Changes to UCR 2008, Change 2, Section 5.8, Security Devices Requirements

SECTION	CORRECTION	EFFECTIVE DATE
Throughout	Moved Information Assurance-specific Requirements to Section 5.4, Information Assurance Requirements	Immediately
5.8.4.6	Added IPS VVoIP Signal and Media Inspection Requirements	Immediately
5.8.4.7	Added Integrated Security Systems	Immediately
5.8.4.8	Added Information Assurance Tools	Immediately
5.8.4.9	Added Network Access Controllers	Immediately

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

SECTION **PAGE**

LIST OF FIGURES

FIGURE **PAGE**

LIST OF TABLES

TABLE **PAGE**

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 version of this section 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. Essentially, two sets of requirements are associated with a complete UC system. The end points (i.e., PCs, EIs, CPE) have one set of physical security requirements while the network (e.g., 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.

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. 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 cannot gain access to nor affect the other segments. In addition, interaction control between various segments is 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, 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.

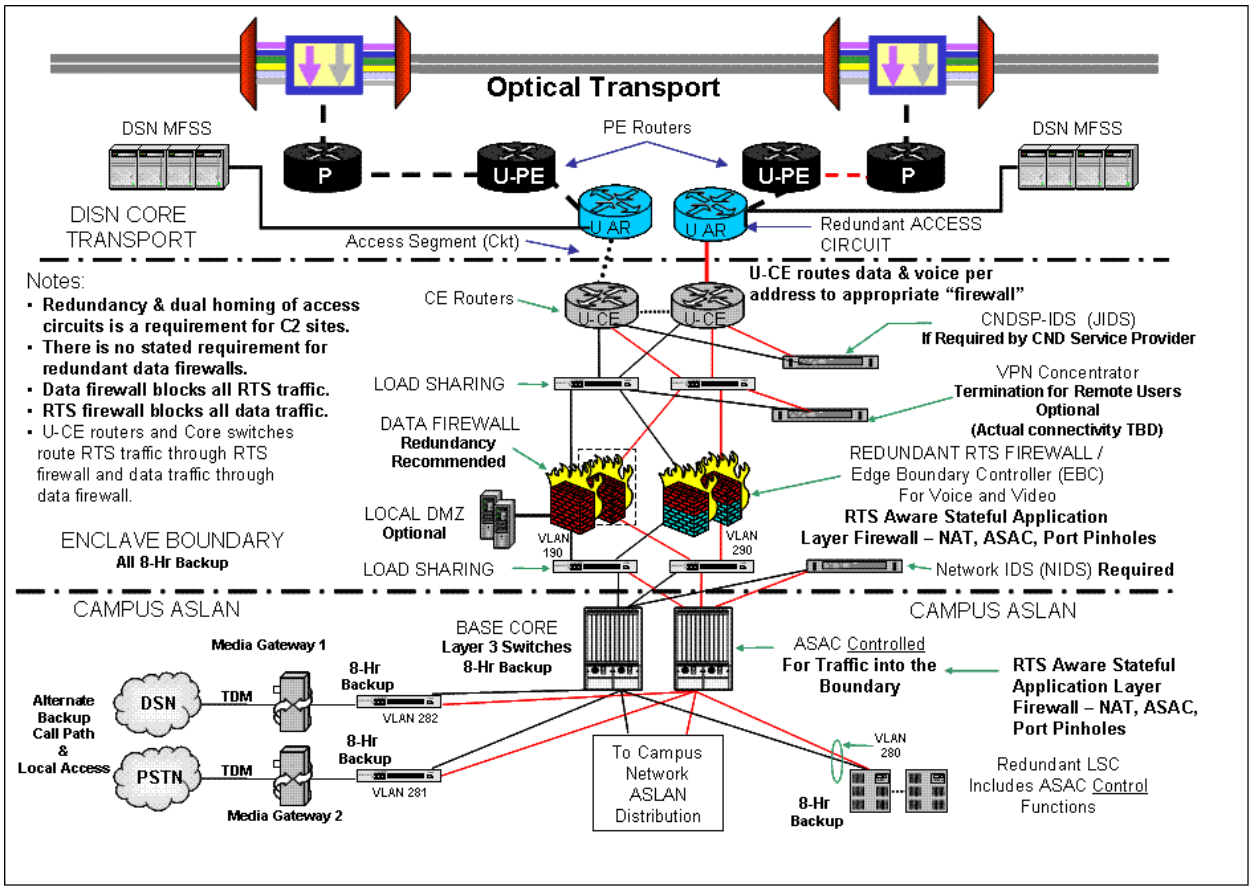

Figure 5.8.3-1. Notional Example of Voice and Data ASLAN Segmentation

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 the UCR, 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 Telcordia Technologies 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 Technical Implementation Guide." This section is intended to provide a level of security requirements consistent with the level of security requirements defined for the UC, 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 in Section 5.1, Requirements Categories and Language. Failure to satisfy a requirement will result in a Category I, II, or III finding.

Finally, the derived requirements do not include all 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
IAT	Information Assurance Tool
IPS	Intrusion Protection System
ISS	Integrated Security System
NAC	Network Access Control
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, NAC]** The DoD IPv6 Profile shall be used for IPv6 requirements for security devices unless otherwise stated either within this section or in UCR, Section 5.3.5, IPv6 Requirements.

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

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

4. **[Required: IPS]** The security device shall conform to all of the MUST requirements found in RFC 3411, "Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks."

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

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

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

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

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

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

12. **[Required: FW, VPN]** 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)."

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

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

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

5.8.4.3 Information Assurance Requirements

5.8.4.3.1 General Requirements

1. **[Required: FW, IPS, VPN, NAC]** The security device shall support SNMP3 and NTPv4.

2. **[Required: VPN]** The security device shall provide ability to push policy to the VPN client and the ability to monitor the client's activity.

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

4. **[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 Reserved

5.8.4.3.3 Configuration Management

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

2. **[Required: FW, IPS, NAC, 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 disable the IP redirects notification service, except in type 3 cases.

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

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

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

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

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

4. **[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.

5. **[Required: IPS]** 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.

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

7. **[Required: FW, IPS, NAC, 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 disable the system automatically if serious Information Assurance violations are detected.

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]** 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.

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

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

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

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

6. **[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.

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

8. **[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.

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

10. **[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.

11. **[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.

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

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

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

15. **[Required: IPS, VPN]** The security device shall be able to collect data accesses.

16. **[Required: IPS, VPN]** The security device shall be able to collect service requests.

17. **[Required: IPS, VPN]** The security device shall be able to collect network traffic.

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

19. **[Required: IPS, VPN]** The security device shall be able to collect data introduction.

20. **[Required: IPS, VPN]** The security device shall be able to collect detected malicious code.

21. **[Required: IPS, VPN]** The security device shall be able to collect access control configuration.

22. **[Required: IPS, VPN]** The security device shall be able to collect service configuration.

23. **[Required: IPS, VPN]** The security device shall be able to collect authentication configuration.

24. **[Required: IPS, VPN]** The security device shall be able to collect accountability policy configuration.

25. **[Required: IPS, VPN]** The security device shall be able to collect detected known vulnerabilities.

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

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

5.8.4.3.6 Reserved

5.8.4.3.7 Documentation

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

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

3. **[Optional: FW, IPS, NAC, VPN]** The developer shall provide user guidance (e.g., a 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, NAC, VPN]** The developer shall provide the internal architectural design of the security device.

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

6. **[Required: FW, IPS, NAC, 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.

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

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

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

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

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

12. **[Required: FW, IPS, NAC, 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.

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

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

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

16. **[Required: FW, IPS, NAC, 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.

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

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

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

20. **[Required: FW, IPS, NAC, 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.

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

22. **[Required: FW, IPS, NAC, 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.

23. **[Required: FW, IPS, NAC, 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 the security device must be done in a known secure manner. It must also protect its cryptologic functions in accordance with NIST developed Federal Information Processing Standards (FIPS) 140-2.

1. **[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.

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, NAC, VPN]** System mechanisms shall be implemented to enforce automatic expiration of passwords, to prevent password reuse, and to ensure password strength.

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

3. **[Required: FW, IPS, NAC, 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 Information Security (IS) perimeter nor result in any external information entering the IS perimeter.

4. [**Required: FW, IPS, NAC, 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.

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

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

7. **[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.

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

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

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

11. **[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.

12. **[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.

13. **[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, except as necessary to perform functions such as Network Address Translation (NAT).

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

15. **[Required: FW, IPS]** The security device shall properly accept or deny Transmission Control Protocol (TCP) traffic from port numbers based on policy.

16. **[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.

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

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

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

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

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

22. **[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.

5.8.4.3.10 Systems and Communication Protection

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

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

5.8.4.3.11 Other Requirements

1. **[Required: FW, IPS, NAC, 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 (IT) entity on a broadcast network.

2. **[Required: FW, NAC, VPN]** The security device shall reject requests for access or services where the presumed source identity of the source subject is an external IT entity on the loopback network.

3. **[Required: FW, IPS, NAC, 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.

4. **[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 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 external network address;

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

5. **[Required: FW, IPS, NAC, 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 either through manual intervention or automatic reboot.

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

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

8. **[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.

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

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

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

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

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

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

15. **[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.

5.8.4.3.12 Performance

Security without performance brings productivity to a standstill. Security devices 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. **[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.

4. **[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.

5. **[Required: FW, IPS, VPN]** The security device shall use a commercial best practice defensive solution and maintain advertised normal operation packet loss rates for all legitimate data packets when under a SYN Flood attack.

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

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

5.8.4.4 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:

- Ceasing to operate (failing to secure),
- Terminating encrypted connections, and/or
- Sending alerts via console message.

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

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

3. **[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.

4. **[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.

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

6. **[Required: FW, VPN]** The security device shall enforce the system administrator's policy options pertaining to violations of network traffic rules within a specified period.

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

5.8.4.4.2 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.

5.8.4.6 IPS VVoIP Signal and Media Inspection Requirements

The following requirements are for any IPS device that has the capability to inspect VVoIP signals correctly.

1. **[Conditional: IPS]** The device shall support the capability to detect and send alarms in responses to threats identified in VVoIP signaling.

    a. **[Conditional: IPS]** The IPS shall support the capability to detect an abnormal number of 401/407 AS-SIP response messages, indicating that a possibly unauthorized user or device is attempting to connect to the system.

    b. **[Conditional: IPS]** The IPS shall support the capability to detect when an abnormal time-out for an AS-SIP request occurs (e.g., large numbers of repeated AS-SIP requests or responses, unusual number of AS-SIP requests sent with no matching response).

NOTE: If an AS-SIP request time-out occurs, it could be an indication that the system has failed because of a DoS attack resulting from a maliciously crafted request.

c. **[Conditional: IPS]** The device shall support the capability to detect when AS-SIP messages exceed a configurable maximum message length.

d. **[Conditional: IPS]** The device shall support the capability to detect when an AS-SIP message contains nonprintable characters.

NOTE: The presence of nonprintable characters could indicate an attempt by an adversary to insert executable code or cause abnormal behavior in a system.

e. **[Conditional: IPS]** The device shall support the capability to detect attempts to inject SQL queries into AS-SIP signaling messages.

f. **[Conditional: IPS]** The device shall support the capability to detect unusual IPv4 or IPv6 addresses contained in AS-SIP messages (for example, the local host/loopback address, link local addresses).

g. **[Conditional: IPS]** The device shall support the capability to detect traffic that does not have the characteristics of AS-SIP traffic, but is still sent over a channel established for sending AS-SIP messages (e.g., strings of characters that are not AS-SIP related).

2. **[Conditional: IPS]** The device shall support the capability to detect and send alarms in response to threats identified in VVoIP media traffic and other traffic that flows across the EBC boundary.

a. **[Conditional: IPS]** The device shall detect attempts to inject packets into a media stream or perform replay attacks (e.g., duplicate sequence numbers appearing in an RTP stream).

b. **[Conditional: IPS]** The device shall support the capability to detect traffic that should be VVoIP traffic based on its headers, but does not have the characteristics of a VVoIP traffic stream.

(1) **[Conditional: IPS]** The device shall support the capability to detect signatures associated with the presence of data, files, executables, SQL commands, viruses, or other unusual data contained within a media stream intended for VVoIP.

(2) **[Conditional: IPS]** The device shall support the capability to detect abnormally sized packets in the VVoIP media stream.

(a) **[Conditional: IPS]** At a minimum, the device shall support the capability to detect unusually large packets associated with the codec types specified in Section 5.3.2.6, End Instruments.

NOTE: This requires the device to support the capability to recognize the codec that should be represented within the packet and determine the appropriate packet size based on that information.

3. **[Conditional: IPS]** The device shall support the capability to receive periodic VVoIP signaling, media, and other threat signature updates from an authenticated source in an automated manner.

5.8.4.7 Integrated Security Systems

Integrated Security Systems (ISSs) are systems that provide the functionality of more than one Information Assurance device in one integrated device.

1. **[Required: ISS]** The device shall ensure that each function implemented shall be logically separate from the other functions.

2. **[Required: ISS]** The device must comply with all applicable UCR requirements for any implemented functions.

5.8.4.8 Information Assurance Tools

Information Assurance tools (IATs) are a category of Information Assurance devices that are not yet fully defined. These devices must meet the Information Assurance requirements for DoD systems as defined in Section 5.4, Information Assurance Requirements. Functional requirements will be added in future versions of this document.

5.8.4.9 Network Access Controllers

1. **[Required: NAC]** The system shall be able to authenticate all devices before allowing access to the network.

2. **[Required: NAC]** The system shall be capable of denying access to any device that fails authentication.

3. **[Required: NAC]** The system shall support 802.1X based policy enforcement points and Layer 3 policy enforcement points with 802.1X based policy enforcement preferred.

4. **[Required: NAC]** The system shall operate in both in-band and out-of-band modes to support both network segments that can and cannot utilize 802.1X.

5. **[Required: NAC]** The system shall allow an administrator to override the authentication assessment and allow or deny a device to enter the authorized network.

6. **[Required: NAC]** The system shall provide the administrator a means for configuring exception policies to accommodate authorized devices that do not support NAC-agents or other means for authentication such as 802.1X.

7. **[Required: NAC]** The system shall allow security managers and administrators the ability to create, manipulate, and maintain multiple device NAC policies for different classes of devices.

8. **[Required: NAC]** The system shall be capable of being configured for both distributed NAC policy and localized NAC policy enforcement administration.

9. **[Required: NAC]** The system shall allow an administrator to manually configure event publication, e.g. set filters on event types to be displayed, alerted.

10. **[Required: NAC]** The system shall have the ability to be configured to log, but not enforce NAC policies. The system shall provide the ability to log and notify, but not enforce, optionally all the following; compliance OR device authentication OR remediation notifications.

11. **[Required: NAC]** The system shall provide the capability to either turn-off or disable the NAC functionality globally, and on a NAC-controlled interface basis.

12. **[Required: NAC]** The system shall allow administrators to receive information on a device's NAC status.

13. **[Required: NAC]** The system shall be capable of placing the end user machine into an alternate network (quarantine) if the end user machine is not authorized to connect to the trusted network, regardless of its enforcement method.

    NOTE: The network components (e.g., VPN, LS) must be configured so that end devices do not have access to other untrusted devices while quarantined.

14. **[Required: NAC]** The system shall allow isolated segments of the network to be designated for clients that meet a specified configuration policy compliance status.

15. **[Required: NAC]** For all devices, the system shall support the capability to remove an asset from the group of its managed assets without sympathetic errors (e.g., pop up window saying "invalid command"), thus allowing the user to remove managed devices without issue.

16. **[Required: NAC]** The system shall require an authentication procedure to process new clients requesting downloads.

17. **[Required: NAC]** The system shall support the capability to allow end devices to automatically and securely download required patches or software when the device is found to be non-compliant. Any NAC agent functionality shall support the capability to install downloaded patches manually.

18. **[Required: NAC]** The system's remediation checks shall be customizable by security managers and administrators.

19. **[Required: NAC]** The system shall not interfere with the operation of DoD-approved antivirus software (e.g., Symantec and McAfee), HBSS, and Federal Desktop Core Configuration (FDCC).

    NOTE: Interoperability with HBSS is preferred.

20. **[Required: NAC]** The system shall be configurable to fail closed.

21. **[Required: NAC]** The system shall provide encrypted communications from the NAC client agent to the NAC device using FIPS-validated encryption.

22. **[Required: NAC]** The system shall protect against subversive network access activity. This may be provided by interfacing with post authentication policy enforcement of third-party devices using standards like Trusted Network Control IF-MAP (Interface - Metadata Access Point) Protocol.

23. **[Required: NAC]** NAC management devices shall have the capability for manual, and optionally, automatic recovery from failed operations to return to normal settings/ operations/systems, to include log merging.

24. **[Required: NAC]** The system shall support the capability to export logs in and open standard format (e.g., Syslog).

25. **[Required: NAC]** The system shall provide the capability to queue events when communication is lost.

26. **[Required: NAC]** The system shall be capable of reporting alerts to multiple management consoles for all administratively specified events.

27. **[Required: NAC]** The system shall provide detailed logs of all administratively specified events.

28. **[Required: NAC]** The system shall have the ability to time-stamp all events using Greenwich Mean Time (GMT), to include log data, in a consistent frame of reference.

29. **[Required: NAC]** The product shall support a concept of operations which allows individual managers to support large numbers of distributed managed elements.

30. **[Required: NAC]** The system shall allow configurable reporting to control how and when reports are generated, based on administrator-selected attributes/thresholds.

31. **[Required: NAC]** The system shall support the capability to identify connecting clients that do not have an 802.1X supplicant or NAC agent/remediation software installed.

32. **[Required: NAC]** The system shall support the capability to check for syntax errors and duplicate policies before NAC policies are implemented.

33. **[Required: NAC]** The system shall support the capability to integrate with and use Active Directory when authenticating connected devices.

34. **[Required: NAC]** The system shall support the capability to periodically perform reauthentication and remediation in automated manner at a configurable interval.

35. **[Required: NAC]** NAC systems using 802.1X must be compliant with the relevant and current IEEE standards for 802.1X.

36. **[Required: NAC]** The system shall have the ability to work with any RADIUS server in 802.1X enforcement mode.

37. **[Required: NAC]** The system shall have the ability to support short term client disconnections, such as taking a laptop to a meeting, and then reconnecting to the network without requiring the client to pass through the testing process.

THIS PAGE INTENTIONALLY LEFT BLANK