



DEFENSE INFORMATION SYSTEMS AGENCY

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

IN REPLY
REFER
TO:

Joint Interoperability Test Command (JITE)

13 May 11

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Special Interoperability Test Certification of the Cisco Adaptive Security Appliance (ASA) 5500 Series Security Device Product with Release 8.3(2)

- References:
- (a) DoD Directive 4630.05, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," 5 May 2004
 - (b) CJCSI 6212.01E, "Interoperability and Supportability of Information Technology and National Security Systems," 15 December 2008
 - (c) through (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 Adaptive Security Appliance (ASA) 5500 Series, Release 8.3(2), hereinafter referred to as the System Under Test (SUT), meets all the critical interoperability requirements for Firewall (FW) and Virtual Private Network (VPN) and is certified for joint use. The Defense Information Systems Agency (DISA) adjudicated all open Test Discrepancy Reports (TDR) to have a minor operational impact. The SUT is a layer-2 device that transports Internet Protocol (IP) version 4 and IP version 6 traffic transparently. 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 DISA via a vendor Plan of Action and Milestones that will address all new critical TDRs within 120 days of identification. Testing was conducted using security device requirements derived from the Unified Capabilities Requirements (UCR), Reference (c), and security device test procedures, Reference (d). No other configurations, features, or functions, except those cited within this memorandum, are certified by JITC or authorized by the Program Management Office for use. This certification expires upon changes that affect interoperability, but no later than three years from the date of this memorandum.
3. This finding is based on interoperability testing conducted by the United States Army Information Systems Engineering Command Technology Integration Center (USA ISEC TIC), a DoD Component Test Lab, review of the vendor's Letters of Compliance (LoC), and the DISA Field Security Operations (FSO) Certifying Authority (CA) approval of the IA configuration. Interoperability testing was conducted by the USA ISEC TIC from 6 September 2010 through 8 November 2010. Review of the vendor's LoC was completed on 1 April 2011. The DISA FSO CA granted certification based on the security testing completed by USA ISEC TIC IA test teams that is published in a separate report, Reference (e). The DISA FSO CA has reviewed the IA Assessment Report for the SUT, Reference (e), and based on the findings in the report granted a positive certification letter dated 4 April 2011. The acquiring agency or site will be responsible for the DoD Information Assurance Certification and Accreditation Process (DIACAP) accreditation. The JITC reviewed the DoD Component Test Lab results, enclosure 2,

JITC Memo, JTE, Special Interoperability Test Certification of the Cisco Adaptive Security Appliance (ASA) 5500 Series Security Device Product, Release 8.3(2)

and certifies the Cisco Adaptive Security Appliance (ASA) 5500 Series, Release 8.3(2) as meeting the UCR for Firewall and VPN. Enclosure 2 documents the test results and describes the tested network and system configurations. Enclosure 3, System Functional and Capability Requirements, lists the Capability Requirements (CR) and Functional Requirements (FR).

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

Table 1. SUT Interface Interoperability Status

| Interface | Critical (See note 1.) | UCR Ref | Threshold CR/FR Requirements (See note 2.) | Status | Remarks (See note 3.) | | | | | | | | | | |
|--|--|------------------------|--|--------|--|--------------------------------|------------------------|--------------------------------|----------------------------|------------------------|--|---------------------------|----------------------------------|------------|--------------|
| FW | | | | | | | | | | | | | | | |
| 10Base-X | N | 5.3.2.4 / 5.3.3.10.1.2 | 1-4 | Met | 802.3i and 802.3j | | | | | | | | | | |
| 100Base-X | N | 5.3.2.4 / 5.3.3.10.1.2 | 1-4 | Met | 802.3u | | | | | | | | | | |
| 1000Base-X | N | 5.3.2.4 / 5.3.3.10.1.2 | 1-4 | Met | 802.3z | | | | | | | | | | |
| 10GBase-X | N | 5.3.2.4 / 5.3.3.10.1.2 | 1-4 | Met | 802.3ae, 802.3ak, 802.3an, 802.3aq, and 802.3av; 5580-20 device only | | | | | | | | | | |
| 40GBase-X | N | 5.3.2.4 / 5.3.3.10.1.2 | 1-4 | N/A | 802.3ba | | | | | | | | | | |
| 100GBase-X | N | 5.3.2.4 / 5.3.3.10.1.2 | 1-4 | N/A | 802.3ba | | | | | | | | | | |
| VPN | | | | | | | | | | | | | | | |
| 10Base-X | N | 5.3.2.4 / 5.3.3.10.1.2 | 1-4 | Met | 802.3i and 802.3j | | | | | | | | | | |
| 100Base-X | N | 5.3.2.4 / 5.3.3.10.1.2 | 1-4 | Met | 802.3u | | | | | | | | | | |
| 1000Base-X | N | 5.3.2.4 / 5.3.3.10.1.2 | 1-4 | Met | 802.3z | | | | | | | | | | |
| 10GBase-X | N | 5.3.2.4 / 5.3.3.10.1.2 | 1-4 | Met | 802.3ae, 802.3ak, 802.3an, 802.3aq, and 802.3av; 5580-20 device only | | | | | | | | | | |
| 40GBase-X | N | 5.3.2.4 / 5.3.3.10.1.2 | 1-4 | N/A | 802.3ba | | | | | | | | | | |
| 100GBase-X | N | 5.3.2.4 / 5.3.3.10.1.2 | 1-4 | N/A | 802.3ba | | | | | | | | | | |
| <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. CR/FR requirements are contained in Table 2. CR/FR numbers represent a roll-up of UCR requirements. Enclosure 3 provides a list of more detailed requirements for security device products.</p> <p>3. SUT will meet applicable standards for interface provided.</p> <p>LEGEND:</p> <table style="width: 100%; border: none;"> <tr> <td style="width: 50%;">CR Capability Requirement</td> <td style="width: 50%;">NA Not Applicable</td> </tr> <tr> <td>FR Functional Requirement</td> <td>SUT System Under Test</td> </tr> <tr> <td>ID Identification</td> <td>UCR Unified capabilities Requirements</td> </tr> <tr> <td>LAN Local Area Network</td> <td>VPN Virtual Private Network</td> </tr> <tr> <td>N No</td> <td>Y Yes</td> </tr> </table> | | | | | | CR Capability Requirement | NA Not Applicable | FR Functional Requirement | SUT System Under Test | ID Identification | UCR Unified capabilities Requirements | LAN Local Area Network | VPN Virtual Private Network | N No | Y Yes |
| CR Capability Requirement | NA Not Applicable | | | | | | | | | | | | | | |
| FR Functional Requirement | SUT System Under Test | | | | | | | | | | | | | | |
| ID Identification | UCR Unified capabilities Requirements | | | | | | | | | | | | | | |
| LAN Local Area Network | VPN Virtual Private Network | | | | | | | | | | | | | | |
| N No | Y Yes | | | | | | | | | | | | | | |

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 | Required | 5.8.4.2 | Partially Met | See note 4 |
| 2 | Information Assurance Requirements | Required | 5.8.4.3 | | |
| | General Requirements | Required | 5.8.4.3.1 | Met | See note 5 |
| | Authentication | Required | 5.8.4.3.2 | Met | See note 6. |
| | Configuration Management | Required | 5.8.4.3.3 | Met | |
| | Alarms & Alerts | Required | 5.8.4.3.4 | Met | See note 4 & 6. |
| | Audit and Logging | Required | 5.8.4.3.5 | Met | See note 7. |
| | Integrity | Required | 5.8.4.3.6 | Met | See note 8. |
| | Documentation | Required | 5.8.4.3.7 | Met | See note 9. |
| | Cryptography | Required (Note 2) | 5.8.4.3.8 | Met | |
| | Security Measures | Required | 5.8.4.3.9 | Met | See note 10. |
| | System and Communication Protection | Required | 5.8.4.3.10 | Met | |
| | Other Requirements | Required | 5.8.4.3.11 | Met | |
| Performance | Required | 5.8.4.3.12 | Met | See note 11. | |
| 3 | Functionality | Required | 5.8.4.4 | Met | See note 12. |
| | Policy | Required | 5.8.4.4.1 | Met | FW & VPN Only |
| | Filtering | Required | 5.8.4.4.2 | Met | FW Only |

NOTES:

- 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.
- Vendor provided letter of compliance.
- ASA5505 supports stateless failover.
- Currently the Army is using Windows 2003 servers, but during migration to Windows 2008 the interoperability between Cisco TACACS+ and Windows 2008 should be considered.
- The required function was met with RAE.
- The procedure to prevent the introduction of malicious code into the system is a site responsibility.
- Administrator and user guides are available for download from vendor site.
- Under system stress, no unauthorized data was released from the SUT.
- SUT was able to perform vendor claimed rates.
- SUT provided functions to limit the number of transport-layer connections.

LEGEND:

| | | | |
|----|-------------------|-----|-----------------------------|
| FW | Firewall | IPS | Intrusion Prevention System |
| IP | Internet Protocol | VPN | Virtual Private Network |

5. No detailed test report was developed, in accordance with the Program Manager's request. JITC distributes interoperability 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 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 DSN testing is on the Telecom Switched Services Interoperability (TSSI)

JITC Memo, JTE, Special Interoperability Test Certification of the Cisco Adaptive Security Appliance (ASA) 5500 Series Security Device Product, Release 8.3(2)

website at <http://jitc.fhu.disa.mil/tssi>. All associated data is available on the Defense Information Systems Agency Unified Capability Coordination Office (UCCO) website located at <https://aplits.disa.mil>.

6. The testing point of contact is Mr. James Hatch, USARMY TIC commercial 520-533-2860 or DSN 821-2860; e-mail address is James.Hatch@us.army.mil. The JITC certification point of contact is Mr. Kevin Holmes, commercial ((301) 744-2763 or DSN 354-2763; e-mail address is kevin.holmes@disa.mil. The JITC's mailing address is P.O. Box 12798, Fort Huachuca, AZ 85670-1298. The Unified Capabilities Connection Office tracking numbers are Cisco ASA 5500 FW: 1002816 and Cisco ASA 5500 VPN: 1002817

FOR THE COMMANDER:



3 Enclosures a/s

for BRADLEY A CLARK

Chief

Battlespace Communications Portfolio

JITC Memo, JTE, Special Interoperability Test Certification of the Cisco Adaptive Security Appliance (ASA) 5500 Series Security Device Product, Release 8.3(2)

Distribution (electronic mail):

United States Army Information Systems Engineering Command (USAISEC), Technology Integration Center (TIC)

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 MARCORSYSCOM, 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

ADDITIONAL REFERENCES

- (c) Office of the Assistant Secretary of Defense, "Department of Defense Unified Capabilities Requirements 2008, Change 1," 22 January 2010
- (d) Department of Defense Instruction 8100.03, "Department of Defense (DoD) Voice Networks", January 16, 2004
- (d) Joint Interoperability Test Command, "Security Device Test Plan," October 2011
- (e) United States Army Technology Integration Center Cisco ASA5500 version 8.3(2) FW IA Findings December 2011
- (f) United States Army Technology Integration Center Cisco ASA5500 version 8.3(2) VPN IA Findings December 2011
- (g) Defense Information Systems Agency Field Security Operations Unified, Capabilities (UC) Approved Products List (APL) Recommendation for Cisco Systems, Inc. Adaptive Security Appliance (ASA) 5500-Series Firewall Appliances (TN# 1002816/CA# 11D-APL-03-200-U) Interoffice Memorandum, 4 April 2011
- (h) Defense Information Systems Agency Field Security Operations, Unified Capabilities (UC) Approved Products List (APL) Recommendation for Cisco Systems, Inc. Adaptive Security Appliance (ASA) 5500-Series Virtual Private Network (VPN) Appliances (TN# 1002817/CA# 11D-APL-03-199-U) Interoffice Memorandum, 4 April 2011

This page intentionally left blank.

CERTIFICATION TESTING SUMMARY

1. SYSTEM TITLE. Cisco Adaptive Security Appliance 5500 Series, Release 8.3(2)

2. SPONSOR. Department of Army

3. SYSTEM POC. Mr. Jordan Silk, United States Army Information Systems Engineering Command (USAISEC), Technology Integration Center (TIC), Building 53302, Fort Huachuca, Arizona (AZ) 85613; email: Jordan.Silk@us.army.mil

4. TESTER. Testing conducted at Department of Army Distributed Testing Lab, United States Army Information Systems Engineering Command, Technology Integration Center (USAISEC TIC), ATTN: James Hatch, Fort Huachuca, Arizona 85613; email: 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: Firewalls (FW), Intrusion Detection Systems (IDS)/Intrusion Prevention Systems (IPS), and Virtual Private Network (VPN) components (concentrator and termination). The Cisco Adaptive Security Appliance (ASA) 5500 Series Release 8.3(2) hereinafter referred to as the System under Test (SUT), was tested for FW and VPN capabilities.

There are many security technologies that a network administrator can use to prevent unauthorized access into private networks or computer systems. Cisco has implemented many of these security technologies into its ASA 5500 product line. The Cisco ASA is designed as a multipurpose network perimeter security device. The Cisco ASA has integrated the following functionalities into a single unit: firewall, intrusion detection and prevention, and VPN. Again, only the FW and VPN capabilities were tested under this evaluation,

The Cisco ASA5505 is the smallest of the three Cisco ASAs tested. It has the basic functionalities of the larger Cisco ASAs and is designed to support small offices and remote users. It features an eight-port 10/100 Megabits per second (Mbps) Fast Ethernet (FE) switch with ports 6 and 7 supporting Power over Ethernet (PoE). The ASA5505 has a maximum throughput of 150 Mbps and supports stateless failover. The basic license supports up to two Secure Sockets Layer (SSL) VPN users, and the upgraded license supports up to 25 SSL VPN users.

The Cisco ASA5540 is the mid-range model of the Cisco ASAs. It is designed to support medium-size enterprise and service provider networks. It has a maximum throughput of 650Mbps and supports stateful failover with active/active (A/A) and active/standby (A/S) modes. It is a one rack unit (1RU) device with four Gigabit Ethernet (GbE) ports and one dedicated FE port for out-of-band management (OOBM).

The Cisco ASA5580-20 is the high-end model of the Cisco ASAs. It is designed to support large data centers with very demanding data networks. It can support up to 5 Gbps of real-world HyperText Transfer Protocol (HTTP) traffic and 90,000 connections per second. It also supports A/A and A/S failover. The ASA5580-20 has two GbE management interfaces, four GbE, and two 10-GbE SR LC. There are expansion slots for up to 24 GbE fiber interfaces.

To configure the Cisco ASA, the functions on the device can be accessed using the command-line interface (CLI). The Cisco ASA can also be configured using a graphical interface called the Cisco Adaptive Security Device Manager (ASDM). One feature of the ASDM is the configuration wizard, with which Internet Protocol Security (IPSec) VPN, SSL VPN, High Availability, and Packet Capture can be configured.

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

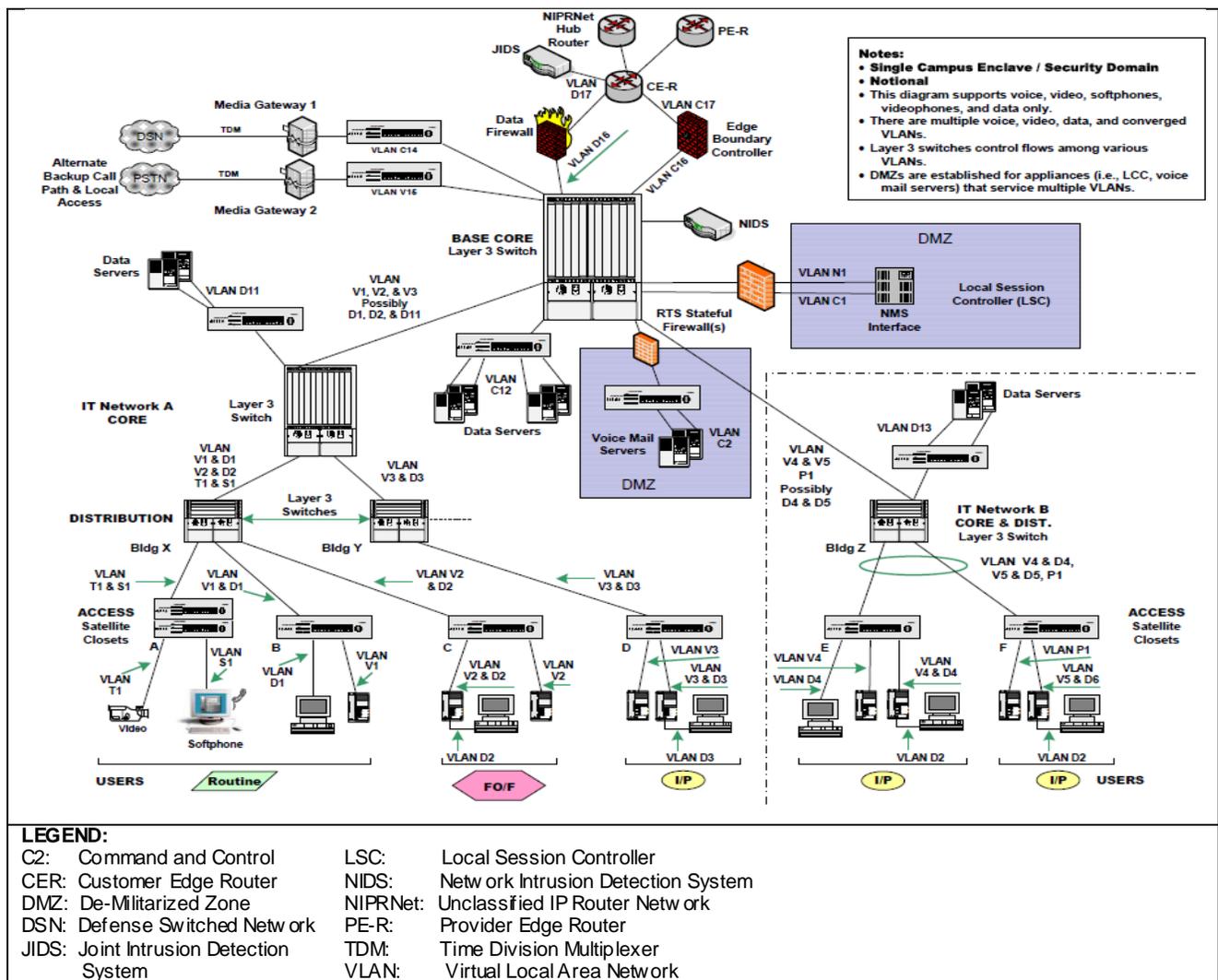


Figure 2-1. Security Device Architecture

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

7.1 Interfaces. The SUT uses the external interfaces to connect to the GIG network. Table 2-1 lists the physical interfaces supported by the SUT. The table documents the physical interfaces and their associated standards.

Table 2-1. Security Device Interface Requirements

| ID | Interface | Critical (Note 1) | UCR Ref. | Threshold CR/FRs (Note 2) | Criteria | Remarks |
|----------------|------------|-------------------|------------------------|---------------------------|---|---------|
| FW | | | | | | |
| FW1 | 10Base-X | N | 5.3.2.4 / 5.3.3.10.1.2 | 1-4 | 802.3i and 802.3j | |
| FW2 | 100Base-X | N | 5.3.2.4 / 5.3.3.10.1.2 | 1-4 | 802.3u | |
| FW3 | 1000Base-X | N | 5.3.2.4 / 5.3.3.10.1.2 | 1-4 | 802.3z | |
| FW4 | 10GBase-X | N | 5.3.2.4 / 5.3.3.10.1.2 | 1-4 | 802.3ae, 802.3ak, 802.3an, 802.3aq, and 802.3av | |
| FW5 | 40GBase-X | N | 5.3.2.4 / 5.3.3.10.1.2 | 1-4 | 802.3ba | |
| FW6 | 100GBase-X | N | 5.3.2.4 / 5.3.3.10.1.2 | 1-4 | 802.3ba | |
| FW7 | Serial | N | 5.3.2.4 / 5.3.3.10.1.2 | 1-4 | EIA/TIA-232 | |
| FR/CR | NA | Y | Note 3 | 1-4 | | |
| IPS/IDS | | | | | | |
| FW1 | 10Base-X | N | 5.3.2.4 / 5.3.3.10.1.2 | 1-4 | 802.3i and 802.3j | |
| FW2 | 100Base-X | N | 5.3.2.4 / 5.3.3.10.1.2 | 1-4 | 802.3u | |
| FW3 | 1000Base-X | N | 5.3.2.4 / 5.3.3.10.1.2 | 1-4 | 802.3z | |
| FW4 | 10GBase-X | N | 5.3.2.4 / 5.3.3.10.1.2 | 1-4 | 802.3ae, 802.3ak, 802.3an, 802.3aq, and 802.3av | |
| FW5 | 40GBase-X | N | 5.3.2.4 / 5.3.3.10.1.2 | 1-4 | 802.3ba | |
| FW6 | 100GBase-X | N | 5.3.2.4 / 5.3.3.10.1.2 | 1-4 | 802.3ba | |
| FW7 | Serial | N | 5.3.2.4 / 5.3.3.10.1.2 | 1-4 | EIA/TIA-232 | |
| FR/CR | NA | Y | Note 3 | 1-4 | | |

Table 2-1. Security Device Interface Requirements (continued)

| ID | Interface | Critical (Note 1) | UCR Ref | Threshold CR/FRs (Note 2) | Criteria | Remarks | | | | | | | | | | | | | | | | | | | | |
|---|------------------------|-------------------|-----------------------------------|---------------------------|--|-------------|----|------------------------|----|----------------|----|------------------------|-----|-------------------|----|----------------|-----|-----------------------------------|-----|--------------------|---|-----|---|----|--|--|
| VPN Concentrator | | | | | | | | | | | | | | | | | | | | | | | | | | |
| FW1 | 10Base-X | N | 5.3.2.4 / 5.3.3.10.1.2 | 1-4 | 802.3i and 802.3j | | | | | | | | | | | | | | | | | | | | | |
| FW2 | 100Base-X | N | 5.3.2.4 / 5.3.3.10.1.2 | 1-4 | 802.3u | | | | | | | | | | | | | | | | | | | | | |
| FW3 | 1000Base-X | N | 5.3.2.4 / 5.3.3.10.1.2 | 1-4 | 802.3z | | | | | | | | | | | | | | | | | | | | | |
| FW4 | 10GBase-X | N | 5.3.2.4 / 5.3.3.10.1.2 | 1-4 | 802.3ae, 802.3ak, 802.3an,802.3aq, and 802.3av | | | | | | | | | | | | | | | | | | | | | |
| FW5 | 40GBase-X | N | 5.3.2.4 / 5.3.3.10.1.2 | 1-4 | 802.3ba | | | | | | | | | | | | | | | | | | | | | |
| FW6 | 100GBase-X | N | 5.3.2.4 / 5.3.3.10.1.2 | 1-4 | 802.3ba | | | | | | | | | | | | | | | | | | | | | |
| FW7 | Serial | N | 5.3.2.4 / 5.3.3.10.1.2 | 1-4 | EIA/TIA-232 | EIA/TIA-512 | | | | | | | | | | | | | | | | | | | | |
| FR/CR | NA | Y | Note 3 | 1-4 | See Table 2-2 | | | | | | | | | | | | | | | | | | | | | |
| <p>NOTES:</p> <ol style="list-style-type: none"> The UCR does not identify individual interface requirements for security devices. The SUT must minimally provide an Ethernet interface (one of those listed). The CR/FR requirements are contained in Table 2-2. The CR/FR numbers represent a roll-up of UCR requirements. Enclosure 3 provides a list of more detailed requirements for security device products. The SUT will meet the 802.3 standard for the interface provided. <p>LEGEND:</p> <table> <tr> <td>CR</td> <td>Capability Requirement</td> <td>NA</td> <td>Not Applicable</td> </tr> <tr> <td>FR</td> <td>Functional Requirement</td> <td>SUT</td> <td>System Under Test</td> </tr> <tr> <td>ID</td> <td>Identification</td> <td>UCR</td> <td>Unified capabilities Requirements</td> </tr> <tr> <td>LAN</td> <td>Local Area Network</td> <td>Y</td> <td>Yes</td> </tr> <tr> <td>N</td> <td>No</td> <td></td> <td></td> </tr> </table> | | | | | | | CR | Capability Requirement | NA | Not Applicable | FR | Functional Requirement | SUT | System Under Test | ID | Identification | UCR | Unified capabilities Requirements | LAN | Local Area Network | Y | Yes | N | No | | |
| CR | Capability Requirement | NA | Not Applicable | | | | | | | | | | | | | | | | | | | | | | | |
| FR | Functional Requirement | SUT | System Under Test | | | | | | | | | | | | | | | | | | | | | | | |
| ID | Identification | UCR | Unified capabilities Requirements | | | | | | | | | | | | | | | | | | | | | | | |
| LAN | Local Area Network | Y | Yes | | | | | | | | | | | | | | | | | | | | | | | |
| N | No | | | | | | | | | | | | | | | | | | | | | | | | | |

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

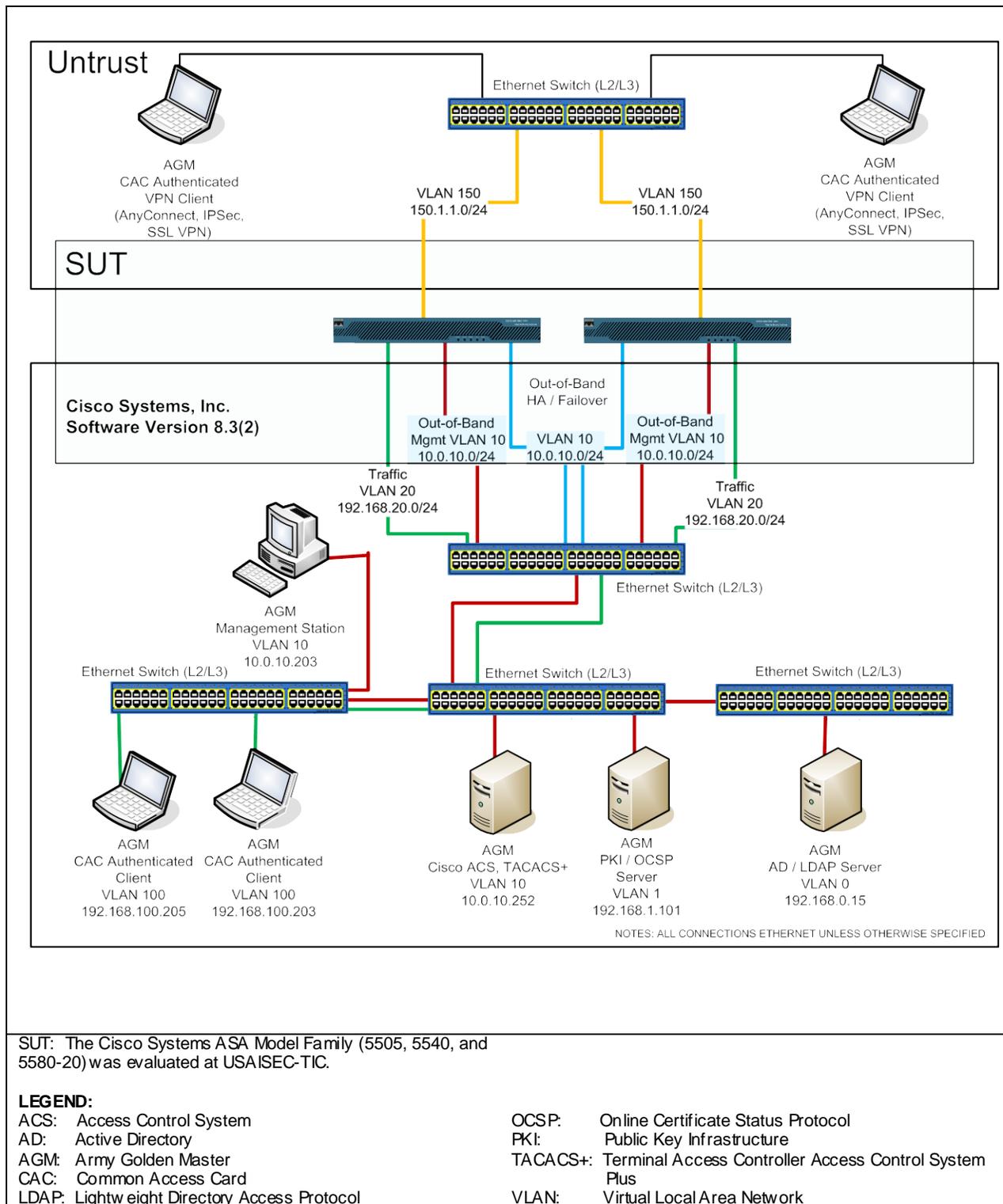


Figure 2-2. SUT Test Configuration 1

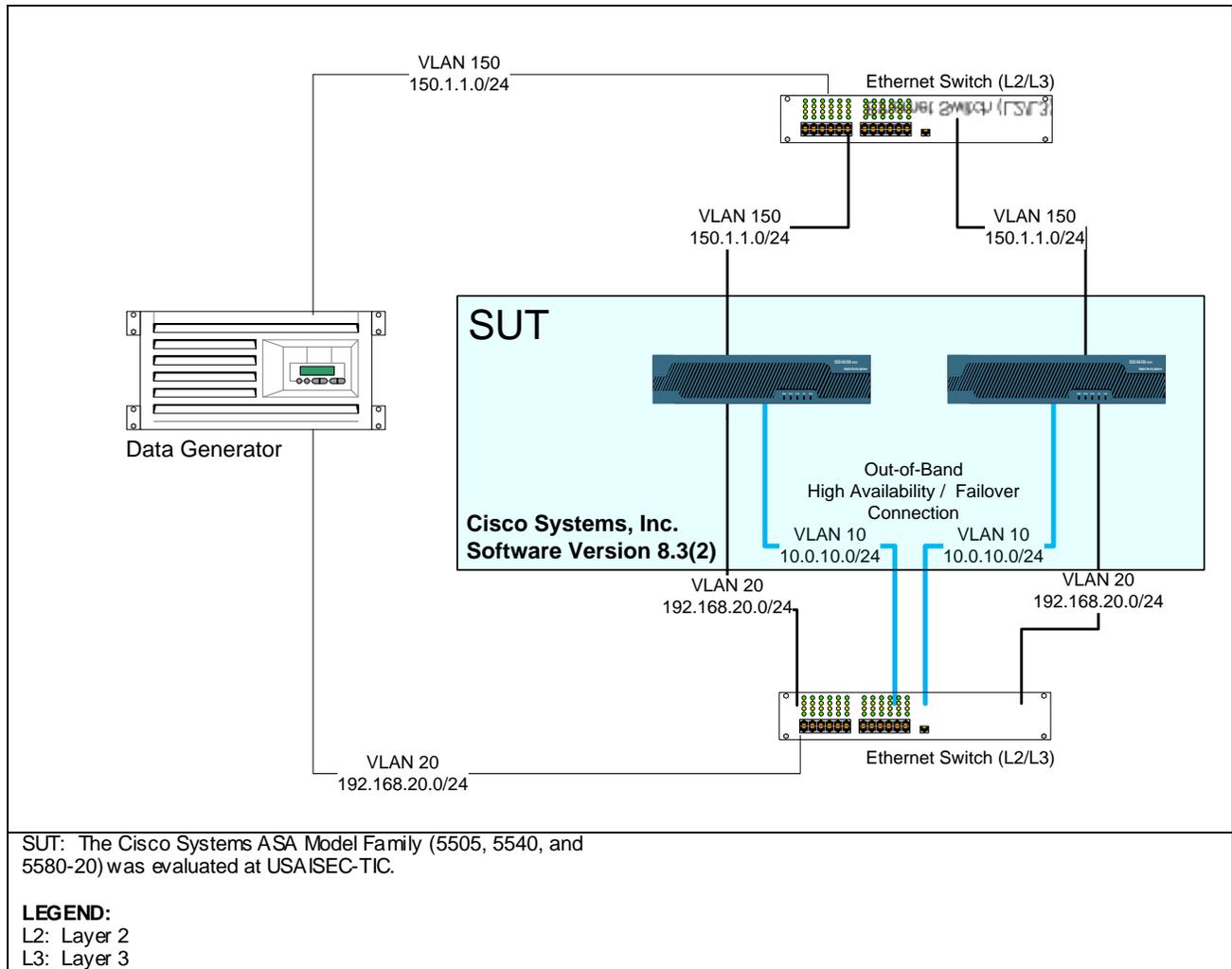


Figure 2-3. SUT Test Configuration 2

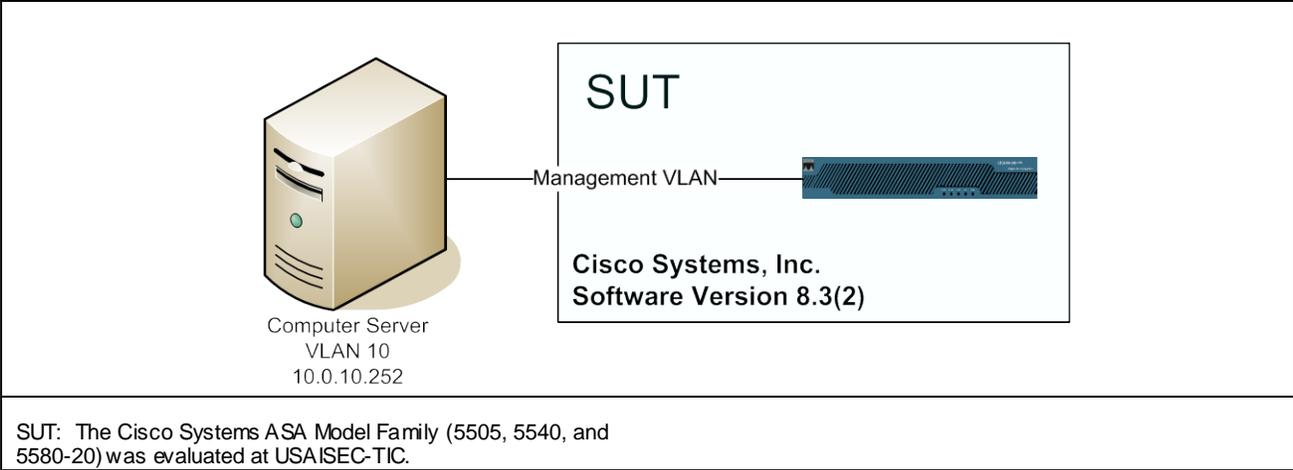


Figure 2-4. SUT Test Configuration 3

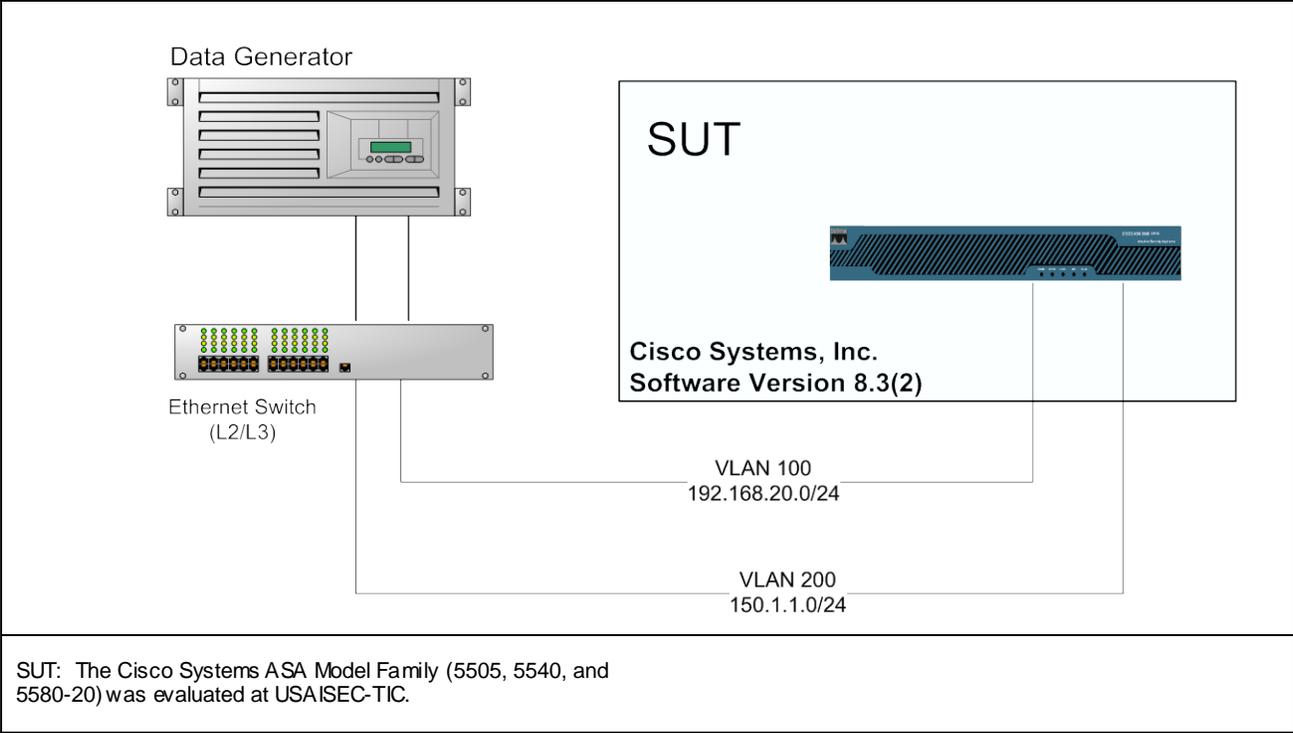


Figure 2-5. SUT Test Configuration 4

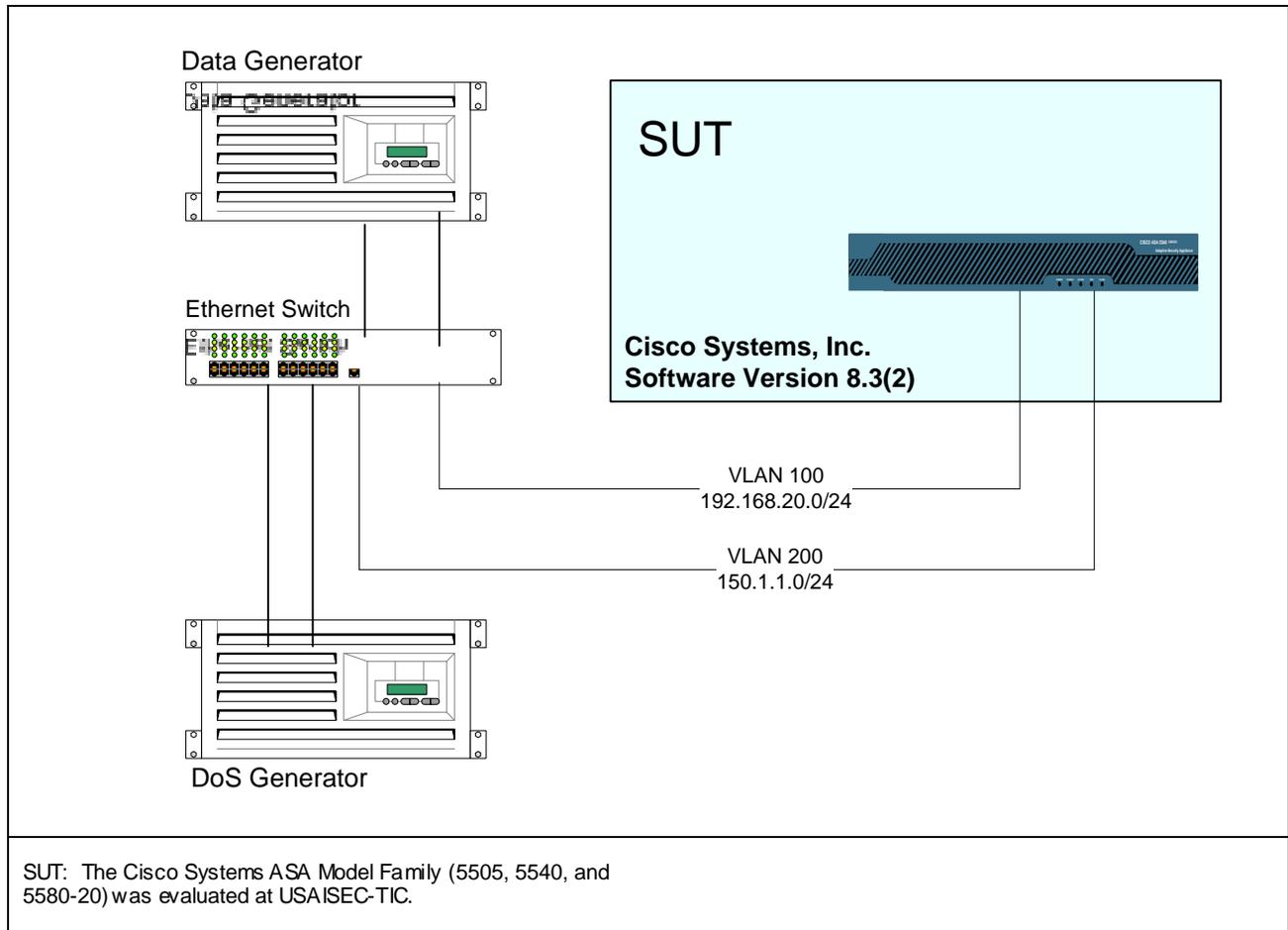


Figure 2-6. SUT Test Configuration 5

9. SYSTEM CONFIGURATIONS. Table 2-3 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 capability with associated network devices and network traffic.

Table 2-3. Tested System Configurations

| System Name | Equipment |
|------------------------------------|---|
| Required Ancillary Equipment (RAE) | Active Directory (LDAP) |
| | Public Key Infrastructure (PKI) |
| | System Log (SysLog) Server |
| | Terminal Access Controller Access Control System Plus (TACACS+) |

Table 2-3. Tested System Configurations (continued)

| System Name | Equipment | | |
|---|--|-------|--|
| | Hardware | Cards | Software/Firmware |
| Cisco Adaptive Security Appliance (ASA) 5500 Series | <u>ASA 5505</u> | N/A | Firmware version 8.3(2) ASDM version 6.3(3) |
| | ASA 5510 ASA 5520 <u>ASA 5540</u> | N/A | Firmware version 8.3(2) ASDM version 6.3(3) |
| | <u>ASA 5580-20</u> ASA 5580-40 | N/A | Firmware version 8.3(2) ASDM version 6.3(3) |

NOTE: Components bolded and underlined were tested by USAISEC-TIC. The other components in the family's series were not tested; however, they utilize the same software and hardware, and USAISEC-TIC analysis determined them to be functionally identical for interoperability certification purposes. They are also certified for joint use.

LEGEND:
ASA Adaptive Security Appliance
ASDM Adaptive Security Device Manager

10. TESTING LIMITATIONS. The ability to scale up a Denial of Service (DoS) attack to cause a system failure on an enterprise system is difficult. The UCR calls for a verification during which the SUT will not leak information when the system performance is degraded or during a system failure. Stressing of the system was limited by the testing generator's ability to maintain a high level of concurrent connections to cause a significant impact on the SUT's system resources.

11. INTEROPERABILITY EVALUATION RESULTS. The SUT meets the critical interoperability requirements for FW and VPN IAW Section 5.8 of the UCR, and it is certified for joint use with other network Infrastructure Products listed on the Approved Products List (APL). Additional discussion regarding specific testing results is provided in subsequent paragraphs.

11.1 Interfaces. The interface status of the SUT is provided in Table 2-4.

Table 2-4. SUT Interface Requirements Status

| ID | Interface | Critical (Note 1) | UCR Ref. | Threshold CR/FR Requirements (Note 2) | Status | Remarks |
|------------|------------|-------------------|---------------------------|---------------------------------------|--------|---|
| FW | | | | | | |
| FW1 | 10Base-X | N | 5.3.2.4 / 5.3.3.10.1.2 | 1-4 | Met | 802.3i and 802.3j |
| FW2 | 100Base-X | N | 5.3.2.4 / 5.3.3.10.1.2 | 1-4 | Met | 802.3u |
| FW3 | 1000Base-X | N | 5.3.2.4 / 5.3.3.10.1.2 | 1-4 | Met | 802.3z |
| FW4 | 10GBase-X | N | 5.3.2.4 / 5.3.3.10.1.2 | 1-4 | Met | 802.3ae, 802.3ak, 802.3an,802.3aq, and 802.3av 5580-20 device only |
| FW5 | 40GBase-X | N | 5.3.2.4 / 5.3.3.10.1.2 | 1-4 | N/A | 802.3ba |
| FW6 | 100GBase-X | N | 5.3.2.4 / 5.3.3.10.1.2 | 1-4 | N/A | 802.3ba |
| FR/CR | NA | Y | Note 3 | | N/A | |
| VPN | | | | | | |
| FW1 | 10Base-X | N | 5.3.2.4 / 5.3.3.10.1.2 | 1-4 | Met | 802.3i and 802.3j |
| FW2 | 100Base-X | N | 5.3.2.4 / 5.3.3.10.1.2 | 1-4 | Met | 802.3u |
| FW3 | 1000Base-X | N | 5.3.2.4 / 5.3.3.10.1.2 | 1-4 | Met | 802.3z |
| FW4 | 10GBase-X | N | 5.3.2.4 / 5.3.3.10.1.2 | 1-4 | Met | 802.3ae, 802.3ak, 802.3an,802.3aq, and 802.3av 5580-20 device only |
| FW5 | 40GBase-X | N | 5.3.2.4 / 5.3.3.10.1.2 | 1-4 | N/A | 802.3ba |
| FW6 | 100GBase-X | N | 5.3.2.4 / 5.3.3.10.1.2 | 1-4 | N/A | 802.3ba |
| FR/CR | NA | Y | Note 3 | | N/A | |

NOTES:

1. "Required definition" means "conditionally required." The SUT need not provide wireless capabilities; however, if such capabilities are provided, all threshold CR/FR requirements must be met.
2. Detailed CR/FR requirements are listed in Enclosure 3.
3. These CR/FRs are not specific to any of the interfaces, but the SUT must demonstrate them to be certified.
4. UCR references for each CR/FR are listed in Enclosure 3.

LEGEND:

| | | | |
|-----|--------------------------------|-----|---|
| CR | Capability Requirement | TIA | Telecommunications Industry Association |
| EIA | Electronic Industries Alliance | UCR | Unified Capabilities Requirements |
| FR | Functional Requirement | Y | Yes |
| FW | Firewall | | |
| ID | Identification | | |
| N | No | | |
| N/A | Not Applicable | | |

11.2 Capability Requirements (CR) and Functional Requirements (FR). The SUT's CR/FR status is depicted in Table 2-5. Detailed CR/FR requirements are provided in Enclosure 3, Table 3-1.

Table 2-5. SUT Capability Requirements and Functional Requirements Status

| CR/FR ID | Capability/ Function | Applicability (Note 1) | UCR Reference | Status | Remarks |
|----------|-------------------------------------|------------------------|---------------|--------|-----------------|
| 1 | Conformance Requirements | Required | 5.8.4.2 | Met | See note 4 |
| 2 | Information Assurance Requirements | Required | 5.8.4.3 | | |
| | General Requirements | Required | 5.8.4.3.1 | Met | See note 5 |
| | Authentication | Required | 5.8.4.3.2 | Met | See note 6. |
| | Configuration Management | Required | 5.8.4.3.3 | Met | |
| | Alarms & Alerts | Required | 5.8.4.3.4 | Met | See note 4 & 6. |
| | Audit and Logging | Required | 5.8.4.3.5 | Met | See note 7. |
| | Integrity | Required | 5.8.4.3.6 | Met | See note 8. |
| | Documentation | Required | 5.8.4.3.7 | Met | See note 9. |
| | Cryptography | Required (Note 2) | 5.8.4.3.8 | Met | |
| | Security Measures | Required | 5.8.4.3.9 | Met | See note 10. |
| | System and Communication Protection | Required | 5.8.4.3.10 | Met | |
| | Other Requirements | Required | 5.8.4.3.11 | Met | |
| | Performance | Required | 5.8.4.3.12 | Met | See note 11. |
| 3 | Functionality | Required | 5.8.4.4 | Met | See note 12. |
| | Policy | Required | 5.8.4.4.1 | Met | FW & VPN Only |
| | Filtering | Required | 5.8.4.4.2 | Met | FW Only |
| 4 | IPS Functionality | Required (Note 3) | 5.8.4.5 | N/A | IDS/IPS Only |

NOTES:

- 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/IDS products. Requirements are not applicable to firewalls or VPN concentrators.
- Vendor provided letter of compliance.
- ASA5505 supports stateless failover.
- Currently the Army is using Windows 2003 servers, but during migration to Windows 2008 the interoperability between Cisco TACACS+ and Windows 2008 should be considered.
- The required function was met with RAE.
- The procedure to prevent the introduction of malicious code into the system is a site responsibility.
- Administrator and user guides are available for download from vendor site.
- Under system stress, no unauthorized data was released from the SUT.
- SUT was able to perform vendor claimed rates.
- SUT provided functions to limit the number of transport-layer connections.

LEGEND:

| | | | |
|-----|----------------------------|-----|-----------------------------|
| FW | Firewall | IPS | Intrusion Prevention System |
| IP | Internet Protocol | VPN | Virtual Private Network |
| IDS | Intrusion Detection System | | |

a. Conformance Requirements.

This requirement is met by the vendor's Letter of Compliance (LoC).

b. Information Assurance Requirements.

1) General Requirements.

The SUT has met all general requirements. Test Configuration 1 (Figure 2-2) and Test Configuration 3 (Figure 2-4) were used to verify the requirements.

For the failover capability, both the ASA5580 and ASA5540 support stateful and stateless failover. Both are able to maintain a state table and share this state table with the standby firewall. The ASA5505 supports failover but does not maintain a state table.

The SUT supports Simple Network Management Protocol version 3 (SNMPv3) and Network Translation Protocol version 4 (NTPv4). The SNMPv3 functionality was verified using the SilverCreek SNMP Test Suite. The SUT supports OOBM. The ASA5580 and ASA5540 have dedicated ports for OOBM, and the ASA 5505 uses VLAN.

2) Authentication.

The SUT has met all Authentication requirements using Required Auxiliary Equipment (RAE). Test Configuration 1 (Figure 2-2) was used to verify this requirement. The SUT can be securely managed, either locally or remotely, using RAE. The SUT was tested using Cisco TACACS+ integrated into Windows 2003 Active Directory to authenticate users.

3) Configuration Management.

The Configuration Management (CM) requirement has been met. The vendor was able to provide documentation on configuration management that is related to the SUT.

4) Alarms & Alerts. 5.8.4.3.4

The SUT has met the Alarms & Alerts requirement with RAE. Test Configuration 1 (Figure 2-2) was used to verify this requirement. The SUT uses an external SysLog server to store all audit events and generate alerts. The alarm functionality was dependent on the external syslog server. In addition to using the SysLog server, the SUT was able to provide a live running update of security events on the ASDM.

5) Audit and Logging. 5.8.4.3.5

The SUT has met the Audit and Logging requirements. Test Configuration 1 (Figure 2-2) was used to verify this requirement. The SUT has the ability to generate audit and logging using RAE. This requirement was verified using the Cisco TACACS+ and Windows 2003 server. The SUT supports the following Authentication, Authorization, and Accounting (AAA) protocols and servers: Remote Authentication Dial-in User Server (RADIUS), TACACS+, Rivest-Shamir-Adleman (RSA) SecurID, Windows NT, Kerberos, and the Lightweight Directory Access Protocol (LDAP).

6) Integrity. 5.8.4.3.6

The SUT has met the integrity requirement. Test Configuration 1 (Figure 2-2) was used to verify this requirement. The SUT was able to perform authentication of Internet Protocol Version 6 (IPv6) Next Header values by accepting or denying the generated traffic coming in on the entrusted interface to maintain the integrity of the transmitted data. The vendor site also has security policy to support notifications and updates to system vulnerabilities.

7) Documentation.

The Documentation requirement has been met. All system documentation, administrator and user guides are available for download from the developer's site.

8) Cryptography.

The SUT has met the Cryptography requirement. Test Configuration 1 (Figure 2-2) was used to verify this requirement. The SUT supports the following VPN types: Clientless SSL VPN, remote access, and LAN-to-LAN.

9) Security Measures.

The SUT has met the Security Measures requirements. Test Configuration 5 (Figure 2-6) was used to verify this requirement. The SUT was successful in detecting DoS types of attacks to its outside interface. When configured with the appropriate filters, the SUT was able to deny DoS types of packets from entering the outside interface.

The interfaces on the SUT are configured to fail close as was verified with a sync flood attack in the evaluation procedure. Even though the SUT's functionalities were impacted, no unauthorized data was released in or out of the system.

10) System and Communication Protection.

The SUT has met the System and Communication Protection requirements. Test Configuration 6 (Figure 2-6) was used to verify these requirements. The SUT was able to protect all entrusted interfaces from unauthorized data traffic.

To verify that the SUT, when under operational failure or degradation, will not release data to the outside interface, the Mu8000 was used to send a sync flood attack to the SUT to create degradation to the system. At the same time, IxLoad was used to send traffic from inside the SUT to the outside interface. A deny rule was created on the SUT to block the IxLoad from sending traffic to the outside interface. If IxLoad was not able to send traffic to the outside interface during the syn flood attack, the SUT has met this requirement.

While the sync flood attack was conducted on the Cisco ASAs, the system availability was impacted. During this time of system degradation, no traffic from the IxLoad was detected on the outside interface, thus verifying that no unauthorized data was leaked to the outside.

11) Performance.

The SUT has met the Performance requirements. Test Configuration 4 (Figure 2-5) was used to verify the bandwidth requirements. IxLoad was used to generate the HTTP traffic to verify the throughput performance of the SUT.

Test Configuration 6 (Figure 2-6) was used to verify that under a DoS attack, the SUT can function within operational requirements. Mu8000 was used to generate the DoS attack; IxLoad was used to create normal traffic.

c. Functionality.

1) Policy.

The SUT has met the Policy requirements. The SUT has the functionality to support the quota of Transmission Control Protocol (TCP) connections. Test Configuration 1 (Figure 2-2) was used to verify this requirement. This functionality is implemented in under Service Policies for the management of network traffic. The SUT blocks replay of data as a default policy.

2) Filtering.

The SUT has met the Filtering requirements. Test Configuration 1 (Figure 2-2) was used to verify this requirement. The SUT supports filtering with Access Control Lists (ACLs). There is a standard set of ACLs and an extended ACL that includes protocols and services that can be selected using the ACL Manager interface. The ACL Manager interface can specify either on the inbound or outbound interface and the type of routing or routed protocols and services.

d. IPS Functionality. Not tested.

11.3 Information Assurance. The IA report is published separately; reference (e).

11.4 Other. None.

12. TEST AND ANALYSIS REPORT. In accordance with the Program Manager's request, no detailed test report was developed.. The JITC distributes interoperability 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 DSN 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. The System under Test need not provide conditional requirements. If such requirements are provided, the product(s) must function according to the specified requirements. The detailed Functional Requirements and Capability Requirements for wireless 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 DoD IPv6 Profile shall be used for IPv6 requirements for security devices unless otherwise stated, either within this section or in UCR 2008, Section 5.3.5, IPv6 Requirements. | 5.8.4.2 (1) | R | R | R |
| 2 | The security device shall conform to all of the MUST requirements found in RFC 2409, "The Internet Key Exchange (IKE)." | 5.8.4.2 (2) | R | | |
| 3 | The security device shall conform to all of the MUST requirements found in RFC 3414, "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol." | 5.8.4.2 (4) | R | R | 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." | 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." | 5.8.4.2 (6) | R | R | R |
| 6 | The security device shall conform to all of the MUST requirements found in RFC 3585, "IPSec Configuration Policy Information Model." | 5.8.4.2 (7) | R | | |
| 7 | The security device shall conform to all of the MUST requirements found in RFC 3586, "IP Security Policy Requirements." | 5.8.4.2 (8) | R | | |
| 8 | The security device shall conform to all of the MUST requirements found in RFC 4302, "IP Authentication Header." | 5.8.4.2 (9) | R | | |
| 9 | The security device shall conform to all of the MUST requirements found in RFC 4303, "IP Encapsulating Security Payload (ESP)." | 5.8.4.2 (10) | R | | |
| 10 | The security device shall conform to all of the MUST requirements found in RFC 4305, "Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)." | 5.8.4.2 (11) | R | | |
| 11 | The security device shall conform to all of the MUST requirements found in RFC 4306, "Internet Key Exchange (IKEv2) Protocol." | 5.8.4.2 (12) | R | | |
| 12 | The security device shall conform to all of the MUST requirements found in RFC 4307, "Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)." | 5.8.4.2 (13) | R | | |
| 13 | The security device shall conform to all of the MUST requirements found in RFC 4308, "Cryptographic Suites for IPSec." | 5.8.4.2 (14) | R | | |
| 14 | The security device shall conform to all of the MUST requirements found in RFC 4309, "Using Advanced Encryption Standard (AES) CCM Mode with IPSec Encapsulating Security Payload (ESP)." | 5.8.4.2 (15) | R | | |
| 15 | The security device shall conform to all of the MUST requirements found in RFC 2473, "Generic Tunneling." | 5.8.4.2 (16) | R | | |
| 16 | The security device shall conform to all of the MUST requirements found in RFC 4301, "Security Architecture for the Internet Protocol." | 5.8.4.2 (17) | R | | |

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

| ID | Requirement | UCR Ref. | FW | IPS | VPN |
|-----------|--|-----------------|-----------|------------|------------|
| 17 | The security device shall conform to all of the MUST requirements found in RFC 3948, "UDP Encapsulation of IPSec Packets." | 5.8.4.2 (18) | R | | |
| 18 | The security device shall conform to all of the MUST requirements found in RFC 3947, "Negotiation of NAT-Traversal in the IKE." | 5.8.4.2 (19) | R | | |
| 19 | All Information Assurance and Information Assurance-enabled IT products shall be capable of being configured in accordance with all applicable DoD-approved security configuration guidelines (i.e., STIGs). | 5.8.4.3.1 (1) | R | R | R |
| 20 | The developer shall provide a statement about the source country for each software module/capability within the device. | 5.8.4.3.1 (2) | R | R | R |
| 21 | Security devices shall be Common Criteria Evaluated Assurance Level 4 (EAL4)-certified or scheduled to be certified in accordance with the current approved protection profile. | 5.8.4.3.1 (3) | R | R | R |
| 22 | Security devices shall only have applications or routines that are necessary to support their specific function. NOTE: The disabling or deletion of applications or routines via hardware or software mechanisms shall satisfy this requirement. For example, if an appliance by default is installed with a web browser, and the web browser is not needed to support the security device function, then the application shall be removed from the appliance. Another example is if a feature is part of the application but is not needed in the DoD environment, that feature shall be disabled via hardware or software mechanisms. | 5.8.4.3.1 (4) | R | R | R |
| 23 | Software patches shall only be installed if they originate from the system manufacturer and are applied in accordance with manufacturer's guidance. | 5.8.4.3.1 (5) | R | R | R |
| 24 | The system shall only accept automatic software updates if they are cryptographically signed by the software vendor. NOTE: It is assumed that manual updates will be validated by an authorized administrator before installation. | 5.8.4.3.1 (5.a) | R | R | R |
| 25 | If the system uses public domain software, unsupported software, or other software, it shall be covered under that system's warranty. NOTE: If a vendor covers in its warranty all software, regardless of its source, within its product, then this requirement is met. An example of unsupported software is Windows™ NT, which is no longer supported by Microsoft®; it is unlikely that a vendor would support this operating system as part of its system. | 5.8.4.3.1 (6) | C | C | C |
| 26 | The systems shall only use open source software if all licensing requirements are met. NOTE: Open source software refers to software that is copyrighted and distributed under a license that provides everyone the right to use, modify, and redistribute the source code of the software. Open source licenses impose certain obligations on users who exercise these rights. Some examples include publishing a copyright notice and placing a disclaimer of warranty on distributed copies. | 5.8.4.3.1 (6.a) | R | R | R |
| 27 | The system shall only use mobile code technologies (e.g., JavaScript, VBScript, and ActiveX) in accordance with the current DoD Mobile Code Policy. | 5.8.4.3.1 (7) | R | R | R |
| 28 | The system shall be capable of being located in physically secure areas. | 5.8.4.3.1 (8) | R | R | R |
| 29 | The system shall be capable of enabling password protection of BIOS settings if they are configurable. | 5.8.4.3.1 (9) | C | C | C |
| 30 | The system shall be capable of disabling the ability to boot from a removable media. | 5.8.4.3.1 (10) | R | R | R |
| 31 | The system shall be capable of using a static IP address. | 5.8.4.3.1(11) | R | R | R |
| 32 | Backup procedures to allow the restoration of operational capabilities with minimal loss of service or data shall require restoration of any security-relevant segment of the system state (e.g., ACLs, cryptologic keys, or deleted system status) without requiring destruction of other system data. | 5.8.4.3.1 (12) | R | R | R |
| 33 | The security device shall support SNMPv3 and NTPv4. | 5.8.4.3.1 (13) | R | R | |
| 34 | The security device shall provide a true Out-of-Band-Management (OOBM) interface that will not forward to or receive from any of the routed interfaces. | 5.8.4.3.1 (14) | O | O | |

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

| ID | Requirement | UCR Ref. | FW | IPS | VPN |
|-----------|---|-------------------|-----------|------------|------------|
| 35 | Hot standard failover capability using a proven reliability protocol. | 5.8.4.3.1 (15) | R | | R |
| 36 | The ability to push policy to the VPN Client and the ability to monitor the client's activity. | 5.8.4.3.1 (16) | | | R |
| 37 | The security device shall be managed from a central place, clients, and servers. | 5.8.4.3.1 (17) | | | R |
| 38 | The security device shall implement NTP to ensure times are synchronized. | 5.8.4.3.1 (18) | R | R | R |
| 39 | The security device shall have three Ethernet ports: one for primary, one for backup, and one for OOBM. | 5.8.4.3.1 (19) | R | | |
| 40 | The security device shall associate users with roles. | 5.8.4.3.2.1 (1) | R | R | R |
| 41 | The security device shall employ Role-Based Access Control (RBAC) in the local and remote administration of all device functions and operations.) | 5.8.4.3.2.1 (1.a) | | | |
| 42 | The security device shall associate all user security attributes with an authorized user. | 5.8.4.3.2.1 (1.b) | R | R | R |
| 43 | The security device shall allow and maintain the following list of security attributes for an authorized user: (1) User identifier(s). (2) Roles (e.g., System Administrator). (3) Any security attributes related to a user identifier (e.g., certificate associate). | 5.8.4.3.2.1 (1.c) | R | R | R |
| 44 | The security device shall immediately enforce: (1) Revocation of a user's role. (2) Revocation of a user's authority to use an authenticated proxy. (3) Changes to the information flow policy rule set when applied. (4) Disabling of service available to unauthenticated users. | 5.8.4.3.2.1 (1.d) | R | R | R |
| 45 | The security device shall ensure all administrators can review the audit trail associated with their role. | 5.8.4.3.2.1 (1.e) | R | R | R |
| 46 | The security device shall ensure all roles can perform their administrative roles on the security device locally. | 5.8.4.3.2.1 (1.f) | R | R | R |
| 47 | The security device shall ensure all roles can perform their administrative roles on the security device remotely. | 5.8.4.3.2.1 (1.g) | R | R | R |
| 48 | The ability to perform the following functions shall be restricted to an Administrator-defined or predefined (i.e., default) access control user role: to modify cryptographic security data and/or the time/date method used for forming time stamps. | 5.8.4.3.2.1 (2) | R | R | R |
| 49 | The ability to perform the following functions shall be restricted to the System Administrator role: (1) Modify security functions. (2) Enable/disable security alarm functions. (3) Enable and/or disable Internet Control Message Protocol (ICMP) (in an IP-based network), or other appropriate network connectivity tool (for a non-IP-based network). (4) Reserved. (5) Determine the administrator-specified period of time for any policy. (6) Set the time/date used for timestamps. (7) Query, modify, delete, and/or create the information flow policy rule set. (8) Specify the limits on transport-layer connections. (9) Revoke security attributes associated with the users, information flow policy rule set, and services available to unauthenticated users within the security device. | 5.8.4.3.2.1 (2.a) | R | R | R |
| 50 | The ability to enable, disable, determine, and/or modify the functions of the Security Audit or the Security Audit Analysis shall be restricted to the AAdmin role. | 5.8.4.3.2.1 (2.b) | R | R | R |
| 51 | The ability to perform the following functions shall be restricted to the CAdmin role: (1) Enable and/or disable the cryptographic functions. (2) Modify security functions. (3) Modify the cryptographic security data. (4) Enable/disable security alarm functions. | 5.8.4.3.2.1 (2.c) | R | R | R |

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

| ID | Requirement | UCR Ref. | FW | IPS | VPN |
|-----------|---|------------------|-----------|------------|------------|
| 52 | The security device shall restrict the ability to determine the administrator-specified network identifier. | 5.8.4.3.2.1 (3) | R | R | R |
| 53 | The security device shall require user identification and authentication via one of the following specified methods before enabling user access to itself or any device under its control: a. Local access authentication mechanism. b. Remote access, two-factor authentication mechanism implementing the DoD Public Key Infrastructure (PKI) authentication (defined in detail in Section 5.4, Information Assurance Requirements), either internal to security device or via an external AAA service such as RADIUS or TACACS+. | 5.8.4.3.2.2 (2) | R | R | R |
| 54 | The security device shall provide a local authentication mechanism to perform user authentication. | 5.8.4.3.2.2 (3) | R | R | R |
| 55 | The security device shall only allow authorized security personnel to configure alert mechanisms. | 5.8.4.3.2.2 (5) | R | R | R |
| 56 | An Identification and Authentication (I&A) management mechanism shall be employed that ensures a unique identifier for each user and that associates that identifier with all auditable actions taken by the user. | 5.8.4.3.2.2 (6) | R | R | R |
| 57 | DoD IS access shall be gained through the presentation of an individual identifier and password. | 5.8.4.3.2.2 (7) | R | R | R |
| 58 | The security device shall be capable of setting and enforcing password syntax in accordance with current DoDDs as defined in the latest JTF-GNO Communications Tasking Order 07-015. | 5.8.4.3.2.2 (8) | R | R | R |
| 59 | The security device shall be able to use at least one external authentication method (e.g., RADIUS, TACACS+, and/or LDAP). | 5.8.4.3.2.2 (9) | R | R | R |
| 60 | Identification and Authentication management mechanisms shall include, in the case of communication between two or more systems (e.g., client server architecture), bi-directional authentication between the two systems. | 5.8.4.3.2.2 (11) | R | R | R |
| 61 | Prior to establishing a user authentication session, a security device shall display the latest approved DoD consent warning message to include verbiage that system usage may be monitored, recorded, and subject to audit.. | 5.8.4.3.2.2 (12) | R | R | R |
| 62 | Enforcement of session controls shall include system actions on unsuccessful log-ons (e.g., blacklisting of the terminal or user identifier). | 5.8.4.3.2.2 (13) | R | R | R |
| 63 | If a security device permits remote administration of its controlled interfaces, then the session must be protected through the use of strong encryption, AES 128 at a minimum. | 5.8.4.3.2.2 (14) | R | R | R |
| 64 | In those instances where the users are remotely accessing the system, the users shall employ a strong authentication mechanism (i.e., an I&A technique that is resistant to replay attacks). | 5.8.4.3.2.2 (15) | R | R | R |
| 65 | Successive log-on attempts shall be controlled using one or more of the following: a. Access is denied after multiple unsuccessful logon attempts. b. The number of access attempts in a given period is limited. c. A time-delay control system is employed. | 5.8.4.3.2.2 (16) | R | R | R |
| 66 | The security device shall require the user to re-authenticate before unlocking the session after activation of a screen saver or other away-from-console event. | 5.8.4.3.2.2 (19) | | R | R |
| 67 | A CM process shall be implemented for hardware and software updates. | 5.8.4.3.3 (1) | R | R | R |
| 68 | The CM system shall provide an automated means by which only authorized changes are made to the security device implementation. | 5.8.4.3.3 (2) | R | R | R |
| 69 | The security device shall disable the Proxy Address Resolution Protocol (ARP) service, unless disabled by default. | 5.8.4.3.3 (3) | R | R | R |
| 70 | The security device shall have the capability to disable the ICMP destination unreachable notification on external interfaces. | 5.8.4.3.3 (4) | R | R | R |
| 71 | The security device shall disable IP redirection capability. | 5.8.4.3.3 (5) | R | R | R |
| 72 | The security device shall disable the Maintenance Operations Protocol (MOP) service in DEC equipment which uses that protocol to perform software loads. | 5.8.4.3.3 (6) | O | O | O |

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

| ID | Requirement | UCR Ref. | FW | IPS | VPN |
|----|--|----------------|----|-----|-----|
| 73 | The security device shall be capable of shutting down any unused interfaces as determined by the administrator. | 5.8.4.3.3 (7) | R | R | R |
| 74 | The security device shall disable the service source-routing. | 5.8.4.3.3 (8) | R | | R |
| 75 | The security device shall properly implement an ordered list policy procedure. | 5.8.4.3.3 (9) | R | R | R |
| 76 | The controlled interface shall enforce configurable thresholds to determine whether all network traffic can be handled and controlled. If a processing threshold or a failure limit has been met then the controlled interface will not continue to process transactions. These thresholds can be set to detect and defend against Denial of Service attacks such as SMURF or SYN Flood. | 5.8.4.3.3 (10) | R | R | |
| 77 | The system administration shall employ security management mechanisms for the management of the controlled interface. This includes configuration and start/stop processing of the controlled interface. For controlled interfaces, the System Administrator may be the same as the System Administrator. | 5.8.4.3.3 (11) | R | R | |
| 78 | The security device shall apply a set of rules in monitoring events and, based on these rules, indicate a potential violation of the security device security policy. | 5.8.4.3.4 (1) | R | R | |
| 79 | Security devices with local consoles shall have the capability to generate and display an alarm message at the local console upon detection of a potential security violation. | 5.8.4.3.4 (2) | O | O | O |
| 80 | The security device shall have the capability to generate an alarm message to a remote administrator console upon detection of a potential security violation. | 5.8.4.3.4 (3) | R | R | R |
| 81 | The security device shall have the capability to generate an alarm message to a new remote administrator's console session if the original alarm has not been acknowledged following a potential security violation. | 5.8.4.3.4 (4) | R | R | R |
| 82 | 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. | 5.8.4.3.4 (5) | | R | |
| 83 | 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. | 5.8.4.3.4 (6) | | R | |
| 84 | The security device shall have the capability to provide proper notification of the audit trail exceeding a set percentage of the device storage capacity. | 5.8.4.3.4 (7) | | R | |
| 85 | The security device shall have the capability to provide a means to notify the administrator of any critical operational events (e.g., near full audit logs) within 30 seconds. | 5.8.4.3.4 (8) | R | R | R |
| 86 | 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. | 5.8.4.3.4 (9) | | R | |
| 87 | 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. | 5.8.4.3.4 (10) | | R | |
| 88 | The security device shall have the capability to configure the timing of alarms and their escalation based upon type and severity of event. | 5.8.4.3.4 (11) | R | R | R |
| 89 | The security device shall generate an audit record of all potential security violations that are detected, complete with the identity (source and destination address) of the potential security violation, time/date, and other identifying data. | 5.8.4.3.5 (1) | R | R | R |
| 90 | The security device shall generate an audit record of each start-up and shutdown of the audit function. | 5.8.4.3.5 (2) | R | R | R |
| 91 | The security device shall generate an audit record of all modifications to the audit configuration that occur while the audit collection functions are operating, to include enabling and disabling of any of the audit analysis mechanisms. | 5.8.4.3.5 (3) | R | R | R |
| 92 | The security device shall generate an audit record of any modification to the audit trail. | 5.8.4.3.5 (4) | R | R | R |

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

| ID | Requirement | UCR Ref. | FW | IPS | VPN |
|-----------|--|-----------------|-----------|------------|------------|
| 93 | The security device shall generate an audit record of any unsuccessful attempts to read information from the audit records. | 5.8.4.3.5 (5) | R | R | R |
| 94 | The security device shall generate an alarm or warning message upon detection of audit activity failures. | 5.8.4.3.5 (6) | R | R | R |
| 95 | The security device shall generate an audit record of all actions taken due to exceeding the audit threshold. | 5.8.4.3.5 (7) | R | R | R |
| 96 | The security device shall generate an alarm or warning message upon detection of an audit storage failure. | 5.8.4.3.5 (8) | R | R | R |
| 97 | The security device shall provide minimum recorded security-relevant events, including any activity caught by the "deny all" rule at the end of the security device rule base. | 5.8.4.3.5 (9) | R | R | |
| 98 | The security device shall provide a means to store audit records to a dedicated server on the internal network. | 5.8.4.3.5 (10) | R | R | R |
| 99 | The security device shall generate an audit record of all failures of cryptographic operations. | 5.8.4.3.5 (12) | R | R | R |
| 100 | The security device shall generate an audit record of all failures to reassemble fragmented packets. | 5.8.4.3.5 (13) | | R | |
| 101 | The security device shall generate an audit record of exceeding the threshold of unsuccessful authentication attempts, the actions taken (e.g., disabling of an account), and the restoration to the normal state. | 5.8.4.3.5 (14) | R | R | R |
| 102 | The security device shall generate an audit record of all use of authentication and user identification mechanisms. | 5.8.4.3.5 (15) | R | R | R |
| 103 | The security device shall generate an audit record of attempts to bind user security attributes to a subject. | 5.8.4.3.5 (16) | R | R | |
| 104 | The security device shall generate an audit record of all modifications to the security functions of the security device. | 5.8.4.3.5 (17) | R | R | R |
| 105 | The security device shall generate an audit record of all enabling or disabling of the key generation self-tests. | 5.8.4.3.5 (18) | R | R | R |
| 106 | The security device shall generate an audit record of all modifications of the values of the security device data by the administrator. | 5.8.4.3.5 (19) | R | R | R |
| 107 | The security device shall generate an audit record of all Administrator actions and/or privileged activities. | 5.8.4.3.5 (20) | R | R | R |
| 108 | The security device shall generate an audit record of all attempted uses of the trusted channel functions. | 5.8.4.3.5 (32) | R | R | R |
| 109 | The security device shall provide the administrator with the capability to read all audit data from the audit record. | 5.8.4.3.5 (33) | R | R | R |
| 110 | The security device shall prohibit all users' read access to the audit records in the audit trail, except an administrator. | 5.8.4.3.5 (34) | R | R | R |
| 111 | The security device, when configured, shall log the event of dropping packets and the reason for dropping them. | 5.8.4.3.5 (35) | R | | |
| 112 | The security device shall log changes to the configuration. | 5.8.4.3.5 (36) | R | R | R |
| 113 | The security device shall log matches to filter rules that deny access when configured to do so. | 5.8.4.3.5 (37) | R | R | |
| 114 | The security device shall log hardware changes since the last maintenance cycle when configured to do so. | 5.8.4.3.5 (38) | R | R | R |
| 115 | The security device shall log new physical connections made to the security device. | 5.8.4.3.5 (39) | R | R | R |
| 116 | The security device shall prevent modifications to the audit records in the audit trail. | 5.8.4.3.5 (40) | R | R | R |
| 117 | The security device shall record access or attempted access via security device to all program initiations and shutdowns that have security implications. | 5.8.4.3.5 (41) | R | | R |
| 118 | Audit records shall include connection attempts to the security device. | 5.8.4.3.5 (42) | R | R | R |

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

| ID | Requirement | UCR Ref. | FW | IPS | VPN |
|-----------|---|-----------------|-----------|------------|------------|
| 119 | The system shall create and maintain an audit trail that includes selected records of access to security-relevant objects and directories, including opens, closes, modifications, and deletions. | 5.8.4.3.5 (43) | R | R | R |
| 120 | The security device shall create an audit trail maintained by an IS that is capable of recording changes to the mechanism's list of users' formal access permissions. | 5.8.4.3.5 (44) | R | R | R |
| 121 | The security device shall record access or attempted access via controlled interfaces to objects or data whose labels are inconsistent with user privileges. | 5.8.4.3.5 (45) | R | R | R |
| 122 | The system shall create and maintain an audit trail that includes selected records of activities at the system console (either physical or logical consoles), and other system-level accesses by privileged users. | 5.8.4.3.5 (46) | R | R | R |
| 123 | The output of such intrusion/attack detection and monitoring tools shall be protected against unauthorized access, modification, or detection. | 5.8.4.3.5 (47) | R | R | R |
| 124 | Audit procedures that include the existence and use of audit reduction and analysis tools shall be implemented. | 5.8.4.3.5 (48) | R | R | R |
| 125 | Tools shall be available for the review of audit records and for report generation from audit records. | 5.8.4.3.5 (49) | R | R | R |
| 126 | Audit records shall include: a. User ID. b. Successful and unsuccessful attempts to access security files. c. Date and time of the event. d. Type of event. e. Success or failure of the event. f. Successful and unsuccessful log-ons. g. Denial of access resulting from an excessive number of log-on attempts. h. Blocking or blacklisting a user ID terminal or access port, and the reason for the action. i. Activities that might modify, bypass, or negate safeguards controlled by the system. j. Data required to audit the possible use of covert channel mechanisms. k. Privileged activities and other system-level access. l. Starting and ending time for access to the system. m. Security-relevant actions associated with periods processing or the changing of security labels or categories of information. | 5.8.4.3.5 (50) | R | R | R |
| 127 | The security device shall log requests for access or services where the presumed source identity of the information received by the security device specifies a broadcast identity. | 5.8.4.3.5 (51) | | R | |
| 128 | The level of events/information audited by the security device shall be configurable. | 5.8.4.3.5 (52) | R | R | R |
| 129 | The security device shall log SMTP traffic that contains source routing symbols (e.g., in the mailer recipient commands). | 5.8.4.3.5 (53) | | R | |
| 130 | The security device intrusion/attack detection and monitoring tools shall build on audit reduction and analysis tools to aid the ISSO in the monitoring and detection of suspicious, intrusive, or attack-like behavior patterns. | 5.8.4.3.5 (54) | R | R | R |
| 131 | Audit procedures shall include the capability of the system to monitor auditable events in real time that may indicate an imminent violation of security policies. | 5.8.4.3.5 (55) | R | R | R |
| 132 | A comprehensive audit trail of each remote session, to include the following, shall be recorded: a. Source and destination IP addresses. b. Connection start and end dates/times. c. Authenticated User IDs. d. Number of unsuccessful logon attempts before successful logon. e. Successful and unsuccessful attempts to access system resources during remote session. f. Privilege Escalation attempts. g. Activities that might modify, bypass, or negate safeguards controlled by the system. | 5.8.4.3.5 (56) | R | 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 log requests in which the information received by the security device contains the route (set of host network identifiers) by which information shall flow from the source subject to the destination subject. | 5.8.4.3.5 (57) | | R | |
| 134 | The security device shall log an information flow between a source subject and a destination subject via a controlled operation if the source subject has successfully authenticated to the security device. | 5.8.4.3.5 (58) | | R | |
| 135 | RESERVED | 5.8.4.3.5 (59) | | | |
| 136 | The security device shall log an information flow between two objects when the information security conditions match the attributes in an information flow policy rule (contained in the information flow policy database). | 5.8.4.3.5 (60) | | R | R |
| 137 | The security device shall log data and audit events when a user session authentication replay attack is detected. | 5.8.4.3.5 (61) | | R | R |
| 138 | The security device shall be able to collect the following: Start-up and Shutdown events. | 5.8.4.3.5 (62) | | R | R |
| 139 | The security device shall be able to collect the following: Identification, Authentication, and Authorization events. | 5.8.4.3.5 (63) | | R | R |
| 140 | The security device shall be able to collect the following: Data Accesses. | 5.8.4.3.5 (64) | | R | R |
| 141 | The security device shall be able to collect the following: Service Requests. | 5.8.4.3.5 (65) | | R | R |
| 142 | The security device shall be able to collect the following: Network traffic. | 5.8.4.3.5 (66) | | R | R |
| 143 | The security device shall be able to collect the Security configuration changes. | 5.8.4.3.5 (67) | | R | R |
| 144 | The security device shall be able to collect the following: Data introduction. | 5.8.4.3.5 (68) | | R | R |
| 145 | The security device shall be able to collect the following: Detected malicious code. | 5.8.4.3.5 (69) | | R | |
| 146 | The security device shall be able to collect the following: Access control configuration. | 5.8.4.3.5 (70) | | R | R |
| 147 | The security device shall be able to collect the following: Service configuration. | 5.8.4.3.5 (71) | | R | R |
| 148 | The security device shall be able to collect the Authentication configuration. | 5.8.4.3.5 (72) | | R | R |
| 149 | The security device shall be able to collect the following: Accountability policy configuration. | 5.8.4.3.5 (73) | | R | R |
| 150 | The security device shall be able to collect the following: Detected known vulnerabilities. | 5.8.4.3.5 (74) | | R | R |
| 151 | The security device shall provide authorized users with the capability to read the system data. | 5.8.4.3.5 (75) | | R | R |
| 152 | The system shall prohibit access to security device data, except those users that have been granted explicit read access. | 5.8.4.3.5(76) | | R | R |
| 153 | The security device shall ensure that security device data will be maintained if the security device: a. Fails. b. Is attacked. c. Storage becomes exhausted (a circular storage method will be employed so that a Denial of Service attack could not be implemented by overloading audit trail with events). d. Fails restart/reboot. | 5.8.4.3.5 (77) | R | R | R |
| 154 | The security device shall have a circular log to ensure that buffers do not fill and the logging stops. They should be required to offload to external SYSLOG RAE. | 5.8.4.3.5 (78) | R | R | R |
| 155 | The security device shall be able to offload audit logs to external SYSLOG RAE. | 5.8.4.3.5 (79) | R | R | R |
| 156 | The security device, when acting as an IPSec Gateway, will perform Authentication Header key checks. | 5.8.4.3.6 (1) | R | | |
| 157 | The security device shall use industry-accepted integrity mechanisms such as parity checks and cyclic redundancy checks (CRCs). | 5.8.4.3.6 (2) | R | R | R |
| 158 | The security device system assurance shall include features and procedures to validate the integrity and the expected operation of the security-relevant software, hardware, and firmware. | 5.8.4.3.6 (3) | R | R | R |
| 159 | System initialization, shutdown, and aborts shall be configured to ensure that the system remains in a secure state. | 5.8.4.3.6 (4) | R | R | R |

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

| ID | Requirement | UCR Ref. | FW | IPS | VPN |
|-----------|--|-----------------|-----------|------------|------------|
| 160 | The security device system assurance shall include control of access to the security support structure (i.e., the hardware, software, and firmware that perform operating system or security functions). | 5.8.4.3.6 (5) | R | R | R |
| 161 | Data and software storage integrity protection, including the use of strong storage integrity mechanisms (e.g., integrity locks, encryption) shall be employed. | 5.8.4.3.6 (6) | | R | R |
| 162 | Procedures to prevent the introduction of malicious code into the system, including the timely updating of those mechanisms intended to prevent the introduction of malicious code (e.g., updating anti-viral software), shall be employed. | 5.8.4.3.6 (7) | | R | R |
| 163 | The developer shall provide CM documentation identifying roles, responsibilities, and procedures, to include the management of Information Assurance information, and documentation shall be formally documented. | 5.8.4.3.7 (1) | R | R | R |
| 164 | The developer shall provide administrator guidance addressed to system administrative personnel (e.g., Administrator's Guide). | 5.8.4.3.7 (2) | R | R | R |
| 165 | The developer shall provide user guidance (e.g., User's Guide) when there are users other than administrators. The User's Guide will describe the protection mechanisms provided, guidelines on how the mechanisms are to be used, and the ways the mechanisms interact. | 5.8.4.3.7 (3) | R | R | R |
| 166 | The developer shall provide the architectural design of the security device. | 5.8.4.3.7 (4) | R | R | R |
| 167 | The developer shall provide a functional specification of the security device. | 5.8.4.3.7 (5) | R | R | R |
| 168 | The developer shall perform strength of security device analysis for each mechanism identified in the Security Target as having strength of security device claim. | 5.8.4.3.7 (6) | R | R | R |
| 169 | The developer shall provide an analysis of the test coverage. | 5.8.4.3.7 (7) | R | R | R |
| 170 | The developer shall provide covert channel analysis documentation identifying any covert channels detected along with alternative strategies for mitigating any associated vulnerabilities. | 5.8.4.3.7 (8) | R | R | R |
| 171 | The developer shall provide vulnerability analysis documentation identifying known security vulnerabilities regarding the configuration and use of administrative functions. The vulnerability analysis documentation shall also describe the analysis of the security device deliverables performed to search for obvious ways in which a user can violate the security device security policy. | 5.8.4.3.7 (9) | R | R | R |
| 172 | The reference document for the security device shall be unique to each version of the security device. | 5.8.4.3.7 (10) | R | R | R |
| 173 | The security device shall be labeled with its reference information, i.e., model and version number. | 5.8.4.3.7 (11) | R | R | R |
| 174 | The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system. | 5.8.4.3.7 (12) | R | R | R |
| 175 | The CM system shall provide measures such that only authorized changes are made to the configuration items. | 5.8.4.3.7 (13) | R | R | R |
| 176 | The guidance documentation shall list all assumptions about the intended environment. | 5.8.4.3.7 (14) | R | R | R |
| 177 | The system shall demonstrate a procedure for accepting and acting upon user reports of potential security flaws and requests for corrections to those flaws. | 5.8.4.3.7 (15) | R | R | R |
| 178 | The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the security device. | 5.8.4.3.7 (16) | R | R | R |
| 179 | The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw. | 5.8.4.3.7 (17) | R | R | R |
| 180 | The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws. | 5.8.4.3.7 (18) | R | R | R |
| 181 | The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections, and guidance on corrective actions to security device users. | 5.8.4.3.7 (19) | R | R | R |

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

| ID | Requirement | UCR Ref. | FW | IPS | VPN |
|-----------|--|-----------------|-----------|------------|------------|
| 182 | The procedures for processing reported security flaws shall ensure that any reported flaws are corrected and the correction issued to security device users. | 5.8.4.3.7 (20) | R | R | R |
| 183 | The developer shall perform a vulnerability analysis. | 5.8.4.3.7 (21) | R | R | R |
| 184 | The vulnerability analysis documentation shall describe the disposition of identified vulnerabilities. | 5.8.4.3.7 (22) | R | R | R |
| 185 | The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the security device. | 5.8.4.3.7 (23) | R | R | R |
| 186 | The vulnerability analysis documentation shall justify that the security device, with the identified vulnerabilities, is resistant to obvious penetration attacks. | 5.8.4.3.7 (24) | R | R | R |
| 187 | The installation, generation, and start-up documentation shall describe all the steps necessary for secure installation, generation, and start-up of the security device. | 5.8.4.3.7 (25) | R | R | R |
| 188 | The administrator guidance shall describe recovery procedures and technical system features to assure that system recovery is done in a trusted and secure manner. | 5.8.4.3.7 (26) | R | R | R |
| 189 | Security devices that provide encryption services shall be FIPS 140-2, Level 2-compliant. | 5.8.4.3.8 (1) | O | O | O |
| 190 | At a minimum, the following confidentiality policy adjudication features shall be provided for each controlled interface. Encrypt, as needed, all outgoing communication, including the body and attachment of the communication. | 5.8.4.3.8 (2) | | | R |
| 191 | Management Interfaces implemented with web servers shall implement secure web technology (e.g., Secure Sockets Layer; Secure HTTP) where capable. | 5.8.4.3.8 (3) | O | O | O |
| 192 | Where encryption is employed, the FIPS-validated crypto-module shall generate cryptographic keys using a FIPS-approved random number generator for all key sizes. | 5.8.4.3.8 (4) | O | O | O |
| 193 | Remote access shall use encryption to protect the confidentiality of the session. | 5.8.4.3.8 (5) | R | R | R |
| 194 | For security devices providing encryption, the suite of self-tests provided by the FIPS 140-2 cryptographic module shall be executed during initial start-up (power on), at the request of an administrator, periodically (at a System Administrator-specified interval not less than at least once a day) to demonstrate the correct operation of the cryptographic components. | 5.8.4.3.8 (6) | R | R | R |
| 195 | The security device shall run the specific set of key-generation self-test procedures provided by the FIPS 140-2 cryptographic module immediately after the generation of a cryptographic key. | 5.8.4.3.8 (7) | R | R | R |
| 196 | The security device shall provide an encrypted communication path between itself and remote administrators and authenticated proxy users that is logically distinct from the other communication paths and provides assured identification of its end points and protection of the communicated data from disclosure | 5.8.4.3.8 (8) | R | R | R |
| 197 | The security device shall use encryption to provide a trusted communication channel between itself and an authorized IT entity that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure. | 5.8.4.3.8 (9) | R | R | R |
| 198 | The security device shall use a cryptographic signature to provide a communication path between itself and remote administrators and authenticated proxy users that is logically distinct from other communication paths and provides assured identification of its end points and protection. | 5.8.4.3.8 (10) | R | R | R |
| 199 | Where encryption is employed, the security device shall provide the capability to implement an internal cryptographic function to verify the integrity of all security function executable code and data except the following: audit data or other dynamic security function data for which no integrity validation is justified. | 5.8.4.3.8 (11) | O | O | O |
| 200 | Minimum hash is HMAC-SHA1. | 5.8.4.3.8 (14) | R | R | R |
| 201 | The security device's crypto-module shall perform encryption and decryption using the AES standard. Encryption minimum is AES-128 with AES 256 as objective. | 5.8.4.3.8 (15) | R | R | R |
| 202 | Passwords shall be changed at least annually, employing system mechanisms that enforce current DoD password complexity policies. | 5.8.4.3.9 (1) | R | R | R |
| 203 | Passwords shall be encrypted both for storage and for transmission. | 5.8.4.3.9 (2) | R | R | R |

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

| ID | Requirement | UCR Ref. | FW | IPS | VPN |
|-----------|--|-----------------|-----------|------------|------------|
| 204 | The security device shall prevent the downloading of mobile code or executable content to itself. | 5.8.4.3.9 (3) | R | R | R |
| 205 | Monitoring tools shall be used for the monitoring and detection of suspicious, intrusive, or attack-like behavior patterns to itself. | 5.8.4.3.9 (4) | R | R | R |
| 206 | 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 IS perimeter. | 5.8.4.3.9 (5) | R | R | R |
| 207 | DoD ISs shall comply with DoD ports, protocols, and services guidance. | 5.8.4.3.9 (6) | R | R | R |
| 208 | Where scanning tools are available, the security device's internal hosts shall be scanned for vulnerabilities in addition to the security device itself to confirm an adequate security policy is being enforced. | 5.8.4.3.9 (7) | R | R | R |
| 209 | The security device must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with security device security functions. | 5.8.4.3.9 (8) | R | R | R |
| 210 | The security device shall block unauthorized directed broadcasts from external networks (Distributed Denial of Service defense). | 5.8.4.3.9 (9) | R | | |
| 211 | The security device shall verify reverse path unicast addresses (Distributed Denial of Service defense) and be able to drop packets that fail verification. | 5.8.4.3.9 (10) | R | | |
| 212 | The security device shall drop all packets with an IPv4 non-routable (RFC 1918) address originating from an external source. | 5.8.4.3.9 (11) | R | R | R |
| 213 | The security device shall drop all packets with an IPv4 source address of all zeros. | 5.8.4.3.9 (12) | R | R | R |
| 214 | The security device shall drop all traffic from the internal network that does not use a legitimate internal address range as its source address. | 5.8.4.3.9 (13) | R | R | R |
| 215 | The security device shall differentiate between authorized and fraudulent attempts to upgrade the operating system, i.e. trying to upgrade system files with the wrong names. | 5.8.4.3.9 (14) | R | R | |
| 216 | The security device shall differentiate between authorized and fraudulent attempts to upgrade the configuration, i.e., if a user is trying to perform an upgrade that is not authorized for that role. | 5.8.4.3.9 (15) | R | R | |
| 217 | The security device shall pass traffic which the security device has not identified as being a security problem without altering the contents. | 5.8.4.3.9 (16) | R | R | |
| 218 | The security device shall properly accept or deny User Datagram Protocol (UDP) traffic from port numbers based on policy. | 5.8.4.3.9 (17) | R | R | |
| 219 | The security device shall properly accept or deny TCP traffic from port numbers based on policy. | 5.8.4.3.9 (18) | R | R | |
| 220 | The security device shall not compromise its resources or those of any connected network upon initial start-up of the security device or recovery from an interruption in security device service. | 5.8.4.3.9 (19) | R | | |
| 221 | A security device shall properly enforce TCP state. | 5.8.4.3.9 (20) | R | | |
| 222 | A security device shall properly accept and deny traffic based on multiple rules. | 5.8.4.3.9 (21) | R | | |
| 223 | A security device shall prevent all known network-based current attack techniques (Common Vulnerabilities and Exploits) from compromising the security device. | 5.8.4.3.9 (22) | R | R | |
| 224 | A security device shall prevent the currently available Information Assurance Penetration techniques, as defined in DISA STIGS and IAVAs, from penetrating the security device. | 5.8.4.3.9 (23) | R | R | R |
| 225 | A security device shall block potentially malicious fragments. | 5.8.4.3.9 (24) | R | R | |
| 226 | The security device shall mediate the flow of all information between a user on an internal network connected to the security device and a user on an external network connected to the security device and must ensure that residual information from a previous information flow is not transmitted. | 5.8.4.3.9 (25) | R | R | |
| 227 | The security device shall not contain unauthorized compilers, editors, and other program development tools on its operational security device systems. | 5.8.4.3.9 (26) | R | R | |
| 228 | Each controlled interface shall be configured to ensure that all (incoming and outgoing) communications protocols, services, and communications not explicitly permitted are prohibited | 5.8.4.3.10 (1) | R | | |

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

| ID | Requirement | UCR Ref. | FW | IPS | VPN |
|-----------|--|-----------------|-----------|------------|------------|
| 229 | 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. | 5.8.4.3.10 (2) | R | | |
| 230 | The controlled interface is configured such that its operational failure or degradation (to include traffic load or corrupt traffic content) does not result in any unauthorized system access. | 5.8.4.3.10 (3) | R | | |
| 231 | The security device's controlled interface enforces configurable thresholds to determine whether all network traffic can be handled and controlled. | 5.8.4.3.10 (5) | R | | |
| 232 | The underlying operating system shall satisfy the confidentiality requirements of Protection Level 2 or higher, integrity requirements for Basic Level-of-Concern or higher, and availability requirements for Basic Level-of-Concern or higher. | 5.8.4.3.10 (7) | R | R | R |
| 233 | The security device shall reject requests for access or services where the presumed source identity of the source subject is an external Information Technology entity on a broadcast network. | 5.8.4.3.11 (5) | R | R | R |
| 234 | The security device shall reject requests for access or services where the presumed source identity of the source subject is an external Information Technology entity on the loopback network. | 5.8.4.3.11 (6) | R | | R |
| 235 | The security device shall permit an information flow between a source subject and a destination subject via a controlled operation if the source subject has successfully authenticated to the security device. | 5.8.4.3.11 (9) | R | R | R |
| 236 | The TSF shall permit an information flow between a controlled subject and another controlled subject via a controlled operation if the following rules hold: a. Subjects on an internal network can cause information to flow through the security device to another connected network if: (1) All the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator; (2) The presumed address of the source subject, in the information, translates to an internal network address; (3) And the presumed address of the destination subject, in the information, translates to an address on the other connected network. b. Subjects on the external network can cause information to flow through the TOE to another connected network if: (1) All the information security attribute values are unambiguously permitted by the 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. | 5.8.4.3.11 (10) | R | | |
| 237 | The security device, after a failure or service discontinuity, shall enter a maintenance mode where the ability to return the security device to a secure state is provided. | 5.8.4.3.11 (11) | R | R | R |
| 238 | The security device shall detect replay attacks using either security device data or security attributes. | 5.8.4.3.11 (12) | | R | R |
| 239 | The security device shall reject data and audit events when a replay is detected. | 5.8.4.3.11 (13) | | R | |
| 240 | The security device shall ensure the security policy enforcement functions are invoked and succeed before each function within the security functions' scope of control is allowed to proceed. | 5.8.4.3.11 (14) | R | R | R |
| 241 | RESERVED | 5.8.4.3.11 (15) | | | |
| 242 | The security device shall lock a local interactive session after a System Administrator-specified time period of inactivity by clearing or overwriting display devices and making the current contents unreadable. | 5.8.4.3.11 (16) | R | R | R |
| 243 | The security device shall lock a local interactive session after a System Administrator-specified time period of inactivity by disabling any activity of the user's data access/display devices other than unlocking the session. | 5.8.4.3.11 (17) | R | R | R |
| 244 | The security device shall allow user-initiated locking of the user's own local interactive session by clearing or overwriting display devices and making the current contents unreadable. | 5.8.4.3.11 (18) | R | R | R |

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

| ID | Requirement | UCR Ref. | FW | IPS | VPN |
|-----------|--|-----------------|-----------|------------|------------|
| 245 | The security device shall allow user-initiated locking of the user's own local interactive session by disabling any activity of the user's data access/display devices other than unlocking the session. | 5.8.4.3.11 (19) | R | R | R |
| 246 | The security device shall terminate a remote session after a System Administrator-configurable time interval of session inactivity. | 5.8.4.3.11 (20) | R | R | R |
| 247 | The security device shall enforce System Administrator policy regarding Instant Messaging traffic. | 5.8.4.3.11 (21) | R | R | R |
| 248 | The security device shall enforce System Administrator policy regarding VVoIP traffic. | 5.8.4.3.11(22) | R | R | R |
| 249 | The security device features or capabilities not required for security device operation shall be disabled to eliminate exposure to possible security vulnerabilities. | 5.8.4.3.11 (23) | R | R | R |
| 250 | Access Control shall include a Discretionary Access Control (DAC) Policy. | 5.8.4.3.11 (25) | R | R | R |
| 251 | Discretionary Access Control access controls shall be capable of including or excluding access to the granularity of a single user. | 5.8.4.3.11 (26) | R | R | R |
| 252 | The security device's controlled interface shall review incoming information for viruses and other malicious code. | 5.8.4.3.11(27) | R | R | R |
| 253 | The controlled interface shall be configured so its operational failure or degradation (to include traffic load or corrupt traffic content) does not result in any external information entering the IS. | 5.8.4.3.11(28) | R | R | R |
| 254 | The controlled interface shall be configured so its operational failure or degradation (to include traffic load or corrupt traffic content) does not result in any unauthorized release of information outside the IS perimeter. | 5.8.4.3.11(29) | R | R | R |
| 255 | The controlled interface shall provide the ability to fully restore its functionality in accordance with documented restoration procedures. | 5.8.4.3.11 (30) | R | R | R |
| 256 | The security device shall prevent or mitigate DoS attacks. Where technically feasible, procedures and mechanisms shall be in place to curtail or prevent well-known, detectable, and preventable DoS attacks (e.g., SYN attack). Only a limited number of DoS attacks are detectable and preventable. Often, prevention of such attacks is handled by a controlled interface. | 5.8.4.3.11(31) | R | R | R |
| 257 | The developer must specify the security device's bandwidth requirements and capabilities. This shall include the maximum bandwidth speeds the device will operate on, as well as the security device bandwidth requirements (bandwidth in Kbps) documented by who the device communicates with, frequency, and Kbps transmitted and received (such as product downloads, signature files). | 5.8.4.3.12 (1) | R | R | R |
| 258 | The security device, as configured, must process new connections at the rate of the expected maximum number of connections as advertised by the vendor within a 1-minute period. | 5.8.4.3.12 (2) | R | R | R |
| 259 | The security device, as configured, must process new HTTP connections at the rate of the expected maximum number of connections as advertised by the vendor within a 1-minute period. | 5.8.4.3.12 (4) | R | R | R |
| 260 | 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. | 5.8.4.3.12 (6) | R | R | R |
| 261 | The security device shall employ a commercial best practice defensive solution along with maintain advertised normal operation packet loss rates for all legitimate data packets when under a SYN Flood attack. | 5.8.4.3.12 (10) | R | R | R |
| 262 | The security device must not degrade IPv4 and IPv6 forwarding when used with a long Access Policy configuration. | 5.8.4.3.12 (11) | R | | R |
| 263 | The security device shall demonstrate a latency variance of less than 20 percent and a packet loss variance of less than 10 percent of the manufacturer-specified nominal values for all operational conditions. | 5.8.4.3.12 (12) | R | | |
| 264 | The security device shall enforce the policy pertaining to a specified number of encryption failures. | 5.8.4.4.1 (1) | R | | R |
| 265 | The security device shall enforce the policy pertaining to a specified number of decryption failures. | 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 |
|-----------|---|-----------------|-----------|------------|------------|
| 266 | The security device shall enforce the policy pertaining to any indication of a potential security violation. | 5.8.4.4.1 (3) | R | | R |
| 267 | The security device shall be configurable to perform actions based upon different information flow policies. | 5.8.4.4.1 (4) | R | | R |
| 268 | The security device shall deny establishment of an authorized user session based on network source (i.e., source IP address) and time of day parameter values. | 5.8.4.4.1 (5) | R | | R |
| 269 | 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 of time. | 5.8.4.4.1 (6) | R | | |
| 270 | The security device shall enforce the System Administrator's policy pertaining to network traffic violations to a specific TCP port within a specified period of time. | 5.8.4.4.1 (7) | R | | R |
| 271 | The security device shall enforce the System Administrator's policy pertaining to violations of network traffic rules within a specified period of time. | 5.8.4.4.1 (8) | R | | R |
| 272 | The security device shall enforce the System Administrator's policy pertaining to any security device-detected replay of data and/or nested security attributes. | 5.8.4.4.1 (9) | R | | R |
| 273 | <p>This section addresses the ability of a firewall to perform basic filtering functions. It does not mandate a specific filtering configuration for firewalls. 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. <ol style="list-style-type: none"> a. Will apply to the following defined services: <ol style="list-style-type: none"> (1) The service UDPecho (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 (| 5.8.4.4.2 | R | | |
| 274 | The security device shall detect and protect against a focused method of attack: Footprinting and Scanning. | 5.8.4.5 (1) | | R | |
| 275 | The security device shall detect and protect against a focused method of attack: Enumeration. | 5.8.4.5 (2) | | R | |
| 276 | The security device shall detect and protect against a focused method of attack: Gaining Access. | 5.8.4.5 (3) | | R | |
| 277 | The security device shall detect and protect against a focused method of attack: Escalation of Privilege. | 5.8.4.5 (4) | | R | |
| 278 | The security device shall detect and protect against a focused method of attack: Maintaining Access. | 5.8.4.5 (5) | | R | |
| 279 | The security device shall detect and protect against a focused method of attack: Network Exploitation. | 5.8.4.5 (6) | | R | |
| 280 | The security device shall detect and protect against a focused method of attack: Cover Tracks. | 5.8.4.5 (7) | | R | |