



DEFENSE INFORMATION SYSTEMS AGENCY

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

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

15 Aug 14

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Extension of the Joint Interoperability Certification of the Cisco Systems Adaptive Security Appliance (ASA) 5500 Series, 5500-X Series (5555-X, 5585-X-SSP-20), and WS-SVC-ASA-SM1 Virtual Private Network (VPN) Concentrator, version 9.1.2(8) to version 9.1.5.

References: (a) Department of Defense Instruction 8100.04, "DoD Unified Capabilities (UC)," 9 December 2010
(b) DoD CIO, Memorandum, "Interim Guidance for Interoperability of Information Technology (IT) and National Security Systems (NSS)," 27 March 2012
(c) through (e), see Enclosure 1

1. **Certification Authority.** References (a) and (b) establish the Joint Interoperability Test Command (JITC) as the Joint Interoperability Certification Authority for the Unified Capabilities (UC) products.

2. **Conditions of Certification.** The Cisco Systems Adaptive Security Appliance (ASA) 5500 Series, 5500-X Series (5555-X, 5585-X-SSP-20), and WS-SVC-ASA-SM1, version 9.1.2(8) to version 9.1.5; hereinafter referred to as the System Under Test (SUT), was originally certified for joint use as a Virtual Private Network (VPN). The SUT met the requirements of the Unified Capabilities Requirements (UCR) 2013, Reference (d), and was certified for joint use as a Virtual Private Network (VPN) Concentrator with the conditions described in Table 1. This certification expires upon changes that affect interoperability, but no later than 3 years from the date of this memorandum.

JITC extends the certification for Desk Top Review (DTR) 1. The vendor submitted DTR 1 to include the new Cisco code release version 9.1.5. The vendor submittal documentation was reviewed by JITC and the United States Army Information Systems Engineering Command (USAISEC) Technology Integration Center (TIC). A determination was made that the updated code version was introduced to address Information Assurance Vulnerability Alerts (IAVAs), and that no IA or IO testing was necessary for DTR 1.

JITC Memo, JTD, Joint Interoperability Certification of the Cisco Systems Adaptive Security Appliance (ASA) 5500 Series, 5500-X Series (5555-X, 5585-X-SSP20), and WS-SVC-ASA-SM1 Virtual Private Network (VPN) Concentrator, version 9.1.2(8) to version 9.1.5

Table 1. Conditions

Condition	Operational Impact	Remarks
UCR Waivers		
None		
Conditions of Fielding		
CoF: Put in deployment guide instructions on manually verify the OSCP CRL, Certificate Revocation Lists. Minor with POA&M March 2015.	Minor with POA&M	UCR 2013 paragraph IA-059040 - If the system supports queries against an online status check responder (an OCSP responder in the case of the DoD PKI), the system shall periodically query the responder to determine if the certificates corresponding to any ongoing sessions have been revoked.
CoF: Put in deployment guide manual procedures verify expired certificates. Minor with POA&M March 2015.	Minor with POA&M	UCR 2013 paragraph IA-060000 - The system shall be capable of sending an alert when installed certificates corresponding to trust chains, OCSP responder certificates, or any other certificates installed on the device that cannot be renewed in an automated manner, are nearing expiration.
CoF: Put in deployment guide manual procedures verify expired certificates. Minor with POA&M March 2015.	Minor with POA&M	UCR 2013 paragraph IA-060010 - The system shall be capable of sending an alert when installed certificates corresponding to trust chains, OCSP responder certificates, or any other certificates installed on the device that cannot be renewed in an automated manner, are nearing expiration.
CoF: The SUT can interconnect only with Cisco client (not with other vendor beyond Cisco).	Minor with No POA&M	UCR 2013 paragraph IA-071040 - If IPSec is used, the product shall be capable of using and interpreting certificate requests for Public-Key Cryptography Standard #7 (PKCS#7) wrapped certificates as a request for the whole path of certificates.
Open Test Discrepancies		
POA&M: This requirement will be met in release ASA 9.4.x in March 2015.	Minor with POA&M	UCR 2013 paragraph IA-060000 - The system shall be capable of sending an alert when installed certificates corresponding to trust chains, OCSP responder certificates, or any other certificates installed on the device that cannot be renewed in an automated manner, are nearing expiration.
POA&M: This requirement will be met in release ASA 9.4.x in March 2015.	Minor with POA&M	UCR 2013 paragraph IA-060010 - The system shall be capable of sending an alert when installed certificates corresponding to trust chains, OCSP responder certificates, or any other certificates installed on the device that cannot be renewed in an automated manner, are nearing expiration.
Open Findings with No Interoperability (IO) impact		
29 October 2013 Adjudication: No IO impacting this IA requirements. Accepts POA&M March 2015.	Minor with POA&M	UCR 2013 paragraph IA-059000 - Periodically, the system shall examine all of the certificates and trust chains associated with ongoing, long-lived, sessions. The system shall terminate any ongoing sessions based on updated revocation/trust information if it is determined that the corresponding certificates have been revoked, are no longer trusted, or are expired.
29 October 2013 Adjudication: No IO impacting this IA requirements. Accepts POA&M March 2015.	Minor with POA&M	UCR 2013 paragraph IA-059040 - If the system supports queries against an online status check responder (an OCSP responder in the case of the DoD PKI), the system shall periodically query the responder to determine if the certificates corresponding to any ongoing sessions have been revoked.
29 October 2013 Adjudication: No IO impacting this IA requirements. Accepts POA&M March 2015.	Minor with POA&M	UCR 2013 paragraph IA-059050 - If the system supports queries against an online status check responder (an OCSP responder in the case of the DoD PKI), by default, for each session, the device shall query the online status check responder every 24 hours for as long as the session remains active'
29 October 2013 Adjudication: No IO impacting this IA requirements. Accepts POA&M March 2015.	Minor with POA&M	UCR 2013 paragraph IA-059060 - If the system supports queries against an online status check responder (an OCSP responder in the case of the DoD PKI), the system shall support the ability to configure the interval at which the system periodically queries the online status check responder.

JITC Memo, JTD, Joint Interoperability Certification of the Cisco Systems Adaptive Security Appliance (ASA) 5500 Series, 5500-X Series (5555-X, 5585-X-SSP20), and WS-SVC-ASA-SM1 Virtual Private Network (VPN) Concentrator, version 9.1.2(8) to version 9.1.5

Table 1. Conditions (continued)

Condition	Operational Impact	Remarks																																
Open Findings with No Interoperability (IO) impact (continued)																																		
29 October 2013 Adjudication: No IO impacting this requirements. Accepts POA&M March 2015.	Minor with POA&M	UCR 2013 paragraph Tab IPv6 - IP6-000770 - If RFC 4301 is supported, then the product should include a management control to allow an administrator to enable or disable the ability of the product to send an IKE notification of an INVALID_SELECTORS. NOTE: Some products may not be able to log all this information (e.g., the product may not have access to this information).																																
29 October 2013 Adjudication: No IO impact. Per JITC, impacts functionality. Accepts POA&M March 2015.	Minor with POA&M	UCR 2013 paragraph A-12 SEC-000090 - 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).																																
<p>LEGEND:</p> <table> <tr> <td>CoF</td> <td>Condition of Fielding</td> <td>RSA</td> <td>Ron Rivest, Adi Shamir, and Leonard Adleman</td> </tr> <tr> <td>DoD</td> <td>Department of Defense</td> <td>SD</td> <td>Security Device</td> </tr> <tr> <td>DR</td> <td>Delete Requirement</td> <td>SHA1</td> <td>Secure Hash Algorithm 1</td> </tr> <tr> <td>IA</td> <td>Information Assurance</td> <td>SSH</td> <td>Secure Shell</td> </tr> <tr> <td>LoC</td> <td>Letter of Compliance</td> <td>SUT</td> <td>System Under Test</td> </tr> <tr> <td>OCSP</td> <td>Online Certificate Status Protocol</td> <td>TDR</td> <td>Technical Discrepancy Report</td> </tr> <tr> <td>PKI</td> <td>Public Key Infrastructure</td> <td>UCR</td> <td>Unified Capabilities Requirements</td> </tr> <tr> <td>POA&M</td> <td>Plan of Actions and Mitigations</td> <td></td> <td></td> </tr> </table>			CoF	Condition of Fielding	RSA	Ron Rivest, Adi Shamir, and Leonard Adleman	DoD	Department of Defense	SD	Security Device	DR	Delete Requirement	SHA1	Secure Hash Algorithm 1	IA	Information Assurance	SSH	Secure Shell	LoC	Letter of Compliance	SUT	System Under Test	OCSP	Online Certificate Status Protocol	TDR	Technical Discrepancy Report	PKI	Public Key Infrastructure	UCR	Unified Capabilities Requirements	POA&M	Plan of Actions and Mitigations		
CoF	Condition of Fielding	RSA	Ron Rivest, Adi Shamir, and Leonard Adleman																															
DoD	Department of Defense	SD	Security Device																															
DR	Delete Requirement	SHA1	Secure Hash Algorithm 1																															
IA	Information Assurance	SSH	Secure Shell																															
LoC	Letter of Compliance	SUT	System Under Test																															
OCSP	Online Certificate Status Protocol	TDR	Technical Discrepancy Report																															
PKI	Public Key Infrastructure	UCR	Unified Capabilities Requirements																															
POA&M	Plan of Actions and Mitigations																																	

3. **Interoperability Status.** Table 2 provides the SUT interface interoperability status and Table 3 provides the Capability Requirements (CR) and Functional Requirements (FR) status. Table 4 provides a Unified Capabilities (UC) Approved Products List (APL) product summary.

Table 2. Interface Status

Interface (See Note 1.)	Threshold CR/FR Requirements (See Note 2.)	Status	Remarks																
Security Devices																			
10Base-X	1-3	Met	None																
100Base-X	1-3	Met	None																
1000Base-X	1-3	Partially Met	See Note 3.																
10GBase-X	1-3	Met	None																
40GBase-X	1-3	N/A	None																
100GBase-X	1-3	N/A	None																
<p>NOTES:</p> <ol style="list-style-type: none"> UCR 2013, Section 13 does not identify individual interface requirements for security devices. The SUT must minimally provide Ethernet interfaces that meet the requirements in Section 2.7.1. The CR/FR requirements are contained in Table 3. The CR/FR numbers represent a roll-up of UCR2013 requirements. Enclosure 3 provides a list of more detailed requirements for security devices. The ASA 5505 only supports media rates of 10/100 Mbps. 																			
<p>LEGEND:</p> <table> <tr> <td>Base-X</td> <td>Ethernet generic designation (Baseband)</td> <td>Mbps</td> <td>Megabits Per Second</td> </tr> <tr> <td>CR</td> <td>Capability Requirements</td> <td>N/A</td> <td>Not Applicable</td> </tr> <tr> <td>FR</td> <td>Functional Requirements</td> <td>SUT</td> <td>System Under Test</td> </tr> <tr> <td>GBase-X</td> <td>Gigabit generic designation (Baseband)</td> <td>UCR</td> <td>Unified Capabilities Requirements</td> </tr> </table>				Base-X	Ethernet generic designation (Baseband)	Mbps	Megabits Per Second	CR	Capability Requirements	N/A	Not Applicable	FR	Functional Requirements	SUT	System Under Test	GBase-X	Gigabit generic designation (Baseband)	UCR	Unified Capabilities Requirements
Base-X	Ethernet generic designation (Baseband)	Mbps	Megabits Per Second																
CR	Capability Requirements	N/A	Not Applicable																
FR	Functional Requirements	SUT	System Under Test																
GBase-X	Gigabit generic designation (Baseband)	UCR	Unified Capabilities Requirements																

JITC Memo, JTD, Joint Interoperability Certification of the Cisco Systems Adaptive Security Appliance (ASA) 5500 Series, 5500-X Series (5555-X, 5585-X-SSP20), and WS-SVC-ASA-SM1 Virtual Private Network (VPN) Concentrator, version 9.1.2(8) to version 9.1.5

4. **Test Details.** DTR 1 was requested to extend the Joint Interoperability Certification of the Cisco Systems Adaptive Security Appliance (ASA) 5500 Series, 5500-X Series (5555-X, 5585-X-SSP-20), and WS-SVC-ASA-SM1 Virtual Private Network (VPN) from code version 9.1.2(8) to 9.1.5. DTR 1 has no impact on the approved and certified IO results, no further IO testing was performed for this DTR 1.

5. **Additional Information.** JITC distributes interoperability information via the JITC Electronic Report Distribution (ERD) system, which uses Unclassified-But-Sensitive Internet Protocol Router Network (NIPRNet) e-mail. Interoperability status information is available via the JITC System Tracking Program (STP). STP is accessible by .mil/.gov users 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 <https://jit.fhu.disa.mil/>. Due to the sensitivity of the information, the Information Assurance Accreditation Package (IAAP) that contains the approved configuration and deployment guide must be requested directly from the Unified Capabilities Certification Office (UCCO), e-mail: disa.meade.ns.list.unified-capabilities-certification-office@mail.mil. All associated information is available on the DISA UCCO website located at <http://www.disa.mil/Services/Network-Services/UCCO>.

6. **Point of Contact (POC).** The USAISEC TIC's testing point of contact is Mr. Eric Sundius, USAISEC TIC; commercial (520) 533-3766 or DSN 821-3766; e-mail address is eric.c.sundius.civ@mail.mil. The JITC certification point of contact is Ms. Jaime Downing, commercial telephone (301) 743-4306; e-mail address jaime.f.downing.civ@mail.mil; mailing address Joint Interoperability Test Command, ATTN: JTD1 (Ms. Jaime Downing) 3341 Strauss Ave., Suite 236, Indian Head, MD 20646-5149. The UCCO tracking number for the SUT is 1306702.

FOR THE COMMANDER:

3 Enclosures a/s


for RIC HARRISON
Chief
Networks/Communications and UC Portfolio

JITC Memo, JTD, Joint Interoperability Certification of the Cisco Systems Adaptive Security Appliance (ASA) 5500 Series, 5500-X Series (5555-X, 5585-X-SSP20), and WS-SVC-ASA-SM1 Virtual Private Network (VPN) Concentrator, version 9.1.2(8) to version 9.1.5

Distribution (electronic mail):

DoD CIO

Joint Staff J-6, JCS

USD(AT&L)

ISG Secretariat, DISA, JTA

US 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

HQUSAISEC, AMSEL-IE-IS

UCCO

ADDITIONAL REFERENCES

- (c) Joint Interoperability Test Command (JTD), "Joint Interoperability Certification of the Cisco Systems Adaptive Security Appliance (ASA) 5500 Series, 5500-X Series (5555-X, 5585-X-SSP-20), and WS-SVC-ASA-SM1 Virtual Private Network (VPN) Concentrator, all with software version 9.1.2(8)", 18 December 2013
- (d) Office of the Department of Defense Chief Information Officer, "Department of Defense Unified Capabilities Requirements 2013", January 2013
- (e) Joint Interoperability Test Command, "Security Device Test Plan"