Changes to UCR 2008, Change 1, Section 5.8, Security Devices

Section 5.8 is added new with UCR 2008, Change 1, and therefore a Change Sheet is not applicable.

TABLE OF CONTENTS

SECTION **PAGE**

5.8 Security Devices Requirements 1459
5.8.1 Section Overview and Scope 1459
5.8.2 Security Device Requirements Structured Process 1459
5.8.3 Security Devices Information Assurance Design 1459
5.8.3.1 Physical Security 1459
5.8.3.2 Security Devices Security Design 1460
5.8.3.3 Network Component Interactions 1460
5.8.4 Requirements 1462
5.8.4.1 Introduction 1462
5.8.4.2 Conformance Requirements 1462
5.8.4.3 Information Assurance Requirements 1464
5.8.4.3.1 General Requirements 1464
5.8.4.3.2 Authentication (Includes Authorization and Access Control) 1466
5.8.4.3.3 Configuration Management 1470
5.8.4.3.4 Alarms and Alerts 1471
5.8.4.3.5 Audit and Logging 1472
5.8.4.3.6 Integrity 1479
5.8.4.3.7 Documentation 1480
5.8.4.3.8 Cryptography 1482
5.8.4.3.9 Security Measures 1484
5.8.4.3.10 Systems and Communication Protection 1486
5.8.4.3.11 Other Requirements 1487
5.8.4.3.12 Performance 1490
5.8.4.4 Functionality 1491
5.8.4.4.1 Policy 1491
5.8.4.4.2 Filtering 1492
5.8.4.5 IPS Functionality 1494

LIST OF FIGURES

FIGURE **PAGE**

5.8.3-1 Notional Example of Voice and Data ASLAN Segmentation.....1461

LIST OF TABLES

TABLE **PAGE**

5.8.4-1 Acronyms and Appliances Specifying Type of Component.....1462

5.8 SECURITY DEVICES REQUIREMENTS

5.8.1 Section Overview and Scope

This section describes the requirements for security devices that will be on the APL. This section currently contains both Information Assurance requirements and functional requirements for security devices. In future versions of the UCR, the Information Assurance requirements for security devices will be merged into Section 5.4, Information Assurance Requirements, with all other Information Assurance requirements. This version of the document contains requirements for firewalls, IPSs, and VPN devices. Future updates to this section will expand on the devices discussed.

5.8.2 Security Device Requirements Structured Process

This section provides an overview of the requirements process for security devices on the converged network.

5.8.3 Security Devices Information Assurance Design

5.8.3.1 Physical Security

Physical security is the responsibility of the installing B/P/C/S. There are essentially two sets of requirements associated with a complete UC system. The end points (i.e., PCs, EIs, CPE) have one set of physical security requirements while the network (LAN switches, security devices, and routers) and signaling products (i.e., LSC, MFSS, SS, MG) require another set of requirements. A full definition of physical security requirements is beyond the scope of this section.

Security devices are located in many different types of facilities. Their physical security is dependent upon the physical security afforded by the facility in which they are housed. The physical security of the facility is dependent upon the sensitivity and/or classification of the information that it contains or processes.

The physical security for the VVoIP product network infrastructure and signaling appliances must limit physical access to all the associated appliances and cable terminations. Sensitivity and/or classification of the product have no bearing on this requirement. This means that the supporting infrastructure for the total product must reside, minimally, behind locked doors. Again, as with the EIs, this is typically afforded by the facility in which the equipment/ infrastructure is housed (e.g., locks and/or access control on doors of rooms and closets housing the equipment). This, however, may be minimally provided by a lock on a cabinet housing a LAN switch in the open (i.e., unsecured area).

Facility security requirements fall under the purview of "DoD Traditional Security." These requirements are well beyond the scope of the UCR 2008.

Vendors must support their customer's need to comply with the DoD system physical security requirements for security devices. This support is to be provided in the form of locking kits for any equipment that the vendor normally provides in a cabinet. If a cabinet lock is not provided normally in the vendor's commercial offering, optional locking kits must be made available that work well with the vendor's cabinet. All cabinet locking mechanisms must be robust enough to resist prying the cabinet open.

5.8.3.2 Security Devices Security Design

Security devices use a defense in-depth approach that is based on best commercial practices. The product security defenses are categorized as follows and are discussed in Section 5.4, Information Assurance Requirements:

- User Roles
- Hardened Operating Systems
- Auditing
- Application Security
- Redundant Systems

Additional defenses may be added dependent on the specific threats associated with a product.

5.8.3.3 Network Component Interactions

One of the principal tenets of any Information Assurance design is the separation of components (i.e., traffic, appliances, and users) and/or services from each other based on their characteristics. Still, a converged network requires the opposite in that appliances within a converged network may service the voice, data, and video applications. As a result of this conflict, the interactions between the various component segments must be controlled to ensure that an attacker that gains access to one segment does not gain access to, nor can affect, the other segments. In addition, interaction control between various segments is also used to prevent configuration or user errors in one segment from affecting other segments. The actions of normal users of converged network services must not affect the other services, more specifically the voice service. The principal mechanisms that are used within this design for segmenting the network are VLANs, segmented IP address space or subnets, and VPNs and are used in combination with filters, access control lists (ACLs), and stateful packet inspection firewalls (VVoIP Stateful Firewalls) to control the flow of traffic between the VLANs and VPNs.

Figure 5.8.3-1, Notional Example of Voice and Data ASLAN Segmentation, presents the simplest type of converged LAN with only voice and data applications. Separate VLANs are

established between voice and data applications and the Layer 3 switches are responsible for providing access control between the different VLANs using filtering techniques, such as ACLs. In this type of deployment, appliances are classified as VVoIP appliances or data appliances and it may be possible to avoid deploying appliances that service both VVoIP and data appliances. At the CE Router, separate VPNs may be established, if necessary, to segment the voice traffic from the data traffic as the packets transit the DISN WAN. In addition, VPNs may be used to extend the local enclave to remote offices of the same organization, telecommuters, and travelers. Also, the VVoIP traffic is routed from the CE Router to the PE Router along the same path as the non-VVoIP traffic. The only connection to the PSTN is through a TDM interface using PRI or CAS signaling so that there is not interaction between the VVoIP system and commercial VVoIP IP networks. Moreover, it is important to note that the LSC has two separate interfaces; one for local NM and a second for the VoIP E2E NM traffic.

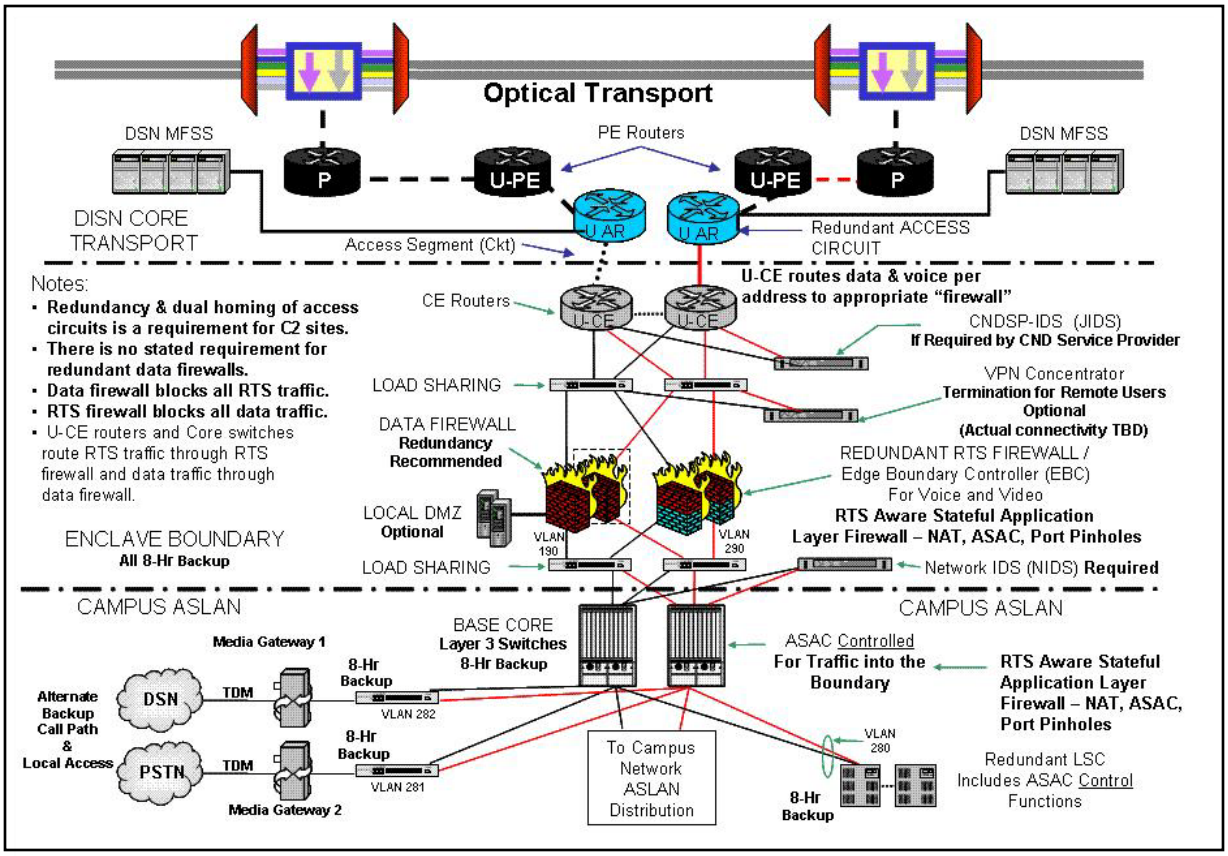

Figure 5.8.3-1. Notional Example of Voice and Data ASLAN Segmentation

5.8.4 Requirements

5.8.4.1 Introduction

Based on the UC Information Assurance design, threats, and countermeasures, a set of derived requirements were developed. Different vendors combine different functions into their appliances to meet the requirements of a particular type of product. For the purposes of UCR 2008, the requirements are levied on the individual appliance, as applicable, to secure the entire product. The terms user and customer are used in the same context as GR-815-CORE. It is understood that the Information Assurance design provides a high-level description of how the security services are applied to the appliance and how the appliances interact in a secure manner. In addition, the appropriate Security Technical Implementation Guides (STIGs) will further clarify how the Information Assurance design and requirements are implemented on the appliance. All Security devices shall comply with the Application Security STIG. Section 5.8, Security Devices Requirements, is intended to provide a level of security requirements consistent with the level of security requirements defined for the Global Information Grid (GIG), but adapted for the unique DoD UC environment consistent with the requirements in the UCR.

The requirement key words (i.e., Required, Conditional) are defined elsewhere in the UCR 2008. Failure to satisfy a requirement will result in a Category I, II, or III finding.

Finally, the derived requirements do not include all of the administrative requirements (nontechnical) associated with policy and the STIGs. For instance, if someone is required to administratively document something (e.g., waiver, pilot request), that requirement is not included. The acronyms and appliances used for specifying the type of component are shown in Table 5.8.4-1, Acronyms and Appliances Specifying Type of Component.

Table 5.8.4-1. Acronyms and Appliances Specifying Type of Component

ACRONYM	APPLIANCES
FW	Firewall
IPS	Intrusion Protection System
VPN	Virtual Private Network – concentrator and termination

5.8.4.2 Conformance Requirements

Security devices must conform to specific standards as described below:

1. **[Required: FW, IPS, VPN]** 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.

2. **[Required: FW]** The security device shall conform to all of the MUST requirements found in RFC 2409, "The Internet Key Exchange (IKE)."

3. **Reserved.**

4. **[Required: FW, IPS, VPN]** 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. **[Required: FW, IPS, VPN]** The security device shall conform to all of the MUST requirements found in RFC 3412, "Message Processing and Dispatching for Simple Network Management Protocol."

6. **[Required: FW, IPS, VPN]** The security device shall conform to all of the MUST requirements found in RFC 3413, "Simple Network Management Protocol Applications."

7. **[Required: FW]** The security device shall conform to all of the MUST requirements found in RFC 3585, "IPSec Configuration Policy Information Model."

8. **[Required: FW]** The security device shall conform to all of the MUST requirements found in RFC 3586, "IP Security Policy Requirements."

9. **[Required: FW]** The security device shall conform to all of the MUST requirements found in RFC 4302, "IP Authentication Header."

10. **[Required: FW]** The security device shall conform to all of the MUST requirements found in RFC 4303, "IP Encapsulating Security Payload (ESP)."

11. **[Required: FW]** 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)."

12. **[Required: FW]** The security device shall conform to all of the MUST requirements found in RFC 4306, "Internet Key Exchange (IKEv2) Protocol."

13. **[Required: FW]** 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)."

14. **[Required: FW]** The security device shall conform to all of the MUST requirements found in RFC 4308, "Cryptographic Suites for IPSec."

15. **[Required: FW]** 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)."

16. **[Required: FW]** The security device shall conform to all of the MUST requirements found in RFC 2473, "Generic Tunneling."

17. **[Required: FW]** The security device shall conform to all of the MUST requirements found in RFC 4301, "Security Architecture for the Internet Protocol."

18. **[Required: FW]** The security device shall conform to all of the MUST requirements found in RFC 3948, "UDP Encapsulation of IPsec Packets."

19. **[Required: FW]** The security device shall conform to all of the MUST requirements found in RFC 3947, "Negotiation of NAT-Traversal in the IKE."

5.8.4.3 Information Assurance Requirements

5.8.4.3.1 General Requirements

1. **[Required: FW, IPS, VPN]** 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).

2. **[Required: FW, IPS, VPN]** The developer shall provide a statement about the source country for each software module/capability within the device.

3. **[Required: FW, IPS, VPN]** 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.

4. **[Required: FW, IPS, VPN]** 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. **[Required: FW, IPS, VPN]** Software patches shall only be installed if they originate from the system manufacturer and are applied in accordance with manufacturer's guidance.

    a. **[Required: FW, IPS, VPN]** 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.

6. **[Conditional: FW, IPS, VPN]** 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 their product then this requirement is met. An example of unsupported software is Windows™ NT, which is no longer supported by Microsoft® and it is unlikely that a vendor would support this operating system as part of its system.

    a. **[Required: FW, IPS, VPN]** 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.

7. **[Required: FW, IPS, VPN]** The system shall only use mobile code technologies (e.g., JavaScript, VBScript, and ActiveX) in accordance with the current DoD Mobile Code Policy.

8. **[Required: FW, IPS, VPN]** The system shall be capable of being located in physically secure areas.

9. **[Conditional: FW, IPS, VPN]** The system shall be capable of enabling password protection of BIOS settings if they are configurable.

10. **[Required: FW, IPS, VPN]** The system shall be capable of disabling the ability to boot from a removable media.

11. **[Required: FW, IPS, VPN]** The system shall be capable of using a static IP address.

12. **[Required: FW, IPS, VPN]** 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.

13. **[Required: FW, IPS]** The security device shall support SNMPv3 and NTPv4.

14. **[Optional: FW, IPS]** 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.

15. **[Required: FW, VPN]** Hot standard failover capability using a proven reliability protocol.

16. **[Required: VPN]** The ability to push policy to the VPN Client and the ability to monitor the client's activity.

17. **[Required: VPN]** The security device shall be managed from a central place, clients, and servers.

18. **[Required: FW, ISP, VPN]** The security device shall implement NTP to ensure times are synchronized.

19. **[Required: FW]** The security device shall have three Ethernet ports, one for primary, one for backup, and one for OOBM.

5.8.4.3.2 Authentication (Includes Authorization and Access Control)

5.8.4.3.2.1 Roles and Functions

Security administration of complex networks is made easier by the introduction of roles. Role-based Access Control (RBAC) has become the predominant model for advanced access control because it reduces the complexity and cost of security administration in large networked architectures. Security Administrators can assign roles specific tasks and limit privileges. Users are assigned roles based upon their responsibilities.

1. **[Required: FW, IPS, VPN]** The security device shall associate users with roles.

    a. **[Required: FW, IPS, VPN]** The security device shall employ Role-Based Access Control (RBAC) in the local and remote administration of all device functions and operations..)

b. **[Required: FW, IPS, VPN]** The security device shall associate all user security attributes with an authorized user.

c. **[Required: FW, IPS, VPN]** 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)

d. **[Required: FW, IPS, VPN]** 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

e. **[Required: FW, IPS, VPN]** The security device shall ensure all administrators can review the audit trail associated with their role.

f. **[Required: FW, IPS, VPN]** The security device shall ensure all roles can perform their administrative roles on the security device locally.

g. **[Required: FW, IPS, VPN]** The security device shall ensure all roles can perform their administrative roles on the security device remotely.

2. **[Required: FW, IPS, VPN]** The ability to perform the following functions shall be restricted to an Administrator defined or predefined (i.e., default) access control user role: to cryptography security data and/or the time/date method used for forming time stamps.

a. **[Required: FW, IPS, VPN]** 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.

b. **[Required: FW, IPS, VPN]** 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.

c. **[Required: FW, IPS, VPN]** 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.

3. **[Required: FW, IPS, VPN]** The security device shall restrict the ability to determine the administrator-specified network identifier.

5.8.4.3.2.2 Identification and Authentication

Identification and Authentication is the process of validating provenance in access control. While it is not possible to "prove" identity across ISs, there are tests that are considered acceptable. These tests fall into three categories based on what the user knows (passwords), what the user has (tokens), and what the user is (biometrics). Combinations of these account for multifactor authentication. Authorization is the process of defining the rights of a user once identity and authentication are validated.

1. **Reserved.**

2. **[Required: FW, IPS, VPN]** 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+.

3. **[Required: FW, IPS, VPN]** The security device shall provide a local authentication mechanism to perform user authentication.

4. **Reserved.**

5. **[Required: FW, IPS, VPN]** The security device shall only allow authorized security personnel to configure alert mechanisms.

6. **[Required: FW, IPS, VPN]** 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.

7. **[Required: FW, IPS, VPN]** DoD IS access shall be gained through the presentation of an individual identifier and password.

8. **[Required: FW, IPS, VPN]** 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.

9. **[Required: FW, IPS, VPN]** The security device shall be able to use at least one external authentication method (e.g., RADIUS, TACACS+, and/or LDAP).

10. **Reserved.**

11. **[Required: FW, IPS, VPN]** Identification and Authentication management mechanisms shall include, in the case of communication between two or more systems (e.g., client server architecture), bidirectional authentication between the two systems.

12. **[Required: FW, IPS, VPN]** 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..

13. **[Required: FW, IPS, VPN]** Enforcement of session controls shall include system actions on unsuccessful log-ons (e.g., blacklisting of the terminal or user identifier).

14. **[Required: FW, IPS, VPN]** 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.

15. **[Required: FW, IPS, VPN]** 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).

16. **[Required: FW, IPS, VPN]** 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.

17. **Reserved.**

18. **Reserved.**

19. **[Required: IPS, VPN]** 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.

5.8.4.3.3 Configuration Management

This section assures the ability to administer the security device in a manner consistent with best practices. It does not mandate a specific configuration for security devices.

1. **[Required: FW, IPS, VPN]** A CM process shall be implemented for hardware and software updates.

2. **[Required: FW, IPS, VPN]** The CM system shall provide an automated means by which only authorized changes are made to the security device implementation.

3. **[Required: FW, IPS, VPN]** The security device shall disable the Proxy Address Resolution Protocol (ARP) service, unless disabled by default.

4. **[Required: FW, IPS, VPN]** The security device shall have the capability to disable the ICMP destination unreachable notification on external interfaces.

5. **[Required: FW, IPS, VPN]** The security device shall disable IP redirection capability.

6. **[Optional: FW, IPS, VPN]** The security device shall disable the Maintenance Operations Protocol (MOP) service in DEC equipment which use that protocol to perform software loads.

7. **[Required: FW, IPS, VPN]** The security device shall be capable of shutting down any unused interfaces as determined by the administrator.

8. **[Required: FW, VPN]** The security device shall disable the service source-routing.

9. **[Required: FW, IPS, VPN]** The security device shall properly implement an ordered list policy procedure.

10. **[Required: FW, IPS]** 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.

11. **[Required: FW, IPS]** 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.

5.8.4.3.4 Alarms and Alerts

This section mandates the need for security devices to inform administrators that an event has occurred.

1. **[Required: FW, IPS]** 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.

2. **[Optional: FW, IPS, VPN]** 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.

3. **[Required: FW, IPS, VPN]** The security device shall have the capability to generate an alarm message to a remote administrator console upon detection of a potential security violation.

4. **[Required: FW, IPS, VPN]** 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. **[Required: IPS]** 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.

6. **[Required: IPS]** 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.

7. **[Required: IPS]** The security device shall have the capability to provide proper notification of the audit trail exceeding a set percentage of the device storage capacity..

8. **[Required: FW, IPS, VPN]** 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.

9. **[Required: IPS]** 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.

10. **[Required: FW, IPS, VPN**] 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.

11. **[Required: FW, IPS, VPN]** The security device shall have the capability to configure the timing of alarms and their escalation based upon type and severity of event.

5.8.4.3.5 Audit and Logging

This section requires a security device to produce records that forensics examiners can use to trace intrusions and other security events. It also mandates the records will be protected against malicious alteration.

1. **[Required: FW, IPS, VPN**] 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.

2. **[Required: FW, IPS, VPN**] The security device shall generate an audit record of each start-up and shutdown of the audit function.

3. **[Required: FW, IPS, VPN**] 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.

4. **[Required: FW, IPS, VPN**] The security device shall generate an audit record of any modification to the audit trail.

5. **[Required: FW, IPS, VPN**] The security device shall generate an audit record of any unsuccessful attempts to read information from the audit records.

6. **[Required: FW, IPS, VPN**] The security device shall generate an alarm or warning message upon detection of audit activity failures.

7. **[Required: FW, IPS, VPN**] The security device shall generate an audit record of all actions taken due to exceeding the audit threshold.

8. **[Required: FW, IPS, VPN]** The security device shall generate an alarm or warning message upon detection of an audit storage failure.

9. **[Required: FW, IPS]** 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.

10. **[Required: FW, IPS, VPN]** The security device shall provide a means to store audit records to a dedicated server on the internal network.

11. Reserved.

12. **[Required: FW, IPS, VPN]** The security device shall generate an audit record of all failures of cryptographic operations.

13. **[Required: IPS]** The security device shall generate an audit record of all failures to reassemble fragmented packets.

14. **[Required: FW, IPS, VPN]** 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.

15. **[Required: FW, IPS, VPN]** The security device shall generate an audit record of all use of authentication and user identification mechanisms.

16. **[Required: FW, IPS]** The security device shall generate an audit record of attempts to bind user security attributes to a subject.

17. **[Required: FW, IPS, VPN]** The security device shall generate an audit record of all modifications to the security functions of the security device.

18. **[Required: FW, IPS, VPN]** The security device shall generate an audit record of all enabling or disabling of the key generation self-tests.

19. **[Required: FW, IPS, VPN]** The security device shall generate an audit record of all modifications of the values of the security device data by the administrator.

20. **[Required: FW, IPS, VPN]** The security device shall generate an audit record of all Administrator actions and/or privileged activities.

21. **Reserved.**

22. **Reserved.**

23. **Reserved.**

24. **Reserved.**

25. **Reserved.**

26. **Reserved.**

27. **Reserved.**

28. **Reserved.**

29. **Reserved.**

30. **Reserved.**

31. **Reserved.**

32. **[Required: FW, IPS, VPN]** The security device shall generate an audit record of all attempted uses of the trusted channel functions.

33. **[Required: FW, IPS, VPN]** The security device shall provide the administrator with the capability to read all audit data from the audit record.

34. **[Required: FW, IPS, VPN]** The security device shall prohibit all users read access to the audit records in the audit trail, except an administrator.

35. **[Required: FW]** The security device, when configured, shall log the event of dropping packets and the reason for dropping them.

36. **[Required: FW, IPS, VPN]** The security device shall log changes to the configuration.

37. **[Required: FW, IPS]** The security device shall log matches to filter rules that deny access when configured to do so.

38. **[Required: FW, IPS, VPN]** The security device shall log hardware changes since the last maintenance cycle when configured to do so.

39. **[Required: FW, IPS, VPN]** The security device shall log new physical connections made to the security device.

40. **[Required: FW, IPS, VPN]** The security device shall prevent modifications to the audit records in the audit trail.

41. **[Required: FW, VPN]** The security device shall record access or attempted access via security device to all program initiations and shutdowns that have security implications.

42. **[Required: FW, IPS, VPN]** Audit records shall include connection attempts to the security device.

43. **[Required: FW, IPS, VPN]** 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.

44. **[Required: FW, IPS, VPN]** 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.

45. **[Required: FW, IPS, VPN]** The security device shall record access or attempted access via controlled interfaces to objects or data whose labels are inconsistent with user privileges.

46. **[Required: FW, IPS, VPN]** 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.

47. **[Required: FW, IPS, VPN]** The output of such intrusion/attack detection and monitoring tools shall be protected against unauthorized access, modification, or detection.

48. **[Required: FW, IPS, VPN]** Audit procedures that include the existence and use of audit reduction and analysis tools shall be implemented.

49. **[Required: FW, IPS, VPN]** Tools shall be available for the review of audit records and for report generation from audit records.

50. **[Required: FW, IPS, VPN]** 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 event

    f. Successful and unsuccessful log-ons

    g. Denial of access resulting from 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

51. **[Required: IPS]** 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.

52. **[Required: FW, IPS, VPN]** The level of events/information audited by the security device shall be configurable.

53. **[Required: IPS]** The security device shall log SMTP traffic that contains source routing symbols (e.g., in the mailer recipient commands).

54. **[Required: FW, IPS, VPN]** 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.

55. **[Required: FW, IPS, VPN]** 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.

56. **[Required: FW, IPS, VPN]** 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.

57. **[Required: IPS]** 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.

58. **[Required: IPS]** 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.

59. **Reserved.**

60. **[Required: IPS, VPN]** 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).

61. **[Required: IPS, VPN]** The security device shall log data and audit events when a user session authentication replay attack is detected.

62. **[Required: IPS, VPN]** The security device shall be able to collect the following: Start-up and Shutdown events.

63. **[Required: IPS, VPN]** The security device shall be able to collect the following: Identification, Authentication, and Authorization events.

64. **[Required: IPS, VPN]** The security device shall be able to collect the following: Data Accesses.

65. **[Required: IPS, VPN]** The security device shall be able to collect the following: Service Requests.

66. **[Required: IPS, VPN]** The security device shall be able to collect the following: Network traffic.

67. **[Required: IPS, VPN]** The security device shall be able to collect the Security configuration changes.

68. **[Required: IPS, VPN]** The security device shall be able to collect the following: Data introduction.

69. **[Required: IPS]** The security device shall be able to collect the following: Detected malicious code.

70. **[Required: IPS, VPN]** The security device shall be able to collect the following: Access control configuration.

71. **[Required: IPS, VPN]** The security device shall be able to collect the following: Service configuration.

72. **[Required: IPS, VPN]** The security device shall be able to collect the Authentication configuration.

73. **[Required: IPS, VPN]** The security device shall be able to collect the following: Accountability policy configuration.

74. **[Required: IPS, VPN]** The security device shall be able to collect the following: Detected known vulnerabilities.

75. **[Required: IPS, VPN]** The security device shall provide authorized users with the capability to read the system data.

76. **[Required: IPS, VPN]** The system shall prohibit access to security device data, except those users that have been granted explicit read access.

77. **[Required: FW, IPS, VPN]** 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

78. **[Required: FW, IPS, VPN]** 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.

79. **[Required: FW, IPS, VPN]** The security device shall be able to offload audit logs to external SYSLOG RAE.

5.8.4.3.6 Integrity

Integrity is protection against unauthorized modification or destruction of information.

1. **[Required: FW,]** The security device, when acting as an IPSec Gateway, will perform Authentication Header key checks.

2. **[Required: FW, IPS, VPN]** The security device shall use industry-accepted integrity mechanisms such as parity checks and cyclic redundancy checks (CRCs).

3. **[Required: FW, IPS, VPN]** 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.

4. **[Required: FW, IPS, VPN]** System initialization, shutdown, and aborts shall be configured to ensure that the system remains in a secure state.

5. **[Required: FW, IPS, VPN]** 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).

6. **[Required: IPS, VPN]** Data and software storage integrity protection, including the use of strong storage integrity mechanisms (e.g., integrity locks, encryption) shall be employed.

7. **[Required: IPS, VPN]** 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.

5.8.4.3.7 Documentation

This section requires documents that show a firewall was designed and implemented using best current practices. Additionally, administrative and user guides are required to ensure the firewall is delivered to sites with the documentation needed to properly secure the enclave.

1. **[Required: FW, IPS, VPN]** 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.

2. **[Required: FW, IPS, VPN]** The developer shall provide administrator guidance addressed to system administrative personnel (e.g., Administrator's Guide).

3. **[Optional: FW, IPS, VPN]** 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.

4. **[Required: FW, IPS, VPN]** The developer shall provide the architectural design of the security device.

5. **[Required: FW, IPS, VPN]** The developer shall provide a functional specification of the security device.

6. **[Required: FW, IPS, VPN]** The developer shall perform strength of security device analysis for each mechanism identified in the Security Target as having strength of security device claim.

7. **[Required: FW, IPS, VPN]** The developer shall provide an analysis of the test coverage.

8. **[Required: FW, IPS, VPN]** The developer shall provide covert channel analysis documentation identifying any covert channels detected along with alternative strategies for mitigating any associated vulnerabilities..

9. **[Required: FW, IPS, VPN]** 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.

10. **[Required: FW, IPS, VPN]** The reference document for the security device shall be unique to each version of the security device.

11. **[Required: FW, IPS, VPN]** The security device shall be labeled with its reference information i.e. model and version number.

12. **[Required: FW, IPS, VPN]** The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

13. **[Required: FW, IPS, VPN]** The CM system shall provide measures such that only authorized changes are made to the configuration items.

14. **[Required: FW, IPS, VPN]** The guidance documentation shall list all assumptions about the intended environment.

15. **[Required: FW, IPS, VPN]** The system shall demonstrate a procedure for accepting and acting upon user reports of potential security flaws and requests for corrections to those flaws.

16. **[Required: FW, IPS, VPN]** The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the security device.

17. **[Required: FW, IPS, VPN]** 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.

18. **[Required: FW, IPS, VPN]** The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

19. **[Required: FW, IPS, VPN]** The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections, and guidance on corrective actions to security device users.

20. **[Required: FW, IPS, VPN]** The procedures for processing reported security flaws shall ensure that any reported flaws are corrected and the correction issued to security device users.

21. **[Required: FW, IPS, VPN]** The developer shall perform a vulnerability analysis.

22. **[Required: FW, IPS, VPN]** The vulnerability analysis documentation shall describe the disposition of identified vulnerabilities.

23. **[Required: FW, IPS, VPN]** The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the security device.

24. **[Required: FW, IPS, VPN]** The vulnerability analysis documentation shall justify that the security device, with the identified vulnerabilities, is resistant to obvious penetration attacks.

25. **[Required: FW, IPS, VPN]** The installation, generation, and start-up documentation shall describe all the steps necessary for secure installation, generation, and start-up of the security device.

26. **[Required: FW, IPS, VPN]** The administrator guidance shall describe recovery procedures and technical system features to assure that system recovery is done in a trusted and secure manner.

5.8.4.3.8 Cryptography

This section specifies that the cryptographic functions such as IPSec performed by a security device such as a firewall, IPS, and/or VPN must be done in a known secure manner. It must also protect its cryptologic functions in accordance with NIST developed FIPS 140-2.

1. **[Optional: FW, IPS, VPN]** Security devices that provide encryption services shall be FIPS 140-2, Level 2 compliant..

2. **[Required: VPN]** 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.

3. **[Optional: FW, IPS, VPN]** Management Interfaces implemented with web servers shall implement secure web technology (e.g., Secure Sockets Layer; Secure HTTP) where capable.

4. **[Optional: FW, IPS, VPN]** 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. **[Required: FW, IPS, VPN]** Remote access shall use encryption to protect the confidentiality of the session.

6. **[Required: FW, IPS, VPN]** 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.

7. **[Required: FW, IPS, VPN]** The security device shall run the specific set of key-generation self-tests procedures provided by the FIPS 140-2 cryptographic module immediately after the generation of a cryptographic key.

8. **[Required: FW, IPS, VPN]** 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

9. **[Required: FW, IPS, VPN]** The security device shall use encryption to provide a trusted communication channel between itself 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.

10. **[Required: FW, IPS, VPN]** 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.

11. **[Optional: FW, IPS, VPN]** 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.

12. **Reserved.**

13. **Reserved.**

14. **[Required: FW, IPS, VPN]** Minimum hash is HMAC-SHA1.

15. **[Required: FW, IPS, VPN]** 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.

5.8.4.3.9 Security Measures

This section enumerates various measures that make the security device and its environment more secure.

1. **[Required: FW, IPS, VPN]** Passwords shall be changed at least annually employing system mechanisms that enforce current DoD password complexity policies.

2. **[Required: FW, IPS, VPN]** Passwords shall be encrypted both for storage and for transmission.

3. **[Required: FW, IPS, VPN]** The security device shall prevent the downloading of mobile code or executable content to itself.

4. **[Required: FW, IPS, VPN]** Monitoring tools shall be used for the monitoring and detection of suspicious, intrusive, or attack-like behavior patterns to itself.

5. **[Required: FW, IPS, VPN]** 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.

6. **[Required: FW, IPS, VPN]** DoD ISs shall comply with DoD ports, protocols, and services guidance.

7. **[Required: FW, IPS, VPN]** 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.

8. **[Required: FW, IPS, VPN]** The security device must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with security device security functions.

9. **[Required: FW]** The security device shall block unauthorized directed broadcasts from external networks (Distributed Denial of Service defense).

10. **[Required: FW]** The security device shall verify reverse path unicast addresses (Distributed Denial of Service defense) and be able to drop packets that fail verification.

11. **[Required: FW, IPS, VPN]** The security device shall drop all packets with an IPv4 non-routable (RFC 1918) address originating from an external source.

12. **[Required: FW, IPS, VPN]** The security device shall drop all packets with an IPv4 source address of all zeros.

13. **[Required: FW, IPS, VPN]** The security device shall drop all traffic from the internal network that does not use a legitimate internal address range as its source address.

14. **[Required: FW, IPS]** 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.

15. **[Required: FW, IPS]** 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.

16. **[Required: FW, IPS]** The security device shall pass traffic, which the security device has not identified as being a security problem, without altering the contents.

17. **[Required: FW, IPS]** The security device shall properly accept or deny User Datagram Protocol (UDP) traffic from port numbers based on policy.

18. **[Required: FW, IPS]** The security device shall properly accept or deny TCP traffic from port numbers based on policy.

19. **[Required: FW]** 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.

20. **[Required: FW]** A security device shall properly enforce TCP state.

21. **[Required: FW]** A security device shall properly accept and deny traffic based on multiple rules.

22. **[Required: FW, IPS]** A security device shall prevent all known network-based current attack techniques (Common Vulnerabilities and Exploits) from compromising the security device.

23. **[Required: FW, IPS, VPN]** A security device shall prevent the currently available Information Assurance Penetration techniques, as defined in DISA STIGS and IAVAs from penetrating the security device.

24. **[Required: FW, IPS]** A security device shall block potentially malicious fragments.

25. **[Required: FW, IPS]** 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.

26. **[Required: FW, IPS]** The security device shall not contain unauthorized compilers, editors, and other program development tools on its operational security device systems.

5.8.4.3.10 Systems and Communication Protection

These requirements enforce the security of individual systems and the communication paths.

1. **[Required: FW]** Each controlled interface shall be configured to ensure that all (incoming and outgoing) communications protocols, services, and communications not explicitly permitted are prohibited

2. **[Required: FW]** 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.

3. **[Required: FW]** 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.

4. **Reserved.**

5. **[Required: FW]** The security device's controlled interface enforces configurable thresholds to determine whether all network traffic can be handled and controlled.

6. **Reserved.**

7. **[Required: FW, IPS, VPN]** 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.

5.8.4.3.11 Other Requirements

This section provides other functional requirements for the firewall that are not listed in previous sections.

1. **Reserved.**

2. **Reserved.**

3. **Reserved.**

4. **Reserved.**

5. **[Required: FW, IPS, VPN]** 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.

6. **[Required: FW, VPN]** 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.

7. **Reserved.**

8. **Reserved.**

9. **[Required: FW, IPS, VPN]** 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.

10. **[Required: FW]** 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;

(2) The presumed address of the source subject, in the information, translates to an external network address;

(3) And the presumed address of the destination subject, in the information, translates to an address on the other connected network.

11. **[Required: FW, IPS, VPN]** 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.

12. **[Required: IPS, VPN]** The security device shall detect replay attacks using either security device data or security attributes.

13. **[Required: IPS]** The security device shall reject data and audit events when a replay is detected.

14. **[Required: FW, IPS, VPN]** 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.

15. **Reserved.**

16. **[Required: FW, IPS, VPN]** The security device shall lock a local interactive session after a System Administrator-specified time periods of inactivity by clearing or overwriting display devices and making the current contents unreadable.

17. **[Required: FW, IPS, VPN]** 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.

18. **[Required: FW, IPS, VPN]** 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.

19. **[Required: FW, IPS, VPN]** 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.

20. **[Required: FW, IPS, VPN]** The security device shall terminate a remote session after a System Administrator-configurable time interval of session inactivity.

21. **[Required: FW, IPS, VPN]** The security device shall enforce System Administrator policy regarding Instant Messaging traffic.

22. **[Required: FW, IPS, VPN]** The security device shall enforce System Administrator policy regarding VVoIP traffic.

23. **[Required: FW, IPS, VPN]** The security device features or capabilities not required for security device operation shall be disabled to eliminate exposure to possible security vulnerabilities.

24. **Reserved.**

25. **[Required: FW, IPS, VPN]** Access Control shall include a Discretionary Access Control (DAC) Policy.

26. **[Required: FW, IPS, VPN]** Discretionary Access Control access controls shall be capable of including or excluding access to the granularity of a single user.

27. **[Required: FW, IPS, VPN]** The security device's controlled interface shall review incoming information for viruses and other malicious code.

28. **[Required: FW, IPS, VPN]** 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.

29. **[Required: FW, IPS, VPN]** 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.

30. **[Required: FW, IPS, VPN]** The controlled interface shall provide the ability to fully restore its functionality in accordance with documented restoration procedures.

31. **[Required: FW, IPS, VPN]** 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.

32. **Reserved.**

5.8.4.3.12 Performance

Security without performance brings productivity to a standstill. Firewalls are intended to mitigate the threats enclaves face from external sources while permitting transmission of legitimate traffic in both directions. Performance tests attempt to validate a security devices' ability to maintain that legitimate traffic stream while the network is under attack.

1. **[Required: FW, IPS, VPN]** 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).

2. **[Required: FW, IPS, VPN]** 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.

3. **Reserved.**

4. **[Required: FW, IPS, VPN]** 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. **Reserved.**

6. **[Required: FW, IPS, VPN]** 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.

7. **Reserved.**

8. **Reserved**.

9. **Reserved**.

10. **[Required: FW, IPS, VPN]** 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.

11. **[Required: FW, VPN]** The security device must not degrade IPv4 and IPv6 forwarding when used with a long Access Policy configuration.

12. **[Required: FW]** he 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.

5.8.4.4 Functionality

5.8.4.4.1 Policy

This section identifies the need for a security device to respond to policy-based actions set by a System Administrator. While not mandating specific options, the System Administrator should have a granular control of the security device. Options of responses the security device could perform due to specific acts might include:

- Cease to operate (fail to secure)
- Terminate encrypted connections, and/or
- Send alerts via console message

1. **[Required: FW, VPN]** The security device shall enforce the policy pertaining to a specified number of encryption failures.

2. **[Required: FW, VPN]** The security device shall enforce the policy pertaining to a specified number of decryption failures.

3. **[Required: FW, VPN]** The security device shall enforce the policy pertaining to any indication of a potential security violation.

4. **[Required: FW, VPN]** The security device shall be configurable to perform actions based upon different information flow policies.

5. **[Required: FW, VPN]** 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.

6. **[Required: FW]** 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.

7. **[Required: FW, VPN]** 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.

8. **[Required: FW, VPN]** The security device shall enforce the System Administrator's policy pertaining to violations of network traffic rules within a specified period of time.

9. **[Required: FW, VPN]** The security device shall enforce the System Administrator's policy pertaining to any security device-detected replay of data and/or nested security attributes.

5.8.4.4.2 Filtering

[Required: FW] 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:

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.

    a. Will apply to the following defined services:
        (1) The service UDP echo (port 7)
        (2) The service UDP discard (port 9)
        (3) The service UDP chargen (port 19)
        (4) The service UDP TCPMUX (port 1)
        (5) The service UDP daytime (port 13)
        (6) The service UDP time (port 37)
        (7) The service UDP supdup (port 95)
        (8) The service UDP sunrpc (port 111)
        (9) The service UDP loc-srv (port 135)
        (10) The service UDP netbios-ns (port 137)
        (11) The service UDP netbios-dgm (port 138)
        (12) The service UDP netbios-ssn (port 139)
        (13) The service UDP BootP (port 67)

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

(55) The service TCP new who (port 550)
(56) The service UDP new who (port 550)
(57) The service NTP (Network Time Protocol)
(58) The service CDP (Cisco Discovery Protocol)
(59) Voice and Video Services (AS-SIP), H.323, and RSVP)
(60) The service UDP SRTP (SRTCP) and RTCP
(61) The service DSCP

5.8.4.5 IPS Functionality

1. **[Required: IPS]** The security device shall detect and protect against a focused method of attack: Footprinting and Scanning.

2. **[Required: IPS]** The security device shall detect and protect against a focused method of attack: Enumeration.

3. **[Required: IPS]** The security device shall detect and protect against a focused method of attack: Gaining Access.

4. **[Required: IPS]** The security device shall detect and protect against a focused method of attack: Escalation of Privilege.

5. **[Required: IPS]** The security device shall detect and protect against a focused method of attack: Maintaining Access.

6. **[Required: IPS]** The security device shall detect and protect against a focused method of attack: Network Exploitation.

7. **[Required: IPS]** The security device shall detect and protect against a focused method of attack: Cover Tracks.