2.civ@mail.mil](mailto:keith.d.watson2.civ@mail.mil) and mailing address is 3341 Strauss Avenue, Suite 236, Indian Head, Maryland 20640-5149. The UCCO tracking number for the SUT is 1021801.

FOR THE COMMANDER:

3 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

HQUSAISEC, AMSEL-IE-IS

## **ADDITIONAL REFERENCES**

- (c) Office of the Assistant Secretary of Defense for Networks and Information Integration Document, "Department of Defense Unified Capabilities Requirements 2008, Change 2," December 2010
- (d) Joint Interoperability Test Command, "Security Device Test Plan," June, 2011
- (e) Joint Interoperability Test Command, "Information Assurance (IA) Findings Report for Sourcefire 3D Systems Release 4.10.X (Tracking Number 1021801)," April 2012
- (f) Department of Defense Instruction 8100.04, "DoD Unified Capabilities (UC)," 9 December 2010

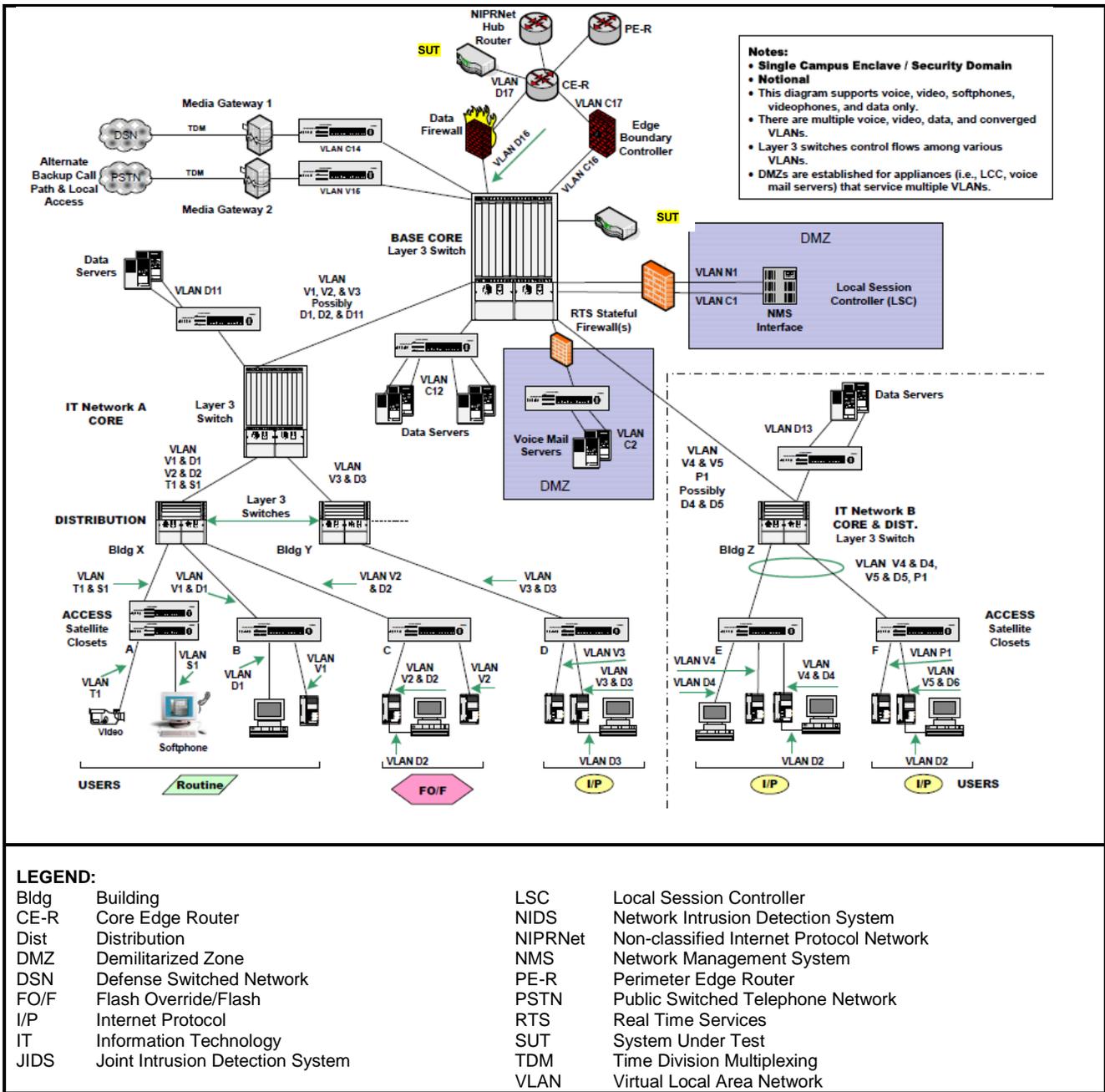
(This page left intentionally blank).

## CERTIFICATION TESTING SUMMARY

- 1. SYSTEM TITLE.** The Sourcefire 3D System Intrusion Protection System and Intrusion Detection System with Software Release 4.10.X.
- 2. SPONSOR.** Ms. Sylvia Mapps, 5275 Leesburg Pike, Falls Church, VA 22041, Email: [sylvia.mapps@disa.mil](mailto:sylvia.mapps@disa.mil).
- 3. SYSTEM POC.** Ms. Sarah Gill, Email: [sgill@sourcefire.com](mailto:sgill@sourcefire.com)
- 4. TESTER.** Joint Interoperability Test Command (JITC)
- 5. SYSTEM DESCRIPTION.** The Sourcefire 3D System Intrusion Protection System and Intrusion Detection System with Software Release (R) 4.10.X, hereinafter referred to as the System Under Test (SUT), provides users with real-time network intelligence for real-time network defense. Sourcefire 3D System provides tools which allow users to:
  - discover the changing assets and vulnerabilities on a network
  - determine the types of attacks against a network and the impact they have to business processes
  - defend a network in real time

Each Sourcefire 3D System sensor has a management interface that allows management over a protected, out-of-band management network while utilizing separate sensing interfaces to monitor network segments on networks where threats are likely to occur.

**6. OPERATIONAL ARCHITECTURE.** JITC tested the SUT to requirements identified for the IPS/IDS UCR product category. A high-level Defense Information Systems Network (DISN) node architecture, as depicted on Figure 2-1, displays the IDS/IPS devices.



**Figure 2-1. DISN Security Device Architecture**

**7. INTEROPERABILITY REQUIREMENTS.** The interface, Capability Requirements (CR) and Functional Requirements (FR), Information Assurance (IA), and other requirements for security devices are established by Section 5.8 of Reference (c).

**7.1. Interfaces.** The Sourcefire 3D System with Software R 4.10.X uses external interfaces to connect to the Global Information Grid (GIG) network. Table 2-1, shows the physical interfaces supported by the SUT. The table documents the physical interfaces and the associated standards.

**Table 2-1. Security Device Interface Requirements**

Interface (Note 1)	UCR Reference (UCR Change 2)	FW	IPS	VPN	Criteria (See Note 2)	Remarks																
10Base-X	5.3.2.4 / 5.3.3.10.1.2	C	C	C	Support minimum threshold CRs/FRs 1-4 and meet interface criteria for 802.3i and 802.3j																	
100Base-X	5.3.2.4 / 5.3.3.10.1.2	C	C	C	Support minimum threshold CRs/FRs 1-4 and meet interface criteria for 802.3u																	
1000Base-X	5.3.2.4 / 5.3.3.10.1.2	C	C	C	Support minimum threshold CRs/FRs 1-4 and meet interface criteria for 802.3z																	
10GBase-X	5.3.2.4 / 5.3.3.10.1.2	C	C	C	Support minimum threshold CRs/FRs 1-4 and meet interface criteria for 802.3ae, 802.3ak, 802.3an,802.3aq, and 802.3av																	
40GBase-X	5.3.2.4 / 5.3.3.10.1.2	C	C	C	Support minimum threshold CRs/FRs 1-3 and meet interface criteria for 802.3ba																	
100GBase-X	5.3.2.4 / 5.3.3.10.1.2	C	C	C	Support minimum threshold CRs/FRs 1-4 and meet interface criteria for 802.3ba																	
<p><b>NOTES:</b></p> <p>1. UCR did not identify individual interface requirements for security devices. SUT must minimally provide an Ethernet interface (one of the listed).</p> <p>2. CR/FR requirements are contained in Table 2-2. CR/FR numbers represent a roll-up of UCR requirements. Enclosure 3, provides a list of more detailed requirements for security device products.</p> <p><b>LEGEND:</b></p> <table> <tr> <td>C</td> <td>Conditional</td> <td>IPS</td> <td>Intrusion Protection System</td> </tr> <tr> <td>CR</td> <td>Capability Requirement</td> <td>UCR</td> <td>Unified Capabilities Requirements</td> </tr> <tr> <td>FR</td> <td>Functional Requirement</td> <td>VPN</td> <td>Virtual Private network</td> </tr> <tr> <td>FW</td> <td>Firewall</td> <td></td> <td></td> </tr> </table>							C	Conditional	IPS	Intrusion Protection System	CR	Capability Requirement	UCR	Unified Capabilities Requirements	FR	Functional Requirement	VPN	Virtual Private network	FW	Firewall		
C	Conditional	IPS	Intrusion Protection System																			
CR	Capability Requirement	UCR	Unified Capabilities Requirements																			
FR	Functional Requirement	VPN	Virtual Private network																			
FW	Firewall																					

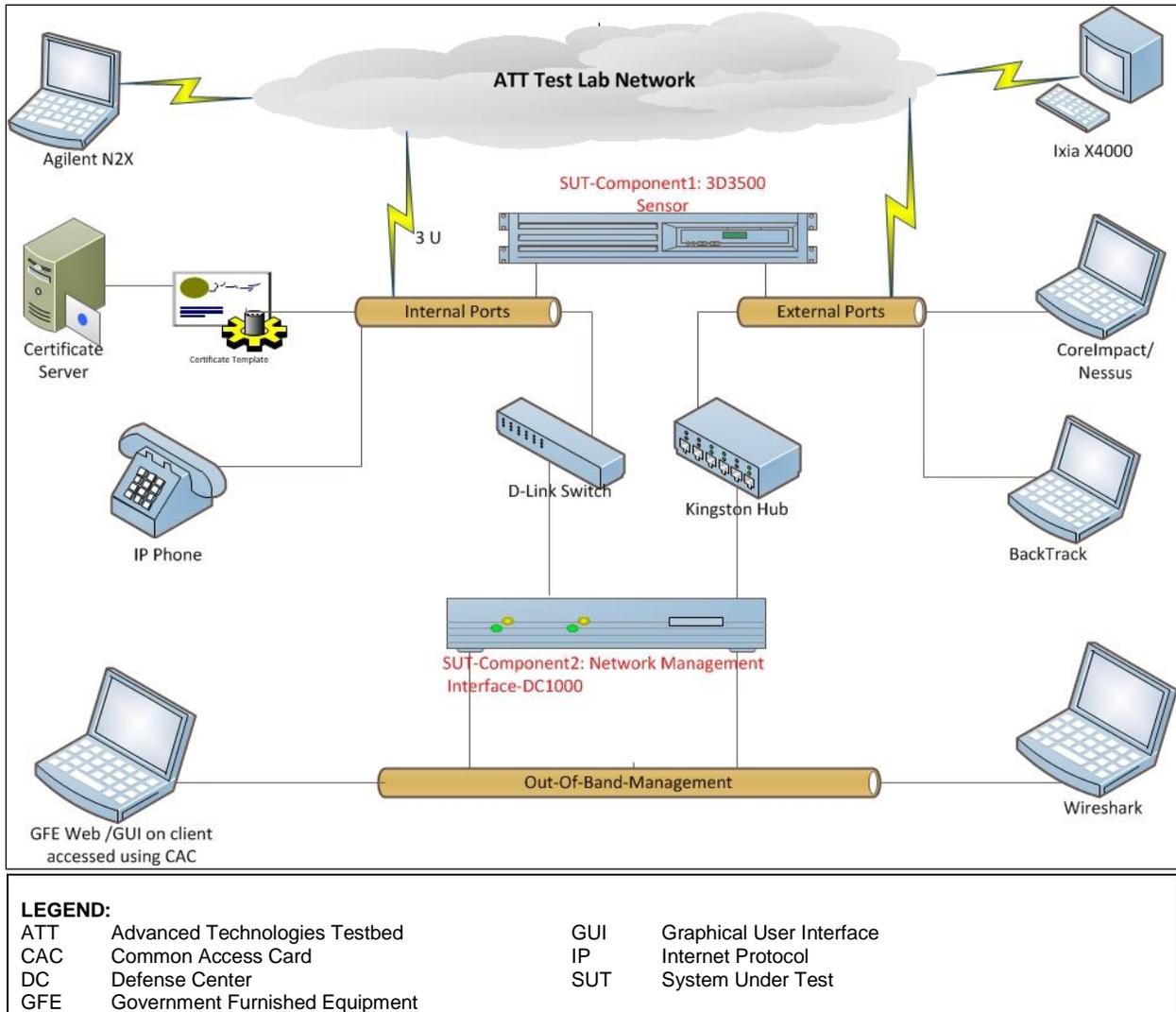
**7.2. Capability Requirement and Functional Requirement.** Security Device products have required and conditional features and capabilities that are established by Section 5.8 of the UCR. The SUT does not need to provide non-critical (conditional) requirements. If they are provided, they must function according to the specified requirements. Table 2-2 lists the features and capabilities and their associated requirements for the SUT products. Table 3-1 of Enclosure 3 provides detailed CR/FR requirements.

**Table 2-2. Capability Requirements and Functional Requirements**

CR/FR ID	Capability/ Function	Applicability (See note)	UCR Reference (UCR 2008 CH 2)	Criteria	Remarks																								
1	<b>Conformance Requirements</b>																												
	Conformance Standards	Required	5.8.4.2	Meet UCR specified standards	Sub-requirements differ by Security Device type.																								
2	<b>Information Assurance Requirements</b>																												
	General Requirements	Required	5.8.4.3.1	Meet UCR 'required' requirements  Enclosure 3, provides detailed functional and capability requirements	Sub-requirements differ by Security Device type.  Cryptography is optional with the exception that all outgoing communications are encrypted.																								
	Reserved	N/A	5.8.4.3.2																										
	Configuration Management	Required	5.8.4.3.3																										
	Alarms & Alerts	Required	5.8.4.3.4																										
	Audit and Logging	Required	5.8.4.3.5																										
	Reserved	NA	5.8.4.3.6																										
	Documentation	Required	5.8.4.3.7																										
	Cryptography	Required	5.8.4.3.8																										
	Security Measures	Required	5.8.4.3.9																										
	System and Communication Protection	Required	5.8.4.3.10																										
	Other Requirements	Required	5.8.4.3.11																										
Performance	Required	5.8.4.3.12																											
3	<b>Functionality</b>																												
	Policy	Required	5.8.4.4.1		FW & VPN Only																								
	Filtering	Required	5.8.4.4.2		FW Only																								
4	<b>IPS Functionality</b>																												
	IPS Security Device Requirements	Required	5.8.4.5	Meet UCR 'required' requirements	IDS/IPS Only																								
<p><b>NOTES:</b> Criticality represents high level roll-up of the CR/FR area. Table 3-1 of Enclosure 3, provides detailed CR/FR for each security device product (FW, IPS/IDS, VPN component).</p> <p><b>LEGEND:</b></p> <table> <tr> <td>CH</td> <td>Change</td> <td>IP</td> <td>Internet Protocol</td> </tr> <tr> <td>CR</td> <td>Capability Requirement</td> <td>IPS</td> <td>Intrusion Prevention System</td> </tr> <tr> <td>FR</td> <td>Functional Requirements</td> <td>N/A</td> <td>Not Applicable</td> </tr> <tr> <td>FW</td> <td>Firewall</td> <td>UCR</td> <td>Unified Capabilities Requirements</td> </tr> <tr> <td>ID</td> <td>Identification</td> <td>VPN</td> <td>Virtual Private Network</td> </tr> <tr> <td>IDS</td> <td>Intrusion Detection System</td> <td></td> <td></td> </tr> </table>						CH	Change	IP	Internet Protocol	CR	Capability Requirement	IPS	Intrusion Prevention System	FR	Functional Requirements	N/A	Not Applicable	FW	Firewall	UCR	Unified Capabilities Requirements	ID	Identification	VPN	Virtual Private Network	IDS	Intrusion Detection System		
CH	Change	IP	Internet Protocol																										
CR	Capability Requirement	IPS	Intrusion Prevention System																										
FR	Functional Requirements	N/A	Not Applicable																										
FW	Firewall	UCR	Unified Capabilities Requirements																										
ID	Identification	VPN	Virtual Private Network																										
IDS	Intrusion Detection System																												

**7.3. Other.** None.

**8. TEST NETWORK DESCRIPTION.** JITC tested the SUT at its Indian Head, Maryland, IA Laboratory from 5 through 29 July 2011. Figure 2-2 shows the SUT's Test Configuration.



**Figure 2-2. SUT Test Configuration**

**9. SYSTEM CONFIGURATIONS.** Table 2-3 lists the tested SUT equipment shown in Figure 2-2, Table 2-4 lists the Non-SUT equipment used to test the SUT, and Table 2-5 lists the test tools used during the assessment.

**Table 2-3. System Equipment**

System Name	Hardware	Software/Firmware Release	Other Software
Sourcefire 3D System	DC1000 Defense Center	SFOS Kernel 206.22 19sf	Apache 2.2.13
	3D3500 Sensor	SFOS Kernel 206.22 19sf	Open SSH 5.1 p1 Open SSL 0.9.8 Apache 2.2.13
<b>LEGEND:</b>			
DC	Defense Center	SSH	Secure Shell
SF	Sourcefire	SSL	Secure Socket Layer
SFOS	Sourcefire Hardening Operating System		

**Table 2-4. Non-SUT Equipment**

Hardware	Software Version	Function	
Management Workstation	Windows XP SP3	Monitors and controls the management application	
PKI/CAC	ActivClient 6.2.0.133	Facilitating the use of PKI authentication and establishing authoritative process for the use of identity credentials	
Cisco IP Phones	CP-7911	Send VOIP over network so the Sourcefire 3D system can detect	
Kingston Hub	Stackable Hub	Connect to the External ports that connected to the ATT lab network test network/tools	
D-Link Switch	DGS-2205 5-Port 10/100/1000 Desktop	Connect to the Internal ports that connected to the ATT lab network test network/tools and patch panel	
<b>LEGEND:</b>			
ATT	Advanced Technology Testbed	PKI	Public Key Infrastructure
CAC	Common Access Card	SP	Service Pack
CP	Cisco Unified Internet Protocol Phone	SUT	System Under Test
D	Manufacturers name	UTP	Unshielded Twisted Pair
DGS	D-Link Gigabit Switch	VOIP	Voice Over Internet Protocol
IP	Internet Protocol	XP	Microsoft Windows Operating System

**Table 2-5. Test Tools**

Manufacture	Type	Port Type	Software Version																
BackTrack	Penetration Testing	8080	V.5 R2																
Core Impact	Penetration Testing	UDP/TCP	V.11																
Nessus	Vulnerability Scanner	TCP	V.4																
Ixia/X4000	Packet/Traffic Generator	AX/4000 mAX IP PoS/ATM/FR OC-12c/OC-3c/STM- 4c/STM-1 Multimode Interface (P/N 401383)	V.4.81.0																
WireShark	Packet Analyzer	UDP/TCP	V.1.4.13																
Agilent N2X	Packet/Traffic Generator	10/100/1000 Base-T	V.N5540A																
		1000 Base-X																	
<b>LEGEND:</b> <table style="width:100%; border:none;"> <tr> <td style="width:50%;">AX Ixia</td> <td style="width:50%;">OC Optical Carrier</td> </tr> <tr> <td>ATM Asynchronous Transfer Mode</td> <td>P/N Part Number</td> </tr> <tr> <td>Base-T Mbps Ethernet generic designation</td> <td>POS Packet Over Synchronous Optical Network</td> </tr> <tr> <td>Base-X 1000 Mbps network connection over twisted-pair copper wire</td> <td>R Release</td> </tr> <tr> <td>FR Frame</td> <td>STM Synchronous Transport Module</td> </tr> <tr> <td>GbE Gigabit Ethernet</td> <td>TCP Transmission Control Protocol</td> </tr> <tr> <td>IP Internet Protocol</td> <td>UDP User Datagram Protocol</td> </tr> <tr> <td></td> <td>V Version</td> </tr> </table>				AX Ixia	OC Optical Carrier	ATM Asynchronous Transfer Mode	P/N Part Number	Base-T Mbps Ethernet generic designation	POS Packet Over Synchronous Optical Network	Base-X 1000 Mbps network connection over twisted-pair copper wire	R Release	FR Frame	STM Synchronous Transport Module	GbE Gigabit Ethernet	TCP Transmission Control Protocol	IP Internet Protocol	UDP User Datagram Protocol		V Version
AX Ixia	OC Optical Carrier																		
ATM Asynchronous Transfer Mode	P/N Part Number																		
Base-T Mbps Ethernet generic designation	POS Packet Over Synchronous Optical Network																		
Base-X 1000 Mbps network connection over twisted-pair copper wire	R Release																		
FR Frame	STM Synchronous Transport Module																		
GbE Gigabit Ethernet	TCP Transmission Control Protocol																		
IP Internet Protocol	UDP User Datagram Protocol																		
	V Version																		

**10. TESTING LIMITATIONS.** None.

**11. INTEROPERABILITY EVALUATION RESULTS.** The SUT meets the critical interoperability requirements for IPS and IDS and JITC certifies its use within the DISN. Additional discussion regarding specific testing results is located in subsequent paragraphs.

**11.1. Interfaces.** The SUT’s interface status is provided in Table 2-6.

**Table 2-6. SUT Interface Requirements Status**

Interface	Critical (See note 1)	UCR Reference (UCR Change 2)	Threshold CR/FR Requirements (See note 2)	Status	Remarks
<b>IPS</b>					
10Base-X	No	5.3.2.4/5.3.3.10.1.2	1-4	Met	SUT met requirements for specified interface
100Base-X	No	5.3.2.4/5.3.3.10.1.2	1-4	Met	SUT met requirements for specified interface
1000Base-X	No	5.3.2.4/5.3.3.10.1.2	1-4	Met	SUT met requirements for specified interface

**Table 2-6. SUT Interface Requirements Status (Continued)**

Interface	Critical (See note 1)	UCR Reference (UCR Change 2)	Threshold CR/FR Requirements (See note 2)	Status	Remarks																				
10GBase-X	No	5.3.2.4/5.3.3.10.1.2	1-4	N/A	Not supported by the SUT																				
40GBase-X	No	5.3.2.4/5.3.3.10.1.2	1-4	N/A	Not supported by the SUT																				
100GBase-X	No	5.3.2.4/5.3.3.10.1.2	1-4	N/A	Not supported by the SUT																				
<p><b>NOTES:</b></p> <p>1. UCR did not identify individual interface requirements for security devices. SUT must minimally provide an Ethernet interface (one of the listed).</p> <p>2. CR/FR requirements are contained in Table 2. CR/FR numbers represent a roll-up of UCR requirements. Enclosure 3, provides a list of more detailed requirements for security device products.</p> <p><b>LEGEND:</b></p> <table> <tr> <td>Base-X</td> <td>Ethernet generic designation</td> <td>IP</td> <td>Internet Protocol</td> </tr> <tr> <td>CH</td> <td>Change</td> <td>N/A</td> <td>Not Applicable</td> </tr> <tr> <td>CR</td> <td>Capability Requirement</td> <td>SUT</td> <td>System Under Test</td> </tr> <tr> <td>FR</td> <td>Functional Requirement</td> <td>UCR</td> <td>Unified Capabilities Requirements</td> </tr> <tr> <td>GBase-X</td> <td>Gigabit generic designation</td> <td></td> <td></td> </tr> </table>						Base-X	Ethernet generic designation	IP	Internet Protocol	CH	Change	N/A	Not Applicable	CR	Capability Requirement	SUT	System Under Test	FR	Functional Requirement	UCR	Unified Capabilities Requirements	GBase-X	Gigabit generic designation		
Base-X	Ethernet generic designation	IP	Internet Protocol																						
CH	Change	N/A	Not Applicable																						
CR	Capability Requirement	SUT	System Under Test																						
FR	Functional Requirement	UCR	Unified Capabilities Requirements																						
GBase-X	Gigabit generic designation																								

**11.2 Capability Requirements and Functional Requirements.** The SUT CR and FR status is provided in Table 2-7. Detailed CR/FR requirements are provided in Enclosure 3, Table 3-1.

**Table 2-7. SUT CRs and FRs Status**

CR/FR ID	Capability/ Function	Applicability (See note)	UCR Reference (UCR CHANGE 2)	Status	Remarks
1	<b>Conformance Requirements</b>				
	Conformance Standards	Required	5.8.4.2	Met	
2	<b>Information Assurance Requirements</b>				
	General Requirements	Required	5.8.4.3.1	Met	
	Reserved	N/A	5.8.4.3.2	N/A	
	Configuration Management	Required	5.8.4.3.3	Met	
	Alarms & Alerts	Required	5.8.4.3.4	Met	See the Information Assurance Findings and Mitigations Summary Report
	Audit and Logging	Required	5.8.4.3.5	Met	See the Information Assurance Findings and Mitigations Summary Report
	Reserved	N/A	5.8.4.3.6	N/A	
	Documentation	Required	5.8.4.3.7	Met	See the Information Assurance Findings and Mitigations Summary Report

**Table 2-7. SUT CRs and FRs Status (Continued)**

CR/FR ID	Capability/ Function	Applicability (See note)	UCR Reference (UCR CHANGE 2)	Status	Remarks																								
	Cryptography	Required	5.8.4.3.8	N/A	Cryptography is optional with the exception that all outgoing communications are encrypted																								
	Security Measures	Required	5.8.4.3.9	Met																									
	System and Communication Protection	Required	5.8.4.3.10	Met																									
	Other Requirements	Required	5.8.4.3.11	Met																									
	Performance	Required	5.8.4.3.12	Met																									
<b>3</b>	<b>Functionality</b>																												
	Policy	Required	5.8.4.4.1	N/A	FW & VPN Only																								
	Filtering	Required	5.8.4.4.2	N/A	FW Only																								
	<b>IPS Functionality</b>																												
<b>4</b>	IPS Security Device Requirements	Required	5.8.4.5	Met	IDS/IPS Only																								
<p><b>NOTE:</b>                      Criticality represents high level roll-up of the CR/FR area. Table 3-1 of Enclosure 3 provides detailed CR/FR for each security device product (FW, IPS/IDS, VPN component).</p> <p><b>LEGEND:</b></p> <table> <tr> <td>CR</td> <td>Capability Requirements</td> <td>IPS</td> <td>Intrusion Prevention System</td> </tr> <tr> <td>FR</td> <td>Functional Requirements</td> <td>N/A</td> <td>Not Applicable</td> </tr> <tr> <td>FW</td> <td>Firewall</td> <td>SUT</td> <td>System Under Test</td> </tr> <tr> <td>ID</td> <td>Identification</td> <td>UCR</td> <td>Unified Capabilities Requirements</td> </tr> <tr> <td>IDS</td> <td>Intrusion Detection System</td> <td>VPN</td> <td>Virtual Private Network</td> </tr> <tr> <td>IP</td> <td>Internet Protocol</td> <td></td> <td></td> </tr> </table>						CR	Capability Requirements	IPS	Intrusion Prevention System	FR	Functional Requirements	N/A	Not Applicable	FW	Firewall	SUT	System Under Test	ID	Identification	UCR	Unified Capabilities Requirements	IDS	Intrusion Detection System	VPN	Virtual Private Network	IP	Internet Protocol		
CR	Capability Requirements	IPS	Intrusion Prevention System																										
FR	Functional Requirements	N/A	Not Applicable																										
FW	Firewall	SUT	System Under Test																										
ID	Identification	UCR	Unified Capabilities Requirements																										
IDS	Intrusion Detection System	VPN	Virtual Private Network																										
IP	Internet Protocol																												

**a. Conformance Requirements.**

(1) Conformance Standards. Security Devices shall meet the appropriate specific standards described in Section 5.8.4.2 of UCR 2008 Change 2 as applicable to Firewalls, IPS, and VPN products. JITC verified that the SUT has met the requirements through vendor submitted Letter of Compliance (LoC).

**b. Information Assurance Requirements.**

(1) General Requirements. Security Devices shall meet the appropriate specific standards described in Section 5.8.4.3.1 of UCR 2008 Change 2 as applicable to Firewalls, IPS/IDS, and VPN products. JITC verified that the SUT has met the General requirements. JITC verified that the SUT has met the requirements for Simple Network Management Protocol Version 3 (SNMP3) and Network Time Protocol Version 4 (NTPv4) by checking with Nessus vulnerability scanning tool and the vendor demonstrating the version of SNMP and NTP within their application. The remainder of the General requirements are not applicable to the SUT.

(2) Reserved.

(3) Configuration Management. Security Devices shall meet the appropriate product specific requirements for Configuration Management described in Section 5.8.4.3.3 of UCR 2008 Change 2 as applicable to Firewalls, IPS, and VPN products. JITC verified the SUT does meet the Configuration Management (CM) requirements by reviewing the CM documentation, procedures and policies for updates and changes made to the SUT implementation.

(4) Alarms and Alerts. Security Devices shall meet the appropriate product specific requirements for alarms and alerts described in Section 5.8.4.3.4 of UCR 2008 Change 2 as applicable to Firewalls, IPS, and VPN products. The SUT does not meet the Alarms and Alerts requirements because the system does not inform administrators by generating an alarm message to the administrator's console session upon detection of a potential security violation. However, the SUT does have the ability to generate alarms and alerts using Required Ancillary Equipment (RAE) and this finding has been documented in the IA Findings Report.

(5) Audit and Logging. Security Devices shall meet the appropriate product specific requirements for audit and logging described in Section 5.8.4.3.5 of UCR 2008 Change 2 as applicable to Firewalls, IPS, and VPN products. JITC verified the SUT partially meet the Audit and Logging requirements because the SUT's does not audit changes to files and folders through the command line. The SUT does log requests at the web interface. The SUT has the ability to generate audit and logging using RAE and this finding has been documented in the IA Findings Report.

(6) Reserved.

(7) Documentation. Security Devices shall meet the appropriate product specific requirements for design and implementation described in Section 5.8.4.3.7 of UCR 2008 Change 2 as applicable to Firewalls, IPS, and VPN products. JITC verified the SUT partially met the Documentation requirements by reviewing the functional specification, internal architectural design, administrator guidance, and vulnerability analysis documentation; however, known security vulnerabilities regarding the configuration and administrative functions were not provided by the vendor. This finding has been documented in the IA Findings Report.

(8) Cryptography. Security Devices shall meet the appropriate product specific requirements for cryptography described in Section 5.8.4.3.8 of UCR 2008 Change 2 as applicable to Firewalls, IPS, and VPN products. The Cryptography requirements are not applicable to the SUT.

(9) Security Measures. Security Devices shall meet the appropriate product specific requirements for security measures as described in Section 5.8.4.3.9 of UCR 2008 Change 2 as applicable to Firewalls, IPS, and VPN products. JITC verified the SUT has met the security measures requirements by successfully detecting Denial of

Service (DoS) and Sync Flood types of attacks to its outside interface. The SUT was configured with the appropriate filters and was able to deny DoS and Sync Flood types of packets from penetrating the outside interface.

(10) Systems and Communication Protection. Security Devices shall meet the appropriate product specific requirements for system and communication protection as described in Section 5.8.4.3.10 of UCR 2008 Change 2 as applicable to Firewalls, IPS, and VPN products. JITC verified the SUT has met the System and Communication Protection requirements. The testers have validated the SUT was able to protect all assigned interfaces from the data traffic that were not permitted.

(11) Other requirements. Security Devices shall meet the appropriate product specific requirements for other functional requirements as described in Section 5.8.4.3.11 of UCR 2008 Change 2 as applicable to Firewalls, IPS, and VPN products. JITC verified the SUT has met the Other Requirements. JITC validated the SUT rejects requests for access or services where the presumed source identity of the source subject is an external Information Technology (IT) entity on a broadcast network/loopback.

(12) Performance. Security Devices shall meet the appropriate product specific requirements for performance as described in Section 5.8.4.3.12 of UCR 2008 Change 2 as applicable to Firewalls, IPS, and VPN products. JITC verified the SUT has met the Performance requirements. Agilent N2X and Ixia / AX4000 were used to generate the Hypertext Transfer Protocol (HTTP) traffic to verify the throughput performance of the SUT. BackTrack was used to generate the DoS attack; Agilent N2X and Ixia/AX4000 were used to create normal traffic.

### **c. Functionality.**

(1) Policy. Security Devices shall meet the appropriate product specific requirements for policy functionality as described in Section 5.8.4.4.1 of UCR 2008 Change 2 as applicable to Firewalls, IPS, and VPN products. JITC verified the SUT has met the Policy requirements. The SUT has the functionality to support the quota of Transmission Control Protocol (TCP) connections. This functionality is implemented in the Service Policies for the management of network traffic. The SUT blocks replay of data as a default policy.

(2) Filtering. Firewalls shall meet the appropriate product specific requirements for filtering as described in Section 5.8.4.4.1 of UCR 2008 Change 2. This requirement is not applicable to the SUT.

### **d. Intrusion Protection System Functionality.**

(1) IPS Security Device Requirements. IPS's shall meet the IPS product specific requirements for functionality as described in Section 5.8.4.5 of UCR 2008 Change 2. JITC verified the SUT has met the IPS Functionality Requirements. The

SUT was successful in detecting and protecting against various methods of attacks distributed by Backtrack and Core Impact penetration testing tools.

**11.3 Information Assurance.** The IA report is published in a separate report, reference (e).

**11.4 Other.** None

**12. TEST AND ANALYSIS REPORT.** In accordance with the Program Manager's request, JITC did not prepare a detailed test report. JITC distributes interoperability information via the JITC Electronic Report Distribution system, which uses Non-secure Internet Protocol Router Network (NIPRNet) e-mail. More comprehensive interoperability status information is available via the JITC System Tracking Program, which .mil/gov users can access on the NIPRNet at <https://stp.fhu.disa.mil>. Test reports, lessons learned, and related testing documents and references are on the JITC Joint Interoperability Tool at <http://jit.fhu.disa.mil> (NIPRNet). Information related to DSN testing is on the Telecommunications Switched Services Interoperability website at <http://jitic.fhu.disa.mil/tssi>.

(This page left intentionally blank.)

## SYSTEM FUNCTIONAL AND CAPABILITY REQUIREMENTS

The Security Device Products have required and conditional features and capabilities that are established by Section 5.8 of the Unified Capabilities Requirements. The System Under Test need not provide conditional requirements. If they are provided, they must function according to the specified requirements. The detailed Functional Requirements and Capability Requirements for Security Device products are listed in Table 3-1.

**Table 3-1. Security Device Products Capability/Functional Requirements Table**

ID	Requirement	UCR Reference	FW	IPS	VPN	NAC	ISS
<b>5.8.4.2 Conformance Requirements</b>							
1	The DoD IPv6 Profile shall be used for IPv6 requirements for security devices unless otherwise stated either within this section or in UCR 2008, Section 5.3.5, IPv6 Requirements.	5.8.4.2 (1)	R	R	R	R	
2	The security device shall conform to all of the MUST requirements found in RFC 2409, "The Internet Key Exchange."	5.8.4.2 (2)		R			
3	The security device shall conform to all of the MUST requirements found in RFC 3414, "User-based Security Model for version 3 of the Simple Network Management Protocol."	5.8.4.2 (3)	R	R	R	R	
4	The security device shall conform to all of the MUST requirements found in RFC 3411, "Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks."	5.8.4.2 (4)		R			
5	The security device shall conform to all of the MUST requirements found in RFC 3412, "Message Processing and Dispatching for Simple Network Management Protocol."	5.8.4.2 (5)	R	R	R	R	
6	The security device shall conform to all of the MUST requirements found in RFC 3413, "Simple Network Management Protocol Applications."	5.8.4.2 (6)	R	R	R	R	
7	The security device shall conform to all of the MUST requirements found in RFC 3585, "IPSec Configuration Policy Information Model."	5.8.4.2 (7)	R	R			
8	The security device shall conform to all of the MUST requirements found in RFC 3586, "IP Security Policy Requirements."	5.8.4.2 (8)	R	R			
9	The security device shall conform to all of the MUST requirements found in RFC 4302, "IP Authentication Header."	5.8.4.2 (9)	R	R	R		
10	The security device shall conform to all of the MUST requirements found in RFC 4303, "IP Encapsulating Security Payload."	5.8.4.2 (10)	R	R	R		
11	The security device shall conform to all of the MUST requirements found in RFC 4308, "Cryptographic Suites for IPSec."	5.8.4.2 (11)	R	R	R		
12	The security device shall conform to all of the MUST requirements found in RFC 4309, "Using Advanced Encryption Standard CCM Mode with IPSec Encapsulating Security Payload."	5.8.4.2 (12)	R		R		
13	The security device shall conform to all of the MUST requirements found in RFC 2473, "Generic Tunneling."	5.8.4.2 (13)	R	R			
14	The security device shall conform to all of the MUST requirements found in RFC 4301, "Security Architecture for the Internet Protocol."	5.8.4.2 (14)			R		

**Table 3-1. Security Device Products Capability/Functional Requirements Table (continued)**

15	The security device shall conform to all of the MUST requirements found in RFC 3948, "UDP Encapsulation of IPSec Packets."	5.8.4.2 (15)			R		
<b>5.8.4.3 Information Assurance Requirements</b>							
<b>5.8.4.3.1 General Requirements</b>							
16	The security device shall support SNMP3 and NTPv4.	5.8.4.3.1 (1)	R	R	R	R	
17	The security device shall provide ability to push policy to the VPN client and the ability to monitor the client's activity.	5.8.4.3.1 (2)			R		
18	The security device shall be managed from a central place, clients, and servers.	5.8.4.3.1 (3)			R	R	
19	The security device shall have three Ethernet ports, one for primary, one for backup, and one for OOBM.	5.8.4.3.1 (4)	R				
<b>5.8.4.3.2 Reserved</b>							
<b>5.8.4.3.3 Configuration Management</b>							
20	A CM process shall be implemented for hardware and software updates.	5.8.4.3.3 (1)	R	R	R	R	
21	The CM system shall provide an automated means by which only authorized changes are made to the security device implementation.	5.8.4.3.3 (2)	R	R	R	R	
22	The security device shall disable the Proxy Address Resolution Protocol service, unless disabled by default.	5.8.4.3.3 (3)	R	R	R		
23	The security device shall disable the IP redirects notification service, except in type 3 cases.	5.8.4.3.3 (4)	R	R	R		
24	The security device shall disable the Maintenance Operations Protocol service in DEC equipment which use that protocol to perform software loads.	5.8.4.3.3 (5)	O	O	O		
25	The security device shall disable the service source-routing	5.8.4.3.3 (6)	R		R		
26	The security device shall properly implement an ordered list policy procedure.	5.8.4.3.3 (7)	R	R	R		
<b>5.8.4.3.4 Alarms and Alerts</b>							
27	The security device shall apply a set of rules in monitoring events and based on these rules indicate a potential violation of the security device security policy.	5.8.4.3.4 (1)	R	R		R	
28	Security devices with local consoles shall have the capability to generate and display an alarm message at the local console upon detection of a potential security violation.	5.8.4.3.4 (2)	R	R	R	R	

**Table 3-1. Security Device Products Capability/Functional Requirements Table (continued)**

29	The security device shall have the capability to generate an alarm message to a new remote administrator's console session if the original alarm has not been acknowledged following a potential security violation.	5.8.4.3.4 (3)	R	R	R	R	
30	The security device shall have the capability to provide proper notification upon detection of a potential security violation or forward event status data to a Network Management System that will take the appropriate action to include providing notification of the event.	5.8.4.3.4 (4)		R			
31	The security device shall have the capability to alert the administrator immediately, by displaying a message at the local and remote administrative consoles when an administrative session exists for each of the defined administrative roles.	5.8.4.3.4 (5)		R			
32	An automated, continuous online monitoring and audit trail creation capability is deployed with the capability to immediately alert personnel of any unusual or inappropriate activity with potential Information Assurance implications.	5.8.4.3.4 (6)	R	R	R		
33	The security device shall have an automated, continuous online monitoring and audit trail creation capability, which shall be deployed with a user configurable capability to disable the system automatically if serious Information Assurance violations are detected.	5.8.4.3.4 (7)	R	R	R	R	
<b>5.8.4.3.5 Audit and Logging</b>							
34	The security device shall provide minimum recorded security-relevant events including any activity caught by the "deny all" rule at the end of the security device rule base.	5.8.4.3.5 (1)	R	R			
35	The security device shall generate an audit record of all failures to reassemble fragmented packets.	5.8.4.3.5 (2)		R			
36	The security device shall generate an audit record of all attempted uses of the trusted channel functions.	5.8.4.3.5 (3)	R	R	R		
37	The security device, when configured, shall log the event of dropping packets and the reason for dropping them.	5.8.4.3.5 (4)	R				
38	The security device shall log matches to filter rules that deny access when configured to do so.	5.8.4.3.5 (5)	R	R			
39	The security device shall record access or attempted access via security device to all program initiations and shutdowns that have security implications.	5.8.4.3.5 (6)	R		R		
40	The output of such intrusion/attack detection and monitoring tools shall be protected against unauthorized access, modification, or detection.	5.8.4.3.5 (7)	R	R	R		

**Table 3-1. Security Device Products Capability/Functional Requirements Table (continued)**

41	The security device shall log requests for access or services where the presumed source identity of the information received by the security device specifies a broadcast identity.	5.8.4.3.5 (8)		R			
42	The security device shall log SMTP traffic that contains source routing symbols (e.g., in the mailer recipient commands).	5.8.4.3.5 (9)		R			
43	The security device shall log requests in which the information received by the security device contains the route (set of host network identifiers) by which information shall flow from the source subject to the destination subject.	5.8.4.3.5 (10)		R			
44	The security device shall log an information flow between a source subject and a destination subject via a controlled operation if the source subject has successfully authenticated to the security device.	5.8.4.3.5 (11)		R			
45	The security device shall log an information flow between a source subject and a destination subject via a controlled operation if the information security attributes match the attributes in an information flow policy rule (contained in the information flow policy).	5.8.4.3.5 (12)		R	R		
46	The security device shall log data and audit events when a replay is detected.	5.8.4.3.5 (13)	R	R			
47	The security device shall be able to collect the following: Identification, Authentication, and Authorization events.	5.8.4.3.5 (14)		R	R		
48	The security device shall be able to collect data accesses.	5.8.4.3.5 (15)		R	R		
49	The security device shall be able to collect service requests.	5.8.4.3.5 (16)		R	R		
50	The security device shall be able to collect network traffic.	5.8.4.3.5 (17)		R	R		
51	The security device shall be able to collect security configuration changes.	5.8.4.3.5 (18)		R	R		
52	The security device shall be able to collect data introduction.	5.8.4.3.5 (19)		R	R		
53	The security device shall be able to collect detected malicious code.	5.8.4.3.5 (20)		R	R		
54	The security device shall be able to collect access control configuration.	5.8.4.3.5 (21)		R	R		
55	The security device shall be able to collect service configuration.	5.8.4.3.5 (22)		R	R		

**Table 3-1. Security Device Products Capability/Functional Requirements Table (continued)**

56	The security device shall be able to collect authentication configuration.	5.8.4.3.5 (23)		R	R		
57	The security device shall be able to collect accountability policy configuration.	5.8.4.3.5 (24)		R	R		
58	The security device shall be able to collect detected known vulnerabilities.	5.8.4.3.5 (25)		R	R		
59	The security device shall provide authorized users with the capability to read the system data.	5.8.4.3.5 (26)		R	R		
60	The system shall prohibit access to security device data, except those users that have been granted explicit read access.	5.8.4.3.5 (27)		R	R		
<b>5.8.4.3.6 Reserved</b>							
<b>5.8.4.3.7 Documentation</b>							
61	The developer shall provide CM documentation identifying roles, responsibilities, and procedures to include the management of Information Assurance information and documentation shall be formally documented.	5.8.4.3.7 (1)	R	R	R	R	
62	The developer shall provide administrator guidance addressed to system administrative personnel (e.g., Administrator's Guide).	5.8.4.3.7 (2)	R	R	R	R	
63	The developer shall provide user guidance (e.g., User's Guide) when there are users other than administrators. The User's Guide will describe the protection mechanisms provided, guidelines on how the mechanisms are to be used, and the ways the mechanisms interact.	5.8.4.3.7 (3)	O	O	O	O	
64	The developer shall provide the architectural design of the security device.	5.8.4.3.7 (4)	R	R	R	R	
65	The developer shall provide a functional specification of the security device.	5.8.4.3.7 (5)	R	R	R	R	
66	The developer shall provide vulnerability analysis documentation identifying known security vulnerabilities regarding the configuration and use of administrative functions. The vulnerability analysis documentation shall also describe the analysis of the security device deliverables performed to search for obvious ways in which a user can violate the security device security policy.	5.8.4.3.7 (6)	R	R	R	R	
67	The reference document for the security device shall be unique to each version of the security device.	5.8.4.3.7 (7)	R	R	R	R	
68	The security device shall be labeled with its reference information, i.e., the model and version number.	5.8.4.3.7 (8)	R	R	R	R	
69	The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.	5.8.4.3.7 (9)	R	R	R	R	

**Table 3-1. Security Device Products Capability/Functional Requirements Table (continued)**

70	The CM system shall provide measures such that only authorized changes are made to the configuration items.	5.8.4.3.7 (10)	R	R	R	R	
71	The guidance documentation shall list all assumptions about the intended environment.	5.8.4.3.7 (11)	R	R	R	R	
72	The system shall demonstrate a procedure for accepting and acting upon user reports of potential security flaws and requests for corrections to those flaws.	5.8.4.3.7 (12)	R	R	R	R	
73	The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the security device.	5.8.4.3.7 (13)	R	R	R	R	
74	The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.	5.8.4.3.7 (14)	R	R	R	R	
75	The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.	5.8.4.3.7 (15)	R	R	R		
76	The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections, and guidance on corrective actions to security device users.	5.8.4.3.7 (16)	R	R	R	R	
77	The procedures for processing reported security flaws shall ensure that any reported flaws are corrected and the correction issued to security device users.	5.8.4.3.7 (17)	R	R	R	R	
78	The developer shall perform a vulnerability analysis.	5.8.4.3.7 (18)	R	R	R	R	
79	The vulnerability analysis documentation shall describe the disposition of identified vulnerabilities.	5.8.4.3.7 (19)	R	R	R	R	
80	The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the security device.	5.8.4.3.7 (20)	R	R	R	R	
81	The vulnerability analysis documentation shall justify that the security device, with the identified vulnerabilities, is resistant to obvious penetration attacks.	5.8.4.3.7 (21)	R	R	R	R	
82	The installation, generation, and start-up documentation shall describe all the steps necessary for secure installation, generation, and start-up of the security device.	5.8.4.3.7 (22)	R	R	R	R	
83	The administrator guidance shall describe recovery procedures and technical system features to assure that system recovery is done in a trusted and secure manner.	5.8.4.3.7 (23)	R	R	R	R	

**5.8.4.3.8 Cryptography**

**Table 3-1. Security Device Products Capability/Functional Requirements Table (continued)**

84	At a minimum, the following confidentiality policy adjudication features shall be provided for each controlled interface. Encrypt, as needed, all outgoing communication including the body and attachment of the communication.	5.8.4.3.8 (1)			R		
<b>5.8.4.3.9 Security Measures</b>							
85	System mechanisms shall be implemented to enforce automatic expiration of passwords, to prevent password reuse, and to ensure password strength.	5.8.4.3.9 (1)	R	R	R	R	
86	Monitoring tools shall be used for the monitoring and detection of suspicious, intrusive, or attack-like behavior patterns to itself.	5.8.4.3.9 (2)	R	R	R	R	
87	The security device's controlled interface shall be configured such that its operational failure or degradation shall not result in any unauthorized release of information outside the Information Security (IS) perimeter nor result in any external information entering the IS perimeter.	5.8.4.3.9 (3)	R	R	R	R	
88	Where scanning tools are available, the security device's internal hosts shall be scanned for vulnerabilities in addition to the security device itself to confirm an adequate security policy is being enforced.	5.8.4.3.9 (4)	R	R	R	R	
89	The security device must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with security device security functions.	5.8.4.3.9 (5)	R	R	R	R	
90	The security device shall block unauthorized directed broadcasts from external networks (Distributed Denial of Service defense).	5.8.4.3.9 (6)	R				
91	The security device shall verify reverse path unicast addresses (Distributed Denial of Service defense) and be able to drop packets that fail verification.	5.8.4.3.9 (7)	R				
92	The security device shall drop all packets with an IPv4 non-routable (RFC 1918) address originating from an external source.	5.8.4.3.9 (8)	R	R	R	R	
93	The security device shall drop all packets with an IPv4 source address of all zeros.	5.8.4.3.9 (9)	R	R	R	R	
94	The security device shall verify reverse path unicast addresses (Distributed Denial of Service defense) and be able to drop packets that fail verification.	5.8.4.3.9 (10)	R	R	R	R	
95	The security device shall differentiate between authorized and fraudulent attempts to upgrade the operating system, i.e., trying to upgrade system files with the wrong names.	5.8.4.3.9 (11)	R	R			

**Table 3-1. Security Device Products Capability/Functional Requirements Table (continued)**

96	The security device shall differentiate between authorized and fraudulent attempts to upgrade the configuration, i.e., if a user trying to perform an upgrade that is not authorized that role.	5.8.4.3.9 (12)	R	R			
97	The security device shall pass traffic, which the security device has not identified as being a security problem, without altering the contents, except as necessary to perform functions such as Network Address Translation.	5.8.4.3.9 (13)	R	R			
98	The security device shall properly accept or deny User Datagram Protocol (UDP) traffic from port numbers based on policy.	5.8.4.3.9 (14)	R	R			
99	The security device shall properly accept or deny Transmission Control Protocol (TCP) traffic from port numbers based on policy.	5.8.4.3.9 (15)	R	R			
100	The security device shall not compromise its resources or those of any connected network upon initial start-up of the security device or recovery from an interruption in security device service.	5.8.4.3.9 (16)	R				
101	A security device shall properly enforce the TCP state.	5.8.4.3.9 (17)	R				
102	A security device shall properly accept and deny traffic based on multiple rules.	5.8.4.3.9 (18)	R				
103	A security device shall prevent all known network-based current attack techniques (Common Vulnerabilities and Exploits) from compromising the security device.	5.8.4.3.9 (19)	R	R			
104	A security device shall prevent the currently available Information Assurance Penetration techniques, as defined in DISA STIGS and Information Assurance Vulnerability Alerts from penetrating the security device.	5.8.4.3.9 (20)	R	R	R		
105	A security device shall block potentially malicious fragments.	5.8.4.3.9 (21)	R	R			
106	The security device shall mediate the flow of all information between a user on an internal network connected to the security device and a user on an external network connected to the security device and must ensure that residual information from a previous information flow is not transmitted.	5.8.4.3.9 (22)	R	R			
<b>5.8.4.3.10 Systems and Communication Protection</b>							

**Table 3-1. Security Device Products Capability/Functional Requirements Table (continued)**

107	Each controlled interface shall be configured to ensure that all (incoming and outgoing) communications protocols, services, and communications not explicitly permitted are prohibited	5.8.4.3.10 (1)	R	R			
108	The security device's controlled interface shall ensure that only traffic that is explicitly permitted (based on traffic review) is released from the perimeter of the interconnected Information System	5.8.4.3.10 (2)	R				
109	The security device's controlled interface enforces configurable thresholds to determine whether all network traffic can be handled and controlled.	5.8.4.3.10 (3)	R				
<b>5.8.4.3.11 Other Requirements</b>							
110	The security device shall reject requests for access or services where the presumed source identity of the source subject is an external Information Technology entity on a broadcast network.	5.8.4.3.11 (1)	R	R	R	R	
111	The security device shall reject requests for access or services where the presumed source identity of the source subject is an external Information Technology entity on the loopback network.	5.8.4.3.11 (2)	R		R	R	
112	The security device shall permit an information flow between a source subject and a destination subject via a controlled operation if the source subject has successfully authenticated to the security device.	5.8.4.3.11 (3)	R	R	R	R	
113	The TSF shall permit an information flow between a controlled subject and another controlled subject via a controlled operation if the following rules hold: a. Subjects on an internal network can cause information to flow through the security device to another connected network if: (1) All the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator; (2) The presumed address of the source subject, in the information, translates to an internal network address;  (3) And the presumed address of the destination subject, in the information, translates to an address on the other connected network. b. Subjects on the external network can cause information to flow through the TOE to another connected network if: (1) All the information security attribute values are unambiguously permitted by the inform (2) The presumed address of the source subject in the information translates to an external network address; (3) And the presumed address of the destination subject in the information translates to an address on the other connected network	5.8.4.3.11 (4)	R				
114	The security device, after a failure or service discontinuity, shall enter a maintenance mode where the ability to return the security device to a secure state is provided.	5.8.4.3.11 (5)	R	R	R	R	
115	The security device shall detect replay attacks using either security device data or security attributes.	5.8.4.3.11 (6)		R	R	R	
116	The security device shall reject data and audit events when a replay is detected.	5.8.4.3.11 (7)		R			
117	The security device shall ensure the security policy enforcement functions are invoked and succeed before each function within the security functions scope of control is allowed to proceed.	5.8.4.3.11 (8)	R	R	R		
118	The security device shall enforce System Administrator policy regarding Instant Messaging traffic.	5.8.4.3.11 (9)	R	R	R		

**Table 3-1. Security Device Products Capability/Functional Requirements Table (continued)**

119	The security device shall enforce System Administrator policy regarding VVoIP traffic.	5.8.4.3.11 (10)	R	R	R		
120	Access Control shall include a Discretionary Access Control Policy.	5.8.4.3.11 (11)	R	R	R	R	
121	Discretionary Access Control access controls shall be capable of including or excluding access to the granularity of a single user.	5.8.4.3.11 (12)	R	R	R	R	
122	The security device's controlled interface shall review incoming information for viruses and other malicious code.	5.8.4.3.11 (13)	R	R	R	R	
123	The controlled interface shall provide the ability to restore its functionality fully in accordance with documented restoration procedures.	5.8.4.3.11 (14)	R	R	R	R	
124	The security device shall prevent or mitigate DoS attacks. Where technically feasible, procedures and mechanisms shall be in place to curtail or prevent well-known, detectable, and preventable DoS attacks (e.g., SYN attack). Only a limited number of DoS attacks are detectable and preventable. Often, prevention of such attacks is handled by a controlled interface.	5.8.4.3.11(15)	R	R	R		
<b>5.8.4.3.12 Performance</b>							
125	The developer must specify the security device's bandwidth requirements and capabilities. This shall include the maximum bandwidth speeds the device will operate on, as well as, the security device bandwidth requirements (bandwidth in kbps) documented by who the device communicates with, frequency, and Kbps transmitted and received (such as product downloads, signature files).	5.8.4.3.12 (1)	R	R	R		
126	The security device, as configured, must process new connections at the rate of the expected maximum number of connections as advertised by the vendor within a 1-minute period.	5.8.4.3.12 (2)	R	R	R		
127	The security device, as configured, must process new HTTP connections at the rate of the expected maximum number of connections as advertised by the vendor within a 1-minute period.	5.8.4.3.12 (3)	R	R	R		
128	The security device, as configured, must process new secure file transfer protocol connections at the rate of the expected maximum number of connections as advertised by the vendor within a 1-minute period.	5.8.4.3.12 (4)	R	R	R		
129	The security device shall employ a commercial best practice defensive solution along with maintain advertised normal operation packet loss rates for all legitimate data packets when under a SYN Flood attack.	5.8.4.3.12 (5)	R	R	R		
130	The security device must not degrade IPv4 and IPv6 forwarding when used with a long Access Policy configuration.	5.8.4.3.12 (6)	R		R		
131	The security device shall demonstrate a latency variance of less than 20 percent and a packet loss variance of less than 10 percent of the manufacturer specified nominal values for all operational conditions.	5.8.4.3.12 (7)	R				
<b>5.8.4.4 Functionality</b>							
5.8.4.4.1 Policy							

**Table 3-1. Security Device Products Capability/Functional Requirements Table (continued)**

132	The security device shall enforce the policy pertaining to any indication of a potential security violation.	5.8.4.4.1 (1)	R		R		
133	The security device shall be configurable to perform actions based on different information flow policies.	5.8.4.4.1 (2)	R		R		
134	The security device shall deny establishment of an authorized user session based on network source (i.e., source IP address) and time of day parameter values.	5.8.4.4.1 (3)	R		R		
135	The security device shall enforce the system administrator's specified maximum quota of transport-layer open connections that a source subject identifier can use over a specified period.	5.8.4.4.1 (4)	R				
136	The security device shall enforce the system administrator's policy options pertaining to network traffic violations to a specific TCP port within a specified period.	5.8.4.4.1 (5)	R		R		
137	The security device shall enforce the system administrator's policy options pertaining to violations of network traffic rules within a specified period.	5.8.4.4.1 (6)	R		R		
138	The security device shall enforce the system administrator's policy options pertaining to any security device-detected replay of data and/or nested security attributes.	5.8.4.4.1 (7)	R		R		
<b>5.8.4.4.2 Filtering</b>							
139	<p>This section addresses the ability of a firewall to perform basic filtering functions. It does not mandate a specific filtering configuration for firewalls.</p> <p>The integrity policy adjudication feature known as filtering shall be provided. The security device's controlled interface must support and filter communications protocols/services from outside the perimeter of the interconnected ISs according to IS-appropriate needs (e.g., filter based on addresses, identity, protocol, authenticated traffic, and applications). The security device shall:</p> <ol style="list-style-type: none"> <li>1. Have the ability to block on a per-interface basis.</li> <li>2. Default to block.</li> <li>3. Default to disabled, if supported on the security device itself.</li> </ol> <p>a. Will apply to the following defined services:</p> <ol style="list-style-type: none"> <li>(1) The service UDP echo (port 7)</li> <li>(2) The service UDP discard (port 9)</li> <li>(3) The service UDP chargen (port 19)</li> <li>(4) The service UDP TCPMUX (port 1)</li> <li>(5) The service UDP daytime (port 13)</li> <li>(6) The service UDP time (port 37)</li> <li>(7) The service UDP supdup (port 95)</li> <li>(8) The service UDP sunrpc (port 111)</li> <li>(9) The service UDP loc-srv (port 135)</li> <li>(10) The service UDP netbios-ns (port 137)</li> <li>(11) The service UDP netbios-dgm (port 138)</li> <li>(12) The service UDP netbios-ssn (port 139)</li> <li>(13) The service UDP BootP (port 67)</li> <li>(14) The service UDP TFTP (port 69)</li> </ol>	5.8.4.4.2	R				

**Table 3-1. Security Device Products Capability/Functional Requirements Table (continued)**

139	(15) The service UDP XDMCP (port 177) (16) The service UDP syslog (port 514) (17) The service UDP talk (port 517) (18) The service UDP ntalk (port 518) (19) The service UDP MS SQL Server (port 1434) (20) The service UDP MS UPnP SSDP (port 5000) (21) The service UDP NFS (port 2049) (22) The service UDP Back Orifice (port 31337) (23) The service TCP tcpmux (port 1) (24) The service TCP echo (port 7) (25) The service TCP discard (port 9) (26) The service TCP systat (port 11) (27) The service TCP daytime (port 13) (28) The service TCP netstat (port 15) (29) The service TCP chargen (port 19) (30) The service TCP time (port 37) (31) The service TCP whois (port 43) (32) The service TCP supdup (port 95) (33) The service TCP sunrpc (port 111) (34) The service TCP loc-srv (port 135) (35) The service TCP netbios-ns (port 137) (36) The service TCP netbios-dgm (port 138) (37) The service TCP netbios-ssn (port 139) (38) The service TCP netbios-ds (port 445) (39) The service TCP rexec (port 512) (40) The service TCP lpr (port 515) (41) The service TCP uucp (port 540) (42) The service TCP Microsoft UPnP System Services Delivery Point (SSDP) (port 1900) (43) The service TCP X-Window System (ports 6000-6063) (44) The service TCP IRC (port 6667) (45) The service TCP NetBus (ports 12345-12346) (46) The service TCP Back Orifice (port 31337) (47) The service TCP finger (port 79) (48) The service TCP SNMP (port 161) (49) The service UDP SNMP (port 161) (50) The service TCP SNMP trap (port 162) (51) The service UDP SNMP trap (port 162) (52) The service TCP rlogin (port 513) (53) The service UDP who (port 513) (54) The service TCP rsh, rcp, rdist, and rdump (port 514) (55) The service TCP new who (port 550) (56) The service UDP new who (port 550) (57) The service NTP (Network Time Protocol) (58) The service CDP (Cisco Discovery Protocol) (59) Voice and Video Services (AS-SIP), H.323, and RSVP (60) The service UDP SRTP (SRTCP) and RTCP (61) The service DSCP							
	<b>5.8.4.5 IPS Functionality</b>							
	140	The security device shall detect and protect against a focused method of attack: Footprinting and Scanning.	5.8.4.5 (1)		R			
	141	The security device shall detect and protect against a focused method of attack: Enumeration.	5.8.4.5 (2)		R			
	142	The security device shall detect and protect against a focused method of attack: Gaining Access.	5.8.4.5 (3)		R			
	143	The security device shall detect and protect against a focused method of attack: Escalation of Privilege.	5.8.4.5 (4)		R			
144	The security device shall detect and protect against a focused method of attack: Maintaining Access.	5.8.4.5 (5)		R				
145	The security device shall detect and protect against a focused method of attack: Network Exploitation.	5.8.4.5 (6)		R				

**Table 3-1. Security Device Products Capability/Functional Requirements Table (continued)**

146	The security device shall detect and protect against a focused method of attack: Cover Tracks.	5.8.4.5 (7)		R			
<b>5.8.4.6 IPS VVoIP Signal and Media Inspection Requirements</b>							
	1. The device shall support the capability to detect and send alarms in responses to threats identified in VVoIP signaling.	5.8.4.6 (1)					
	a. The IPS shall support the capability to detect an abnormal number of 401/407 AS-SIP response messages, indicating that a possibly unauthorized user or device is attempting to connect to the system.	5.8.4.6 (1a)					
	b. The IPS shall support the capability to detect when an abnormal time-out for an AS-SIP request occurs (e.g., large numbers of repeated AS-SIP requests or responses, unusual number of AS-SIP requests sent with no matching response).	5.8.4.6 (1b)					
	NOTE: If an AS-SIP request time-out occurs, it could be an indication that the system has failed because of a DoS attack resulting from a maliciously crafted request.						
147	c. The device shall support the capability to detect when AS-SIP messages exceed a configurable maximum message length.	5.8.4.6 (1c)		C			
	d. The device shall support the capability to detect when an AS-SIP message contains nonprintable characters. NOTE: The presence of nonprintable characters could indicate an attempt by an adversary to insert executable code or cause abnormal behavior in a system.	5.8.4.6 (1d)					
	e. The device shall support the capability to detect attempts to inject SQL queries into AS-SIP signaling messages.	5.8.4.6 (1e)					
	f. The device shall support the capability to detect unusual IPv4 or IPv6 addresses contained in AS-SIP messages (for example, the local host/loopback address, link local addresses).	5.8.4.6 (1f)					
	g. The device shall support the capability to detect traffic that does not have the characteristics of AS-SIP traffic, but is still sent over a channel established for sending AS-SIP messages (e.g., strings of characters that are not AS-SIP related).	5.8.4.6 (1g)					

**Table 3-1. Security Device Products Capability/Functional Requirements Table (continued)**

148	2. The device shall support the capability to detect and send alarms in response to threats identified in VVoIP media traffic and other traffic that flows across the EBC boundary.	5.8.4.6 (2)					
	a. The device shall detect attempts to inject packets into a media stream or perform replay attacks (e.g., duplicate sequence numbers appearing in an RTP stream).	5.8.4.6 (2a)					
	b. The device shall support the capability to detect traffic that should be VVoIP traffic based on its headers, but does not have the characteristics of a VVoIP traffic stream.	5.8.4.6 (2b)					
	1. The device shall support the capability to detect signatures associated with the presence of data, files, executables, SQL commands, viruses, or other unusual data contained within a media stream intended for VVoIP.	5.8.4.6 (2.1)		C			
	2. The device shall support the capability to detect abnormally sized packets in the VVoIP media stream. a. At a minimum, the device shall support the capability to detect unusually large packets associated with the codec types specified in Section 5.3.2.6, End Instruments. NOTE: This requires the device to support the capability to recognize the codec that should be represented within the packet and determine the appropriate packet size based on that information.	5.8.4.6 (2.2)					
149	The device shall support the capability to receive periodic VVoIP signaling, media, and other threat signature updates from an authenticated source in an automated manner.	5.8.4.6 (3)		C			
<b>5.8.4.7 Integrated Security Systems</b>							
150	The device shall ensure that each function implemented shall be logically separate from the other functions.	5.8.4.7 (1)					R
151	The device must comply with all applicable UCR requirements for any implemented functions.	5.8.4.7 (2)					R
<b>5.8.4.8 Information Assurance Tools</b>							
<b>5.8.4.9 Network Access Controls</b>							
152	The system shall be able to authenticate all devices before allowing access to the network.	5.8.4.9 (1)				R	R
153	The system shall be capable of denying access to any device that fails authentication.	5.8.4.9 (2)				R	R
154	The system shall support 802.1X based policy enforcement points and Layer 3 policy enforcement points with 802.1X based policy enforcement preferred.	5.8.4.9 (3)				R	R
155	The system shall operate in both in-band and out-of-band modes to support both network segments that can and cannot utilize 802.1X.	5.8.4.9 (4)				R	R
156	The system shall allow an administrator to override the authentication assessment and allow or deny a device to enter the authorized network.	5.8.4.9 (5)				R	R
157	The system shall provide the administrator a means for configuring exception policies to accommodate authorized devices that do not support NAC-agents or other means for authentication such as 802.1X.	5.8.4.9 (6)				R	R
158	The system shall allow security managers and administrators the ability to create, manipulate, and maintain multiple device NAC policies for different classes of devices.	5.8.4.9 (7)				R	R
159	The system shall be capable of being configured for both distributed NAC policy and localized NAC policy enforcement administration.	5.8.4.9 (8)				R	R
160	The system shall allow an administrator to manually configure event publication, e.g. set filters on event types to be displayed, alerted.	5.8.4.9 (9)				R	R

**Table 3-1. Security Device Products Capability/Functional Requirements Table (continued)**

161	The system shall have the ability to be configured to log, but not enforce NAC policies. The system shall provide the ability to log and notify, but not enforce, optionally all the following: compliance OR device authentication OR remediation notifications.	5.8.4.9 (10)				R	R
162	The system shall provide the capability to either turn-off or disable the NAC functionality globally, and on a NAC-controlled interface basis.	5.8.4.9 (11)				R	R
163	The system shall allow administrators to receive information on a device's NAC status.	5.8.4.9 (12)				R	R
164	The system shall be capable of placing the end user machine into an alternate network (quarantine) if the end user machine is not authorized to connect to the trusted network, regardless of its enforcement method. NOTE: The network components (e.g., VPN, LS) must be configured so that end devices do not have access to other untrusted devices while quarantined.	5.8.4.9 (13)				R	R
165	The system shall allow isolated segments of the network to be designated for clients that meet a specified configuration policy compliance status.	5.8.4.9 (14)				R	R
166	For all devices, the system shall support the capability to remove an asset from the group of its managed assets without sympathetic errors (e.g., pop up window saying "invalid command"), thus allowing the user to remove managed devices without issue.	5.8.4.9 (15)				R	R
167	The system shall require an authentication procedure to process new clients requesting downloads.	5.8.4.9 (16)				R	R
168	The system shall support the capability to allow end devices to automatically and securely download required patches or software when the device is found to be non-compliant. Any NAC agent functionality shall support the capability to install downloaded patches manually.	5.8.4.9 (17)				R	R
169	The system's remediation checks shall be customizable by security managers and administrators.	5.8.4.9 (18)				R	R
170	The system shall not interfere with the operation of DoD-approved antivirus software (e.g., Symantec and McAfee), HBSS, and Federal Desktop Core Configuration. NOTE: Interoperability with HBSS is preferred.	5.8.4.9 (19)				R	R
171	The system shall be configurable to fail closed.	5.8.4.9 (20)				R	R
172	The system shall provide encrypted communications from the NAC client agent to the NAC device using FIPS-validated encryption.	5.8.4.9 (21)				R	R
173	The system shall protect against subversive network access activity. This may be provided by interfacing with post authentication policy enforcement of third-party devices using standards like Trusted Network Control Interface - Metadata Access Point Protocol.	5.8.4.9 (22)				R	R
174	NAC management devices shall have the capability for manual, and optionally, automatic recovery from failed operations to return to normal settings/operations/systems, to include log merging.	5.8.4.9 (23)				R	R
175	The system shall support the capability to export logs in and open standard format (e.g., Syslog).	5.8.4.9 (24)				R	R
176	The system shall provide the capability to queue events when communication is lost.	5.8.4.9 (25)				R	R
177	The system shall be capable of reporting alerts to multiple management consoles for all administratively specified events.	5.8.4.9 (26)				R	R
178	The system shall provide detailed logs of all administratively specified events.	5.8.4.9 (27)				R	R
179	The system shall have the ability to time-stamp all events using Greenwich Mean Time, to include log data, in a consistent frame of reference.	5.8.4.9 (28)				R	R
180	The product shall support a concept of operations which allows individual managers to support large numbers of distributed managed elements.	5.8.4.9 (29)				R	R

**Table 3-1. Security Device Products Capability/Functional Requirements Table (continued)**

181	The system shall allow configurable reporting to control how and when reports are generated, based on administrator-selected attributes/thresholds.	5.8.4.9 (30)				R	R
182	The system shall support the capability to identify connecting clients that do not have an 802.1X supplicant or NAC agent/remediation software installed.	5.8.4.9 (31)				R	R
183	The system shall support the capability to check for syntax errors and duplicate policies before NAC policies are implemented.	5.8.4.9 (32)				R	R
184	The system shall support the capability to integrate with and use Active Directory when authenticating connected devices.	5.8.4.9 (33)				R	R
185	The system shall support the capability to periodically perform re-authentication and remediation in automated manner at a configurable interval.	5.8.4.9 (34)				R	R
186	NAC systems using 802.1X must be compliant with the relevant and current IEEE standards for 802.1X.	5.8.4.9 (35)				R	R
187	The system shall have the ability to work with any RADIUS server in 802.1X enforcement mode.	5.8.4.9 (36)				R	R
188	The system shall have the ability to support short term client disconnections, such as taking a laptop to a meeting, and then reconnecting to the network without requiring the client to pass through the testing process.	5.8.4.9 (37)				R	R

**LEGEND:**

AS-SIP	Assured Services Session Initiation Protocol
BOOTP	Bootstrap Protocol
C	Conditional
CCM	Counter with CBC-MAC Conditional
CM	Configuration Management
DEC	Digital Equipment Corporation
DISA	Defense Information Systems Agency
DoD	Department of Defense
DoS	Denial of Service
DSCP	Differentiated Services Code Point
EBC	Edge Boundary Controller
FIPS	Federal Information Processing Standards
FW	Firewall
HBSS	Host Based Security System
HTTP	Hypertext Transfer Protocol
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPS	Intrusion Protection System
IPSec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IRC	Internet Relay Chat
IS	Information System
ISS	Integrated Security System
KBPS	Kilobits per second
LOC-SRV	Location Service
LPR	Local Printer
LS	Local Session
MS	Microsoft
NAC	Network Access Control
NETBIOS-dgm	Network Basic Input/Output System datagram
NETBIOS-ns	Network Basic Input/Output System-name service
NETBIOS-ssn	Network Basic Input/Output System-session service
NETBUS	Name of software
NETSTAT	Network Status
NFS	Network File System
NTALK	UNIX Talk
NTPv4	Network Time Protocol version 4