Requirement ID: [SRS-7-388]

The event management toolset SHALL support trend and abnormal behaviour analysis.

Requirement ID: [SRS-7-389]

MG_MGMT_EM SHALL be able to generate reports of the following types:

- SLA compliance reports;
- Error/exception reports;
- Service usage reports;

Requirement ID: [SRS-7-390]

Other customizable reports based on captured metrics which can be filtered and sorted based on various criteria.

Requirement ID: [SRS-7-391]

MG_MGMT_EM SHALL pass outgoing SMC Messages to interface ‘Core Services Management’ ([SRS-7-60]) for further processing.

7.7.7.1 Interfaces

Requirement ID: [SRS-7-392]

MG_MGMT_EM MUST offer an interface ‘Event Management’ that generates and forwards ‘SMC Messages’ in support of the operations ‘Log’ (7.7.7.1.1), ‘Alert’ (7.7.7.1.2) and ‘Report’ (7.7.7.1.3).

7.7.7.1.1 Log

Requirement ID: [SRS-7-393]

The interface ‘Event Management’ MUST support an operation ‘Log’ that provides the capability to record events that occur in software, or messages between components.

Requirement ID: [SRS-7-394]

The operation ‘Log’ SHALL support writing log messages to a log file.

Requirement ID: [SRS-7-395]

The operation ‘Log’ MUST provide the capability to log request and response attributes. These include:

- Time-stamp;
- Source and target address(es);
- URL;
- Operation;
- Size;
- Unique request id (extracted from the request/response or automatically generated by MG_MGMT_EM).

Requirement ID: [SRS-7-396]

The operation ‘Log’ MUST provide the capability to log attributes extracted from the SMTP headers and SMTP body.

Requirement ID: [SRS-7-397]

The operation ‘Log’ MUST provide the capability to selectively log whole messages based on pre-configured criteria or filter (e.g. policy based).

Requirement ID: [SRS-7-398]

The operation ‘Log’ SHALL support SMC Messages of the following types:

- Syslog [IETF RFC 5424, 2009];
- HTTP Message [IETF RFC 7230, 2014].

7.7.7.1.2 Alert

Requirement ID: [SRS-7-399]

The interface ‘Event Management’ MUST support an operation ‘Alert’ that provides the capability to generate an alert event when the acceptable threshold for a service has been reached, or is approached within a certain range.

Requirement ID: [SRS-7-400]

The operation ‘Alert’ SHALL be able to support the generation of an alert of type ‘Warning’ that indicates it is necessary to take action in order to prevent an exception occurring.

Requirement ID: [SRS-7-401]

The operation ‘Alert’ SHALL be able to support the generation of an alert of type ‘Exception’ that indicates that a given service is operating below the normal predefined parameters/indicators.

Requirement ID: [SRS-7-402]

The operation ‘Alert’ SHALL support SMC Messages of the type SNMP v3 [IETF RFC, 3412, 2002].

7.7.7.1.3 Report

Requirement ID: [SRS-7-403]

The interface ‘Event Management’ MUST support an operation ‘Report’ that provides the capability to generate reports in support of compliance, auditing, billing and service value determination.

Requirement ID: [SRS-7-404]

The operation ‘Report’ SHALL support SMC Messages of the type SNMP v3 [IETF RFC 3412, 2002].

7.7.8 Performance Management

Requirement ID: [SRS-7-405]

MG_MGMT MUST provide a management capability MG_MGMT_PM that enables the management of the performance and capacity of the MG.

Requirement ID: [SRS-7-406]

MG_MGMT_PM SHALL provide customizable dashboards for monitoring selected statistics and metrics for MG services.

Requirement ID: [SRS-7-407]

MG_MGMT_PM SHALL pass outgoing SMC Messages to interface ‘Core Services Management’ ([SRS-7-60] for further processing.

7.7.8.1 Interfaces

Requirement ID: [SRS-7-408]

MG_MGMT_PM MUST offer an interface ‘Performance Management’ that generates and forwards ‘SMC Messages’ in support of the operations ‘Monitor’(7.7.8.1.1), ‘Meter’ (7.7.8.1.2) and ‘Track Messages’ (7.7.8.1.3.

7.7.8.1.1 Monitor

Requirement ID: [SRS-7-409]

The interface ‘Performance Management’ MUST support an operation ‘Monitor’ that provides the capability to observe and track the operations and activities of end users (services) on the MG.

Requirement ID: [SRS-7-410]

The operation ‘Monitor’ SHALL support the real-time monitoring of MG services against expected KPI, SLA or other metric thresholds as configured.

Requirement ID: [SRS-7-411]

The operation ‘Monitor’ SHALL support the monitoring service faults and exceptions.

Requirement ID: [SRS-7-412]

The operation ‘Monitor’ SHALL support SMC Messages of the type SNMP v3 [IETF RFC 3412, 2002].

7.7.8.1.2 Meter

Requirement ID: [SRS-7-413]

The interface ‘Performance Management’ MUST support an operation ‘Meter’ that provides the capability to measure levels of resource utilization consumed by service subscribers.

Requirement ID: [SRS-7-414]

The operation ‘Meter’ SHALL support the storing of measured data for the purpose of summarizing and analysis.

Requirement ID: [SRS-7-415]

The operation ‘Meter’ SHALL provide the capability to collect and present the statistics on service utilisation broken down by end user or system.

Requirement ID: [SRS-7-416]

The operation ‘Meter’ SHALL support the collection of statistics for a given end user or system or group of end user or system over specified periods of time.

Requirement ID: [SRS-7-417]

The operation ‘Meter’ SHALL support SMC Messages of the type SNMP v3 [IETF RFC 3412, 2002].

7.7.8.1.3 Track Messages

Requirement ID: [SRS-7-418]

The interface ‘Performance Management’ MUST support an operation ‘Track Messages’ that provides the capability to track, monitor and log all message routing and service invocation activities.

Requirement ID: [SRS-7-419]

The operation ‘Track Messages’ SHALL provide the capability to track, monitor, and log all SMTP messages from the high domain to the low domain.

Requirement ID: [SRS-7-420]

The operation ‘Track Messages’ SHALL provide the capability to track, monitor, and log all delivery reports and status notifications from the low domain to the high domain.

Requirement ID: [SRS-7-421]

The operation ‘Track Messages’ SHALL provide the capability to track, monitor, and log all SMTP messages from the low domain to the high domain.

Requirement ID: [SRS-7-422]

The operation ‘Track Messages’ SHALL provide the capability to track, monitor, and log all delivery reports and status notifications from the high domain to the high domain.

Requirement ID: [SRS-7-423]

The operation ‘Track Messages’ SHALL support SMC Messages of the type SNMP v3 [IETF RFC 3412, 2002].

7.8 Security Functional Requirements

7.8.1 Introduction

The security functional requirements for the MG are drawn from the Protection Profile for the IEG-C defined in section 8.

Requirement ID: [SRS-7-424]

The MG SHALL be evaluated to EAL4(+) based on the Protection Profile defined in Section 8.

7.8.2 Requirements

7.8.2.1 Infrastructure Platform

Requirement ID: [SRS-7-425]

The MG SHALL include malware/virus protection for its server.

Requirement ID: [SRS-7-426]

The MG malware/virus protection SHALL be maintained/updated from the NATO Service Operation Centre (SOC).

7.8.2.2 Trusted Base Platform (TBP)

Requirement ID: [SRS-7-428]

The MG SHALL protect components and areas of main memory from being directly accessed (without that access being mediated by the operating system) by untrusted subjects.

Requirement ID: [SRS-7-429]

The MG SHALL protect any other function of the underlying platform from being used by untrusted subjects in a way that would violate the security policy of the operating system.

Requirement ID: [SRS-7-430]

The MG SHALL provide mechanisms that control a user's logical access to the Mail Guard and to explicitly deny access to specific users when appropriate.

7.8.2.3 Policy Enforcement Module

Requirement ID: [SRS-7-431]

The MG SHALL be capable of maintaining protection policy enforcement if it is unable to communicate with the Policy Enforcement module which provided it the policy.

Requirement ID: [SRS-7-432]

The MG SHALL enable the enforcement of information flows email messages.

Requirement ID: [SRS-7-433]

The MG SHALL enable the enforcement of content inspection of email messages.

Requirement ID: [SRS-7-434]

The MG SHALL validate the origin, integrity and binding [STANAG 4778] of a confidentiality label [STANAG 4774] to a data object before it is used.

Requirement ID: [SRS-7-506]

The MG SHALL validate a confidentiality label [STANAG 4774] against the corresponding SPIF before it is used.

7.8.2.4 Data Protection Module

Requirement ID: [SRS-7-435]

The MG Data Protection Module SHALL provide a NATO approved cryptographic sub-component with NATO-approved methods for key management (i.e.; generation, access, distribution, destruction, handling, and storage of keys), and for cryptographic operations (i.e.; encryption, decryption, signature, hashing, key exchange, and random number generation services) as described in [NAC AC/322-D(2007)0002-REV1, 2015].

Requirement ID: [SRS-7-436]

The MG Data Protection Module cryptographic sub-component SHALL be validated to at least FIPS 140-2 Level 2 [FIPS 140-2, 2001], or otherwise verified to an equivalent level of functionality and assurance by a NATO nation COMSEC authority.

Requirement ID: [SRS-7-437]

The MG Data Protection Module SHALL provide capability to protect against disclosing or transmitting information in violation of the policy.

Requirement ID: [SRS-7-438]

The MG SHALL provide mechanisms that mitigate attempts to exhaust its resources.

Requirement ID: [SRS-7-439]

The MG Data Protection Module SHALL provide capability to protect against gaining inappropriate access to one or more networks, endpoints, or services, such as through transmitting malicious executable code, scripts, or commands.

7.8.2.5 Protected Communications

Requirement ID: [SRS-7-440]

The MG SHALL ensure that is protection policy information is transmitted to the Policy Enforcement Module in a secure and timely manner so that there is assurance that the correct policy is being enforced.

Requirement ID: [SRS-7-441]

The MG SHALL ensure that communications are not subject to unauthorized modification or disclosure.

Requirement ID: [SRS-7-442]

The MG SHALL provide a means to ensure that administrators are not communicating with some other entity pretending to be the MG when supplying identification and authentication data.

7.8.2.6 Authentication

Requirement ID: [SRS-7-443]

The MG SHALL validate the identity of other peer entities prior to distributing data to them.

Requirement ID: [SRS-7-444]

The MG SHALL provide a means to detect and reject the replay of authentication data as well as other security data and attributes.

Requirement ID: [SRS-7-445]

The MG SHALL use a NPKI provided device certificate to validate its identity to other peer entities.

Requirement ID: [SRS-7-446]

The MG SHALL validate the identity of other peer identities by validating the peer entities device certificate to an NPKI trust point

7.8.2.7 Audit

Requirement ID: [SRS-7-447]

The MG SHALL provide measures for generating and storing audit information for security relevant events that will record access attempts to MG-protected resources by users.

7.8.2.8 Management

There are no Management security functional requirements identified for the Mail Guard.

7.8.2.9 Trusted Update

Requirement ID: [SRS-7-448]

The MG firmware and software SHALL be updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.

Requirement ID: [SRS-7-449]

The MG SHALL ensure the integrity of its update packages prior to installation.

8 Security Requirements

8.1 General

Requirement ID: [SRS-8-2]

Utilisation of modern IA techniques and compliancy with the cyber-defence services SHALL be followed.

8.2 Interconnection of Networks

Requirement ID: [SRS-8-3]

The IEG-C SHALL consider and apply the following directions, guidance and obligation within the INFOSEC technical and implementation directive for the interconnection of networks:

- AC/322-D(2004)0024-REV3-COR1 "CIS Security Technical and Implementation Directive on the NATO PKI Certificate Policy"
- AC/35-D/1021-REV3, dated 31 Jan 2012 "Guidelines for the security accreditation of communication and information systems (CIS)"
- AC/35 D/2004 Rev3 15 Nov 2013 "Primary Directive on CIS Security"
- AC/322-D/0047-REV2 (INV) 11 March 2009 "INFOSEC Technical & Implementation Directive on cryptographic security and cryptographic mechanisms"

8.3 Protection Profile

8.3.1 Applicability of Protection Profiles relevant for IEG-C

For the purposes of specifying the security requirements for an IEG-C an approach based upon the National Information Assurance Partnership (NIAP) Protection Profile (PP) scheme [NIAP] has been adopted. The IEG-C consists of a number of components to provide a solution for automated cross-domain information exchange between NATO Secret and NATO-led Mission Secret networks while offering the required level of assurance for the interconnection. These components have been identified and functionally specified in Section 4. NIAP contains a number of PPs that are applicable for IEG-C components as listed below:

- Protection Profile for Application Software Version 1.2 [NIAP PP_APP_V.1.2, 2016]
- Protection Profile for General Purpose Operating Systems [NIAP PP_OS_V.4.1, 2016]
- Collaborative Protection Profile for Stateful Traffic Filter Firewalls [NIAP CPP_FW_V.1.0, 2015]
- Collaborative Protection Profile for Network Devices [NIAP CPP_ND_V.1.0, 2015]

- Collaborative Protection Profile for Network Devices/collaborative Protection Profile for Stateful Traffic Filter Firewalls Extended Package (EP) for Intrusion Prevention Systems (IPS) [NIAP PP_NDCP_IPP_EP_V.2.1, 2016]
- Standard Protection Profile for Enterprise Security Management Policy Management [NIAP PP_ESM_V.2.1, 2013]
- Standard Protection Profile for Enterprise Security Management Access Control [NIAP PP_ESM_AC_V.2.1, 2013]

To support industry in developing a commercial alternative to the NC3A Medium Assurance XML Labelling Guard, NATO developed a Common Criteria (CC) Protection Profile [NCIA TN-1485 v1.1, 2012]. The NATO PP can be used as a target specification for the implementation of a CC Evaluation Assurance Level (EAL) 4+ evaluation of commercial products that provide a Web Guard capability in an IEG-C.

The main purpose for specifying the security requirements based on the NIAP-approved PP scheme is to be able to re-use existing, up-to-date and agreed profiles in order to establish a consistent approach for describing the security requirements and evaluating the IEG-C capability to meet those security requirements. The security requirements have been developed as a result of analysing and assessing, from the NIAP and NATO PPs, the security objectives based on identified threats, assumptions and organizational security policies deemed applicable for an IEG-C capability and commensurate with the threats that may be active within the operational environment that the IEG-C will be deployed.

The PP scheme provides rationale whereby the PP illustrates how the security objectives are addressed by security functional requirements (SFRs). Each security requirement specified for the IEG-C will identify the security objectives detailed in Section 8.3.4 and list (by reference) the security functional requirements (SFRs), specified in the appropriate NIAP or NATO PP, relevant to that security requirement where applicable. It is not the intention to map all SFRs defined in each of the relevant PPs for the following reasons:

- The definitions for the PP Target of Evaluation (TOE) and the TOE Security Functionality (TSF) are influenced by assumptions within the IT operational environment defined in the TOE that may not be applicable to the IEG-C; and,
- SFRs may be defined for TSF components that do not exist in the IEG-C TOE.

The security requirements for specifying the security functionality required by the IEG-C are written in a manner that reflects the overall objective intended by an SFR. This means that SFRs that are too implementation-specific, for example an SFR that refers to a particular protocol and version that differs from the protocol version required to be supported by the IEG-C, are still relevant and can still be referenced without the need to rewrite the SFR.

8.3.2 Target of Evaluation (TOE) Overview

The IEG-C is composed of a number of IEG-C components that contain logical sub-components, providing overlapping capabilities for the IEG-C components, which have different relevance for enforcing the security functional requirements (SFRs). The logical sub-components are:

- Trusted Base Platform - consists of the operating system (OS) kernel, the tools and applications which are part of the OS, and the hardware, on which the OS runs.

- Policy Enforcement Module - central component for enforcing security requirements of the IEG-C. It is application software that implements the protection policies (IFPs and CIPs). This module provides functionality described by the Protection Policy Enforcement Services [NCIA TR/2016/NSE010871/01, 2017].
- Data Protection Module – helps to protect confidentiality, integrity and availability of the High Domain. The Data Protection Module provides functionality to process cryptographically protected data and implement specific scanning for malicious contents. This module includes the capabilities described for the PKE and Malware Scanner modules as specified in [NCIA TN-1485 v1.1, 2012] and provides the functionality described by the Protection Services [[NCIA TR/2016/NSE010871/01, 2017].

The TOE Security Functionality (TSF) of the TOE (illustrating the IEG-C components and the relationships with the logical sub-components) is highlighted in Figure 22 for an IEG-C .

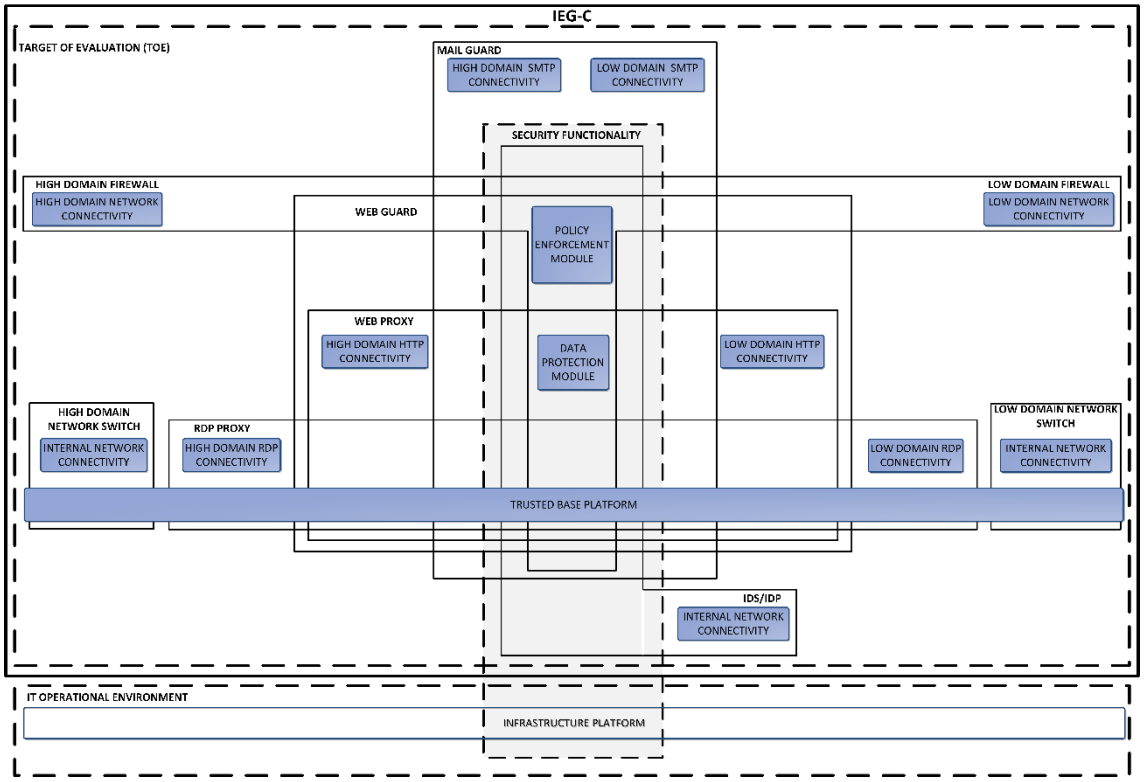

Figure 29 TOE, TSF and Operational Environment for a static IEG-C

Figure 22 illustrates the Infrastructure Platform component as part of the TSF provided by the operational environment.

Table 16 below lists the sub-components that are part of the TSF for a static IEG-C and illustrates which IEG-C components, provided as a part of the TOE, relates to those sub-components.

Table 23 IEG-C TSF sub-components for static IEG-C

	Trusted Base Platform	**Policy Enforcement Module**	**Data Protection Module**
High Domain Firewall	X	X	X
Low Domain Firewall	X	X	X
High Domain Network Switch	X		
Low Domain Network Switch	X		
RDP Proxy	X		
Web Proxy	X		X
Web Guard	X	X	X
Mail Guard	X	X	X
Intrusion Detection / Prevention System	X	X	X
Management	X	X	X

8.3.3 Security Problem Definition

8.3.3.1 Threats

The security threats identified in Appendix C.1.1 SHALL be addressed by the TOE or its operational environment.

8.3.3.2 Assumptions

The specific conditions identified in Appendix C.1.2 are assumed to exist in a PP-compliant TOE environment.

8.3.3.3 Organizational Security Policies

Appendix C.1.3 lists applicable Organizational Security Policies (OSPs) provided.

8.3.4 Security Objectives

Appendix C.2 describes the Security Objectives and the associated security functional requirements (SFRs) that address the Security Objectives.

8.3.5 Security Functional Requirements

If applicable, for each security requirement the source(s) from the PPs is identified (the associated SFRs are referenced through the relationship with the Security Objectives listed in Appendix C.2). The security requirements are categorised into the logical sub-components identified in the TSF and IT operational environment, and the underlying functionality that the TOE provides, as illustrated in Figure 24. Each security requirement identifies to which IEG-C component(s) the requirement is applicable.

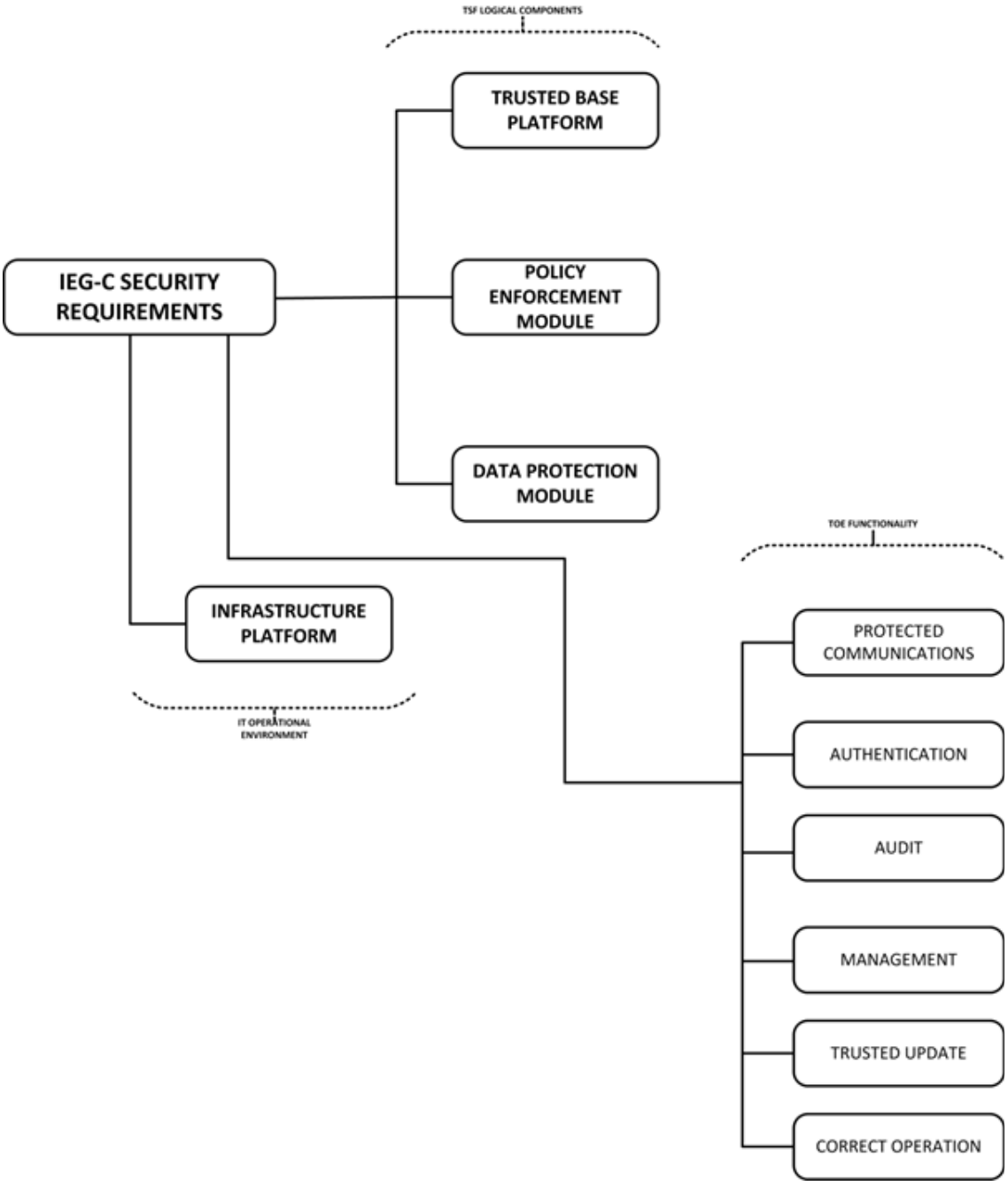

Figure 30 Graphical representation of security requirements to TSF and IT Operational Environment components and TOE functionality

8.3.5.1 Infrastructure Platform

Table 24 Infrastructure Platform: requirements, sources (including SFRs, if applicable) and applicability to IEG-C components

Requirement	Sources	IEG-C	Firewall	Network Switch	RDP Proxy	Web Proxy	Web Guard	Mail Guard	IDS	Management
Requirement ID: [SRS-8-1] The IEG-C SHALL be located in a restricted or monitored environment that provides protection from unmanaged access to the physical components and data interfaces of the IEG-C.	A.PHYSICAL_PROTECTION A.PHYSICAL_ACCESS_MANAGED OE.PHYSICAL_ACCESS_MANAGED	X								
Requirement ID: [SRS-8-2] The Infrastructure Platform SHALL provide a NATO approved malware scanning capability [NC3B AC/322-D(2004)0019 (INV), 2004].	P.ANALYZE OE.MALWARE_SCANNER OE.ROBUST								X	
Requirement ID: [SRS-8-3] The Infrastructure Platform SHALL provide capability to ensure that only authorized communications are allowed between the high and low networks.	OE.NO_TOE_BYPASS OE.CONNECTIONS		X							

Requirement	Sources	IEG-C	Firewall	Network Switch	RDP Proxy	Web Proxy	Web Guard	Mail Guard	IDS	Management
Requirement ID: [SRS-8-4] The Infrastructure Platform SHALL provide reliable time data to the IEG-C.	OE.SYSTIME	X								

8.3.5.2 Trusted Base Platform (TBP)

Table 25 Trusted Base Platform: requirements, sources (including SFRs, if applicable) and applicability to IEG-C components

Requirement	Sources	IEG-C	Firewall	Network Switch	RDP Proxy	Web Proxy	Web Guard	Mail Guard	IDS	Management
Requirement ID: [SRS-8-5] The IEG-C is a distributed system, therefore, the TBP SHALL implement measures to protect against eavesdropping between components of the IEG-C that are distributed.	A.PLATFORM O.TRUSTED_COMMUNICATIONS O.TRUSTED_PATH O.DATAPROT	X	X	X	X	X	X	X	X	X

Requirement	Sources	IEG-C	Firewall	Network Switch	RDP Proxy	Web Proxy	Web Guard	Mail Guard	IDS	Management
Requirement ID: [SRS-8-6] The TBP consists of hardware (processors, memory, and devices), firmware and the operating system(s). The TBP SHALL be configured according to relevant NATO guidance and directives [NAC AC/322-D/0048-REV3, 2019]		X	X	X	X	X	X	X	X	X
Requirement ID: [SRS-8-7] The TBP SHALL protect components and areas of main memory from being directly accessed (without that access being mediated by the operating system) by untrusted subjects.	O.ACCESSID O.AUTH	X	X	X	X	X	X	X	X	X
Requirement ID: [SRS-8-8] The TBP SHALL protect any other function of the underlying platform from being used by untrusted subjects in a way that would violate the security policy of the operating system.	O.PROTECTED_STORAGE O.ACCESSID O.AUTH	X	X	X	X	X	X	X	X	X

Requirement	Sources	IEG-C	Firewall	Network Switch	RDP Proxy	Web Proxy	Web Guard	Mail Guard	IDS	Management
Requirement ID: [SRS-8-9] The TBP SHALL provide reliable time data to all components of the IEG-C.		X	X	X	X	X	X	X	X	X
Requirement ID: [SRS-8-10] The TBP SHALL provide mechanisms that control a user's logical access to the TOE and to explicitly deny access to specific users when appropriate.	O.TOE_ROBUST_ACCESS	X	X	X	X	X	X	X	X	X

8.3.5.3 Policy Enforcement Module

Table 26 Policy Enforcement Module: requirements, sources (including SFRs, if applicable) and applicability to IEG-C components

Requirement	Sources	IEG-C	Firewall	Network Switch	RDP Proxy	Web Proxy	Web Guard	Mail Guard	IDS	Management
Requirement ID: [SRS-8-11] The IEG-C SHALL be able to recognize and discard invalid or malicious input provided by users.	O.OFLOWS	X								X
Requirement ID: [SRS-8-12] The IEG-C SHALL be capable of maintaining protection policy enforcement if it is unable to communicate with the Policy Enforcement module which provided it the policy.	O.MAINTAIN	X	X				X	X	X	
Requirement ID: [SRS-8-13] The IEG-C SHALL provide a mechanism to identify and rectify contradictory policy data.	O.CONSISTENT	X								X
Requirement ID: [SRS-8-14] The IEG-C SHALL enable enforcement of information flow between the IEG-C components.	O.MEDIATE_FLOW O.MESSAGE_VETTING	X	X				X	X	X	X

Requirement	Sources	IEG-C	Firewall	Network Switch	RDP Proxy	Web Proxy	Web Guard	Mail Guard	IDS	Management
Requirement ID: [SRS-8-15] The IEG-C SHALL enable enforcement of content inspection between the IEG-C components.	O.REVERSE_PROXY O.MINIMAL_PROXY O.MESSAGE_VETTING	X	X				X	X	X	X
Requirement ID: [SRS-8-16] The IEG-C SHALL validate the origin, integrity and binding [STANAG 4778 of a security label [STANAG 4774] to a data object before it is used.	O.VALID_LABEL	X					X	X		

8.3.5.4 Data Protection Module

Table 27 Data Protection Module: requirements, sources (including SFRs, if applicable) and applicability to IEG-C components

Requirement	Sources	IEG-C	Firewall	Network Switch	RDP Proxy	Web Proxy	Web Guard	Mail Guard	IDS	Management
Requirement ID: [SRS-8-17] The Data Protection Module SHALL provide a NATO approved cryptographic sub-component with NATO-approved methods for key management (i.e.; generation, access, distribution, destruction, handling, and storage of keys), and for cryptographic operations (i.e.; encryption, decryption, signature, hashing, key exchange, and random number generation services) as described in [NAC AC/322-D(2007)0002-REV1, 2015].	A.CRYPTOGRAPHY_NATO_APPROVED A.PKI_NATO_COMPLIANT O.CRYPTO_NATO_APPROVED	X	X	X		X	X	X	X	X

Requirement	Sources	IEG-C	Firewall	Network Switch	RDP Proxy	Web Proxy	Web Guard	Mail Guard	IDS	Management
Requirement ID: [SRS-8-18] The Data Protection Module cryptographic sub-component is validated according validated to at least FIPS 140-2 Level 2 [FIPS 140-2, 2001], or otherwise verified to an equivalent level of functionality and assurance by a NATO nation COMSEC authority. Ref: [NAC AC/322-D(2004)0024-REV3-COR1, 2018]	A.CRYPTOGRAPHY_MODULE_VALIDATED A.PKI_NATO_COMPLIANT	X	X	X		X	X	X	X	X
Requirement ID: [SRS-8-19] The Data Protection Module SHALL provide capability to protect against network-based reconnaissance (probing for information about a monitored network or its endpoints), such as through use of various scanning or mapping techniques. Ref: [NC3B AC/322-D(2004)0019 (INV), 2004]	O.SYSTEMT_MONITORING O_ANALYZE O_REACT OE.MALWARE_SCANNER	X							X	

Requirement	Sources	IEG-C	Firewall	Network Switch	RDP Proxy	Web Proxy	Web Guard	Mail Guard	IDS	Management
Requirement ID: [SRS-8-20] The Data Protection Module SHALL provide capability to protect against attacks that are targeted at obstructing the normal function of monitored networks, endpoints, or services, such as through denial of service attacks. Ref: [NC3B AC/322-D(2004)0019 (INV), 2004]	O.SYSTEMT_MONITORING O_ANALYZE O_REACT OE.MALWARE_SCANNER	X							X	
Requirement ID: [SRS-8-21] The Data Protection Module SHALL provide capability to protect against disclosing or transmitting information in violation of the policy.	O.VALID_LABEL	X					X	X		
Requirement ID: [SRS-8-22] The IEG-C SHALL apply analytical processes to network traffic data collected from monitored networks and derive conclusions about potential intrusions or network traffic policy violations.	O.ANALYZE	X							X	X

Requirement	Sources	IEG-C	Firewall	Network Switch	RDP Proxy	Web Proxy	Web Guard	Mail Guard	IDS	Management
Requirement ID: [SRS-8-23] The IEG-C shall provide mechanisms that mitigate attempts to exhaust resources provided by the TOE (e.g., resulting in denying access to high network resources).	O.RESOURCE_SHARING	X					X	X	X	
Requirement ID: [SRS-8-24] The Data Protection Module SHALL provide capability to protect against gaining inappropriate access to one or more networks, endpoints, or services, such as through transmitting malicious executable code, scripts, or commands. Ref: [NC3B AC/322-D(2004)0019 (INV), 2004]	O.SYSTEMT_MONITORING O_ANALYZE O_REACT OE.MALWARE_SCANNER	X					X	X	X	

8.3.5.5 Protected Communications

Table 28 Protected Communications: requirements, sources (including SFRs, if applicable) and applicability to IEG-C components

Requirement	Sources	IEG-C	Firewall	Network Switch	RDP Proxy	Web Proxy	Web Guard	Mail Guard	IDS	Management
Requirement ID: [SRS-8-25]	O.DISTRIB	X	X				X	X	X	X

The IEG-C SHALL ensure that is protection policy information is transmitted to the Policy Enforcement Module in a secure and timely manner so that there is assurance that the correct policy is being enforced.										
Requirement ID: [SRS-8-26] The IEG-C SHALL ensure that communications between distributed components of the TOE are not subject to unauthorized modification or disclosure.	O.TRUSTED_COMMUNICATIONS	X	X	X	X	X	X	X	X	X
Requirement ID: [SRS-8-27] The IEG-C SHALL provide a means to ensure that administrators are not communicating with some other entity pretending to be the TOE when supplying identification and authentication data.	O.TRUSTED_PATH	X	X	X	X	X	X	X	X	X

8.3.5.6 Authentication

Table 29 Authentication: requirements, sources (including SFRs, if applicable) and applicability to IEG-C components

Requirement	Sources	IEG-C	Firewall	Network Switch	RDP Proxy	Web Proxy	Web Guard	Mail Guard	IDS	Management
Requirement ID: [SRS-8-28] The IEG-C SHALL provide a mechanism to securely validate requested authentication attempts and to determine the extent to which any validated subject is able to interact with the TSF.	O.AUTH	X								X
Requirement ID: [SRS-8-29] The IEG-C SHALL contain the ability to validate the identity of other TOE components prior to distributing data to them.	O.ACCESSID	X	X	X	X	X	X	X	X	X

Requirement	Sources	IEG-C	Firewall	Network Switch	RDP Proxy	Web Proxy	Web Guard	Mail Guard	IDS	Management
Requirement ID: [SRS-8-30] The IEG-C SHALL provide a means to detect and reject the replay of authentication data as well as other TSF data and security attributes.	O.REPLAY_DETECTION	X					X	X		

8.3.5.7 Audit

Table 30 Audit: requirements, sources (including SFRs, if applicable) and applicability to IEG-C components

Requirement	Sources	IEG-C	Firewall	Network Switch	RDP Proxy	Web Proxy	Web Guard	Mail Guard	IDS	Management
Requirement ID: [SRS-8-31] The IEG-C SHALL provide measures for generating and recording security relevant events that will detect access attempts to TOE-protected resources by users.	O.AUDIT_GENERATION	X	X	X	X	X	X	X	X	X
Requirement ID: [SRS-8-32] The IEG-C shall provide the capability to protect audit information.	O.AUDIT_PROTECTION	X								X

Requirement	Sources	IEG-C	Firewall	Network Switch	RDP Proxy	Web Proxy	Web Guard	Mail Guard	IDS	Management
Requirement ID: [SRS-8-33] The IEG-C SHALL provide the capability to selectively view audit information, and alert the administrator of identified potential security violations.	O.AUDIT_REVIEW	X								X
Requirement ID: [SRS-8-34] The IEG-C SHALL provide reliable time stamps and the capability for the administrator to set the time used for these time stamps.	O.TIME_STAMPS	X								X
Requirement ID: [SRS-8-35] An IEG-C SHALL ensure that information exists that allows administrators to discover unintentional issues with the configuration and operation of the operating system and discover its cause. Gathering event information and immediately transmitting it to another system can also enable incident response in the event of system compromise.	O.ACCOUNTABILITY	X								X

8.3.5.8 Management

Table 31 Management: requirements, sources (including SFRs, if applicable) and applicability to IEG-C components

Requirement	Sources	IEG-C	Firewall	Network Switch	RDP Proxy	Web Proxy	Web Guard	Mail Guard	IDS	Management
Requirement ID: [SRS-8-36] The IEG-C SHALL provide an administrator role to isolate administrative actions, and to make the administrative functions available locally and remotely.	O.ADMIN_ROLE	X								X
Requirement ID: [SRS-8-37] The IEG-C SHALL provide all the functions and facilities necessary to support the administrators in their management of the security of the IEG-C, and restrict these functions and facilities from unauthorized use.	O.MANAGE	X								X
Requirement ID: [SRS-8-38] The IEG-C SHALL display an advisory warning regarding use of the IEG-C.	O.DISPLAY_BANNER	X								X

Requirement	Sources	IEG-C	Firewall	Network Switch	RDP Proxy	Web Proxy	Web Guard	Mail Guard	IDS	Management
Requirement ID: [SRS-8-39] The configuration of, and all changes to, the IEG-C and its development evidence SHALL be analysed, tracked, and controlled throughout the IEG-C's development.	O.CHANGE_MANAGEMENT	X								X
Requirement ID: [SRS-8-40] The IEG-C SHALL provide a mode from which recovery or initial start-up procedures can be performed.	O.MAINT_MODE	X								X
Requirement ID: [SRS-8-41] The IEG-C SHALL collect and store information about all events that may indicate a policy violation related to misuse, inappropriate access, or malicious activity on monitored networks.	O.SYSTEM_MONITORING	X								X

8.3.5.9 Trusted Update

Table 32 Trusted Update: requirements, sources (including SFRs, if applicable) and applicability to IEG-C components

Requirement	Sources	IEG-C	Firewall	Network Switch	RDP Proxy	Web Proxy	Web Guard	Mail Guard	IDS	Management
Requirement ID: [SRS-8-42]	A.REGULAR_UPDATES OE.UPDATES	X	X						X	
The IEG-C firmware and software SHALL be updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.	A.REGULAR_UPDATES O.UPDATES	X	X	X	X	X	X	X	X	
Requirement ID: [SRS-8-43] The IEG-C SHALL ensure the integrity of their update packages. OSs are seldom if ever shipped without errors, and the ability to deploy patches and updates with integrity is critical to enterprise network security. Conformant IEG-Cs provide execution environment-based mitigations that increase the cost to attackers by adding complexity to the task of compromising systems.	O.INTEGRITY	X	X	X	X	X	X	X	X	

8.3.5.10 Correct Operation

Table 33 Correct Operation: requirements, sources (including SFRs, if applicable) and applicability to IEG-C components

Requirement	Sources	IEG-C	Firewall	Network Switch	RDP Proxy	Web Proxy	Web Guard	Mail Guard	IDS	Management
Requirement ID: [SRS-8-44] The IEG-C SHALL provide a capability to test the TSF to ensure the correct operation of the TSF in its operational environment.		X	X	X	X	X	X	X	X	X
Requirement ID: [SRS-8-45] The IEG-C SHALL undergo appropriate independent vulnerability analysis and penetration testing to demonstrate the design and implementation of the TOE does not allow attackers with medium attack potential to violate the TOE's security policies.	O.VULNERABILITY_ANALYSIS	X	X	X	X	X	X	X	X	X
Requirement ID: [SRS-8-46] The IEG-C SHALL undergo appropriate security functional testing that demonstrates the TSF satisfies the security functional requirements.	O.THOROUGH_FUNCTIONAL_TESTING	X	X	X	X	X	X	X	X	X

Requirement	Sources	IEG-C	Firewall	Network Switch	RDP Proxy	Web Proxy	Web Guard	Mail Guard	IDS	Management
Requirement ID: [SRS-8-47] The IEG-C SHALL respond appropriately to its analytical conclusions about policy violations.	O.REACT	X							X	
Requirement ID: [SRS-8-48] The IEG-C SHALL ensure that any information contained in a protected resource is not released when the resource is reallocated; this includes that no residual information from a previously relayed message is transmitted.	O.RESIDUAL_INFORMATION	X	X				X	X	X	
Requirement ID: [SRS-8-49] The TSF SHALL maintain a domain for its own execution that protects itself and its resources from external interference, tampering or unauthorized disclosure.	O.SELF_PROTECTION	X	X				X	X		

9 Management Requirements

9.1 General

The management of the IEG-C can be categorised into the following categories for providing the functionality required to be supported by the IEG-C administrators performing the different administrative management roles (further specified in [SRS-3-24]):

- Service Management and Control (SMC);
- Communications and Information (CIS) Security; and,
- Cyber Defence.

Requirement ID: [SRS-9-1]

All Management capabilities MUST provide support for multiple concurrent administrators with access control to enable simultaneous access to the management capability from potentially distributed consoles with appropriately administered levels of access.

Requirement ID: [SRS-9-2]

Figure 32 illustrates the interfaces that MUST be provided by the IEG-C for managing the IEG-C remotely and locally.

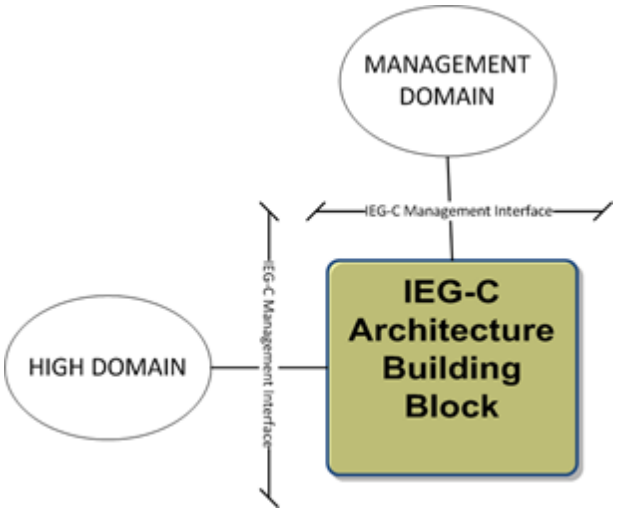

Figure 31 Management Interfaces exposed by IEG-C ABB

Requirement ID: [SRS-9-3]

The IEG-C MUST provide the capability to be managed remotely from a central location on the HIGH DOMAIN.

Requirement ID: [SRS-9-4]

To support remote management from a central location the IEG-C MUST offer the physical (or logical) IEG-C Management Interface implemented on top of the IEG-C High Domain Interface as described in Section 3.2.

Requirement ID: [SRS-9-5]

The IEG-C MUST provide the capability to be managed locally.

Requirement ID: [SRS-9-6]

To support local management the IEG-C MUST offer a physical network interface providing Ethernet connectivity to the management users on a separate security domain depicted as the MANAGEMENT DOMAIN in Figure 32

Requirement ID: [SRS-9-7]

The IEG-C Management Interface MUST support the operation 'ReceiveNetworkManagement' as specified in [NCIA TR/2016/NSE010871/01, 2017] section A.2.2.3.

Requirement ID: [SRS-9-8]

The IEG-C Management Interface MUST support the operation 'ForwardNetworkManagement' as specified in [NCIA TR/2016/NSE010871/01, 2017] section A.2.2.3.

Requirement ID: [SRS-9-9]

The IEG-C Management Interface SHALL be managed using one or more of the following protocols:

- HyperText Transport Protocol (HTTP) [IETF RFC 7230, 2014];
- Secure Shell Protocol (SSH) [IETF RFC 4251, 2006];
- Remote Desktop Protocol;
- Keyboard, Video and Mouse (KVM) over Ethernet;
- Simple Network Management Protocol (SNMP) v3 [IETF RFC 3410 – 3418, 2002].

Requirement ID: [SRS-9-10]

Remote Management traffic MUST be encrypted.

Requirement ID: [SRS-9-11]

The IEG-C Management Interface MUST support Transport Layer Security (TLS, [IETF RFC 8446, 2018]).

Requirement ID: [SRS-9-12]

The IEG-C Management Interface MUST support Datagram Transport Layer Security (DTLS, [IETF RFC 6353, 2011]).

Requirement ID: [SRS-9-13]

The IEG-C MUST offer the 'Communications Access Management' Interface on top of the IEG-C Management interface.

Requirement ID: [SRS-9-14]

The IEG-C MUST offer the 'Core Services Management' Interface on top of the 'Communications Access Management' Interface

Requirement ID: [SRS-9-15]

The IEG-C MUST support the 'ReceiveManagementContent' operation to provide connectivity for administrators on the MANAGEMENT DOMAIN.

Requirement ID: [SRS-9-16]

The operation 'ReceiveManagementContent' SHALL pass management content to the appropriate interface (see Sections 9.2, [SRS-9-83] and [SRS-9-98]).

Requirement ID: [SRS-9-17]

The IEG-C MUST support the 'ForwardManagementContent' operation that forwards management traffic to the MANAGEMENT DOMAIN.

Requirement ID: [SRS-9-18]

After receiving management content from the appropriate interface (see Sections 9.2, [SRS-9-83] and [SRS-9-98].), the operation 'ForwardManagementContent' SHALL forward the management content to the MANAGEMENT DOMAIN.

9.2 Service Management and Control

9.2.1 Management and Control functions

Effective management of the IEG-C and its services is critical. The ability to monitor and manage IEG-C services' performance and availability, configure and control IEG-C services for automating and improving end-to-end processes cross domain is a core capability provided by the IEG-C.

The IEG-C Element Management Services provide a suite of capabilities needed to facilitate Service Management and Control (SMC) Services and ensure that the Data Exchange Services, Protection Policy Enforcement Protection Services, and Protection Services are up and running, are accessible and available and that they are operating performing within agreed upon Quality of Service and Service Level Agreement (SLA) parameters for the IEG-C.

The IEG-C Element Management Services provide the following management and control functions:

- Configuration Management
- Event Management (including Logging, Alerting and Reporting)
- Performance and Capacity Management (including Monitoring, Metering and Message Tracking)

9.2.2 Configuration Management

In ITIL terms, Configuration Management is the process responsible for maintaining information about the Configuration Items (CI) required to deliver a Service, including their Relationships with one another. This information is managed throughout the lifecycle of the CI, and it typically stored in a Configuration Management Database (CMDB).

The Configuration Management process is most concerned with configuring, deploying and later decommissioning Data Exchange Services and Protection Services and their supporting platform. The IEG-C needs to provide the ability to change, capture, duplicate, backup or restore the configuration of the Data Exchange Services and Protection Services. The IEG-C needs to provide the ability to manage the operating systems that the IEG-C services are running on.

Requirement ID: [SRS-9-19]

An Enterprise CMDB already exists, and SHALL be used as the underpinning of the Platform's configuration management as well.

Requirement ID: [SRS-9-20]

The IEG-C SHALL support the Enterprise Configuration Management via an interface with the Enterprise configuration management database (BMC ITSM Atrium CMDB) to track IEG-C assets and their configuration information.

Requirement ID: [SRS-9-21]

The IEG-C MUST offer an interface 'SMC Configuration Management' that accepts an incoming 'SMC Message' for further processing.

Requirement ID: [SRS-9-22]

The 'SMC Configuration Management' Interface MUST provide the capability to manage the underlying operating system(s) hosting all the services provided by the IEG-C.

Requirement ID: [SRS-9-23]

The 'SMC Configuration Management' Interface MUST provide the capability to configure, deploy and decommission Data Exchange Services depending upon the information exchange requirement(s) that is (are) being supported.

Requirement ID: [SRS-9-24]

The 'SMC Configuration Management' Interface MUST provide the capability to configure, deploy and decommission Protection Services depending upon the information exchange requirement(s) that is (are) being supported.

Requirement ID: [SRS-9-25]

The 'SMC Configuration Management' Interface MUST provide the capability to provides the ability to change, capture, duplicate, backup or restore the configuration of the Protection Policy Enforcement Services depending upon the information exchange requirement(s) that is (are) being supported.

Requirement ID: [SRS-9-26]

The 'SMC Configuration Management' Interface MUST support the following operations:

- ‘Configure OS’;
- ‘Configure Data Exchange Services’;
- ‘Configure Protection Services’; and,
- ‘Configure Protection Policy Enforcement Services’.

Requirement ID: [SRS-9-27]

The operation 'Configure OS' SHALL support SMC Messages of the following types:

- Secure Shell (SSH, [IETF RFC 4253, 2006]);
- Network Time Protocol (NTP, [IETF RFC 5905, 2010]);
- Remote Desktop Protocol (RDP);
- Intelligent Platform Management Interface (IPMI, [IPMI V2.0, 2013]);
- Hypertext Transport Protocol Message (HTTP, [IETF RFC 7230, 2014]).

Requirement ID: [SRS-9-28]

The operation 'Configure OS' SHALL support the management of the IEG-C hardware (virtual or physical) and software resources including configuration of common services provided by the operating system (OS) for applications running on the operating system. These common services include application execution, input/output operations, file system, communication, resource allocation, control access to OS resources and time synchronisation.

Requirement ID: [SRS-9-29]

The operation 'Configure Data Exchange Services' SHALL support SMC Messages of the following types:

- Secure Shell (SSH, [IETF RFC 4253, 2006]);
- Remote Desktop Protocol (RDP);
- Hypertext Transport Protocol Message (HTTP, [IETF RFC 7230, 2014]).

Requirement ID: [SRS-9-30]

The operation 'Configure Protection Services' SHALL support SMC Messages of the following types:

- Secure Shell (SSH, [IETF RFC 4253, 2006]);
- Remote Desktop Protocol (RDP);
- Hypertext Transport Protocol Message (HTTP, [IETF RFC 7230, 2014]).

Requirement ID: [SRS-9-31]

The operation 'Configure Protection Policy Enforcement Services' SHALL support SMC Messages of the following types:

- Secure Shell (SSH, [IETF RFC 4253, 2006]);
- Remote Desktop Protocol (RDP);
- Hypertext Transport Protocol Message (HTTP, [IETF RFC 7230, 2014]).

Requirement ID: [SRS-9-32]

The IEG-C 'SMC Configuration Management' Interface SHALL pass outgoing SMC Messages to the interface 'Core Services Management' for further processing.

9.2.3 Event Management

In ITIL terms, an “event” can be defined as any detectable or discernible occurrence that has significance for the management of the infrastructure or the delivery of a Service. Event Management is the process that monitors all events that occur throughout the Platform. It allows for normal operation, but also detects and escalates exception conditions.

For the Platform, Event Management includes:

- Logging,
- Alerting
- Reporting

Requirement ID: [SRS-9-34]

The IEG-C SHALL collect events generated from all IEG-C services and forward them to the Enterprise Event Management System.

Requirement ID: [SRS-9-35]

The IEG-C SHOULD support monitoring based on the Microsoft System Center Operations Manager (SCOM).

Requirement ID: [SRS-9-36]

The IEG-C SHALL support SNMP v3 [IETF RFC 3412, 2002] with standards-based and proprietary-specific Management Information Bases (MIBs).

Requirement ID: [SRS-9-37]

The IEG-C SHALL provide a toolset which allows Administrators to define, filter, correlate and group events according to their context, criticality, source and impacts.

Requirement ID: [SRS-9-38]

The IEG-C SHALL provide an event correlation toolset that can be either customizable or adaptive to detect normal and abnormal behaviour patterns.

Requirement ID: [SRS-9-39]

The IEG-C MUST offer an interface 'SMC Event Management' that accepts an incoming 'SMC Message' for further processing.

Requirement ID: [SRS-9-40]

The 'SMC Event Management' Interface MUST support the following operations:

- ‘Log’;
- ‘Alert’; and,
- ‘Report’.

9.2.3.1 Logging

Logging is the act of keeping a log, which is a file that records either events that occur in software or messages between different users. In the simplest case, messages are written to a single log-file.

Requirement ID: [SRS-9-41]

The IEG-C SHALL support Data Exchange Services logging for monitoring access requests for information from both the High Domain and the Low Domain.

Requirement ID: [SRS-9-42]

The IEG-C SHALL provide the capability to examine recorded historical logs and archives.

Requirement ID: [SRS-9-43]

The IEG-C SHALL support the correlation of requests and responses in order to track all responses (or faults) with the correct request for information access.

Requirement ID: [SRS-9-44]

The IEG-C SHALL log request and response attributes to include:

- time-stamp;
- source and target address(es);
- URL;
- Operation;
- Size; and
- Unique request id (extracted from the request/response or automatically generated by the IEG-C Logging Services).

Requirement ID: [SRS-9-45]

The IEG-C SHALL also provide functionality to log attributes extracted from the payload.

Requirement ID: [SRS-9-46]

The IEG-C SHALL provide functionality to log selectively whole messages based on pre-configured criteria or filter (e.g. policy based).

Requirement ID: [SRS-9-47]

The IEG-C SHALL provide a log analysis tool that allows a search for log events based on combinations of search criteria across all fields in the log record format supported by this system.

Requirement ID: [SRS-9-49]

The IEG-C SHALL provide the capability to aggregate generated log messages for all instances of services of IEG-C.

Requirement ID: [SRS-9-50]

The operation 'Log' SHALL support SMC Messages of the following types:

- Syslog Message [IETF RFC 5424, 2009]; and,
- Hypertext Transport Protocol Message (HTTP/1.1, [IETF RFC 7230, 2014], HTPP/2.0 [IETF RFC 7540, 2015]).

Requirement ID: [SRS-9-51]

The IEG-C 'SMC Event Management' Interface SHALL pass outgoing 'Log' SMC Messages to the interface 'Core Services Management' for further processing.

9.2.3.2 Alerting

The IEG-C and the services hosted on it, will have certain expectations of service availability, performance, security and other parameters. These may be expressed as Key Performance Indicators (KPI), Service Level Agreements (SLA) or other metrics.

The Alerting functionality of the IEG-C SMC capability is closely tied to the Monitoring functionality, in which the “health” of the system is continually evaluated. In all cases, when the acceptable threshold for a service (or the IEG-C) is detected to be approaching or reached, the system will automatically generate an Alert event.

An Alert can either be a:

- “Warning” (indicating that it is necessary to take action in order to prevent an exception occurring); or,
- “Exception” (indicating that the service is currently operating below the normal predefined parameters/indicators)

While this functionality is closely related to the Event Management system, there are some unique requirements for the IEG-C, including the ability to alert on intrusion attacks.

Requirement ID: [SRS-9-52]

The IEG-C SHALL provide a toolset to configure rule based event filtering, and to automate alert triggering capabilities.

Requirement ID: [SRS-9-53]

The IEG-C SHALL provide functionality to generate alerts associated with IEG-C services to include:

- breach of performance or capacity thresholds;
- SLAs can't be met; and
- specific mechanisms to enforce SLAs were activated (e.g. throttling).

Requirement ID: [SRS-9-54]

The IEG-C SHALL provide functionality to generate an alert about stalled processes (e.g. a compromised content filter).

Requirement ID: [SRS-9-55]

The operation 'Alert' SHALL support SMC Messages of the following types:

- Simple Network Management Protocol (SNMP) v3 Message [IETF RFC 3410-3418, 2002]
- Syslog [IETF RFC 5424, 2009];

Requirement ID: [SRS-9-56]

The IEG-C 'SMC Event Management' Interface SHALL pass outgoing 'Alert' SMC Messages to the interface 'Core Services Management' for further processing.

9.2.3.3 Reporting

An SMC system needs to provide thorough, highly customizable reports for compliance, auditing, billing, service value determination, and so on.

The Reporting component is distinct from the Monitoring component in that Monitoring occurs in real time, while Reporting (usually) happens *post facto*.

Requirement ID: [SRS-9-57]

The IEG-C SHALL provide operational and historical reports on events.

Requirement ID: [SRS-9-58]

The IEG-C SHALL provide a toolset allowing for custom report building and saving.

Requirement ID: [SRS-9-59]

The IEG-C SHALL be able to generate

- SLA compliance reports
- error/exception reports
- service usage reports
- other customizable reports based on captured metrics which can be filtered and sorted based on various criteria

Requirement ID: [SRS-9-60]

The IEG-C SHALL be able to provide performance trend analysis.

Requirement ID: [SRS-9-61]

The operation 'Report' SHALL support SMC Messages of the following types:

- Simple Network Management Protocol (SNMP) v3 Message [IETF RFC 3410-3418, 2002]
- Comma Separated Values (CSV)

Requirement ID: [SRS-9-62]

The IEG-C 'SMC Event Management' Interface SHALL pass outgoing 'Report' SMC Messages to the interface 'Core Services Management' for further processing.

9.2.4 Performance and Capacity Management

In order to be able to identify problems and bottlenecks in the network or service infrastructure the need for sophisticated traffic monitoring and performance analysis platform was identified. The IEG-C System Administrators require insight into basic performance parameters, including network utilization levels (instantaneous, peak, average or trends), statistics on the collected traffic (protocol distribution, to/from information, packet lengths or errors), network response times and measured throughputs, error counters of interfaces etc.

Such a capability will provide immediate identification of potential bottlenecks or outages, and enable the IEG-C System Administrators to take proactive measures to circumvent bottlenecks or to throttle down low priority traffic in case overall bandwidth is not sufficient to satisfy all communication requirements.

For the Platform, Performance and Capacity Management includes:

- Monitoring
- Metering

Requirement ID: [SRS-9-63]

The IEG-C MUST offer an interface 'SMC Performance Management' that accepts an incoming 'SMC Message' for further processing.

Requirement ID: [SRS-9-64]

The 'SMC Performance Management' Interface MUST support the following operations:

- ‘Monitor’; and
- ‘Meter’;

9.2.4.1 Monitoring

Monitoring observes and tracks the operations and activities of end users on the IEG-C, thus providing a way to supervise the overall processes that are performed.

Requirement ID: [SRS-9-65]

The IEG-C SHALL monitor the status and quality of service, (including availability, performance, and utilisation) of the IEG-C infrastructure and the IEG-C Services hosted on the IEG-C.

Requirement ID: [SRS-9-66]

The IEG-C SHALL provide functionality for real time monitoring of IEG-C Services against expected KPI, SLA, or other metric thresholds as configured.

Requirement ID: [SRS-9-67]

The IEG-C SHALL provide visibility on usage patterns over daily, monthly and variable periods. This toolset shall support trend and abnormal behaviour analysis.

Requirement ID: [SRS-9-68]

The IEG-C SHALL provide customizable dashboards for monitoring selected statistics and metrics for IEG-C services.

Requirement ID: [SRS-9-69]

The IEG-C SHALL provide the capability to monitor requests for information access attempts cross domain through the IEG-C services.

Requirement ID: [SRS-9-70]

The IEG-C SHALL provide functionality to monitor service faults and exceptions.

Requirement ID: [SRS-9-71]

The operation 'Monitor' SHALL support SMC Messages of the following types:

- Simple Network Management Protocol (SNMP) v3 Message [IETF RFC 3410-3418, 2002]

Requirement ID: [SRS-9-72]

The IEG-C 'SMC Performance Management' Interface SHALL pass outgoing 'Monitor' SMC Messages to the interface 'Core Services Management' for further processing.

9.2.4.2 Metering

Metering measures levels of resource utilization consumed by service subscribers. Measured data is stored for summarizing and analysing.

Requirement ID: [SRS-9-73]

The IEG-C SHALL be able to collect and present the statistics on service utilisation broken down by end user or system which can be used for metering, billing and other purposes.

Requirement ID: [SRS-9-74]

The IEG-C SHALL aggregate collected statistics for a given end user or system or group of end user or system over specified periods of time.

Requirement ID: [SRS-9-75]

The IEG-C SHALL archive and make available for retrieval and reporting collected and aggregated statistics.

Requirement ID: [SRS-9-76]

The operation 'Meter' SHALL support SMC Messages of the following types:

- Simple Network Management Protocol (SNMP) v3 Message [IETF RFC 3410-3418, 2002]

Requirement ID: [SRS-9-77]

The IEG-C 'SMC Performance Management' Interface SHALL pass outgoing 'Meter' SMC Messages to the interface 'Core Services Management' for further processing.

9.3 CIS Security Management

Requirement ID: [SRS-9-78]

The IEG-C SHALL provide the capability to allow the CIS Security Administrator to fulfil their role.

Requirement ID: [SRS-9-79]

The IEG-C MUST offer an interface 'CIS Security' that accepts an incoming 'CIS Security Message' for further processing.

Requirement ID: [SRS-9-80]

The 'Cyber Defence' Interface MUST support the following operations:

- ‘Manage Public Key Material’;
- ‘Manage Protection Policies’; and,
- ‘Review’.

9.3.1 Manage Public Key Material

Requirement ID: [SRS-9-81]

The IEG-C SHALL provide the Security administrator the ability to perform all necessary functions regarding the management of cryptographic key material.

Requirement ID: [SRS-9-82]

The management of key material SHALL be compliant with CIS Security Technical and Implementation Guidance in Support of Public Key Infrastructure - Cryptographic Aspects [NAC AC/322-D(2007)0002-REV1, 2015].

Requirement ID: [SRS-9-84]

The IEG-C 'CIS Security' Interface SHALL pass outgoing 'Manage Public Key Material' CIS Security Messages to the interface 'Core Services Management' for further processing.

9.3.2 Manage Protection Policies

Requirement ID: [SRS-9-85]

The IEG-C SHALL provide the capability for a Security administrator to manage the full lifecycle of the Information Flow Control Policies and the Content Inspection Policies that are required to be enforced by the Protection Policy Enforcement Services dependent upon the information exchange requirements.

Requirement ID: [SRS-9-86]

The IEG-C SHALL provide the capability to support the creation, modification and deletion of the protection policies including the activation and de-activation of those protection policies.

Requirement ID: [SRS-9-87]

The IEG-C 'Manage Protection Policies' operation SHALL also support backing up and restoring of policies.

Requirement ID: [SRS-9-88]

The IEG-C SHALL provide the Security administrator with the capability to manage the Protection Services with tasks such as update IDS signatures, anti-virus signatures, manage content filters and patch hardware and software.

Requirement ID: [SRS-9-200]

The patching of IEG-C components SHAL be performed centrally from the Service Operation Centre (SOC).

Requirement ID: [SRS-9-89]

The operation 'Manage Protection Policies' SHALL support CIS Security Messages of the following types:

- Secure Shell (SSH, [IETF RFC 4253, 2006]);
- Hypertext Transport Protocol Message (HTTP, [IETF RFC 7230, 2014]);
- HTTP over TLS ([IETF RFC 2818, 2000]).

Requirement ID: [SRS-9-90]

The IEG-C 'CIS Security' Interface SHALL pass outgoing 'Manage Protection Policies' CIS Security Messages to the interface 'Core Services Management' for further processing.

9.3.3 Review

Requirement ID: [SRS-9-91]

The IEG-C SHALL provide the capability to the Audit manager to review audit logs.

Requirement ID: [SRS-9-92]

The operation 'Review' SHALL support CIS Security Messages of the following types:

- Secure Shell (SSH, [IETF RFC 4253, 2006]);
- Hypertext Transport Protocol Message (HTTP, [IETF RFC 7230, 2014]);
- HTTP over TLS ([IETF RFC 2818, 2000]).

9.4 Cyber Defence Management

Requirement ID: [SRS-9-93]

The IEG-C SHALL provide the capability to allow the Cyber Defence Administrator to fulfil their role.

Requirement ID: [SRS-9-94]

The IEG-C MUST offer an interface 'Cyber Defence' that accepts an incoming 'Cyber Defence Message' for further processing.

Requirement ID: [SRS-9-95]

The 'Cyber Defence' Interface MUST support the following operations:

- ‘Assess’;
- ‘Respond’; and,
- ‘Recover’.

9.4.1 Assess

Requirement ID: [SRS-9-96]

The IEG-C SHALL provide the Cyber Defence administrator with the capability to assess damage and attacks/faults identifying IEG-C components that have been affected by attacks and faults.

Requirement ID: [SRS-9-97]

The IEG-C SHALL support analysis and evaluation of attacks.

Requirement ID: [SRS-9-201]

For all its components the IEG-C SHALL support the generation of cybersecurity-related log, alert, and event data in accordance with the NATO Enterprise Security Monitoring Guidance [NCI Agency TR/2017/NCB010400/12, 2017] and the Technical and Implementation Directive on CIS Security [NAC AC/322-D/0048-REV3, 2019].

Requirement ID: [SRS-9-98]

For all its components the IEG-C SHALL support the aggregation of cybersecurity-related log, alert, and event data to a central repository or log aggregator as provided by the monitoring infrastructure in use by NCSC..

Requirement ID: [SRS-9-202]

For all its components the IEG-C SHALL support the ingestion of cybersecurity-related log, alert, and event data in the SIEM solution that is operated by NCSC.

Requirement ID: [SRS-9-203]

For all its components the IEG-C SHALL ensure that all cybersecurity-related log, alert, and event data can be parsed correctly by the SIEM solution that is operated by NCSC.

Requirement ID: [SRS-9-99]

The operation 'Assess' SHALL support Cyber Defence Messages of the following types:

- Secure Shell (SSH, [IETF RFC 4253, 2006]);
- Hypertext Transport Protocol Message (HTTP, [IETF RFC 7230, 2014]);
- HTTP over TLS ([IETF RFC 2818, 2000]).

Requirement ID: [SRS-9-100]

The IEG-C 'Cyber Defence' Interface SHALL pass outgoing 'Assess' Cyber Defence Messages to the interface 'Core Services Management' for further processing.

9.4.2 Respond

Requirement ID: [SRS-9-101]

The IEG-C SHALL provide the Cyber Defence administrator with the required functionality to take the required action to dynamically mitigate the risk identified by a suspected attack/fault.

Requirement ID: [SRS-9-102]

The IEG-C SHALL provide the capability to control traffic flows including termination, throttling to a certain level of bandwidth or with a certain delay, redirection, or otherwise modify the flow for the purpose of stopping or mitigating an attack or fault.

Requirement ID: [SRS-9-103]

The IEG-C SHALL provide capability for traffic flows to be terminated or limited in capacity in order to stop or reduce the effect of an attack or a fault.

Requirement ID: [SRS-9-105]

The operation 'Respond' SHALL support Cyber Defence Messages of the following types:

- Secure Shell (SSH, [IETF RFC 4253, 2006]);
- Hypertext Transport Protocol Message (HTTP, [IETF RFC 7230, 2014]);
- HTTP over TLS ([IETF RFC 2818, 2000]).

Requirement ID: [SRS-9-106]

The IEG-C 'Cyber Defence' Interface SHALL pass outgoing 'Respond' Cyber Defence Messages to the interface 'Core Services Management' for further processing.

9.4.3 Recover

Requirement ID: [SRS-9-107]

The IEG-C SHALL provide the Cyber Defence administrator with the required functionality to take the required action to recover from an attack/fault.

Requirement ID: [SRS-9-108]

The IEG-C SHALL provide the capability to restore IEG-C components that were affected by an attack/fault.

Requirement ID: [SRS-9-109]

The operation 'Recover' SHALL support Cyber Defence Messages of the following types:

- Secure Shell (SSH, [IETF RFC 4253, 2006]);
- Hypertext Transport Protocol Message (HTTP, [IETF RFC 7230, 2014]);
- HTTP over TLS ([IETF RFC 2818, 2000]).

Requirement ID: [SRS-9-110]

The IEG-C 'Cyber Defence' Interface SHALL pass outgoing 'Recover' Cyber Defence Messages to the interface 'Core Services Management' for further processing.

9.5 Audit Management

Requirement ID: [SRS-9-111]

The IEG-C SHALL provide the capability to allow the Audit Administrator to fulfil their role.

Requirement ID: [SRS-9-112]

The IEG-C SHALL be interoperable with NATO auditing and system management tools.

Requirement ID: [SRS-9-113]

The IEG-C SHALL provide the capability to detect and create records of security-relevant events associated with users.

Requirement ID: [SRS-9-114]

The IEG-C SHALL provide the capability to detect and create records of security-relevant events associated with end users requests for accessing information cross domain.

Requirement ID: [SRS-9-115]

The IEG-C SHALL provide the capability to appropriately classify and protect audit information in accordance with NATO security policy.

Requirement ID: [SRS-9-116]

The IEG-C SHALL include mechanisms to protect audit logs from unauthorised access, modification and deletion.

Requirement ID: [SRS-9-117]

The IEG-C SHALL provide the capability to selectively view audit information, and alert the Audit Administrator of identified potential security violations.

Requirement ID: [SRS-9-118]

The IEG-C SHALL provide reliable time stamps and the capability for the Audit Administrator to set the time used for these time stamps.

Requirement ID: [SRS-9-119]

The IEG-C SHALL generate and maintain an audit log for each of the general auditable events:

- IEG-C start-up and shutdown
- IEG-C Users logon and logoff
- Creation, modification (i.e. changes to permissions) or deletion of user accounts
- Changes to security related system management functions
- Audit log access
- Creation, modification or deletion of audit log records
- Invocation of privileged operations
- Modification to IEG-C access rights
- Unauthorised attempts to access IEG-C system files

Requirement ID: [SRS-9-204]

All audit logs SHALL record the date, time, details of change and the user.

Requirement ID: [SRS-9-120]

The IEG-C SHALL generate and maintain an audit log for each of the Data Exchange Services auditable events:

- Data Exchange Services Start-up and shutdown
- Unauthorised attempts to request access to information cross domain
- Unauthorised attempts to modify Data Exchange Services configuration
- Failed Data Exchange Services operations

Requirement ID: [SRS-9-121]

The IEG-C SHALL generate and maintain an audit log for each of the Protection Services auditable events:

- Protection Services start-up and shutdown
- Failed Protection Services operations

- Unauthorised attempts to modify Protection Services configuration
- Creation, modification and deletion of Public Key Cryptographic Services keying material
- Updates of Intrusion Detection Services IDS signatures
- Updates of Content Inspection Services content filters
- Failed certificate path validation and revocation

Requirement ID: [SRS-9-122]

The IEG-C SHALL generate and maintain an audit log for each of the Protection Policy Enforcement Services auditable events:

- Protection Policy Enforcement Services start-up and shutdown
- Failed Protection Policy Enforcement Services operations
- Unauthorised attempts to create, modify or delete Information Flow Control policies
- Unauthorised attempts to create, modify or delete Content Inspection policies

Requirement ID: [SRS-9-123]

The IEG-C SHALL archive the audit log after a period of time as configured by the Audit Administrator.

Requirement ID: [SRS-9-124]

By default the audit log SHALL be archived daily.

Requirement ID: [SRS-9-125]

The IEG-C SHALL automatically back up audit logs at configurable intervals.

Requirement ID: [SRS-9-126]

The IEG-C SHALL provide integrity checking countermeasures to ensure that the audit log has been archived correctly.

Requirement ID: [SRS-9-127]

The IEG-C SHALL alert the Audit Administrator when the audit log exceeds a configurable percentage of the configurable maximum permitted size.

Requirement ID: [SRS-9-128]

By default the configurable percentage SHALL be 90% of the configurable maximum permitted size.

APPENDIX A: Web Guard General System Description

A.1 Purpose of the system

A.1.1 Introduction

This section provides a general overview of the expected role and functionality of an implementation of a 'Web Guard Capability' (WG). Note that the abbreviation 'WG' stands for the capability, and not necessarily for a single (physical or virtual) system; in other words, a Web Guard Capability may be composed of more than one system.

A.1.2 Enabling cross-domain information exchange

The WG is part of the Information Exchange Gateway (IEG) case C (IEG-C) and enables information exchange between communities-of-interest (COIs) in the NATO Secret ('High') and Mission Secret ('Low') network domains. The WG does not mediate all traffic that passes through the IEG-C; a subset of the information transfer is handled by the WG. This subset is characterized by:

- the COIs that exchange information;
- the protocol used (HTTP);
- the type of information exchange scenario used by the COI; and
- the use of NATO labelling [STANAG 4774], [STANAG 4778], i.e. the WG mediates information transfer for information that is labelled following the [STANAG 4774], [STANAG 4778].

For example, the WG will not mediate e-mail traffic or directory service traffic, however it is able to mediate HTTP traffic with labelled HTTP message content, see Section A.2. HTTP traffic with unlabelled HTTP message content will be handled be a separate proxy, i.e. Web Proxy, see section 4.4. Figure A.1 illustrates the role of the Web Guard Capability in the IEG-C.

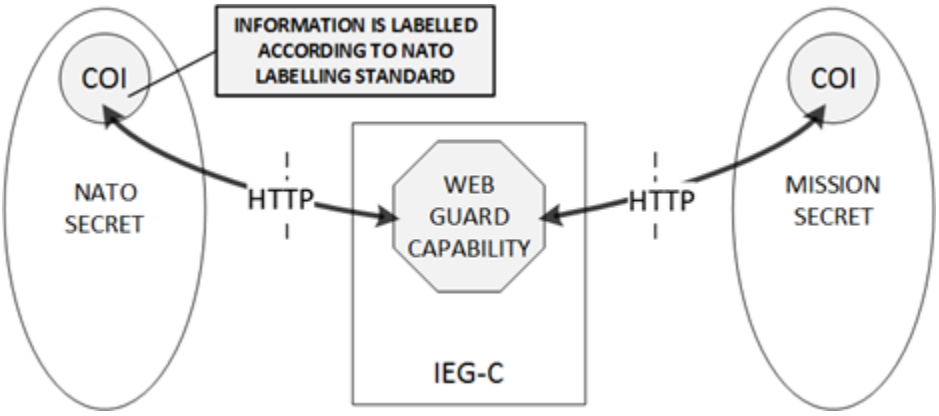

Figure 32 The Web Guard Capability is part of the IEG-C and handles the subset of the IEG-C information transfer that is labelled according to the NATO Labelling standard [STANAG 4774] and transferred over HTTP

A.1.3 Cross-domain solution

The WG offers a cross-domain solution (CDS) that is based on the use of labels (conformant to [STANAG 4774]), following the concept of Object Level Protection (OLP, [NCIA TR-2012-SPW008418-29, 2014]). The key function of the WG is to allow