



DEFENSE INFORMATION SYSTEMS AGENCY

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

IN REPLY
REFER
TO:

Joint Interoperability Test Command (JTE)

23 Oct 12

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Extension of the Special Interoperability (IO) Test Certification of the Cisco Adaptive Security Appliance (ASA) 5585 Firewall/VPN with Software from Version 8.4(2) to Version 8.4(4)1

References: (a) Department of Defense (DoD) Directive 4630.05, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," 5 May 2004
(b) Chairman, Joint Chiefs of Staff Instruction 6212.01F, "Net Ready Key Performance Parameter (NR-KPP)," 21 March 2012
(c) through (g), see Enclosure

1. References (a) and (b) establish the Joint Interoperability Test Command (JITC), as the responsible organization for Interoperability (IO) test certification.
2. The Cisco ASA 5585 with software release Version 8.4(4)1, hereinafter referred to as the System Under Test (SUT), meets all the critical IO requirements for a Firewall and Virtual Private Network (VPN) and is certified for joint use within the Defense Information Systems Network (DISN). The certification status of the SUT will be verified during operational deployment. Any new discrepancies noted in the operational environment will be evaluated for impact on the existing certification. These discrepancies will be adjudicated to the satisfaction of the Defense Information Systems Agency (DISA) via a vendor Plan of Actions and Milestones (POA&M) which addresses all new critical Test Discrepancy Reports (TDRs) within 120 days of identification. Testing was conducted using product requirements derived from the Unified Capabilities Requirements (UCR), Reference (c), and test procedures, Reference (d). No other configurations, features, or functions, except those cited within this memorandum, are certified by JITC. This certification expires upon changes that affect IO, but no later than three years from the date of the signed Department of Defense (DoD) Unified Capabilities (UC) Approved Product List (APL) approval memorandum 11 Jun 2012.
3. The extension of this certification is based upon Desktop Review (DTR) 1. The original certification is based on IO testing conducted by the United States Army Information Systems Engineering Command, Technology Integration Center (USAISEC-TIC), DISA adjudication of open TDRs, review of the vendor's Letters of Compliance (LoCs), and DISA Certifying Authority (CA) approval of the IA configuration. The USAISEC-TIC, Fort Huachuca, Arizona conducted IO testing from 24 October to 9 November 2011. The vendor completed the Internet Protocol Version 6 (IPv6) LoC review on 21 February 2012. DISA completed adjudication of outstanding IPv6 TDRs on 13 March 2012 and accepted the vendor IPv6 TDR POA&M mitigation timeframe of June 2012. Reference (e) documents the test results and describes the

JITC Memo, JTE, Extension of the Special Interoperability (IO) Test Certification of the Cisco Adaptive Security Appliance (ASA) 5585 Firewall/VPN with Software from Version 8.4(2) to Version 8.4(4)1

tested network and system configurations including specified patch releases. The DISA CA has reviewed the IA Assessment Report for the SUT (Reference (f) and (g)) and based on the findings in the report provided a positive recommendation on 08 May 2012. The acquiring agency or site will be responsible for the DoD Information Assurance Certification and Accreditation Process (DIACAP). JITC certifies the SUT as meeting the UCR for a Firewall/VPN. DTR 1 was requested for a change in software from code version 8.4(2) to 8.4(4)1. The USAISEC-TIC determined that Verification and Validation (V&V) testing was required prior to approval to ensure that when IKEv2 functionality was added the functionality of IKEv1 was not negatively impacted. The V&V IO testing of the changes associated with DTR 1 was successfully verified on 20 August 2012. Therefore, DTR 1 is approved by JITC and the SUT is now certified for joint use within the DISN. The DISA CA concurred with the USAISEC-TIC's determination that IA testing is not required for DTR1. The DISA CA, based on the original security testing completed and published in separate reports (References (f) and (g)), provided a positive recommendation for DTR1 on 13 September 2012.

4. The interface Capability Requirements (CRs), Functional Requirements (FRs), and the component status of the SUT are listed in Table 1. The threshold CRs/FRs for security devices are established by Section 5.8 of Reference (c) and were used to evaluate the IO of the SUT.

Extension of the special Interoperability (IO) Test Certification of the Cisco Adaptive Security Appliance (ASA) 5585 Firewall/VPN with Software from Version 8.4(2) to Version 8.4(4)1

Table 1. SUT Interface Interoperability Status

Interface	Critical (See note 1.)	UCR Reference	Threshold CRs/FRs Requirements (See note 2.)	Status	Remarks (See note 3.)																
FW																					
10Base-X	No	5.3.2.4 / 5.3.3.10.1.2	1-4	Met	See Note 4																
100Base-X	No	5.3.2.4 / 5.3.3.10.1.2	1-4	Met	See Note 4																
1000Base-X	No	5.3.2.4 / 5.3.3.10.1.2	1-4	Met	See Note 4																
10GBase-X	No	5.3.2.4 / 5.3.3.10.1.2	1-4	Met	See Note 5																
40GBase-X	No	5.3.2.4 / 5.3.3.10.1.2	1-4	N/A																	
100GBase-X	No	5.3.2.4 / 5.3.3.10.1.2	1-4	N/A																	
VPN																					
10Base-X	No	5.3.2.4 / 5.3.3.10.1.2	1-3	Met	See Note 4																
100Base-X	No	5.3.2.4 / 5.3.3.10.1.2	1-3	Met	See Note 4																
1000Base-X	No	5.3.2.4 / 5.3.3.10.1.2	1-3	Met	See Note 4																
10GBase-X	No	5.3.2.4 / 5.3.3.10.1.2	1-3	Met	See Note 5																
40GBase-X	No	5.3.2.4 / 5.3.3.10.1.2	1-3	N/A																	
100GBase-X	No	5.3.2.4 / 5.3.3.10.1.2	1-3	N/A																	
<p>NOTES:</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. CRs/FRs are contained in Table 2. CR/FR numbers represent a rollup of the UCR. Enclosure 3 of the Original IO Certification provides a list of more detailed requirements for security device products.</p> <p>3. SUT will meet applicable standards for interface provided.</p> <p>4. SUT has eight 10/100/1000-Base-T integrated ports.</p> <p>5. SUT has two 10-GbE ports.</p> <p>LEGEND:</p> <table style="width: 100%; border: none;"> <tr> <td style="width: 30%;">10 GbE</td> <td style="width: 30%;">10 Gigabit Ethernet</td> <td style="width: 30%;">N/A</td> <td style="width: 30%;">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>FW</td> <td>Firewall</td> <td>VPN</td> <td>Virtual Private Network</td> </tr> </table>						10 GbE	10 Gigabit Ethernet	N/A	Not Applicable	CR	Capability Requirement	SUT	System Under Test	FR	Functional Requirement	UCR	Unified Capabilities Requirements	FW	Firewall	VPN	Virtual Private Network
10 GbE	10 Gigabit Ethernet	N/A	Not Applicable																		
CR	Capability Requirement	SUT	System Under Test																		
FR	Functional Requirement	UCR	Unified Capabilities Requirements																		
FW	Firewall	VPN	Virtual Private Network																		

JITC Memo, JTE, Extension of the Special Interoperability (IO) Test Certification of the Cisco Adaptive Security Appliance (ASA) 5585 Firewall/VPN with Software from Version 8.4(2) to Version 8.4(4)1

Table 2. SUT Capability Requirements and Functional Requirements Status

CR/FR ID	Capability/Function	Applicability (See note 1.)	UCR Reference	Status	Remarks
1	Conformance Requirements				
	Conformance Standards	Required	5.8.4.2	Met	See note 4
2	Information Assurance Requirements				
	General Requirements	Required	5.8.4.3.1	Met	See note 5
	Configuration Management	Required	5.8.4.3.3	Met	See note 5
	Alarms & Alerts	Required	5.8.4.3.4	Met	See note 5
	Audit and Logging	Required	5.8.4.3.5	Met	See note 6
	Integrity	Required	5.8.4.3.6	Met	See note 5
	Documentation	Required	5.8.4.3.7	Met	See note 7
	Cryptography	Required (See note 2.)	5.8.4.3.8	Met	See note 8
	Security Measures	Required	5.8.4.3.9	Met	See note 9
	System and Communication Protection	Required	5.8.4.3.10	Met	See note 10
	Other Requirements	Required	5.8.4.3.11	Met	See note 5
	Performance	Required	5.8.4.3.12	Met	See note 11
3	Functionality				
	Policy	Required	5.8.4.4.1	Met	See note 9
	Filtering	Required	5.8.4.4.2	Met	See note 10
4	IPS Functionality				
	IPS Security Device Requirements	Required (See note 3.)	5.8.4.5	N/A	IDS/IPS Only

NOTES:

1. Criticality represents high-level rollup of the CR/FR area. Table 3-1 of Enclosure 3 of the Original IO Certification provides a detailed CR/FR for each security device product (FW, IPS/IDS, VPN component).
2. Cryptography is optional with the exception that all outgoing communications are encrypted.
3. IPS functionality only applies to IPS products. Requirements are not applicable to firewalls or VPN concentrators.
4. Cisco provided a LoC.
5. This requirement was not tested on this evaluation because of a previous evaluation on a similar ASA product that has been placed on the DISA APL (Tracking Number 1002816).
6. The SUT logged critical security events during the evaluation.
7. Cisco has full documentation on their website on configuration, management, and implementation of the ASA5585.
8. The management and VPN session was secured with FIP-140-2-approved encryption.
9. This requirement is met by RAE.
10. SUT was able to secure the data traffic with port and protocol filters.
11. SUT performance was not fully tested because of the limitation of the traffic generator.

LEGEND:

APL	Approved Products List	IDS	Intrusion Detection System
ASA	Adaptive Security Appliance	IPS	Intrusion Prevention System
CR	Capability Requirement	LoC	Letter of Compliance
DISA	Defense Information Systems Agency	N/A	Not Applicable
FIPS	Federal Information Processing Standards	RAE	Required Ancillary Equipment
FR	Functional Requirement	SUT	System Under Test
FW	Firewall	UCR	Unified Capabilities Requirements
ID	Identification	VPN	Virtual Private Network

Extension of the special Interoperability (IO) Test Certification of the Cisco Adaptive Security Appliance (ASA) 5585 Firewall/VPN with Software from Version 8.4(2) to Version 8.4(4)1

5. No detailed test report was developed in accordance with the Program Manager's request. JITC distributes IO information via the JITC Electronic Report Distribution (ERD) system, which uses Unclassified-But-Sensitive Internet Protocol Router Network (NIPRNet) e-mail. More comprehensive IO 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>. Test reports, lessons learned, and related testing documents and references are on the JITC Joint Interoperability Tool (JIT) at <http://jit.fhu.disa.mil> (NIPRNet). Information related to Defense Switched Network (DSN) testing is on the Telecom Switched Services Interoperability (TSSI) website at <http://jitc.fhu.disa.mil/tssi>. All associated data is available on the Defense Information Systems Agency Unified Capabilities Certification Office (UCCO) website located at <https://aplits.disa.mil>.

6. The testing point of contact is Mr. Eric Sundius, USAISEC-TIC; commercial (520) 533-3749 or DSN 821-3749; e-mail address is Eric.C.Sundius.civ@mail.mil. The JITC certification point of contact is Mr. Kevin Holmes; commercial (301) 743-4300; e-mail address is Timothy.K.Holmes.civ@mail.mil. JITC's mailing address is P.O. Box 12798, Fort Huachuca, Arizona 85670-1298. The Unified Capabilities Certification Office tracking numbers are 1116101 and 1116102.

FOR THE COMMANDER:

Enclosure a/s



for BRADLEY A. CLARK
Acting Chief
Battlespace Communications Portfolio

JITC Memo, JTE, Extension of the Special Interoperability (IO) Test Certification of the Cisco Adaptive Security Appliance (ASA) 5585 Firewall/VPN with Software from Version 8.4(2) to Version 8.4(4)1

Distribution (electronic mail):

DoD CIO

Joint Staff J-6, JCS

USD(AT&L)

ISG Secretariat, DISA, JTA

U.S. Strategic Command, J665

US Navy, OPNAV N2/N6FP12

US Army, DA-OSA, CIO/G-6 ASA(ALT), SAIS-IOQ

US Air Force, A3CNN/A6CNN

US Marine Corps, MARCORSSYSCOM, SIAT, A&CE Division

US Coast Guard, CG-64

DISA/TEMC

DIA, Office of the Acquisition Executive

NSG Interoperability Assessment Team

DOT&E, Netcentric Systems and Naval Warfare

Medical Health Systems, JMIS IV&V

UCCO

ADDITIONAL REFERENCES

- (c) Office of the Assistant Secretary of Defense, "Department of Defense Unified Capabilities Requirements 2008, Change 2," December 2010
- (d) Joint Interoperability Test Command, "Unified Capabilities Information Assurance Test Plan Version 2," December 2010
- (e) Joint Interoperability Test Command, Special Interoperability (IO) Test Certification of the Cisco Adaptive Security Appliance (ASA) 5585 Firewall/VPN with Software Version 8.4(2)," 6 June 2012
- (f) Joint Interoperability Test Command, "Information Assurance (IA) Assessment of Cisco Systems, Inc. Adaptive Security Appliance 5585 Virtual Private Network Concentrator Appliance" (Tracking Number 1116101)," 2 June 2012
- (g) Joint Interoperability Test Command, "Information Assurance (IA) Assessment Cisco Systems, Inc. Adaptive Security Appliance 5585 Firewall Appliance" (Tracking Number 1116102)," 2 June 2012