



DEFENSE INFORMATION SYSTEMS AGENCY

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

IN REPLY
REFER
TO:

Joint Interoperability Test Command (JTE)

6 Jun 12

MEMORANDUM FOR DISTRIBUTION

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

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 (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 Cisco ASA 5585 with software release 8.4, hereinafter referred to as the System Under Test (SUT), meets all the critical Interoperability (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 discrepancy 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 Action 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 (e). 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 this memorandum.

3. This finding 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 Information Assurance (IA) Certification Authority (CA) approval of the IA configuration. The USAISEC-TIC, Fort Huachuca, Arizona conducted IO testing from 24 October 2011 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 these IPv6 TDRs were accepted as minor with a vendor POA&M for June 2012. The DISA CA has reviewed the IA Assessment Report for the SUT, Reference (f), and based on the findings in the report provided a positive recommendation on 02 June 2012. The acquiring agency or site will be responsible for the DoD Information Assurance Certification and Accreditation Process

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

(DIACAP). The JITC certifies the SUT as meeting the UCR for a firewall/VPN. Enclosure 2 documents the test results and describes the tested network and system configurations including specified patch releases.

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.

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 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: 50%;">10 GbE 10 Gigabit Ethernet</td> <td style="width: 50%;">NA 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 Requirements</td> </tr> <tr> <td>FW Firewall</td> <td>VPN Virtual Private Network</td> </tr> </table>						10 GbE 10 Gigabit Ethernet	NA 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	NA 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, Special Interoperability (IO) Test Certification of the Cisco Adaptive Security Appliance (ASA) 5585 Firewall/VPN with Software Version 8.4 (2)

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:

- Criticality represents high-level rollup of the CR/FR area. Table 3-1 of Enclosure 3 provides a detailed CR/FR for each security device product (FW, IPS/IDS, VPN component).
- Cryptography is optional with the exception that all outgoing communications are encrypted.
- IPS functionality only applies to IPS products. Requirements are not applicable to firewalls or VPN concentrators.
- Cisco provided a LoC.
- 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).
- The SUT logged critical security events during the evaluation.
- Cisco has full documentation on their website on configuration, management, and implementation of the ASA5585.
- The management and VPN session was secured with FIP-140-2-approved encryption.
- This requirement is met by RAE.
- SUT was able to secure the data traffic with port and protocol filters.
- 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	NA	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

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

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 Switch 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. Jim Hatch, USAISEC-TIC; commercial (520) 533-2860 or DSN 821-2860; e-mail address is james.d.hatch12.civ@mail.mil. The JITC certification point of contact is Mr. Kevin Holmes; commercial (301) 744-2763 or DSN 354-2763; e-mail address is timothy.k.holmes.civ@mail.mil. The JITC's mailing address is P.O. Box 12798, Fort Huachuca, Arizona 85670-1298. The Unified Capabilities Certification Office tracking number is 1116101/1116102.

FOR THE COMMANDER:

3 Enclosures a/s


for RICHARD A. MEADOR
Chief
Battlespace Communications Portfolio

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

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

This page intentionally left blank.

ADDITIONAL REFERENCES

- (c) Office of the Assistant Secretary of Defense, "Department of Defense Unified Capabilities Requirements 2008, Change 3," December 2010.
- (d) Department of Defense Instruction 8100.04, "Department of Defense (DoD) Voice Networks", 9 December 2010.
- (e) Joint Interoperability Test Command, "Unified Capabilities Information Assurance Test Plan Version 2," December 2010.
- (f) Field Security Office, "Unified Capabilities (UC) Approved Products List (APL) Recommendation for Cisco Adaptive Security Appliance (ASA) 5585 Rel. 8.4 Virtual Private Network (VPN) (TN# 1116101/CA# 12D-APL-05-378-U)", May 2012.

This page intentionally left blank.

CERTIFICATION TESTING SUMMARY

- 1. SYSTEM TITLE.** Cisco Adaptive Security Appliance (ASA) 5500 Series, Release 8.4(2), Unified Capabilities Tracking Number (TN) 1116101 virtual private network (VPN)/1116102 firewall (FW)
- 2. SPONSOR.** Department of the Army (DA)
- 3. SYSTEM POC.** Mr. Jordan Silk, United States Army Information Systems Engineering Command, Technology Integration Center (USAISEC-TIC), Building 53302, Fort Huachuca, Arizona 85613; e-mail: Jordan.Silk@us.army.mil.
- 4. TESTER.** Testing conducted at DA Distributed Testing Lab, United States Army Information USAISEC-TIC, ATTN: Mr. James Hatch, Fort Huachuca, Arizona 85613; e-mail: James.Hatch@us.army.mil.
- 5. SYSTEM DESCRIPTION.** Security Devices provide a Global Information Grid (GIG) architectural defense-in-depth capability to protect and define critical warfighting missions. The Unified Capabilities Requirements (UCR) defines three security device products: FWs, Intrusion Detection Systems (IDSs)/Intrusion Prevention Systems (IPSs), and VPN components (concentrator and termination). The Cisco ASA 5585 Series, Release 8.4 (2), hereinafter referred to as the system under test (SUT), provides the following FW and VPN capabilities.

The Cisco ASA is designed as a multipurpose network perimeter security device. The Cisco ASA has integrated the following functionalities into a single unit: FW, IDS/IPS, and VPN. Only the FW and VPN capabilities were tested under this evaluation.

The Cisco ASA5585-X SSP-20 is the high-end model of the Cisco ASAs. It is designed to support large enterprise and data centers with demanding data networks. The ASA5585-20 has eight Gigabit Ethernet (GbE) and two 10-GbE small form-factor pluggable plus (SFP+) integrated ports. It is a stateful firewall that can determine whether the connections are new or established. Based on the connection state, filters and access policies can be applied.

The ASA5585 can be configured to integrate with Active Directory to create access policies and authenticate Common Access Card (CAC) users. Users from remote locations can access protected network resources by going through the ASA5585 using the Internet Protocol Security (IPSec) VPN client, AnyConnect client, or clientless Secure Sockets Layer (SSL) VPN. When an authorized VPN user is connected, the ASA creates the tunnel, authenticates the user, and encrypts and decrypts the traffic using Federal Information Processing Standard (FIPS)-approved cipher suites.

Management access to the ASA5585 can be configured for Adaptive Security Device Manager (ASDM), Telnet, Secure Shell (SSH), or console. The ASDM is a web-based

graphical user interface (GUI) application accessible using a supported Internet browser.

6. OPERATIONAL ARCHITECTURE. Figure 2-1 depicts a notional operational architecture in which the SUT may be used.

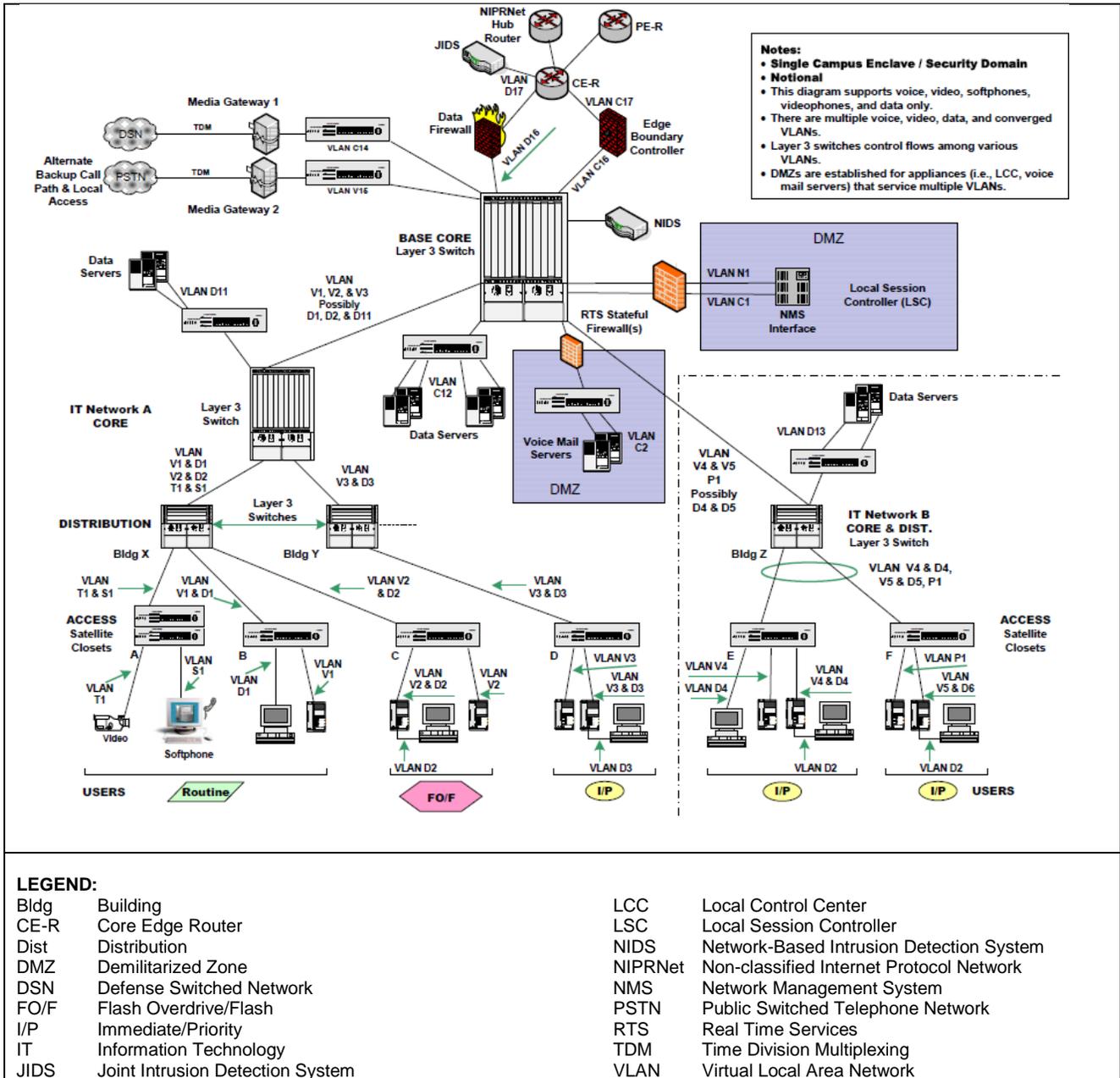


Figure 2-1. Security Device Architecture

7. INTEROPERABILITY REQUIREMENTS. Section 5.8 of Reference (c) establishes the interface, Capability Requirements (CRs) and Functional Requirements (FRs), Information Assurance (IA), and other requirements for security devices.

7.1 Interfaces. The ASA5585 uses the external interfaces to connect to the 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 Ref	FW	IPS	VPN	Criteria	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	

NOTES:
1. UCR did not identify individual interface requirements for security devices. SUT must minimally provide an Ethernet interface (one of the listed).
2. CRs/FRs are contained in Table 2-2. CR/FR numbers represent a roll-up of the UCR. Enclosure 3 provides a list of more detailed requirements for security device products.

LEGEND:
C Conditional
CR Capability Requirement
FR Functional Requirement
FW Firewall
IPS Intrusion Protection System
SUT System Under Test
UCR Unified capabilities Requirements
VPN Virtual Private network

7.2 Capability Requirements and Functional Requirements. Security Device products have required and conditional features and capabilities established by Section 5.8 of the UCR. The SUT does not need to provide non-critical (conditional) requirements. If provided, they must function according to the specified requirements. The SUT's features and capabilities and its aggregated requirements, IAW the security device requirements, are listed in Table 2-2. Detailed CRs/FRs are provided in Table 3-1 of Enclosure 3.

Table 2-2. Security Device Requirements and Functional Requirements

CR/FR ID	Capability/Function	Applicability (See note 1.)	UCR Reference	Status	Remarks																
1	Conformance Requirements																				
	Conformance Standards	Required	5.8.4.2																		
2	Information Assurance Requirements																				
	General Requirements	Required	5.8.4.3.1																		
	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																		
	Integrity	Required	5.8.4.3.6																		
	Documentation	Required	5.8.4.3.7																		
	Cryptography	Required (See note 2.)	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	Functionality																				
	Policy	Required	5.8.4.4.1																		
	Filtering	Required	5.8.4.4.2																		
4	IPS Functionality																				
	IPS Security Device Requirements	Required (See note 3.)	5.8.4.5																		
<p>NOTES:</p> <p>1. 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>2. Cryptography is optional with the exception that all outgoing communications are encrypted.</p> <p>3. IPS functionality only applies to IPS products. Requirements are not applicable to firewalls or VPN concentrators.</p> <p>LEGEND:</p> <table> <tr> <td>CR</td> <td>Capability Requirement</td> <td>IDS</td> <td>Intrusion Detection System</td> </tr> <tr> <td>FR</td> <td>Functional Requirement</td> <td>IPS</td> <td>Intrusion Prevention System</td> </tr> <tr> <td>FW</td> <td>Firewall</td> <td>VPN</td> <td>Virtual Private Network</td> </tr> <tr> <td>ID</td> <td>Identification</td> <td>UCR</td> <td>Unified Capabilities Requirements</td> </tr> </table>						CR	Capability Requirement	IDS	Intrusion Detection System	FR	Functional Requirement	IPS	Intrusion Prevention System	FW	Firewall	VPN	Virtual Private Network	ID	Identification	UCR	Unified Capabilities Requirements
CR	Capability Requirement	IDS	Intrusion Detection System																		
FR	Functional Requirement	IPS	Intrusion Prevention System																		
FW	Firewall	VPN	Virtual Private Network																		
ID	Identification	UCR	Unified Capabilities Requirements																		

7.3 Information Assurance. Table 2-3 details the IA requirements applicable to the security device products.

Table 2-3. Security Device IA Requirements

Capability/Function	Applicability (Note 1)	UCR Reference	Criteria	Remarks
General Requirements	Required	5.8.4.3.1	Meet UCR 'required' requirements. Enclosure 3 provides detailed functional requirements for each specified FR/CR	Applies to all Security Devices
Configuration Management	Required	5.8.4.3.3		Applies to all Security Devices
Alarms & Alerts	Required	5.8.4.3.4		Applies to all Security Devices
Audit and Logging	Required	5.8.4.3.5		Applies to all Security Devices
Integrity	Required	5.8.4.3.6		Applies to all Security Devices
Documentation	Required	5.8.4.3.7		Applies to all Security Devices
Cryptography	Required (Note 2)	5.8.4.3.8		Applies to all Security Devices
Security Measures	Required	5.8.4.3.9		Applies to all Security Devices
System and Communication Protection	Required	5.8.4.3.10		Applies to all Security Devices
Other Requirements	Required	5.8.4.3.11		Applies to all Security Devices
Performance	Required	5.8.4.3.12	Applies to all Security Devices	

NOTES:

1. Criticality represents high-level rollup of the CR/FR area. Table 3-1 of Enclosure 3 provides a detailed CR/FR for each security device product (FW, IPS, VPN).
2. Cryptography is optional with the exception that all outgoing communications are encrypted.

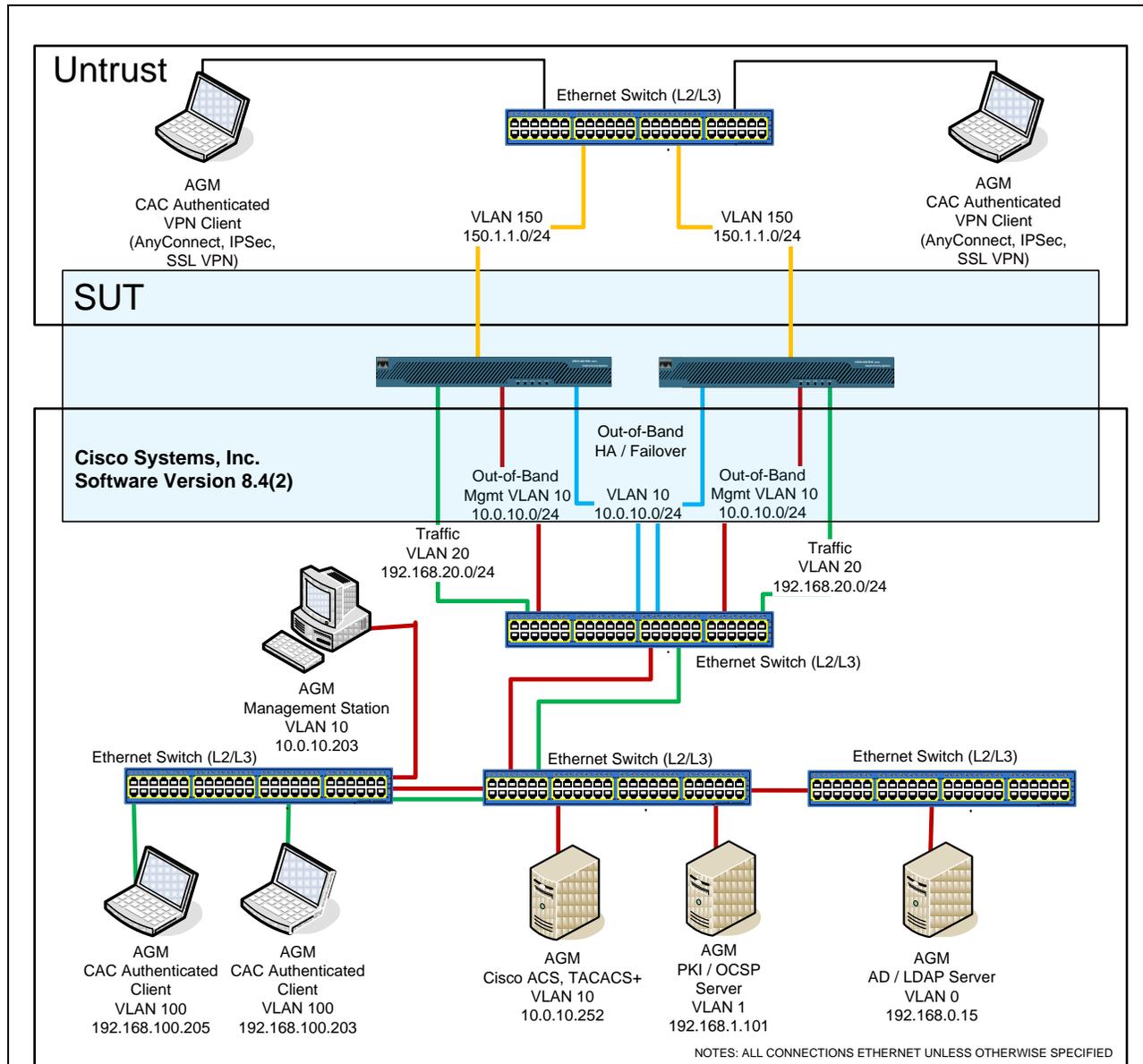
LEGEND:

CR	Capability Requirement	RFC	Request for Comment
FR	Functional Requirement	UCR	Unified Capabilities Requirements
FW	Firewall	VPN	Virtual Private Network
IPS	Intrusion Prevention System		

7.4 Other. None.

8. TEST NETWORK DESCRIPTION. The SUT was tested at USAISEC-TIC in a manner and configuration similar to that of a notional operational environment. Testing of the system's required functions and features was conducted using the test configurations depicted in Figure 2-2.

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



SUT: The Cisco Systems ASA Model Family (5505, 5540, and 5580-20) was evaluated at USAISEC-TIC.

LEGEND:

AD	Active Directory	SSL	Secure Sockets Layer
AGM	Army Golden Master	SUT	System Under Test
ASA	Adaptive Security Appliance	TACACS+	Terminal Access Controller Access Control System Plus
CAC	Common Access Card	TIC	Technology Integration Center
LDAP	Lightweight Directory Access Protocol	USAISEC	U.S. Army Information Systems Engineering Command
HA	High Availability	VLAN	Virtual Local Area Network
IPSec	Internet Protocol Security	VPN	Virtual Private Network
OCSP	Online Certificate Status Protocol		
PKI	Public Key Infrastructure		

Figure 2-2. SUT Test Configuration

9. SYSTEM CONFIGURATIONS. Table 2-4 provides the system configurations and hardware and software components tested with the SUT. The SUT was tested in an operationally realistic environment to determine its interoperability (IO) capability with associated network devices and network traffic.

Table 2-4. Tested System Configurations

System Name	Equipment																										
Required Ancillary Equipment	Active Directory																										
	Public Key Infrastructure (PKI)																										
	Terminal Access Controller Access Control System Plus (TACACS+)																										
	System Log (SysLog) Server																										
System Name	Equipment																										
Cisco Adaptive Security Appliance (ASA) 5585 Series	Hardware	Cards	Software/Firmware																								
	ASA 5585-X SSP-10	N/A	Firmware version 8.4(2) ASDM version 6.4(5)																								
	<u>ASA 5585-X SSP-20</u>																										
	ASA 5585-X SSP-40																										
	ASA 5585-X SSP-60																										
Cisco VPN Client	N/A	N/A	5.0.07.0290																								
Cisco AnyConnect Client	N/A	N/A	3.0.4235																								
<p>NOTE: Components bolded and underlined above were tested by USAISEC-TIC. The other components in the family series were not tested; however, they utilize the same software and hardware. The USAISEC-TIC analysis determined the models to be functionally identical for interoperability certification purposes; therefore, they are certified for joint use</p> <p>LEGEND:</p> <table> <tr> <td>ASA</td> <td>Adaptive Security Appliances</td> <td>TACACS+</td> <td>Terminal Access Controller Access Control System Plus</td> </tr> <tr> <td>ASDM</td> <td>Adaptive Security Device Manager</td> <td>TIC</td> <td>Technology Integration Center</td> </tr> <tr> <td>LDAP</td> <td>Lightweight Directory Access Protocol</td> <td>USAISEC</td> <td>U.S. Army Information Systems Engineering Command</td> </tr> <tr> <td>NA</td> <td>Not Applicable</td> <td>VPN</td> <td>Virtual Private Network</td> </tr> <tr> <td>PKI</td> <td>Public Key Infrastructure</td> <td></td> <td></td> </tr> <tr> <td>SysLog</td> <td>System Log</td> <td></td> <td></td> </tr> </table>				ASA	Adaptive Security Appliances	TACACS+	Terminal Access Controller Access Control System Plus	ASDM	Adaptive Security Device Manager	TIC	Technology Integration Center	LDAP	Lightweight Directory Access Protocol	USAISEC	U.S. Army Information Systems Engineering Command	NA	Not Applicable	VPN	Virtual Private Network	PKI	Public Key Infrastructure			SysLog	System Log		
ASA	Adaptive Security Appliances	TACACS+	Terminal Access Controller Access Control System Plus																								
ASDM	Adaptive Security Device Manager	TIC	Technology Integration Center																								
LDAP	Lightweight Directory Access Protocol	USAISEC	U.S. Army Information Systems Engineering Command																								
NA	Not Applicable	VPN	Virtual Private Network																								
PKI	Public Key Infrastructure																										
SysLog	System Log																										

10. TESTING LIMITATIONS. For IO Test A-16, the vendor claimed performance was not fully tested due to the testing limitation of the traffic generator.

11. INTEROPERABILITY EVALUATION RESULTS. The SUT meets the critical IO requirements for FW/VPN in accordance with Section 5.8 of the UCR and is certified for joint use with other network infrastructure products listed on the Approved Products List (APL). Additional discussion regarding specific testing results is located in subsequent paragraphs.

11.1 Interfaces. The interface status of the SUT is provided in Table 2-5.

Table 2-5. SUT Interface Requirements Status

Interface	Critical (See note 1.)	UCR Reference	Threshold CRs/FRs (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	
NOTES:					
1. UCR did not identify individual interface requirements for security devices. SUT must minimally provide an Ethernet interface (one of the listed).					
2. CRs/FRs are contained in Table 2. CR/FR numbers represent a roll-up of the UCR. Enclosure 3 provides a list of more detailed requirements for security device products.					
3. SUT will meet applicable standards for interface provided.					
4. SUT has eight 10/100/1000Base-T integrated ports.					
5. SUT has two 10GbE ports.					
LEGEND:					
10GbE	10 Gigabit Ethernet		NA	Not Applicable	
CR	Capability Requirement		SUT	System Under Test	
FR	Functional Requirement		UCR	Unified Capabilities Requirements	
FW	Firewall		VPN	Virtual Private Network	

11.2 Capability Requirements and Functional Requirements. The SUT CR and FR status is depicted in Table 2-6. Detailed CRs/FRs are provided in Enclosure 3, Table 3-1.

Table 2-6. 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																																				
<p>NOTES:</p> <ol style="list-style-type: none"> 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). Cryptography is optional with the exception that all outgoing communications are encrypted. IPS functionality only applies to IPS products. Requirements are not applicable to firewalls or VPN concentrators. Cisco provided LoC. This requirement was not tested on this evaluation because of a previous evaluation on similar ASA product that has been placed on the DISA APL (Tracking Number 1002816). The SUT logged critical security events during the evaluation. Cisco has full documentation on their Website on configuration, management, and implementation on the ASA5585. The management and VPN session was secured with FIPS-140-2 approved encryption. This requirement is met by RAE. SUT was able to secure the data traffic with port and protocol filters. SUT performance was not fully tested because of limitation of the traffic generator. <p>LEGEND:</p> <table> <tr> <td>APL</td> <td>Approved Products List</td> <td>IP</td> <td>Internet Protocol</td> </tr> <tr> <td>ASA</td> <td>Adaptive Security Appliance</td> <td>IPS</td> <td>Intrusion Prevention System</td> </tr> <tr> <td>CR</td> <td>Capability Requirement</td> <td>LoC</td> <td>Letter of Compliance</td> </tr> <tr> <td>DISA</td> <td>Defense Information Systems Agency</td> <td>NA</td> <td>Not Applicable</td> </tr> <tr> <td>FIPS</td> <td>Federal Information Processing Standards</td> <td>RAE</td> <td>Required Ancillary Equipment</td> </tr> <tr> <td>FR</td> <td>Functional Requirement</td> <td>SUT</td> <td>System Under Test</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>						APL	Approved Products List	IP	Internet Protocol	ASA	Adaptive Security Appliance	IPS	Intrusion Prevention System	CR	Capability Requirement	LoC	Letter of Compliance	DISA	Defense Information Systems Agency	NA	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	IDS	Intrusion Detection System		
APL	Approved Products List	IP	Internet Protocol																																						
ASA	Adaptive Security Appliance	IPS	Intrusion Prevention System																																						
CR	Capability Requirement	LoC	Letter of Compliance																																						
DISA	Defense Information Systems Agency	NA	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																																						
IDS	Intrusion Detection System																																								

a. Conformance Requirements.

(1) Conformance Standards. The SUT has met the Conformance Requirements described in Section 5.8.4.2 of UCR 2008, Change 2 as applicable to FWs and VPN products. This requirement was met by Cisco's Letter of Compliance (LoC).

b. IA Requirements.

(1) General Requirements. The SUT has met the IA Requirements described in Section 5.8.4.3.1 of UCR 2008, Change 2, as applicable to FWs and VPN products. Some of the requirement was not tested in this evaluation because of a similar ASA5500 family of product already on the Defense Information systems Agency (DISA) APL (TN1002816). The non-tested item was agreed to by Cisco and Joint Interoperability Test Center (JITC).

(2) Configuration Management. The SUT has met the Configuration Management Requirements described in Section 5.8.4.3.1 of UCR 2008, Change 2, as applicable to FWs and VPN products. The configuration requirement was not tested in this evaluation because of a similar ASA5500 family of product already on the DISA APL (TN 1002816). The non-tested item was agreed to by Cisco and JITC.

(3) Alarms and Alerts. The SUT has met the Alarms and Alerts described in Section 5.8.4.3.5 of UCR 2008, Change 2, as applicable to FWs and VPN products. Some of the Alarms and Alerts Requirement was not tested in this evaluation because of a similar ASA5500 family of product already on the DISA APL (TN 1002816). The non-tested item was agreed to by Cisco and JITC.

(4) Audit and Logging. The SUT has met the IA Requirements described in Section 5.8.4.3.5 of UCR 2008, Change 2, as applicable to FWs and VPN products. The SUT has the ability to generate audit and logging data using Required Ancillary Equipment (RAE).

(5) Integrity. The SUT has met the Integrity Requirements described in Section 5.8.4.3.6 of UCR 2008, Change 2 as applicable to FWs and VPN products. The Integrity requirement was not tested in this evaluation because of a similar ASA5500 family of product already on the DISA APL (TN 1002816). The non-tested item was agreed to by Cisco and JITC.

(6) Documentation. The SUT has met the Documentation Requirements described in Section 5.8.4.3.1 of UCR 2008, Change 2, as applicable to FWs and VPN products. The applicable administrator and user guide has been provided by Cisco. The guides contain procedures and guidelines on how to configure the SUT.

(7) Cryptography. The SUT has met the Cryptography Requirements described in Section 5.8.4.3.1 of UCR 2008, Change 2, as applicable to FWs and VPN

products. The SUT uses FIPS-140-2-approved ciphers suite for the IPsec and Transport Layer Security sessions.

(8) Security Measures. The SUT has met the Security Measures Requirements described in Section 5.8.4.3.9 of UCR 2008, Change 2, as applicable to FWs and VPN products. The SUT met the Security Measures Requirement. Enforcement of user access is managed with RAE. The security device enforces internal administrative access based on source address and IP version, and external administrative access is not applicable because of the out-of-band management (OOBM) and fielding guidance. The SUT was able to block potentially malicious fragments.

(9) System and Communication Protection. The SUT has met the System and Communication Protection Requirements described in Section 5.8.4.3.10 of UCR 2008, Change 2, as applicable to FWs and VPN products. The security device can be configured to secure traffic from remote clients with encrypted VPN connections, using FIPS-certified cipher suites. The user authenticate was configured to use CAC.

(10) Other Requirements. The SUT has met the Other Requirements described in Section 5.8.4.3.11 of UCR 2008, Change 2, as applicable to FWs and VPN products. The Other Requirement was not tested in this evaluation because of a similar ASA5500 family of product already on the DISA APL (TN 1002816). The non-tested item was agreed to by the vendor and JITC.

(11) Performance. The SUT has met the Performance Requirements described in Section 5.8.4.3.12 of UCR 2008, Change 2, as applicable to FWs and VPN products. The performance of the SUT was not fully tested due to the limitation of the traffic generator.

c. Functionality.

(1) Policy. The SUT has met the Policy Requirements as described in Section 5.8.4.4.1 of UCR 2008, Change 2, as applicable to FWs and VPN products. Security policies are enforced with RAE.

(2) Filtering. The SUT has met the Policy Requirements as described in Section 5.8.4.4.2 of UCR 2008, Change 2, as applicable to FWs and VPN products. The SUT has abilities to restrict access based on interfaces and service ports.

d. IPS Functionality.

(1) IPS Security Device Requirements. This requirement is not applicable.

11.3 Information Assurance. The IA report is published in a separate report, Reference (f).

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

11.4 Other. None.

12. TEST AND ANALYSIS REPORT. 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 interoperability status information is available via the JITC System 2-7 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 testing is on the Telecom Switched Services Interoperability (TSSI) website at <http://jitc.fhu.disa.mil/tssi>.

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 (UCR). The SUT need not provide conditional requirements. If provided, they must function according to the specified requirements. The detailed Functional Requirement (FRs) and Capability Requirement (CRs) for Security Device products are listed in Table 3-1.

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

ID	Requirement	UCR REF	FW	IPS	VPN
1	The security device shall conform to all of the MUST requirements found in Request for Comment (RFC) 2409, "The Internet Key Exchange (IKE)."	UCR 5.8.4.2-2		R	
2	The security device shall conform to all of the MUST requirements found in RFC 3414, "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMP)."	UCR 5.8.4.2-3	R	R	R
3	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."	UCR 5.8.4.2-4		R	
4	The security device shall conform to all of the MUST requirements found in RFC 3412, "Message Processing and Dispatching for Simple Network Management Protocol."	UCR 5.8.4.2-5	R	R	R
5	The security device shall conform to all of the MUST requirements found in RFC 3413, "Simple Network Management Protocol Applications."	UCR 5.8.4.2-6	R	R	R
6	The security device shall conform to all of the MUST requirements found in RFC 3585, "Internet Protocol (IP) Security (IPSec) Configuration Policy Information Model."	UCR 5.8.4.2-7	R	R	
7	The security device shall conform to all of the MUST requirements found in RFC 3586, "IP Security Policy Requirements."	UCR 5.8.4.2-8	R	R	
8	The security device shall conform to all of the MUST requirements found in RFC 4302, "IP Authentication Header."	UCR 5.8.4.2-9	R	R	R
9	The security device shall conform to all of the MUST requirements found in RFC 4303, "IP Encapsulating Security Payload (ESP)."	UCR 5.8.4.2-10	R	R	R
10	The security device shall conform to all of the MUST requirements found in RFC 4308, "Cryptographic Suites for IPSec."	UCR 5.8.4.2-11	R	R	R
11	The security device shall conform to all of the MUST requirements found in RFC 4309, "Using Advanced Encryption Standard (AES) Configuration Control Manager Mode with IPSec Encapsulating Security Payload (ESP)."	UCR 5.8.4.2-12	R		R
12	The security device shall conform to all of the MUST requirements found in RFC 2473, "Generic Tunneling."	UCR 5.8.4.2-13	R	R	
13	The security device shall conform to all of the MUST requirements found in RFC 4301, "Security Architecture for the Internet Protocol."	UCR 5.8.4.2-14			R
14	The security device shall conform to all of the MUST requirements found in RFC 3948, "User Datagram Protocol (UDP) Encapsulation of IPSec Packets."	UCR 5.8.4.2-15			R
15	The security device shall support SNMPv3 and NTPv4.	UCR 5.8.4.3.1-1	R	R	R
16	The security device shall provide ability to push policy to the VPN Client and the ability to monitor the client's activity.	UCR 5.8.4.3.1-2			R
17	The security device shall be managed from a central place, clients, and servers.	UCR 5.8.4.3.1-3			R
18	The security device shall have three Ethernet ports, one for primary, one for backup, and one for OOBM.	UCR 5.8.4.3.1-4	R		
19	A CM process shall be implemented for hardware and software updates.	UCR 5.8.4.3.3-1	R	R	R
20	The CM system shall provide an automated means by which only authorized	UCR 5.8.4.3.3-2	R	R	R

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

ID	Requirement	UCR REF	FW	IPS	VPN
	changes are made to the security device implementation.				
21	The security device shall disable the Proxy Address Resolution Protocol (ARP) service, unless disabled by default.	UCR 5.8.4.3.3-3	R	R	R
22	The security device shall disable IP redirects notification service, except in type 3 cases.	UCR 5.8.4.3.3-4	R	R	R
23	The security device shall disable the Maintenance Operations Protocol (MOP) service in DEC equipment which use that protocol to perform software loads.	UCR 5.8.4.3.3-5	R	R	R
24	The security device shall disable the service source-routing.	UCR 5.8.4.3.3-6	R		R
25	The security device shall properly implement an ordered list policy procedure.	UCR 5.8.4.3.3-7	R	R	R
26	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.	UCR 5.8.4.3.4-1	R	R	
27	The security device shall have the capability to generate an alarm message to a remote administrator console upon detection of a potential security violation.	UCR 5.8.4.3.4-2	R		R
28	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.	UCR 5.8.4.3.4-3	R	R	R
29	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 (NMS) that will take the appropriate action to include providing notification of the event.	UCR 5.8.4.3.4-4		G	
30	The security device shall have the capability to immediately alert the administrator by displaying a message at the local and remote administrative consoles when an administrative session exists for each of the defined administrative roles.	UCR 5.8.4.3.4-5		G	
31	An automated, continuous, on-line monitoring and audit trail creation capability is deployed with the capability to immediately alert personnel of any suspicious activity contrary to normal expected and recorded baseline operations.	UCR 5.8.4.3.4-6	G	G	G
32	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 automatically disable the system if serious Information Assurance violations are detected.	UCR 5.8.4.3.4-7	R	R	R
33	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.	UCR 5.8.4.3.5-1		R	
34	The security device shall generate an audit record of all failures to reassemble fragmented packets.	UCR 5.8.4.3.5-2		R	
35	The security device shall generate an audit record of all attempted uses of the trusted channel functions.	UCR 5.8.4.3.5-3	R	R	R
36	The security device, when configured, shall log the event of dropping packets and the reason for dropping them.	UCR 5.8.4.3.5-4	R		
37	The security device shall log matches to filter rules that deny access when configured to do so.	UCR 5.8.4.3.5-5	R	R	
38	The security device shall record access or attempted access via security device to all program initiations and shutdowns that have security implications	UCR 5.8.4.3.5-6	R		R
39	The output of such intrusion/attack detection and monitoring tools shall be protected against unauthorized access, modification, or detection.	UCR 5.8.4.3.5-7	R	R	R
40	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.	UCR 5.8.4.3.5-8		R	
41	The security device shall log SMTP traffic that contains source routing symbols (e.g., in the mailer recipient commands).	UCR 5.8.4.3.5-9		R	
42	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.	UCR 5.8.4.3.5-10		R	
43	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	UCR 5.8.4.3.5-11		R	

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

ID	Requirement	UCR REF	FW	IPS	VPN
	successfully authenticated to the security device.				
44	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).	UCR 5.8.4.3.5-12		R	
45	The security device shall log data and audit events when a replay is detected.	UCR 5.8.4.3.5-13		R	R
46	The security device shall be able to collect the following: Identification, Authentication, and Authorization events.	UCR 5.8.4.3.5-14		R	R
47	The security device shall be able to collect the following: Data Accesses.	UCR 5.8.4.3.5-15		R	R
48	The security device shall be able to collect the following: Service Requests.	UCR 5.8.4.3.5-16		R	R
49	The security device shall be able to collect the following: Network traffic.	UCR 5.8.4.3.5-17		R	R
50	The security device shall be able to collect the Security configuration changes.	UCR 5.8.4.3.5-18		R	R
51	The security device shall be able to collect the following: Data introduction.	UCR 5.8.4.3.5-19		R	R
52	The security device shall be able to collect the following: Detected malicious code.	UCR 5.8.4.3.5-20		R	R
53	The security device shall be able to collect the following: Access control configuration.	UCR 5.8.4.3.5-21		R	R
54	The security device shall be able to collect the following: Service configuration.	UCR 5.8.4.3.5-22		R	R
55	The security device shall be able to collect the Authentication configuration.	UCR 5.8.4.3.5-23		R	R
56	The security device shall be able to collect the following: Accountability policy configuration.	UCR 5.8.4.3.5-24		R	R
57	The security device shall be able to collect the following: Detected known vulnerabilities.	UCR 5.8.4.3.5-25		R	R
58	The security device shall provide authorized users with the capability to read the system data.	UCR 5.8.4.3.5-26		R	R
59	The system shall prohibit access to security device data, except those users that have been granted explicit read access.	UCR 5.8.4.3.5-27		R	R
60	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.	UCR 5.8.4.3.7-1	R	R	R
61	The developer shall provide administrator guidance addressed to system administrative personnel (e.g., Administrator's Guide).	UCR 5.8.4.3.7-2	R	R	R
62	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.	UCR 5.8.4.3.7-3	R	R	R
63	The developer shall provide the architectural design of the security device.	UCR 5.8.4.3.7-4	R	R	R
64	The developer shall provide a functional specification of the security device.	UCR 5.8.4.3.7-5	R	R	R
65	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.	UCR 5.8.4.3.7-6	R	R	R
66	The reference document for the security device shall be unique to each version of the security device.	UCR 5.8.4.3.7-7	R	R	R
67	The security device shall be labeled with its reference information (i.e., model and version number).	UCR 5.8.4.3.7-8	R	R	R
68	The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.	UCR 5.8.4.3.7-9	R	R	R
69	The CM system shall provide measures such that only authorized changes are made to the configuration items.	UCR 5.8.4.3.7-10	R	R	R
70	The guidance documentation shall list all assumptions about the intended environment.	UCR 5.8.4.3.7-11	R	R	R
71	The system shall demonstrate a procedure for accepting and acting upon user	UCR 5.8.4.3.7-12	R	R	R

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

ID	Requirement	UCR REF	FW	IPS	VPN
	reports of potential security flaws and requests for corrections to those flaws.				
72	The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the security device.	UCR 5.8.4.3.7-13	R	R	R
73	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.	UCR 5.8.4.3.7-14	R	R	R
74	The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.	UCR 5.8.4.3.7-15	R	R	R
75	The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections, and guidance on corrective actions to security device users.	UCR 5.8.4.3.7-16	R	R	R
76	The procedures for processing reported security flaws shall ensure that any reported flaws are corrected and the correction issued to security device users.	UCR 5.8.4.3.7-17	R	R	R
77	The developer shall perform a vulnerability analysis.	UCR 5.8.4.3.7-18	R	R	R
78	The vulnerability analysis documentation shall describe the disposition of identified vulnerabilities.	UCR 5.8.4.3.7-19	R	R	R
79	The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the security device.	UCR 5.8.4.3.7-20	R	R	R
80	The vulnerability analysis documentation shall justify that the security device, with the identified vulnerabilities, is resistant to obvious penetration attacks.	UCR 5.8.4.3.7-21	R	R	R
81	The installation, generation, and start-up documentation shall describe all the steps necessary for secure installation, generation, and start-up of the security device.	UCR 5.8.4.3.7-22	R	R	R
82	The administrator guidance shall describe recovery procedures and technical system features to assure that system recovery is done in a trusted and secure manner.	UCR 5.8.4.3.7-23	R	R	R
83	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.	UCR 5.8.4.3.8-1			R
84	System mechanisms shall be implemented to enforce automatic expiration of passwords, to prevent password reuse, and to ensure password strength.	UCR 5.8.4.3.9-1	R	R	R
85	Monitoring tools shall be used for the monitoring and detection of suspicious, intrusive, or attack-like behavior patterns to itself.	UCR 5.8.4.3.9-2	R	R	R
86	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.	UCR 5.8.4.3.9-3	R	R	R
87	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.	UCR 5.8.4.3.9-4	R	R	R
88	The security device must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with security device security functions.	UCR 5.8.4.3.9-5	R	R	R
89	The security device shall block unauthorized directed broadcasts from external networks (Distributed Denial of Service defense).	UCR 5.8.4.3.9-6	R		
90	The security device shall verify reverse path unicast addresses (Distributed Denial of Service defense) and be able to drop packets that fail verification.	UCR 5.8.4.3.9-7	R		
91	The security device shall drop all packets with an IPv4 non-routable (RFC 1918) address originating from an external source.	UCR 5.8.4.3.9-8	R	R	R
92	The security device shall drop all packets with an IPv4 source address of all zeros.	UCR 5.8.4.3.9-9	R	R	R
93	The security device shall drop all traffic from the internal network that does not use a legitimate internal address range as its source address.	UCR 5.8.4.3.9-10	R	R	R
94	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).	UCR 5.8.4.3.9-11	R	R	R
95	The security device shall differentiate between authorized and fraudulent	UCR 5.8.4.3.9-12	R	R	

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

ID	Requirement	UCR REF	FW	IPS	VPN
	attempts to upgrade the configuration (i.e., if a user trying to perform an upgrade that is not authorized that role).				
96	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 (NAT).	UCR 5.8.4.3.9-13	R	R	
97	The security device shall properly accept or deny User Datagram Protocol (UDP) traffic from port numbers based on policy.	UCR 5.8.4.3.9-14	R	R	
98	The security device shall properly accept or deny TCP traffic from port numbers based on policy.	UCR 5.8.4.3.9-15	R	R	
99	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.	UCR 5.8.4.3.9-16	R		
100	A security device shall properly enforce TCP state.	UCR 5.8.4.3.9-17	R		
101	A security device shall properly accept and deny traffic based on multiple rules.	UCR 5.8.4.3.9-18	R		
102	A security device shall prevent all known network-based current attack techniques (Common Vulnerabilities and Exploits) from compromising the security device.	UCR 5.8.4.3.9-19	R		
103	A security device shall prevent the currently available Information Assurance Penetration techniques, as defined in DISA STIGS and IAVAs from penetrating the security device.	UCR 5.8.4.3.9-20	R	R	R
104	A security device shall block potentially malicious fragments.	UCR 5.8.4.3.9-21	R	R	R
105	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.	UCR 5.8.4.3.9-22	R	R	
106	Each controlled interface shall be configured to ensure that all (incoming and outgoing) communications protocols, services, and communications not explicitly permitted are prohibited.	UCR 5.8.4.3.10-1	R	R	
107	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 IS.	UCR 5.8.4.3.10-2	R		
108	The security device's controlled interface enforces configurable thresholds to determine whether all network traffic can be handled and controlled.	UCR 5.8.4.3.10-3	R		
109	The security device shall reject 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.	UCR 5.8.4.3.11-1	R	R	R
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 the loopback network.	UCR 5.8.4.3.11-2	R		R
111	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.	UCR 5.8.4.3.11-3	R	R	R
112	<p>The TSF shall permit an information flow between a controlled subject and another controlled subject via a controlled operation if the following rules hold:</p> <p>a. Subjects on an internal network can cause information to flow through the security device to another connected network if:</p> <p>(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;</p> <p>(2) The presumed address of the source subject, in the information, translates to an internal network address;</p> <p>(3) And the presumed address of the destination subject, in the information, translates to an address on the other connected network.</p>	UCR 5.8.4.3.11-4	R		

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

ID	Requirement	UCR REF	FW	IPS	VPN
	<p>b. Subjects on the external network can cause information to flow through the TOE to another connected network if:</p> <p>(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;</p> <p>(2) The presumed address of the source subject, in the information, translates to an external network address;</p> <p>(3) And the presumed address of the destination subject, in the information, translates to an address on the other connected network.</p>				
113	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 either through manual intervention or automatic reboot.	UCR 5.8.4.3.11-5	R	R	R
114	The security device shall detect replay attacks using either security device data or security attributes.	UCR 5.8.4.3.11-6		R	R
115	The security device shall reject data and audit events when a replay is detected.	UCR 5.8.4.3.11-7		R	
116	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.	UCR 5.8.4.3.11-8	R	R	R
117	The security device shall enforce System Administrator policy regarding Instant Messaging traffic.	UCR 5.8.4.3.11-9	R	R	R
118	The security device shall enforce System Administrator policy regarding VVoIP traffic.	UCR 5.8.4.3.11-10	R	R	R
119	Access Control shall include a Discretionary Access Control (DAC) Policy.	UCR 5.8.4.3.11-11	R	R	R
120	Discretionary Access Control access controls shall be capable of including or excluding access to the granularity of a single user.	UCR 5.8.4.3.11-12	R	R	R
121	The security device's controlled interface shall review incoming information for viruses and other malicious code.	UCR 5.8.4.3.11-13	R	R	R
122	The controlled interface shall provide the ability to fully restore its functionality in accordance with documented restoration procedures.	UCR 5.8.4.3.11-14	R	R	R
123	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.	UCR 5.8.4.3.11-15	R	R	R
124	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).	UCR 5.8.4.3.12-1	R	R	R
125	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.	UCR 5.8.4.3.12-2	R	R	R
126	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.	UCR 5.8.4.3.12-3	R	R	R
127	The security device, as configured, must process new secure file transfer protocol (FTP) connections at the rate of the expected maximum number of connections as advertised by the vendor within a 1-minute period.	UCR 5.8.4.3.12-4	R	R	R
128	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.	UCR 5.8.4.3.12-5	R	R	R
129	The security device must not degrade IPv4 and IPv6 forwarding when used with a long Access Policy configuration.	UCR 5.8.4.3.12-6	R		R
130	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.	UCR 5.8.4.3.12-7	R		
131	The security device shall enforce the policy pertaining to any indication of a potential security violation.	UCR 5.8.4.4.1-1	R		R
132	The security device shall be configurable to perform actions based upon different information flow policies.	UCR 5.8.4.4.1-2	R		R

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

ID	Requirement	UCR REF	FW	IPS	VPN
133	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.	UCR 5.8.4.4.1-3	R		R
134	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.	UCR 5.8.4.4.1-4	R		
135	The security device shall enforce the System Administrator's policy pertaining to network traffic violations to a specific TCP port within a specified period.	UCR 5.8.4.4.1-5	R		R
136	The security device shall enforce the System Administrator's policy pertaining to violations of network traffic rules within a specified period.	UCR 5.8.4.4.1-6	R		R
137	The security device shall enforce the System Administrator's policy pertaining to any security device-detected replay of data and/or nested security attributes.	UCR 5.8.4.4.1-7	R		R
138	<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"> 1. Have the ability to block on a per-interface basis. 2. Default to block. 3. Default to disabled, if supported on the security device itself. <p>a. Will apply to the following defined services:</p> <ol style="list-style-type: none"> (1) The service UDP echo (port 7) (2) The service UDP discard (port 9) (3) The service UDP chargen (port 19) (4) The service UDP TCPMUX (port 1) (5) The service UDP daytime (port 13) (6) The service UDP time (port 37) (7) The service UDP supdup (port 95) (8) The service UDP sunrpc (port 111) (9) The service UDP loc-srv (port 135) (10) The service UDP netbios-ns (port 137) (11) The service UDP netbios-dgm (port 138) (12) The service UDP netbios-ssn (port 139) (13) The service UDP BootP (port 67) (14) The service UDP TFTP (port 69) (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) 	UCR 5.8.4.4.2	R		

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

ID	Requirement	UCR REF	FW	IPS	VPN
	(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				
139	The security device shall detect and protect against a focused method of attack: Footprinting and Scanning.	UCR 5.8.4.5-1		R	
140	The security device shall detect and protect against a focused method of attack: Enumeration.	UCR 5.8.4.5-2		R	
141	The security device shall detect and protect against a focused method of attack: Gaining Access.	UCR 5.8.4.5-3		R	
142	The security device shall detect and protect against a focused method of attack: Escalation of Privilege.	UCR 5.8.4.5-4		R	
143	The security device shall detect and protect against a focused method of attack: Maintaining Access.	UCR 5.8.4.5-5		R	
144	The security device shall detect and protect against a focused method of attack: Network Exploitation.	UCR 5.8.4.5-6		R	
145	The security device shall detect and protect against a focused method of attack: Cover Tracks.	UCR 5.8.4.5-7		R	
146	The device shall support the capability to detect and send alarms in responses to threats identified in VVoIP signaling.	UCR 5.8.4.6-1		R	
147	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.	UCR 5.8.4.6-1.a		R	
148	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). 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.	UCR 5.8.4.6-1.b		R	
149	The device shall support the capability to detect when AS-SIP messages exceed a configurable maximum message length.	UCR 5.8.4.6-1.c		R	
150	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.	UCR 5.8.4.6-1.d		R	
151	The device shall support the capability to detect attempts to inject SQL queries into AS-SIP signaling messages.	UCR 5.8.4.6-1.e		R	
152	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).	UCR 5.8.4.6-1.f		R	
153	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).	UCR 5.8.4.6-1.g		R	
154	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.	UCR 5.8.4.6-2		R	
155	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).	UCR 5.8.4.6-2.a		R	

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

ID	Requirement	UCR REF	FW	IPS	VPN
156	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.	UCR 5.8.4.6-2.b		R	
157	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.	UCR 5.8.4.6-2.b.1		R	
158	<p>The device shall support the capability to detect abnormally sized packets in the VVoIP media stream.</p> <p>(a) [Conditional: IPS] 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.</p> <p>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.</p>	UCR 5.8.4.6-2.b.2		R	
159	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.	UCR 5.8.4.6-3		R	

This page intentionally left blank.