



DEFENSE INFORMATION SYSTEMS AGENCY

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

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

1 May 13

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Joint Interoperability Certification of the Check Point Software Technologies Firewall 21400 and 4800 Software Release 7X

References: (a) DoD Directive 4630.05, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," 5 May 2004
(b) DoD Instruction 8100.04, "DoD Unified Capabilities (UC)," 9 December 2010
(c) through (f), see Enclosure 1

1. References (a) and (b) establish the Joint Interoperability Test Command (JITC), as the responsible organization for interoperability (IO) certification.
2. The Check Point Software Technologies Firewall (FW) models 21400 and 4800 Software Release (R) 7X, hereinafter referred to as the Systems Under Test (SUT), met all the critical IO requirements and are certified for joint use within the Defense Information System Network (DISN) as a FW. Testing was conducted using product requirements derived from the Unified Capabilities Requirements (UCR) 2008, Change 3, in Reference (c); and test procedures derived from Reference (d). The operational status of the SUT must be verified during deployment. Any new discrepancies discovered in the operational environment will be evaluated for impact and adjudication to the satisfaction of the Defense Information Systems Agency (DISA) via a vendor Plan of Action and Milestones (POA&M) to address concern(s) within 120 days of identification. No other configurations, features, or functions, except those cited within this memorandum, are certified by the JITC. This certification expires upon changes that affect IO, but no later than three years from the date of this memorandum.
3. This certification is based on IO testing conducted by the JITC, Indian Head, Maryland, from 06 through 17 August 2012. The DISA Certifying Authority (CA) provided a positive recommendation on 27 March 2013 for model 4800 and on 15 April 2013 for model 21400, based on the security testing completed by DISA Information Assurance (IA) test team and published in a separate report, Reference (e).
4. The Interface, Compatibility Requirements (CRs) and Functional Requirements (FRs), and component status of the SUT are listed in Tables 1 and 2. The threshold CR/FR for FWs are established by UCR 2008, Change 3, Section 5.8 of Reference (c) and were used to evaluate the IO of the SUT. Enclosure 3 provides a detailed list of the interface, CRs, and FRs.

Table 1. SUT Interface Interoperability Status

Interface	Critical	UCR Reference (See Note 1.)	Threshold CR/FR Requirements (See note 2.)	Status	Remarks																
Data Firewall																					
10Base-X	No	5.3.2.4 / 5.3.3.10.1.2	1-4	Met	SUT met requirements for specified interfaces																
100Base-X	No	5.3.2.4 / 5.3.3.10.1.2	1-4	Met	SUT met requirements for specified interfaces																
1000Base-X	No	5.3.2.4 / 5.3.3.10.1.2	1-4	Met	SUT met requirements for specified interfaces																
10GBase-X	No	5.3.2.4 / 5.3.3.10.1.2	1-4	Met	SUT met requirements for specified interfaces																
40GBase-X	No	5.3.2.4 / 5.3.3.10.1.2	1-4	N/A	Not supported by SUT																
100GBase-X	No	5.3.2.4 / 5.3.3.10.1.2	1-4	N/A	Not supported by SUT																
<p>NOTES:</p> <p>1. UCR 2008, Change 3, Section 5.8 does not identify individual interface requirements for security devices. SUT must minimally provide Ethernet interfaces that meet the requirements in the identified sections.</p> <p>2. The CR/FR requirements are contained in Table 2. The CR/FR numbers represent a roll-up of UCR requirements. Enclosure 3 provides a list of more detailed requirements for firewall products.</p> <p>LEGEND:</p> <table style="width: 100%; border: none;"> <tr> <td style="width: 50%;">Base-X</td> <td style="width: 30%;">Ethernet generic designation</td> <td style="width: 10%;">N/A</td> <td style="width: 10%;">Not Applicable</td> </tr> <tr> <td>CR</td> <td>Capability Requirement</td> <td>SUT</td> <td>System Under Test</td> </tr> <tr> <td>FR</td> <td>Functional Requirement</td> <td>UCR</td> <td>Unified Capabilities Requirements</td> </tr> <tr> <td>GBaseX</td> <td>Gigabit Generic Designation</td> <td></td> <td></td> </tr> </table>						Base-X	Ethernet generic designation	N/A	Not Applicable	CR	Capability Requirement	SUT	System Under Test	FR	Functional Requirement	UCR	Unified Capabilities Requirements	GBaseX	Gigabit Generic Designation		
Base-X	Ethernet generic designation	N/A	Not Applicable																		
CR	Capability Requirement	SUT	System Under Test																		
FR	Functional Requirement	UCR	Unified Capabilities Requirements																		
GBaseX	Gigabit Generic Designation																				

Table 2. SUT Capability Requirements and Functional Requirements Status

CR/FR ID	Capability/ Function	Applicability (See note)	UCR Reference (UCR 2008 CH3)	Status	Remarks
1	Conformance Requirements				
	Conformance Standards	Required	5.8.4.2	N/A	VPN
2	Information Assurance Requirements				
	General Requirements	Required	5.8.4.3.1	Met	
	Configuration Management	Required	5.8.4.3.3	Met	
	Alarms & Alerts	Required	5.8.4.3.4	Met	See Reference (e).
	Audit and Logging	Required	5.8.4.3.5	Met	See Reference (e).
	Cryptography	Required	5.8.4.3.8	Met	Cryptography is optional with the exception that all outgoing communications are encrypted.
	Security Measures	Required	5.8.4.3.9	Met	See Reference (e).
	System and Communication Protection	Required	5.8.4.3.10	Met	
	Other Requirements	Required	5.8.4.3.11	Met	
	Performance	Required	5.8.4.3.12	Met	
3	Functionality				
	Policy	Required	5.8.4.4.1	Met	
	Filtering	Required	5.8.4.4.2	Met	

Table 2. SUT Capability Requirements and Functional Requirements Status (continued)

Internet Protocol Version 6 (IPv6)																									
4	IPv6 Requirements	Required	5.3.5	Met																					
<p>NOTE: The annotation of 'required' refers to a high-level requirement category. The applicability of each sub-requirement is provided in Enclosure 3; Table 3-1 provides detailed CR/FR for firewalls.</p> <p>LEGEND:</p> <table style="width: 100%; border: none;"> <tr> <td style="width: 15%;">CH</td> <td style="width: 35%;">Change</td> <td style="width: 15%;">N/A</td> <td style="width: 35%;">Not Applicable</td> </tr> <tr> <td>CR</td> <td>Capability Requirement</td> <td>SUT</td> <td>System Under Test</td> </tr> <tr> <td>FR</td> <td>Functional Requirement</td> <td>UCR</td> <td>Unified Capabilities Requirements</td> </tr> <tr> <td>ID</td> <td>Identification</td> <td>VPN</td> <td>Virtual Private Network</td> </tr> <tr> <td>IPv6</td> <td>Internet Protocol Version 6</td> <td></td> <td></td> </tr> </table>						CH	Change	N/A	Not Applicable	CR	Capability Requirement	SUT	System Under Test	FR	Functional Requirement	UCR	Unified Capabilities Requirements	ID	Identification	VPN	Virtual Private Network	IPv6	Internet Protocol Version 6		
CH	Change	N/A	Not Applicable																						
CR	Capability Requirement	SUT	System Under Test																						
FR	Functional Requirement	UCR	Unified Capabilities Requirements																						
ID	Identification	VPN	Virtual Private Network																						
IPv6	Internet Protocol Version 6																								

5. In accordance with the Program Manager’s request, JITC did not develop a detailed test report. JITC distributes IO information via the JITC Electronic Report Distribution system, which uses Unclassified-But-Sensitive Internet Protocol Router Network (NIPRNet) e-mail. More comprehensive IO status information is available via the JITC System Tracking Program (STP), which .mil/.gov users can access on the NIPRNet at <https://stp.fhu.disa.mil>. Test reports, lessons learned, and related testing documents and references are on the JITC Joint Interoperability Tool (JIT) at <https://jit.fhu.disa.mil>. Information related to Approved Product List (APL) testing is available on the DISA APL Testing and Certification website located at <http://www.disa.mil/Services/Network-Services/UCCO>. All associated test information is available on the DISA Unified Capability Coordination Office (UCCO) APL Integrated Tracking System website located at <https://aplits.disa.mil>.

6. JITC testing point of contact is Mr. Keith Watson, commercial (301) 743-4305; e-mail address is keith.d.watson2.civ@mail.mil. JITC certification point of contact is Ms. Baotram (BT) Tran; commercial (301) 743-4319; e-mail address is baotram.tran.civ@mail.mil. JITC’s mailing address is 3341 Strauss Avenue, Suite 236, Indian Head, Maryland, 20640-5149. The UCCO tracking numbers are 1216303 and 1216305.

FOR THE COMMANDER:



for Richard A. Meador
Chief
Battlespace Communications Portfolio

3 Enclosures a/s

JITC Memo, JTG, Joint Interoperability Certification of the Check Point Software Technologies
Firewall 21400 and 4800 Software Release 7X

Distribution (electronic mail):

DoD CIO

Joint Staff J-6, JCS

USD(AT&L)

ISG Secretariat, DISA, JTA

US Strategic Command, J665

US Navy, OPNAV N2/N6FP12

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

US Air Force, A3CNN/A6CNN

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

US Coast Guard, CG-64

DISA/TEMC

DIA, Office of the Acquisition Executive

NSG Interoperability Assessment Team

DOT&E, Netcentric Systems and Naval Warfare

Medical Health Systems, JMIS IV&V

ADDITIONAL REFERENCES

- (c) Office of the Assistant Secretary of Defense, “Department of Defense Unified Capabilities Requirements 2008, Change 3,” September 2011
- (d) Joint Interoperability Test Command, “Security Device Test Plan”
- (e) Joint Interoperability Test Command, “Information Assurance (IA) Assessment Report for Check Point Software Technologies Data Firewall 21400 Software Release 7X, TN1216303” and “IA Assessment Report for Check Point Software Technologies Data Firewall 4800 Software Release 7X, TN 1216305”

(This page left intentionally blank).

CERTIFICATION TESTING SUMMARY

1. SYSTEM TITLE. Check Point Software Technologies Data Firewall 21400 and 4800 Software Version Release 7X

2. SPONSOR. Christopher Bayliss, Defense Information System Agency, Phone: 301-225-4785, e-mail: Christopher.M.Bayliss.civ@mail.mil.

3. SYSTEM POC. Gustavo Coronel, Phone: 202-468-9538, e-mail: gcoronel@checkpoint.com.

4. TESTER. Joint Interoperability Test Command (JITC), Indian Head, Maryland.

5. SYSTEM DESCRIPTION. Security Devices provide a Global Information Grid architectural defense-in-depth capability to protect and define critical warfighting missions. The Unified Capabilities Requirements (UCR) defines six security device products: Firewalls (FW), Information Assurance Tool, Intrusion Detection Systems (IDS) / Intrusion Prevention Systems (IPS), Integrated Security System, Network Access Control, and Virtual Private Network (VPN) components (concentrator and termination). The Check Point Software Technologies Data Firewall (FW) 21400 and 4800 Software Release (R) 7X, hereinafter referred to as the Systems Under Test (SUT), provides the following firewall capabilities.

a. Check Point 21400 firewall. The Check Point Technologies 21400 Firewall Software Blade is an element of Check Point Software Blades R7X. Software Blades are independent and flexible security modules that enable you to select the functions you want to build a custom Check Point Security Gateway. The Check Point Software Blades R7X is a network perimeter security gateway that provides controlled connectivity between two or more network environments. Gateways may be installed as a standalone appliance, or as clusters of two or more appliances in a high-availability or load sharing configuration. Cluster members synchronize state tables, ensuring fault-tolerance with sub-second failover.

The product provides a broad set of information flow controls, including traffic filtering, application-level proxies, Network Address Translation (NAT), and intrusion detection and prevention capabilities. Internet Key Exchange/Internet Protocol Security and Secure Sockets Layer VPN functionality encrypts and authenticates network traffic to and from selected peers, in order to protect the traffic from disclosure or modification over un-trusted networks.

Leveraging its multi-core and acceleration technologies, with 2900 Security Power Units, the Check Point 21400 appliance supports lightning fast firewall throughput of up to 110 Gigabits Per Second (Gbps) with sub 5 μ s latency and IPS throughput of more than 21 Gbps. The 21400 is designed from the ground up for unmatched flexibility for even the most demanding enterprise and data center network environments.

The 21400 appliance has 3 expansion slots supporting a wide range of network options. The 21400 standard configuration includes a twelve 1 Gigabit Ethernet copper port card. A maximally configured 21400 provides up to 36 Gigabit Ethernet copper or fiber ports or twelve 10 Gigabit Ethernet fiber ports.

Furthermore, the 21400 also has a slot for an optional Security Acceleration Module. In addition to hot-swappable redundant disk drives and power supply units, the 21400 appliance also supports the Lights-Out-Management option for remote support and maintenance capabilities. The 21400 Appliance is a highly serviceable chassis. Access to all components is easily available from the front and the back of the unit when mounted in the rack.

b. Check Point 4800 firewall. The Check Point 4800 Firewall Software Blade is an element of Check Point Software Blades R7X. Software Blades are independent and flexible security modules that enable you to select the functions you want to build a custom Check Point Security Gateway. The Check Point Software Blades R7X is a network perimeter security gateway that provides controlled connectivity between two or more network environments. Gateways may be installed as a standalone appliance, or as clusters of two or more appliances in a high-availability or load sharing configuration. Cluster members synchronize state tables, ensuring fault-tolerance with sub-second failover.

The 4800 firewall supports the Check Point 3D security vision of combining policies, people and enforcement for unbeatable protection and is optimized for enabling any combination of the following Software Blades: (1) FW, (2) VPN, (3) IPS, (4) Application Control, (5) Mobile Access, (6) Data Loss Prevention, (7) Uniform Resource Locator Filtering, (8) Antivirus, (9) Anti-spam, (10) Anti-Bot, (11) Identity Awareness and (12) Advanced Networking & Clustering. In addition to eight onboard 1 Gigabit copper Ethernet ports, the 4800 also comes with an available expansion slot which provides the option to add four or eight 1 Gigabit copper Ethernet ports, two or four 1 Gigabit fiber Ethernet ports or two 10 Gigabit fiber Ethernet ports.

With 623 SecurityPower Units, the 4800 Appliance offers superior performance for its price range with a firewall throughput of 11 Gbps and IPS throughput of 6 Gbps.

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

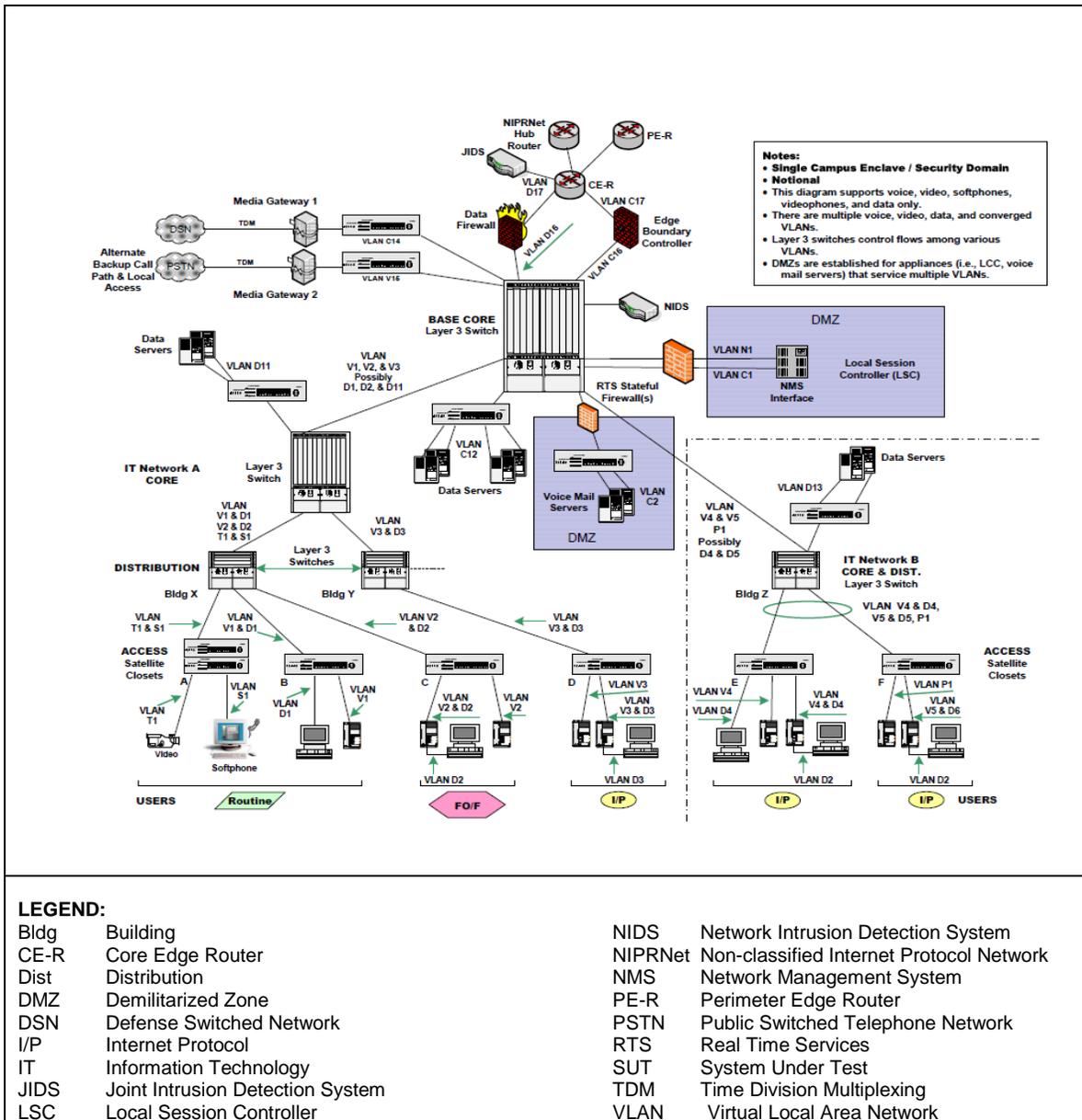


Figure 2-1. Security Device Architecture

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

7.1 Interfaces. Table 2-1, shows the physical interfaces and associated standards supported by the SUT.

Table 2-2. Security Device CRs and FRs (continued)

CR/FR ID	Capability/ Function	Applicability (See note)	UCR Reference (UCR 2008 CH3)	Criteria																
2	Other Requirements	Required	5.8.4.3.11	Sub-requirements differ by Security Device type. Cryptography is optional with the exception that all outgoing communications are encrypted.																
	Performance	Required	5.8.4.3.12																	
3	Functionality																			
	Policy	Required	5.8.4.4.1	FW & VPN Only																
	Filtering	Required	5.8.4.4.2	FW Only																
Internet Protocol Version 6 (IPv6)																				
4	IPv6 Requirements	Required	5.3.5	Security Device types																
<p>NOTE: The annotation of "required" refers to a high-level requirement category. The applicability of each sub-requirement is provided in Enclosure 3. Table 3-1 provides detailed CR/FR for Data Firewalls.</p> <p>LEGEND:</p> <table> <tr> <td>CH</td> <td>Change</td> <td>ID</td> <td>Identification</td> </tr> <tr> <td>CR</td> <td>Capability Requirements</td> <td>IPv6</td> <td>Internet Protocol version 6</td> </tr> <tr> <td>FR</td> <td>Functional Requirements</td> <td>UCR</td> <td>Unified Capabilities Requirements</td> </tr> <tr> <td>FW</td> <td>Firewall</td> <td>VPN</td> <td>Virtual Private Network</td> </tr> </table>					CH	Change	ID	Identification	CR	Capability Requirements	IPv6	Internet Protocol version 6	FR	Functional Requirements	UCR	Unified Capabilities Requirements	FW	Firewall	VPN	Virtual Private Network
CH	Change	ID	Identification																	
CR	Capability Requirements	IPv6	Internet Protocol version 6																	
FR	Functional Requirements	UCR	Unified Capabilities Requirements																	
FW	Firewall	VPN	Virtual Private Network																	

7.3 Information Assurance. Table 2-3 details the IA requirements applicable to the Security Device products.

Table 2-3. Security Device IA Requirements

Capability/ Function	Applicability (See Note)	UCR Reference (UCR 2008 CH 3)	Criteria												
General Requirements	Required	5.8.4.3.1	Meet UCR 'required' requirements.												
Configuration Management	Required	5.8.4.3.3													
Alarms & Alerts	Required	5.8.4.3.4	Enclosure 3 provides detailed functional requirements for each specified CR/FR.												
Audit and Logging	Required	5.8.4.3.5													
Cryptography	Required	5.8.4.3.8													
Security Measures	Required	5.8.4.3.9													
System and Communication Protection	Required	5.8.4.3.10	Cryptography is optional with the exception that all outgoing communications are encrypted.												
Other Requirements	Required	5.8.4.3.11													
Performance	Required	5.8.4.3.12													
<p>NOTE: Criticality represents high level roll-up of the CR/FR area. Table 3-1 of Enclosure 3 provides detailed CR/FR for Firewalls.</p> <p>LEGEND:</p> <table> <tr> <td>CH</td> <td>Change</td> <td>FR</td> <td>Functionality Requirements</td> </tr> <tr> <td>CR</td> <td>Capabilities Requirements</td> <td>UCR</td> <td>Unified Capabilities Requirements</td> </tr> <tr> <td>FR</td> <td>Functionality Requirements</td> <td></td> <td></td> </tr> </table>				CH	Change	FR	Functionality Requirements	CR	Capabilities Requirements	UCR	Unified Capabilities Requirements	FR	Functionality Requirements		
CH	Change	FR	Functionality Requirements												
CR	Capabilities Requirements	UCR	Unified Capabilities Requirements												
FR	Functionality Requirements														

7.4 Other. None

8. TEST NETWORK DESCRIPTION. The JITC tested the SUT at its Indian Head, Maryland, Test Facility in a manner and configuration similar to that of a notional operational environment. Testing the system's required functions and features was conducted using the test configurations depicted in Figure 2-2.

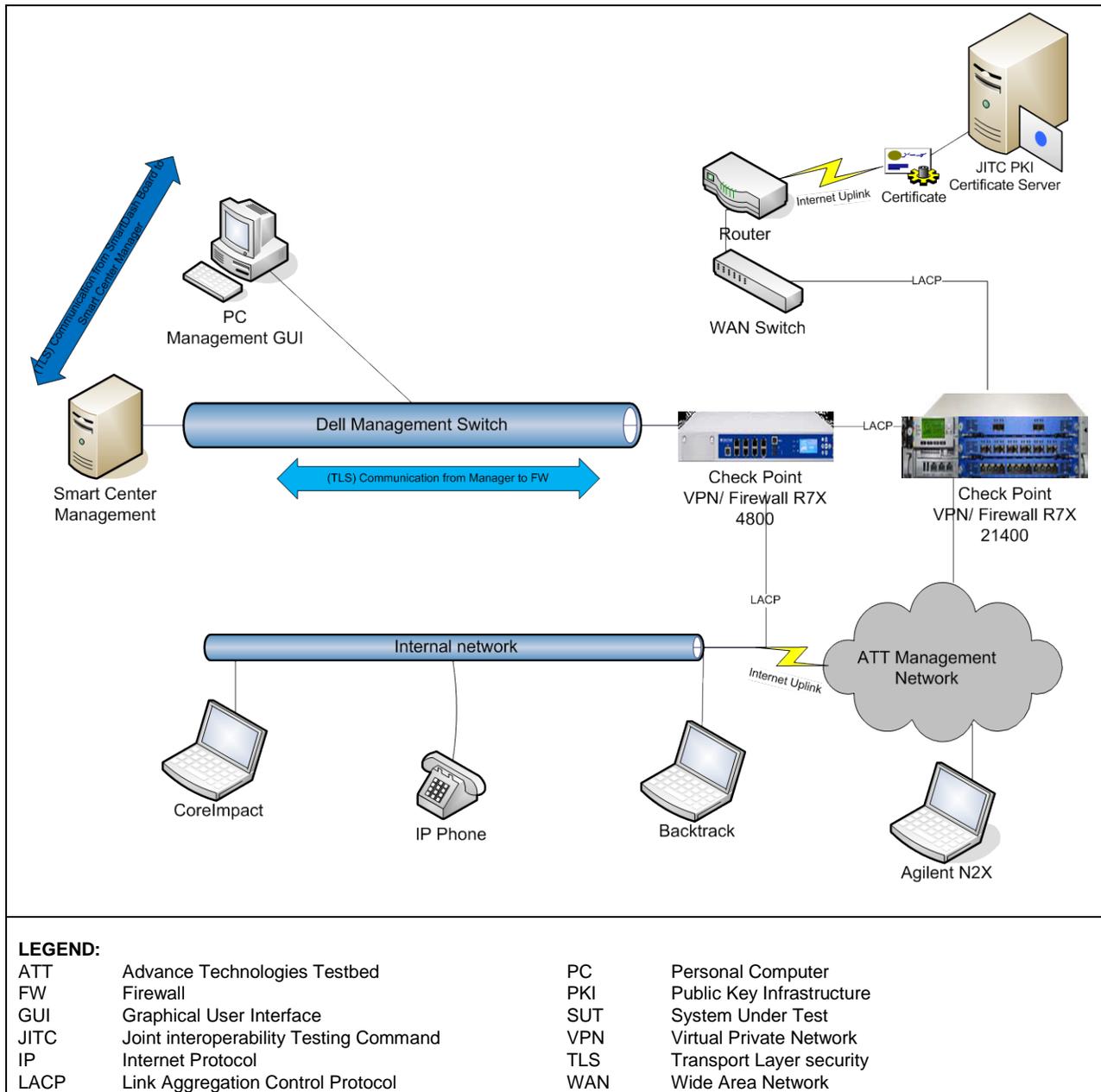


Figure 2-2. SUT Test Configuration

Table 2-6. SUT Interface Requirements Status

Interface	Critical	UCR Reference (See Note 1.)	Threshold CR/FR Requirements (See note 2.)	Status	Remarks																
Firewall																					
10Base-X	No	5.3.2.4 / 5.3.3.10.1.2	1-4	Met	SUT met requirements for specified interfaces																
100Base-X	No	5.3.2.4 / 5.3.3.10.1.2	1-4	Met	SUT met requirements for specified interfaces																
1000Base-X	No	5.3.2.4 / 5.3.3.10.1.2	1-4	Met	SUT met requirements for specified interfaces																
10GBase-X	No	5.3.2.4 / 5.3.3.10.1.2	1-4	Met	SUT met requirements for specified interfaces																
40GBase-X	No	5.3.2.4 / 5.3.3.10.1.2	1-4	N/A	Not supported by SUT																
100GBase-X	No	5.3.2.4 / 5.3.3.10.1.2	1-4	N/A	Not supported by SUT																
<p>NOTES:</p> <p>1. UCR 2008, Change 3, Section 5.8 does not identify individual interface requirements for security devices. SUT must minimally provide Ethernet interfaces that meet the requirements in the identified sections.</p> <p>2. The CR/FR requirements are contained in Table 2. The CR/FR numbers represent a roll-up of UCR requirements. Enclosure 3 provides a list of more detailed requirements for Firewall products.</p> <p>LEGEND:</p> <table style="width: 100%; border: none;"> <tr> <td style="width: 15%;">Base-X</td> <td style="width: 45%;">Ethernet generic designation</td> <td style="width: 15%;">N/A</td> <td style="width: 25%;">Not Applicable</td> </tr> <tr> <td>CR</td> <td>Capability Requirement</td> <td>SUT</td> <td>System Under Test</td> </tr> <tr> <td>FR</td> <td>Functional Requirement</td> <td>UCR</td> <td>Unified capabilities Requirements</td> </tr> <tr> <td>GBase-X</td> <td>Gigabit generic designation</td> <td></td> <td></td> </tr> </table>						Base-X	Ethernet generic designation	N/A	Not Applicable	CR	Capability Requirement	SUT	System Under Test	FR	Functional Requirement	UCR	Unified capabilities Requirements	GBase-X	Gigabit generic designation		
Base-X	Ethernet generic designation	N/A	Not Applicable																		
CR	Capability Requirement	SUT	System Under Test																		
FR	Functional Requirement	UCR	Unified capabilities Requirements																		
GBase-X	Gigabit generic designation																				

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

Table 2-7. SUT CR and FR Status

CR/FR ID	Capability/ Function	Applicability (See note)	UCR Reference (UCR 2008 CH3)	Status	Remarks
1	Conformance Requirements				
	Conformance Standards	Required	5.8.4.2	N/A	VPN
2	Information Assurance Requirements				
	General Requirements	Required	5.8.4.3.1	Met	
	Configuration Management	Required	5.8.4.3.3	Met	
	Alarms & Alerts	Required	5.8.4.3.4	Met	See Reference (e)
	Audit and Logging	Required	5.8.4.3.5	Met	See Reference (e)

Table 2-7. SUT CR and FR Status (continued)

CR/FR ID	Capability/ Function	Applicability (See note)	UCR Reference (UCR 2008 CH3)	Status	Remarks																				
2	Cryptography	Required	5.8.4.3.8	Met	Cryptography is optional with the exception that all outgoing communications are encrypted.																				
	Security Measures	Required	5.8.4.3.9	Met	See Reference (e)																				
	Systems and Communication Protection	Required	5.8.4.3.10	Met																					
	Other Requirements	Required	5.8.4.3.11	Met																					
	Performance	Required	5.8.4.3.12	Met																					
3	Functionality																								
	Policy	Required	5.8.4.4.1	Met																					
	Filtering	Required	5.8.4.4.2	Met																					
4	Internet Protocol version 6																								
	IPv6 Requirements	Required	5.8.4.5	Met																					
<p>NOTES: The annotation of "required" refers to a high-level requirement category. The applicability of each sub-requirement is provided in Enclosure 3. Table 3-1 provides detailed CR/FR for Firewalls.</p> <p>LEGEND:</p> <table> <tr> <td>CH</td> <td>Change</td> <td>N/A</td> <td>Not Applicable</td> </tr> <tr> <td>CR</td> <td>Capability Requirements</td> <td>IPv6</td> <td>Internet Protocol version 6e</td> </tr> <tr> <td>FR</td> <td>Functionality Requirements</td> <td>UCR</td> <td>Unified Capabilities Requirements</td> </tr> <tr> <td>FW</td> <td>Firewall</td> <td>VPN</td> <td>Virtual Private Network</td> </tr> <tr> <td>ID</td> <td>Identification</td> <td></td> <td></td> </tr> </table>						CH	Change	N/A	Not Applicable	CR	Capability Requirements	IPv6	Internet Protocol version 6e	FR	Functionality Requirements	UCR	Unified Capabilities Requirements	FW	Firewall	VPN	Virtual Private Network	ID	Identification		
CH	Change	N/A	Not Applicable																						
CR	Capability Requirements	IPv6	Internet Protocol version 6e																						
FR	Functionality Requirements	UCR	Unified Capabilities Requirements																						
FW	Firewall	VPN	Virtual Private Network																						
ID	Identification																								

a. Conformance Requirements.

Security Devices shall meet the appropriate specific standards described in UCR 2008 Change 3, Section 5.8.4.2 as applicable to Firewalls products. No applicable requirements.

b. Information Assurance Requirements.

(1) General Requirements. Security Devices shall meet the appropriate specific standards described in Section 5.8.4.3.1 of UCR 2008 Change 3 as applicable to Firewall products. JITC verified that the SUT has met the General Requirements. JITC verified that the SUT has met the requirements for Network Time Protocol Version 4 (NTP) by checking with Nessus Vulnerability scanning tool and the vendor demonstrating the version of NTP within their application. JITC verified that the SUT has the ability to push policy to the VPN client and the ability to monitor the client's activity. The SUT was managed from central place, clients, and servers. The SUT have more than five Ethernet ports, one pair for primary ingress and egress, one pair for backup, and one for Out of Band Management.

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

(3) Alarms and Alerts. Security Devices shall meet the appropriate product specific requirements for alarms and alerts described in Section 5.8.4.3.4 of UCR 2008 Change 3 as applicable to Firewall products. The SUT partially meet the Alarms and Alerts Requirements because the system does not inform administrators by generating an alarm message to the administrator's console session upon detection of potential security violation. However, the SUT does have the ability to generate alarms and alerts using Required Ancillary Equipment (RAE) and this finding is documented in a separate report, Reference (e).

(4) Audit and Logging. Security Devices shall meet the appropriate product specific requirements for audit and logging described in Section 5.8.4.3.5 of UCR 2008 Change 3 as applicable to Firewall products. JITC verified the SUT partially meet the Audit and Logging Requirements because the SUT's does not audit changes to files and folders through the command line. In spite of this, the SUT does log the requests at the web interface. The SUT has the ability to generate audit and logging using RAE and this finding has been documented in a separate report, Reference (e).

(5) Cryptography. Security Devices shall meet the appropriate product specific requirements for cryptography described in Section 5.8.4.3.8 of UCR 2008 Change 3 as applicable to Firewall products. JITC verified that all outgoing communication including the body of the communication is encrypted using WireShark Packet Analyzer tool for validation.

(6) Security Measures. Security Devices shall meet the appropriate product specific requirements for security measures as described in Section 5.8.4.3.9 of UCR 2008 Change 3 as applicable to Firewall products. JITC verified that the SUT partially meets the Security Requirements by successfully detecting Denial of Service, Ping of Death and SYN Flood types of attacks to its outside interface through penetration testing tools such as CoreImpact and Backtrack. The SUT does not enforce automatic expiration of passwords, password reuse and ensure password strength. Nonetheless, the SUT does have the ability to generate alarms and alerts using RAE and this finding is documented in a separate report, Reference (e).

(7) System and Communication Protection. Security Devices shall meet the appropriate product specific requirements for system and communication protection as described in Section 5.8.4.3.10 of UCR 2008 Change 3 applicable

to Firewall products. JITC verified the SUT has met the System and Communication Protection Requirements. JITC validated the SUT was able to protect all assigned interfaces from the data traffic that were not permitted.

(8) Other requirements. Security Devices shall meet the appropriate product specific requirements for other functional requirements as described in Section 5.8.4.3.11 of UCR 2008 Change 3 as applicable to Firewall products. JITC verified the SUT has met the Other Requirements. JITC validated the SUT rejects requests for access or services where the presumed source identity of the source subject is an external Information Technology (IT) entity on a broadcast network/loopback.

(9) Performance. Security Devices shall meet the appropriate product specific requirements for performance as described in Section 5.8.4.3.11 of UCR 2008 Change 3 as applicable to Firewall products. JITC verified the SUT has met the Performance Requirements. The SUT used commercial best practice defensive solution and maintain advertised normal packet loss rates for all legitimate data packets when under a SYN Flood attack with the use of Agilent N2X. The SUT does not degrade Internet Protocol (IP) version 4 (IPv4) and IP version 6 (IPv6) forwarding when used with a long access policy configuration using WireShark.

c. Functionality.

(1) Policy. Security Devices shall meet the appropriate product specific requirements for policy functionality as described in Section 5.8.4.4.1 of UCR 2008 Change 3 as applicable to Firewall products. JITC verified the SUT has met the Policy Requirements. The SUT enforces the policy pertaining to any indication of a potential security violation, configurable to perform actions based on different information policies and blocks replay of data as a default policy. The SUT has functionality to support the quota of Transmission Control Protocol connections. This functionality is implemented in the Service Policies for the management of network traffic.

(2) Filtering. Firewalls shall meet the appropriate product specific requirements for filtering as described in Section 5.8.4.4.2 of UCR 2008 Change 3. JITC verified that the SUT support and filter communication protocols / services from outside the perimeter of the interconnected Information Systems (IS) according to IS appropriate needs such as the ability to block on a per-interface basis, default to block and to disable.

d. IPv6.

The SUT met all critical CRs and FRs with testing and the vendor's Letter of Compliance (LoC).

11.3 Information Assurance. The SUT was tested by DISA IA test team and the IA findings are published in a separate report, Reference (e).

11.4 Other. None.

12. TEST AND ANALYSIS REPORT. In accordance with the Program Manager's request, JITC did not develop a detailed test report. JITC distributes interoperability information via the JITC Electronic Report Distribution system, which uses Unclassified-But-Sensitive Internet Protocol Router Network (NIPRNet) e-mail. More comprehensive IO status information is available via the JITC System Tracking Program (STP), which .mil/.gov users can access on the NIPRNet at <https://stp.fhu.disa.mil>. Test reports, lessons learned, and related testing documents and references are on the JITC Joint Interoperability Tool (JIT) at <http://jit.fhu.disa.mil>. Information related to Approved Product List (APL) testing is available on the DISA APL Testing and Certification website located at <http://www.disa.mil/Services/Network-Services/UCCO>. All associated test information is available on the DISA Unified Capability Coordination Office (UCCO) APL Integrated Tracking System website located at <https://aplits.disa.mil>.

(This page left intentionally blank.)

CAPABILITY AND FUNCTIONAL REQUIREMENTS

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

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

ID	Requirement	UCR Reference	FW
5.8.4.2 Conformance Requirements			
1.	The security device shall conform to all of the MUST requirements found in RFC 3948, "UDP Encapsulation of IPSec Packets."	5.8.4.2 (15)	NA
5.8.4.3 Information Assurance Requirements			
2.	The security device shall support SNMP3 and NTPv4.	5.8.4.3.1 (1)	R
3.	The security device shall provide ability to push policy to the VPN client and the ability to monitor the client's activity.	5.8.4.3.1 (2)	N/A
4.	The security device shall be managed from a central place, clients, and servers.	5.8.4.3.1 (3)	N/A
5.	The security device shall have three Ethernet ports, one for primary, one for backup, and one for OOBM.	5.8.4.3.1 (4)	R
6.	A CM process shall be implemented for hardware and software updates.	5.8.4.3.3 (1)	R
7.	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
8.	The security device shall disable the Proxy Address Resolution Protocol service, unless disabled by default.	5.8.4.3.3 (3)	R
9.	The security device shall disable the IP redirects notification service, except in type 3 cases.	5.8.4.3.3 (4)	R
10.	The security device shall disable the Maintenance Operations Protocol service in DEC equipment which uses that protocol to perform software loads.	5.8.4.3.3 (5)	O
11.	The security device shall disable the service source-routing	5.8.4.3.3 (6)	R
12.	The security device shall properly implement an ordered list policy procedure.	5.8.4.3.3 (7)	R
13.	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
14.	Security devices with local consoles shall have the capability to generate and display an alarm message at the local console upon detection of a potential security violation.	5.8.4.3.4 (2)	R
15.	The security device shall have the capability to generate an alarm message to a new remote administrator's console session if the original alarm has not been acknowledged following a potential security violation.	5.8.4.3.4 (3)	R
16.	The security device shall have the capability to provide proper notification upon detection of a potential security violation or forward event status data to a Network Management System that will take the appropriate action to include providing notification of the event.	5.8.4.3.4 (4)	N/A
17.	The security device shall have the capability to alert the administrator immediately, by displaying a message at the local and remote administrative consoles when an administrative session exists for each of the defined administrative roles.	5.8.4.3.4 (5)	N/A

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

ID	Requirement	UCR Reference	FW
18.	An automated, continuous online monitoring and audit trail creation capability is deployed with the capability to immediately alert personnel of any unusual or inappropriate activity with potential Information Assurance implications.	5.8.4.3.4 (6)	R
19.	The security device shall have an automated, continuous online monitoring and audit trail creation capability, which shall be deployed with a user configurable capability to disable the system automatically if serious Information Assurance violations are detected.	5.8.4.3.4 (7)	R
20.	The security device shall provide minimum recorded security-relevant events including any activity caught by the "deny all" rule at the end of the security device rule base.	5.8.4.3.5 (1)	R
21.	The security device shall generate an audit record of all failures to reassemble fragmented packets.	5.8.4.3.5 (2)	N/A
22.	The security device shall generate an audit record of all attempted uses of the trusted channel functions.	5.8.4.3.5 (3)	R
23.	The security device, when configured, shall log the event of dropping packets and the reason for dropping them.	5.8.4.3.5 (4)	R
24.	The security device shall log matches to filter rules that deny access when configured to do so.	5.8.4.3.5 (5)	R
25.	The security device shall record access or attempted access via security device to all program initiations and shutdowns that have security implications.	5.8.4.3.5 (6)	R
26.	The output of such intrusion/attack detection and monitoring tools shall be protected against unauthorized access, modification, or detection	5.8.4.3.5 (7)	R
27.	The security device shall log requests for access or services where the presumed source identity of the information received by the security device specifies a broadcast identity.	5.8.4.3.5 (8)	N/A
28.	The security device shall log SMTP traffic that contains source routing symbols (e.g., in the mailer recipient commands).	5.8.4.3.5 (9)	N/A
29.	The security device shall log requests in which the information received by the security device contains the route (set of host network identifiers) by which information shall flow from the source subject to the destination subject.	5.8.4.3.5 (10)	N/A
30.	The security device shall log an information flow between a source subject and a destination subject via a controlled operation if the source subject has successfully authenticated to the security device.	5.8.4.3.5 (11)	N/A
31.	The security device shall log an information flow between a source subject and a destination subject via a controlled operation if the information security attributes match the attributes in an information flow policy rule (contained in the information flow policy).	5.8.4.3.5 (12)	N/A
32.	The security device shall log data and audit events when a replay is detected.	5.8.4.3.5 (13)	N/A
33.	The security device shall be able to collect the following: Identification, Authentication, and Authorization events.	5.8.4.3.5 (14)	N/A
34.	The security device shall be able to collect data accesses.	5.8.4.3.5 (15)	N/A
35.	The security device shall be able to collect service requests.	5.8.4.3.5 (16)	N/A
36.	The security device shall be able to collect network traffic.	5.8.4.3.5 (17)	N/A
37.	The security device shall be able to collect security configuration changes.	5.8.4.3.5 (18)	N/A
38.	The security device shall be able to collect data introduction.	5.8.4.3.5 (19)	N/A
39.	The security device shall be able to collect detected malicious code.	5.8.4.3.5 (20)	N/A
40.	The security device shall be able to collect access control configuration.	5.8.4.3.5 (21)	N/A
41.	The security device shall be able to collect service configuration.	5.8.4.3.5 (22)	N/A
42.	The security device shall be able to collect authentication configuration.	5.8.4.3.5 (23)	N/A

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

ID	Requirement	UCR Reference	FW
43.	The security device shall be able to collect accountability policy configuration.	5.8.4.3.5 (24)	N/A
44.	The security device shall be able to collect detected known vulnerabilities.	5.8.4.3.5 (25)	N/A
45.	The security device shall provide authorized users with the capability to read the system data.	5.8.4.3.5 (26)	N/A
46.	The system shall prohibit access to security device data, except those users that have been granted explicit read access.	5.8.4.3.5 (27)	N/A
47.	At a minimum, the following confidentiality policy adjudication features shall be provided for each controlled interface. Encrypt, as needed, all outgoing communication including the body and attachment of the communication	5.8.4.3.8 (1)	N/A
48.	System mechanisms shall be implemented to enforce automatic expiration of passwords, to prevent password reuse, and to ensure password strength.	5.8.4.3.9 (1)	R
49.	Monitoring tools shall be used for the monitoring and detection of suspicious, intrusive, or attack-like behavior patterns to itself.	5.8.4.3.9 (2)	R
50.	The security device's controlled interface shall be configured such that its operational failure or degradation shall not result in any unauthorized release of information outside the Information Security (IS) perimeter nor result in any external information entering the IS perimeter	5.8.4.3.9 (3)	R
51.	Where scanning tools are available, the security device's internal hosts shall be scanned for vulnerabilities in addition to the security device itself to confirm an adequate security policy is being enforced.	5.8.4.3.9 (4)	R
52.	The security device must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with security device security functions. .	5.8.4.3.9 (5)	R
53.	The security device shall drop all packets with an IPv4 non-routable (RFC 1918) address originating from an external source.	5.8.4.3.9 (8)	R
54.	The security device shall drop all packets with an IPv4 source address of all zeros.	5.8.4.3.9 (9)	R
55.	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 (10)	R
56.	The security device shall differentiate between authorized and fraudulent attempts to upgrade the operating system, i.e., trying to upgrade system files with the wrong names.	5.8.4.3.9 (11)	R
57.	The security device shall differentiate between authorized and fraudulent attempts to upgrade the configuration, i.e., if a user trying to perform an upgrade that is not authorized that role.	5.8.4.3.9 (12)	R
58.	The security device shall pass traffic, which the security device has not identified as being a security problem, without altering the contents, except as necessary to perform functions such as Network Address Translation.	5.8.4.3.9 (13)	R
59.	The security device shall properly accept or deny User Datagram Protocol (UDP) traffic from port numbers based on policy.	5.8.4.3.9 (14)	R
60.	The security device shall properly accept or deny Transmission Control Protocol (TCP) traffic from port numbers based on policy.	5.8.4.3.9 (15)	R
61.	The security device shall not compromise its resources or those of any connected network upon initial start-up of the security device or recovery from an interruption in security device service.	5.8.4.3.9 (16)	R
62.	A security device shall properly enforce the TCP state.	5.8.4.3.9 (17)	R
63.	A security device shall properly accept and deny traffic based on multiple rules.	5.8.4.3.9 (18)	R
64.	A security device shall prevent all known network-based current attack techniques (Common Vulnerabilities and Exploits) from compromising the security device.	5.8.4.3.9 (19)	R
65.	A security device shall prevent the currently available Information Assurance Penetration techniques, as defined in DISA STIGS and Information Assurance Vulnerability Alerts from penetrating the security device.	5.8.4.3.9 (20)	R
66.	A security device shall block potentially malicious fragments.	5.8.4.3.9 (21)	R

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

ID	Requirement	UCR Reference	FW
67.	The security device shall mediate the flow of all information between a user on an internal network connected to the security device and a user on an external network connected to the security device and must ensure that residual information from a previous information flow is not transmitted.	5.8.4.3.9 (22)	R
68.	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
69.	The security device's controlled interface shall ensure that only traffic that is explicitly permitted (based on traffic review) is released from the perimeter of the interconnected Information System	5.8.4.3.10 (2)	R
70.	The security device shall reject requests for access or services where the presumed source identity of the source subject is an external Information Technology entity on a broadcast network.	5.8.4.3.11 (1)	R
71.	The security device shall reject requests for access or services where the presumed source identity of the source subject is an external Information Technology entity on the loopback network.	5.8.4.3.11 (2)	R
72.	The security device shall permit an information flow between a source subject and a destination subject via a controlled operation if the source subject has successfully authenticated to the security device.	5.8.4.3.11 (3)	R
73.	<p>The TSF shall permit an information flow between a controlled subject and another controlled subject via a controlled operation if the following rules hold:</p> <p>a. Subjects on an internal network can cause information to flow through the security device to another connected network if:</p> <p>(1) All the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;</p> <p>(2) The presumed address of the source subject, in the information, translates to an internal network address;</p> <p>(3) And the presumed address of the destination subject, in the information, translates to an address on the other connected network.</p> <p>b. Subjects on the external network can cause information to flow through the TOE to another connected network if:</p> <p>(1) All the information security attribute values are unambiguously permitted by the inform</p> <p>(2) The presumed address of the source subject in the information translates to an external network address;</p> <p>(3) And the presumed address of the destination subject in the information translates to an address on the other connected network</p>	5.8.4.3.11 (4)	R
74.	The security device, after a failure or service discontinuity, shall enter a maintenance mode where the ability to return the security device to a secure state is provided either through manual intervention or automatic reboot.	5.8.4.3.11 (5)	R
75.	The security device shall detect replay attacks using either security device data or security attributes.	5.8.4.3.11 (6)	N/A
76.	The security device shall reject data and audit events when a replay is detected.	5.8.4.3.11 (7)	N/A
77.	The security device shall ensure the security policy enforcement functions are invoked and succeed before each function within the security functions scope of control is allowed to proceed.	5.8.4.3.11 (8)	R
78.	The security device shall enforce System Administrator policy regarding Instant Messaging traffic.	5.8.4.3.11 (9)	R
79.	The security device shall enforce System Administrator policy regarding VVoIP traffic.	5.8.4.3.11 (10)	R
80.	Access Control shall include a Discretionary Access Control Policy.	5.8.4.3.11 (11)	R
81.	Discretionary Access Control access controls shall be capable of including or excluding access to the granularity of a single user.	5.8.4.3.11 (12)	R

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

ID	Requirement	UCR Reference	FW
82.	The security device's controlled interface shall review incoming information for viruses and other malicious code.	5.8.4.3.11 (13)	R
83.	The controlled interface shall provide the ability to restore its functionality fully in accordance with documented restoration procedures.	5.8.4.3.11 (14)	R
84.	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
85.	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
86.	The security device, as configured, must process new HTTP connections at the rate of the expected maximum number of connections as advertised by the vendor within a 1-minute period.	5.8.4.3.12 (3)	R
87.	The security device, as configured, must process new secure file transfer protocol connections at the rate of the expected maximum number of connections as advertised by the vendor within a 1-minute period.	5.8.4.3.12 (4)	R
88.	The security device shall employ a commercial best practice defensive solution along with maintain advertised normal operation packet loss rates for all legitimate data packets when under a SYN Flood attack.	5.8.4.3.12 (5)	R
89.	The security device must not degrade IPv4 and IPv6 forwarding when used with a long Access Policy configuration.	5.8.4.3.12 (6)	R
90.	The security device shall demonstrate a latency variance of less than 20 percent and a packet loss variance of less than 10 percent of the manufacturer specified nominal values for all operational conditions.	5.8.4.3.12 (7)	R
5.8.4.4 Functionality Requirements			
91.	The security device shall enforce the policy pertaining to any indication of a potential security violation.	5.8.4.4.1 (1)	R
92.	The security device shall be configurable to perform actions based on different information flow policies.	5.8.4.4.1 (2)	R
93.	The security device shall deny establishment of an authorized user session based on network source (i.e., source IP address) and time of day parameter values.	5.8.4.4.1 (3)	R
94.	The security device shall enforce the system administrator's specified maximum quota of transport-layer open connections that a source subject identifier can use over a specified period.	5.8.4.4.1 (4)	R
95.	The security device shall enforce the system administrator's policy options pertaining to network traffic violations to a specific TCP port within a specified period.	5.8.4.4.1 (5)	R
96.	The security device shall enforce the system administrator's policy options pertaining to violations of network traffic rules within a specified period.	5.8.4.4.1 (6)	R
97.	The security device shall enforce the system administrator's policy options pertaining to any security device-detected replay of data and/or nested security attributes.	5.8.4.4.1 (7)	R

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

ID	Requirement	UCR Reference	FW
98.	<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 UDP echo (port 7) (2) The service UDP discard (port 9) (3) The service UDP chargen (port 19) (4) The service UDP TCPMUX (port 1) (5) The service UDP daytime (port 13) (6) The service UDP time (port 37) (7) The service UDP supdup (port 95) (8) The service UDP sunrpc (port 111) (9) The service UDP loc-srv (port 135) (10) The service UDP netbios-ns (port 137) (11) The service UDP netbios-dgm (port 138) (12) The service UDP netbios-ssn (port 139) (13) The service UDP BootP (port 67) (14) The service UDP TFTP (port 69)(15) The service UDP XDMCP (port 177) (16) The service UDP syslog (port 514) (17) The service UDP talk (port 517) (18) The service UDP ntalk (port 518) (19) The service UDP MS SQL Server (port 1434) (20) The service UDP MS UPnP SSDP (port 5000) (21) The service UDP NFS (port 2049) (22) The service UDP Back Orifice (port 31337) (23) The service TCP tcpmux (port 1) (24) The service TCP echo (port 7) (25) The service TCP discard (port 9) (26) The service TCP systat (port 11) (27) The service TCP daytime (port 13) (28) The service TCP netstat (port 15) (29) The service TCP chargen (port 19) (30) The service TCP time (port 37) (31) The service TCP whois (port 43) (32) The service TCP supdup (port 95) (33) The service TCP sunrpc (port 111) (34) The service TCP loc-srv (port 135) (35) The service TCP netbios-ns (port 137) (36) The service TCP netbios-dgm (port 138) (37) The service TCP netbios-ssn (port 139) (38) The service TCP netbios-ds (port 445) (39) The service TCP rexec (port 512) (40) The service TCP lpr (port 515) (41) The service TCP uucp (port 540) (42) The service TCP Microsoft UPnP System Services Delivery Point (port 1900) (43) The service TCP X-Window System (ports 6000-6063) (44) The service TCP IRC (port 6667) (45) The service TCP NetBus (ports 12345-12346) (46) The service TCP Back Orifice (port 31337) (47) The service TCP finger (port 79) (48) The service TCP SNMP (port 161) (49) The service UDP SNMP (port 161) (50) The service TCP SNMP trap (port 162) (51) The service UDP SNMP trap (port 162) (52) The service TCP rlogin (port 513) (53) The service UDP who (port 513) 	5.8.4.4.2	R

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

ID	Requirement	UCR Reference	FW
98.	(54) The service TCP rsh, rcp, rdist, and rdump (port 514) (55) The service TCP new who (port 550) (56) The service UDP new who (port 550) (57) The service NTP (Network Time Protocol) (58) The service CDP (Cisco Discovery Protocol) (59) Voice and Video Services (AS-SIP), H.323, and RSVP (60) The service UDP SRTP (SRTCP) and RTCP (61) The service DSCP		
IPv6 Requirements			
99.	RFC 1981: Path MTU Discovery for IPv6	Table 5.3.5-7	R
100.	RFC 2407: The Internet IP Security Domain of Interpretation for ISAKMP	Table 5.3.5-7	C
101.	RFC 2408:ISAKMP (ISAKMP)	Table 5.3.5-7	C
102.	RFC 2409: The IKE	Table 5.3.5-7	C
103.	RFC 2460:IPv6 Specification	Table 5.3.5-7	R-2
104.	RFC 2464: Transmission of IPv6 Packets over Ethernet Networks	Table 5.3.5-7	R-3
105.	RFC 2474: Definition of the DS Field (DS Field) in the IPv4 and IPv6 Headers	Table 5.3.5-7	R-4
106.	RFC 2710: MLDv2 for IPv6	Table 5.3.5-7	R
107.	RFC 3162: RADIUS and IPv6	Table 5.3.5-7	C
108.	RFC 3986: URI: Generic Syntax	Table 5.3.5-7	C
109.	RFC 4007: IPv6 Scoped Address Architecture	Table 5.3.5-7	R
110.	RFC 4109: Algorithms for IKE Version 1 (IKEv1)	Table 5.3.5-7	C
111.	RFC 4213: Basic Transition Mechanisms for IPv6 Hosts and Routers	Table 5.3.5-7	R-1
112.	RFC 4291: IP Version 6 Addressing Architecture	Table 5.3.5-7	R
113.	RFC 4301: Security Architecture for the Internet Protocol	Table 5.3.5-7	C
114.	RFC 4302: IP Authentication Header C	Table 5.3.5-7	C
115.	RFC 4303: IP Encapsulating Security Payload	Table 5.3.5-7	C
116.	RFC 4443: ICMPv6 for the IPv6 Specification	Table 5.3.5-7	R
117.	RFC 4566 SDP: Session Description Protocol	Table 5.3.5-7	C
118.	RFC 4835 Cryptographic Algorithm Implementation Requirements for ESP and AH	Table 5.3.5-7	C
119.	RFC 4861 Neighbor Discovery for IPv6	Table 5.3.5-7	R
120.	RFC 4862 IPv6 Stateless Address Autoconfiguration	Table 5.3.5-7	C
121.	RFC 5095 Deprecation of Type 0 Routing Headers in IPv6	Table 5.3.5-7	R

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

NOTES:			
R-1:	Only meets the dual-stack requirements of this RFC.		
R-2:	Only meets IPv6 formatting requirements of this RFC.		
R-3:	Only meets framing format aspects of RFC.		
R-4:	Requirement covered in Section 5.3.3, WAN General System Requirements.		
LEGEND:			
AS-SIP	Assured Services Session initiation Protocol	IS	Information Security
BOOTP	Bootstrap Protocol	ISAKMP	Internet Security Association and Key Management Protocol
C	Conditional	MLD	Multicast Listener Discovery
CM	Configuration Management	MTU	Maximum Transmission Unit
DEC	Digital Equipment Corporation	N/A	Not Applicable
DISA	Defense Information Systems Agency	NTP	Network Time Protocol
DoD	Department of Defense	O	Optional
DoS	Denial of Service	OOBM	Out-of-Band Management
DS	Differentiated Services	R	Required
DSCP	Differentiated Services Code Point	RFC	Request For Comment
ESP	Encapsulating Security Payload	UDP	User Datagram Protocol
FIPS	Federal Information Processing Standards	SMTP	Simple Mail Transfer Protocol
FW	Firewall	SNMP	Simple Network Management Protocol
HTTP	Hypertext Transfer Protocol	STIGs	Security Technical Implementation Guide
ICMP	Internet Control Message Protocol	TCP	Transport Control Protocol
IEEE	Institute of Electrical and Electronics Engineers	TCPMUX	TCP Port Service Multiplexer
IKE	Internet Key Exchange	TFTP	Trivial File Transfer Protocol
IP	Internet Protocol	URI	Uniform Resource Identifier
IPS	Intrusion Protection System	VVoIP	Voice and Video over Internet Protocol
IPSec	Internet Protocol Security	VPN	Virtual Private Network
IPv4	Internet Protocol version 4	WAN	Wide Area Network