It is responsible of any support that involves a change to the system baseline, such as software patches or new releases. It is responsible of specialised hardware repair, if applicable. Third level maintenance is activated by third level support and can be initiated either to define the solution to a problem (corrective maintenance) or to maintain up to date software configuration (adaptive maintenance following changes to the underpinning hardware, firmware and software environment) e.g. security patches, operating system upgrades, minor software configuration changes due to operational/interface needs.

It implement the initial preventive Maintenance procedures and any additional Service/Capability and/or site specific procedures that are defined in the corresponding Manual. 3rd Level Maintenance procedures can require specialised tools and/or Personnel.

Fourth Level of Maintenance

It is the responsibility of the hardware vendor or the software original developer. It is activated from the 3rd level of maintenance only when it is needed.

Annex G Independent Verification and Validation Templates

In this annex are attached the templates which will be utilized during the contract execution and they are referred to in the main body of this SOW. These templates are evolving and are provided here for indication and estimation of effort only. Definite versions will be communicated and incorporated before Contract Signature. These templates will also be provided electronically.

Test Plan template

Test Case Specification Template

Test Completion Report Template

Project Master Test Plan Template

Test Readiness Review -Checklist

Project Requirements Traceability Matrix Template

Annex H NCIA monitoring capability systems and services

H1. The integration between IEG-C infrastructure (systems and software) and NCIA's monitoring capability systems and services will conform to the NATO Enterprise Security Monitoring Guidance [NCI Agency TR/2017/NCB010400/12, 2017]

H2. This integration comprises the following activities and corresponding roles and responsibilities for the Contractor and the Purchaser:

Activity	Contractor	Purchaser
Site survey	Develop and provide site survey workbooks (with appropriate detail)	Validate and approve site survey workbooks
	Execute surveys: On each site the requirements of the NCSC Enclaves must be covered (e.g. requirements on connectivity between IEG-C and NCSC Enclaves)	Guide and validate surveys
Design	Draft and propose a design of the integration of the IEG-C with the NCSC monitoring capability • Include the physical, hardware and software interfaces in the design. • Address the aspect of scaleability of the design, taking into account: • The number of events per second that will be consumed by the NCSC monitoring capability upon deployment of the IEG-C and as expected in the future. • Impact on NCSC back-end systems and services (CSOC).	Provide information, review and approve the design
Identify necessary changes and updates to existing NCSC monitoring capability systems and services	Based on the site surveys and design, identify necessary changes and updates to NCSC monitoring capability systems and services and NSCN enclaves (also referred to as "NCIRC enclaves"). • Include consideration of module additions, component capacity changes, configuration changes etc. • Ensure proposed changes are aligned with the existing solution in terms of choice of equipment and vendors.	Review and approve the changes

Install components	Enable network connectivity between IEG-C and the NCSC monitoring capability. Install (software) agents on IEG-C components as required	Provide support and oversight to installation process, and perform CSOC-configuration as required
Configure monitoring components and IEG-C systems	In the event additional hardware components are procured, perform basic configuration based on NCSC guidance so that central management of these components by NCSC becomes possible	Provide supporting information (e.g. IP-addresses)
	Perform configuration of IEG-C components in accordance with the Purchaser's Guidance	Provide guidance and validate configuration
Migrate configurations of existing systems/solutions	Provide support to NCSC team to migrate and update necessary configurations within the NCSC enclave	Review existing system configurations, develop migration plan, and perform migration
Plan and execute test activities	Prepare test plan and procedures in accordance with the other test activities within the scope of this project	Review and approve test plan
	Execute test activities and document results	Provide oversight and validate results
Document the IEG-C monitoring solution as built	Prepare documentation	Validate and approve documentation
Provide training	Provide training material on the part of the IEG-C monitoring solution, which is not covered by the existing NCSC monitoring capability	Review and approve material
	Provide training to Purchaser (NCSC)	Participate and validate
Handover IEG-C monitoring solution	Finalize handover requirements regarding the part of the IEG-C monitoring solution, which is not covered by the existing NCSC monitoring capability	Review, validate and take over

Table 27

NATO Communications and Information Agency
Agence OTAN d'information et de communication

IEG Case C

IFB-CO-14314-IEG-C

BOOK II - PART IV SOW Annex A

SYSTEM REQUIREMENTS SPECIFICATION (SRS)

Table of Contents

Figures

Tables

1 Introduction

1.1 Purpose

This System Requirement Specification (SRS) describes the external behaviour of the system to be delivered under the IEG-C project, hereinafter referred to as 'IEG-C'. It also describes non-functional requirements, design constraints and other factors necessary to provide a comprehensive description of the requirements for the system.

This document supports increment 1 of Project 2014/0IS03102, which is included in Capability Package (CP) 9C0150, which covers the Information Exchange Gateway (IEG) Services for NATO SECRET to MISSION SECRET.

1.2 Scope

The Bi-SC CP9C0150 Project OIS03102 "Provide Information Exchange Service" increment 1 "Information exchange between NATO classified networks and NATO-led Mission Secret (MS) networks (Scenario C)" is to provide the IEG static capability to connect NATO CIS and Mission CIS at Secret level domain.

The scope of this document is to define the requirements for a standardized IEG-C architecture to provide a standardized gateway between NATO Secret (NS) networks and NATO-led Mission Secret (MS) networks for both Static and Deployable envionments that:

- Allows the Information Exchange between NATO Secret (NS) Network Domain and Mission Secret (MS) Network Domain instances implemented within the existing NATO Secret physical infrastructure at centralized locations;
- Releases information from NS to MS based on predefined criteria tailored to the specific Mission requirement; data failing to meet the release criteria shall be blocked and the internal domain notified accordingly;
- Allows the transfer of the information from MS to NS based on predefined criteria tailored to specific Mission requirement; data failing to meet the acceptance criteria shall be rejected or dropped and the sender notified accordingly. This functionality can be configurable depending on the operation.

1.3 Acronyms and Abbreviations

The acronyms and abbreviations used in this SRS are defined in Annex D of the Statement of Work.

1.4 Definitions

The definitions used in this SRS are defined in Annex E of the Statement of Work.

1.5 Overview

This SRS comprises 9 sections:

- Section 1 provide an introduction and describes the use of his document
- Section 2 provides a general description of the IEG-C, the roles involved and the project constraints.
- Section 3 provides an overview of the IEG-C Target Architecture and Logical Architecture.

- Section 4 specifies requirements for IEG-C components in general, interfaces, and integration of components.
- Section 5 specifies the non-functional requirements for the IEG-C.
- Section 6 specifies the functional requirements (including security functional requirements) for the Web Guard.
- Section 7 specifies the functional requirements (including security functional requirements) for the Mail Guard.
- Section 8 specifies the IEG-C security requirements.
- Section 9 specifies the IEG-C management requirements.
- Appendix A provides a general system description of the Web Guard.
- Appendix B provides an overview of relevant service interface profiles.
- Appendix C provides the security problem definition and security objectives for the IEG-C.
- Appendix D provides details of the Equipment Specifications.
- Appendix E provide a summary of the Component Names used in the SRS

1.6 SRS Conventions

The system requirements, defined in this document, are individually identified by a unique number which shall be used at all times as the specific reference for each.

No meaning is associated with the order of serial numbering. There could be gaps in numbering and requirement identifiers in a group do not have to be sequential.

Requirement identifiers are encapsulated in square brackets.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [IETF RFC 2119, 1997].

The requirements in this SRS have an identifier of the form [SRS-Section Number-Requirement Number], e.g. [SRS-1-228], and are enclosed within a box.

Requirement ID: [SRS-1-228]

Example SRS requirement.

The requirements in this SRS make use of logical names to describe the components of the system and their associated requirements. The logical names follow the naming used in the IEG-C Target Architecture [TR/2016/NSE010871/01, 2016], and a complete list of names is provided for reference in Appendix E.

1.7 Applicable References

The abbreviated document titles given in square brackets, […], are used to refer to documents in the reference lists in section 2 of Book II – Part IV Statement of Work (SOW).

1.8 Standards and Specifications

The standards and specifications are indicated in square brackets, […], and refer to documents in the reference lists in section 2 of Book II – Part IV Statement of Work (SOW).

1.9 Verification Methods

The requirements in this SRS will be verified through qualification, herein defined as an endorsement with a guarantee and supporting documentation that the item being qualified satisfies the specified requirement(s). The different verification methods applicable to the requirements herein are described in the following paragraphs.

Note: In some cases, more than one verification method might be required in order to verify fulfilment of a requirement.

1.9.1 Inspection

Inspection is the visual examination of an item (hardware and software) and associated descriptive documentation. Verification is based on the human senses (sight, touch) or other means that use simple measurement and handling methods. No stimulus is necessary. Passive resources such as meter rule, gauge may be used.

For Non-Developmental Items (NDI), Modified NDI and Developmental Items, hardware inspection is used to determine if physical constraints are met, and hardware and/or software, inspection is used to determine if physical quantity lists are met.

1.9.2 Analysis

Analysis is the review and processing of design products (documentation, drawings, presentations, etc.) or accumulated data obtained from other qualification methods, such as manufacturer's tests of a product to be mass-produced, to verify that the system/component design meets required design criteria.

1.9.3 Testing

Testing is the operation of the system, or a part of the system, under controlled and specified conditions, generally using instrumentation, other special test equipment or specific test patterns to collect data for later analysis. This verification method usually requires recorded results to verify that the requirements have been satisfied.

2 General System Description

2.1 Operational and Technical Overview

The IEG-C is a Data Loss Prevention guard at the interface between the (or a) NATO SECRET (NS) domain and a NATO-led ‘mission’ domain, such as ‘Resolute Support’ and KFOR. The guard approves or rejects the transmission of data between the two security domains based on either a STANAG-compliant trusted classification label, such as ‘NATO <classification> Releasable to <mission>’ or trusted source to trusted destination mediated by firewall rule sets. The reason for the trusted source/destination path is that not all current NATO services and apps are ‘label aware’.

The overall requirement for the IEG-C is to allow a mission command structure to operate the full range of military command and control IT functions where the staff and users include NATO and non-NATO mission partners. All non-NATO mission partners will have security agreements with NATO such that they are authorised to access information classified up to NATO SECRET Releasable to

<Mission>. In such a situation, two IT systems are provided; one classified ‘NATO SECRET’ to process information that is required for the mission but not releasable to non-NATO partners (typically J2 data) and one classified <Mission> SECRET that is accessible to all authorised mission partners, both NATO and non-NATO.

For practical purposes, the majority of users are typically provided with access to the mission IT system. Users in the NS domain (both local and in the static NS domain) can be granted access to services and data in the <Mission> SECRET domain, but users in the <Mission> SECRET domain are prevented from any access to the NS domain. The NATO requirement for users with elevated privileges (e.g. system administrators) to have a security clearance higher than the level of the system they operate means that only NATO cleared users can be granted such permissions. Where both NS and <Mission> SECRET IT systems are provided, data transfer requirements typically require the IEG-C to be deployed to the mission HQ so that LAN-level transfer speeds can be provided between the two IT systems. Where a mission has no NS component, the IEG-C can be located at the supporting HQ at the reach-back or mission anchor location. Possible configurations are shown in the Figure 1 Possible IEG-C configurations:

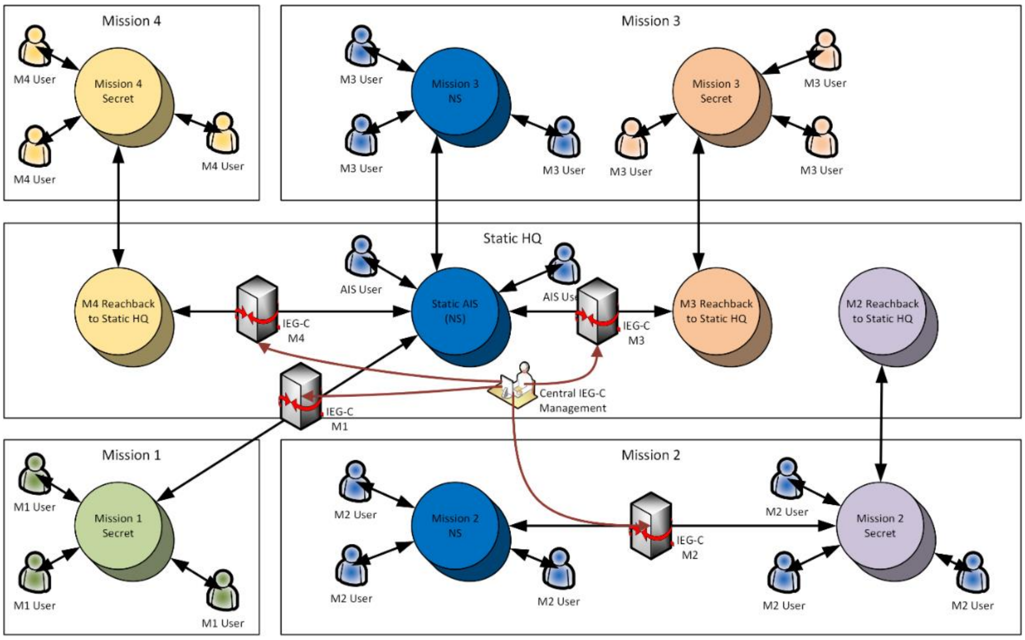

Figure 1 Possible IEG-C configurations

The IEG-C requirement and operational prototype solutions have evolved over many years to a situation where there are two main variants in operation today; those with a ‘DMZ’ and those without. In the ‘without’ case, a firewall and a mail guard are connected in parallel between the two security domains. The ‘DMZ’ configuration adds a third domain mediated by the firewall that contains the mail guard and other guards and proxies, such as an XML web-guard and web reverse proxy.

The objective of the IEG-C project is to modernise and standardise the configurations to a single layout as in Figure 2 IEG-C Management and Components, and to add additional features required by, for instance, evolving security protection measures. It should be noted that configurations will never be fully identical as different missions will always operate different C2 tools and information exchange requirements due to the nature of the operation (Maritime-based, Land-based etc.). So there will be differences in the firewall rule sets and, of course, all missions have specific releasability labels.

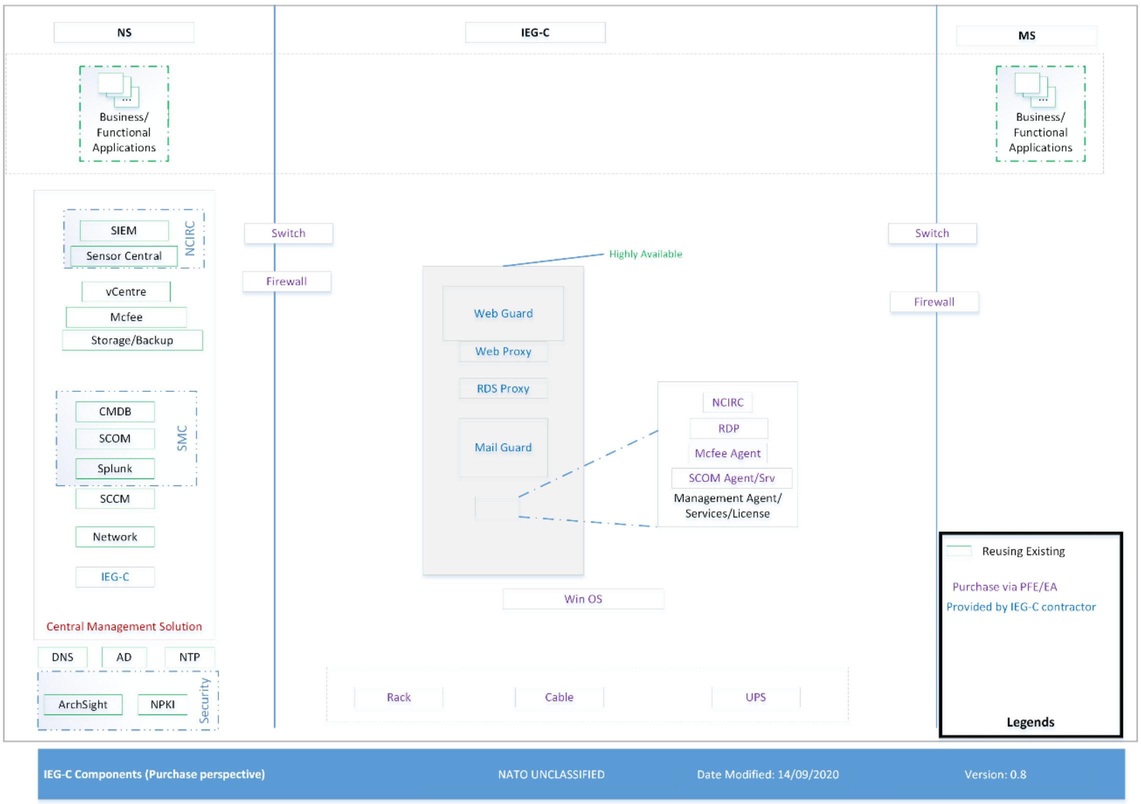

Figure 2 IEG-C Management and Components

As the IEG-C is a data release guard, it does not support any on-line users and, other than log files, only supports transient data. All of the IEG-C components will be centrally managed by a Boundary Services management team from a central location. IEG-C components and services will also be locally monitored. In case of loss of connectivity from central management team and the distant IEG-C, it will be possible to perform any management functions locally.

The logical layout and data flows of the IEG-C is shown in Figure 3. Features to note are that physically separate firewalls are required for the interface to the NS domain and the interface to the <Mission> SECRET domain and that separate IEG-Cs are required for each mission. The diagram is illustrative of the data flows between the NS and <Mission> SECRET domains and shows both operational and management streams.

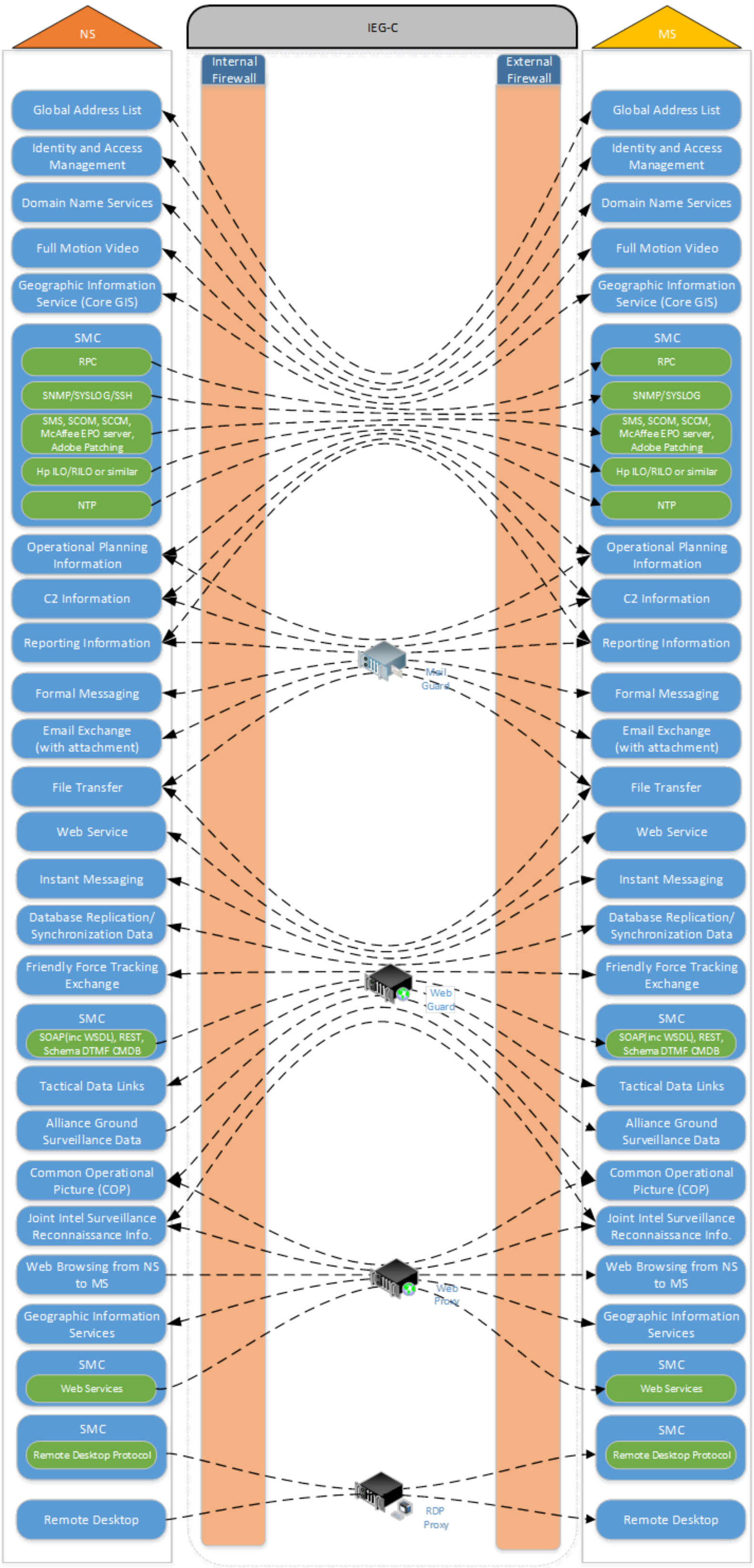
NS
IEG-C
MS
Internal Firewall
External Firewall
Global Address List
Identity and Access Management
Domain Name Services
Full Motion Video
Geographic Information Service (Core GIS)
SMC
RPC
SNMP/SYSLOG/SSH
SNMP/SYSLOG
SMS, SCOM, SCCM, McAffee EPO server, Adobe Patching
Hp ILO/RILO or similar
NTP
Operational Planning Information
C2 Information
Reporting Information
Mail Guard
Formal Messaging
Email Exchange (with attachment)
File Transfer
Web Service
Instant Messaging
Database Replication/ Synchronization Data
Friendly Force Tracking Exchange
Web Guard
SOAP(inc WSDL), REST, Schema DTMF CMDB
Tactical Data Links
Alliance Ground Surveillance Data
Common Operational Picture (COP)
Joint Intel Surveillance Reconnaissance Info.
Web Browsing from NS to MS
Web Proxy
Geographic Information Services
Web Services
Remote Desktop Protocol
Remote Desktop
RDP Proxy

Figure 3 IEG-C Data Flows

2.2 Deployment Overview

The IEG Scenario C is intended to work on Secret level only. The IEG-C has three principal deployment options (as depicted in Figure 4):

- in a static configuration where it acts as the interface between the static NS domain and MS domain at the mission HQ (e.g. IEG-C M1);
- in a deployed configuration where it acts as the interface between the NS domain and MS domain at the mission HQ (e.g. IEG-C M2); and
- in a static configuration where it acts as the interface between the static NS domain and the MS domain at the reach-back location (e.g. IEG-C M3 and IEG-C M4).

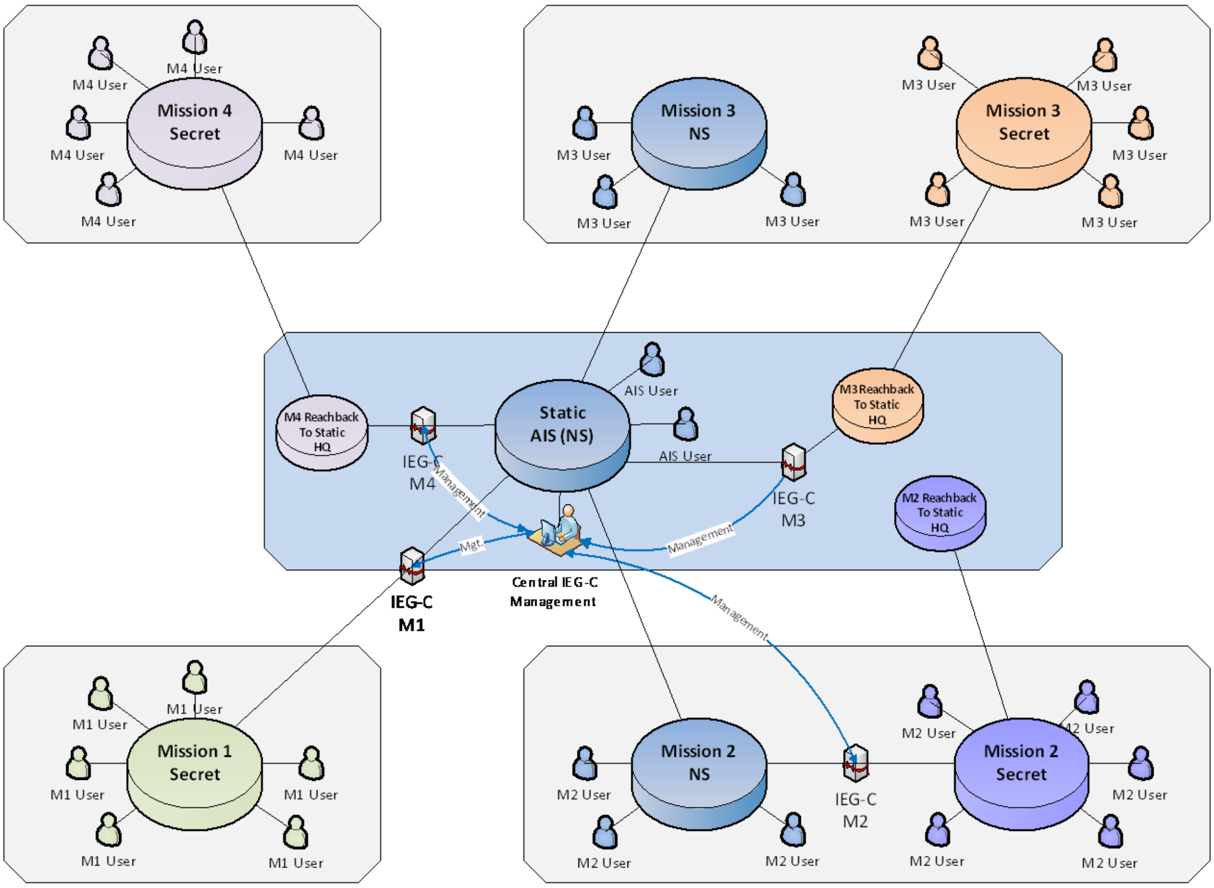

Figure 4 Principal modes of operation of the IEG-C

3 IEG-C Architecture

3.1 General

The IEG-C target architecture (TA, [TR/2016/NSE010871/01, 2016]) is described in terms of a set of composite IEG-C Architecture Building Blocks (ABBs), each of which has a set of associated functions, interfaces and attributes. The ABB methodology, as defined by NATO Enterprise Architecture (EA) Policy, Annex 9 of the Alliance C3 Policy, [NAC C-M(2015)0041-REV1, 2016], is used as the basis for defining an IEG-C Target Architecture.

The approach taken for describing the ABBs was driven by the need to design, implement and accredit a modular set of information assurance services, mediation services and associated service management and control services to enable information exchange between the NATO Secret (NS) network and NATO-led mission classified networks. The Target Architecture describes a standardized architecture for IEG-C addressing:

- Static implementation at centralized locations;
- IEG-C at deployable Point of Presence; and,
- IEG-C prototypes currently installed at static and deployed.

The ABBs are used within the Target Architecture to describe the overall functionality of the IEG-C and how each information exchange requirement (IER) can be supported through the IEG-C in terms of a pattern describing the interactions between ABBs and their service operations and interfaces. In turn, the architecture identifies the class of device (e.g. network switch, firewall, proxy, guard) which may be used to support each of the identified patterns, and associates the patterns with the IERs required to be supported by the IEG-C. Note that an IER may make use of more than one pattern.

Finally, the Target Architecture, derived from the ABBs, their functions, interfaces, attributes and patterns provided the basis for describing the system specification for IEG-C against which actual IEG-Cs can be procured.

3.2 IEG-C Primary Interfaces

The logical architecture allows for a standard gateway to be implemented that provides interfaces (see Figure 5) between NATO Secret (NS) CIS (high domain) and NATO-led Mission Secret (MS) CIS (low domain) whereby the security of the NS CIS shall be improved by providing:

- standardized components;
    - standardized hardware; and,
    - standardized software.
- standardized configuration;
- centralized management; and,
- centralized maintenance.

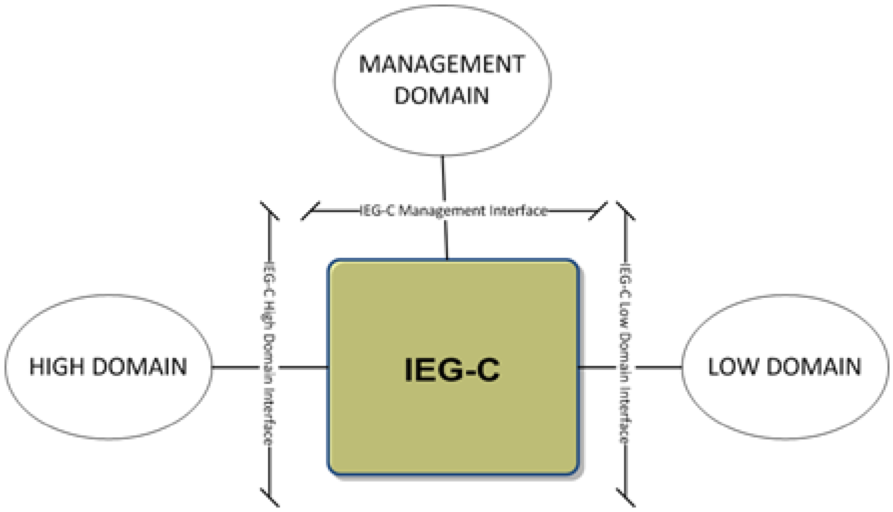
MANAGEMENT DOMAIN
IEG-C Management Interface
IEG-C High Domain Interface
HIGH DOMAIN
IEG-C
IEG-C Low Domain Interface
LOW DOMAIN

Figure 5 IEG-C Primary Interfaces

Requirement ID: [SRS-3-1]

The IEG-C SHALL provide a data exchange capability IEG-C_DEX that facilitates the mediation of data between the High Domain and the Low Domain.

Requirement ID: [SRS-3-2]

IEG-C_DEX SHALL offer the physical network interface IEG-C High Domain Interface [NCIA TR/2016/NSE010871/01, 2017] (IEG-C_IF_NET_HIGH) that provides Ethernet connectivity to the High Domain.

Requirement ID: [SRS-3-3]

IEG-C_DEX SHALL offer the physical network interfaces IEG-C Low Domain Interfaces [NCIA TR/2016/NSE010871/01, 2017] (IEG-C_IF_NET_LOW) that provides Ethernet connectivity to the Low Domains.

Requirement ID: [SRS-3-4]

IEG-C_DEX MAY offer the physical network interface IEG-C Management Interface [NCIA TR/2016/NSE010871/01, 2017] (IEG-C_IF_MGMT) that provides Ethernet connectivity to the High Domain.

Requirement ID: [SRS-3-5]

In the case that IEG-C_DEX cannot offer the physical network interface IEG-C_IF_MGMT, it SHALL offer a logical network interface IEG-C_IF_MGMT on top of IEG-C_IF_NET_HIGH.

Requirement ID: [SRS-3-6]

The IEG-C SHALL offer the following functionality as described in the IEG-C Architecture Building Blocks [NCIA TR/2016/NSE010871/01, 2017]:

- Provide CIS connectivity;
- Create Network Boundary;

- Create Domain Boundary;
- Protect Confidentiality of High Domain;
- Protect Integrity of High Domain;
- Protect Availability of High Domain;
- Mediate Data Exchange; and,
- Centralize Management.

Requirement ID: [SRS-3-101]

All IEG-C components SHALL support 1GbE.

Requirement ID: [SRS-3-102]

All IEG-C components SHALL be upgradeable, through the use of pluggable transceivers, to support 10GbE.

3.3 IEG-C Capabilities

Requirement ID: [SRS-3-7]

The design and architecture of the IEG-C for providing protected cross domain information exchange between NATO Secret and NATO-led Mission Secret SHALL be implemented in accordance with the self-protecting node principle [NAC AC/35-D/2004-REV3, 2013].

The critical technical capabilities for enabling protected cross domain information exchange are illustrated in Figure 6.

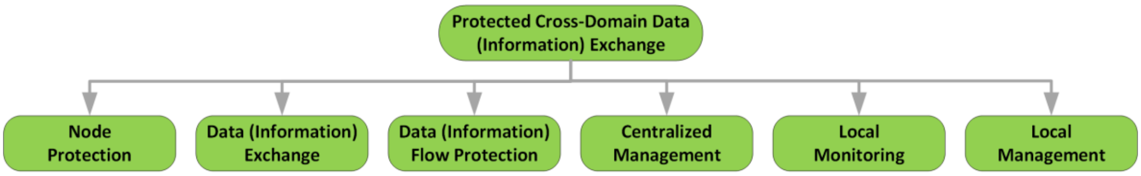
Protected Cross-Domain Data (Information) Exchange
Node Protection
Data (Information) Exchange
Data (Information) Flow Protection
Centralized Management
Local Monitoring
Local Management

Figure 6 IEG-C Capabilities

The technical capabilities delivered by the IEG-C are summarised in Table 1.

Table 1 IEG-C Capabilities and Capability Statement

Capability Name	Capability Statement
Node Protection	The ability of the gateway to protect the infrastructure and to mitigate risks introduced by interconnecting NATO Secret and Mission secret networks.
Data (Information) Exchange	The ability of the gateway to ensure an efficient cross domain flow of data (information) between NATO Secret and Mission Secret for selected COI and Core Services.
Data (Information) Flow Protection	The ability of the gateway to enforce the protection policies, to prevent unauthorized and uncontrolled release of information, and to ensure that only the information intended to be exchanged are effectively transmitted under a controlled, security monitored regime (security label filtering compliant with NATO policy, document scanning, etc.).
Centralized Management	The ability of the gateway to be managed from a centralized system that provides enterprise level monitoring of information to support Service Management and Control (SMC) and Cyber Defence.
Local Monitoring	The ability to monitor all IEG-C components and services from a co-located monitoring suite, independent from the centralized management.
Local Management	Alternative solution to the Centralized Management to allow co-located support teams to perform (reduced) management activities if connectivity to central management is lost.

3.4 IEG-C Architecture Building Block Services

The IEG-C TA further subdivides the IEG-C ABB into the following ABBs:

- Data Exchange Services;
- Protection Services;
- Protection Policy Enforcement Services; and,
- Element Management Services.

The ABBs have been defined in a generic manner in order to support any information exchange requirements (IERs), specifically to:

- support the mediation of any type of data over any type of protocol;
- enforce the protection policy required for that information exchange requirement; and,
- centrally manage the IEG-C.

For each ABB a list of defined functions, service interfaces and service attributes is defined. The functionality provided by the IEG-C ABBS can be mapped to the IEG-C capabilities summarised in Table 1 as illustrated in Table 2.

Table 2 Mapping between IEG-C Capabilities and IEG-C ABB Services

	Data Exchange Services	**Protection Services**	**Protection Policy Enforcement Services**	**Element Management Services**
Node Protection	X	X		
Data (Information) Exchange	X			
Data (Information) Flow Protection		X	X	
Centralized Management				X

3.4.1 Data Exchange Services

The Data Exchange Services facilitates the mediation of data between a high network domain (High Domain) and a low network domain (Low Domain). The Data Exchange Services can be logically grouped to the following NATO C3 Taxonomy [NC3B AC/322-D(2019)0034 (INV), 2019] defined services classifications for supporting data mediation services:

- Communications Access Services;
- Infrastructure Services;
- SOA Platform Services; and,
- Business Support Services.

Requirement ID: [SRS-3-8]

The Data Exchange Services SHALL offer the following functionality to provide CIS Interconnectivity and Mediate Data Exchange:

- Exchange Email Services Data;
- Exchange Web Services Data;
- Provide Remote Desktop Access;
- Exchange Network Services Data; and,
- Exchange Text Based Collaboration Services Data

3.4.2 Protection Services

Requirement ID: [SRS-3-9]

The Protection Services SHALL provide the capability to protect data at the network layer and the application layer. The Protection Services consists of the following three atomic services:

- Intrusion Detection Services;
- Public Key Cryptographic Services; and,
- Content Inspection Services.

3.4.2.1 Intrusion Detection Services

Requirement ID: [SRS-3-10]

The Intrusion Detection Services SHALL offer the following functionality to provide protection for the integrity of the NATO Secret network and protection for availability of the NATO Secret network:

- Detect Malicious Activities and Faults;
- Prevent and mitigate Attacks and Faults

3.4.2.2 Public Key Cryptographic Services

Requirement ID: [SRS-3-11]

The Public Key Cryptographic Services SHALL offer the following functionality to provide protection for the confidentiality of the NATO Secret network and protection for the integrity of the NATO Secret network:

- Process Public Key Cryptographic Data
- Manage Cryptographic Keys

3.4.2.3 Content Inspection Services

Requirement ID: [SRS-3-12]

The Content Inspection Services SHALL offer the following functionality to provide protection for the confidentiality, integrity and availability of the NATO Secret network:

- Identify Content;
- Verify Content; and,
- Transform Content.

3.4.3 Policy Protection Enforcement Services

Requirement ID: [SRS-3-13]

The Protection Policy Enforcement Services SHALL enforce protection policies on mediated data.

Requirement ID: [SRS-3-14]

The Protection Policy Enforcement Services SHALL consider all aspects relevant to protection of confidentiality, integrity and availability. The Protection Policy Enforcement Services consists of the following two services:

- Information Flow Control Policy Enforcement (IFCPE) Services; and,
- Content Inspection Policy Enforcement (CIPE) Services.

3.4.4 IFCPE Services

Requirement ID: [SRS-3-15]

The IFCPE Services SHALL enforce Information flow policies (IFP), which constitute a subset of protection policies.

Requirement ID: [SRS-3-16]

The IFPs SHALL define the way information moves between the NATO Secret network and the Mission Secret network, and vice-versa based upon the following criteria:

- the subjects (for example, this may be the IP address of the source and destination, or originator and recipient domain for email or text-based collaboration chat, or the source and destination interfaces within the IEG-C where the IFP is being enforced) under control of the policy;
- the content (the data type i.e. XML, that is being exchanged by the Data Exchange Service supporting the information exchange requirement) under control of the policy; and
- the operations which cause information to flow to and from controlled subjects covered by the policy.

For each IEG-C an information flow control policy (IFP) is enforced. This is referred to as IEG-C_IFP. The IEG-C_IFP can be viewed as the union of the following three sub-policies:

- IEC-C_IFP_HL: for traffic flowing from the High Domain to the Low Domain;
- IEG-C_IFP_LH: for traffic flowing from the Low Domain to the High Domain; and,
- IEG-C_IFP_MGMT: for management traffic flowing between the Management Domain and the IEG-C.

Requirement ID: [SRS-3-17]

The Information Flow Control Policy Enforcement (IFCPE) Services SHALL enforce the following general IFPs:

- IEG-C_IFP_CA_HL - Communications Access Services High to Low IFP;
- IEG-C_IFP_CA_LH - Communications Access Services Low to High IFP;
- IEG-C_IFP_IS_HL - Infrastructure Services High to Low IFP;
- IEG-C_IFP_SOA_HL - SOA Platform Services High to Low IFP;
- IEG-C_IFP_SOA_LH - SOA Platform Services Low to High IFP;
- IEG-C_IFP_BS_HL - Business Support Services High to Low IFP;
- IEG-C_IFP_BS_LH - Business Support Services Low to High IFP; and,
- IEG-C_IFP_CS_MGMT - Core Services Management Services IFP.

3.4.5 CIPE Services

Requirement ID: [SRS-3-18]

The Content Inspection Policy Enforcement (CIPE) Services SHALL enforce Content Inspection Policies (CIPs) which define how the data mediated between the NATO Secret network and NATO-led Mission network is to be inspected.

Requirement ID: [SRS-3-19]

The CIPs SHALL be designed to protect the confidentiality of the NATO Secret network by inspecting data for unauthorised information that should not be released to the NATO-led Mission Network.

Requirement ID: [SRS-3-20]

The CIPs SHALL be designed to protect the integrity and availability of the NATO Secret network by identifying and verifying the structure of the data and removing or blocking malicious content.

Requirement ID: [SRS-3-21]

CIPE Services SHALL enforce the following general CIPs:

- IEG-C_CIP_SOA_HL - SOA Platform Services High to Low CIP;
- IEG-C_CIP_SOA_LH - SOA Platform Services Low to High CIP;
- IEG-C_CIP_BS_HL - Business Support Services High to Low CIP;
- IEG-C_CIP_BS_LH - Business Support Services Low to High CIP;
- IEG-C_CIP_COI-ES_HL - COI-Enabling Services High to Low CIP;
- IEG-C_CIP_COI-ES_LH - COI-Enabling Services Low to High CIP;
- IEG-C_CIP_COI_HL - COI-Specific Services High to Low CIP; and
- IEG-C_CIP_COI_LH - COI-Specific Services Low to High CIP.

3.4.6 Element Management Services

Requirement ID: [SRS-3-22]

The IEG-C Element Management Services SHALL provide interfaces that can be managed from a centralized management system to support activities such as Service Management and Control (SMC), Cyber-Defence, security policy administration, audit management and IEG-C configuration and maintenance.

Requirement ID: [SRS-3-25]

The IEG-C Element Management Services SHALL provide interfaces to support local management activities such as Service Management and Control (SMC), Cyber-

Defence, security policy administration, audit management and IEG-C configuration and maintenance, in case of loss of connectivity with the Central Management system.

Requirement ID: [SRS-3-23]

The Element Management Services SHALL support the different administrative roles that are required for managing the IEG-C.

Requirement ID: [SRS-3-24]

The administrative roles of the IEG-C SHALL be categorised as follows:

- System Administrator: responsible for installation, configuration and maintenance of the IEG-C;
- Local System Administrator: responsible for installation, configuration and maintenance of a subset of IEG-C's;
- Local System Maintainer: responsible for some maintenance activities of a subset of IEG-C's;
- Audit Administrator: responsible for regular review of IEG-C audit logs;
- CIS Security Administrator: responsible for performing the IEG-C CIS security-related tasks, such as security policy management;
- Cyber Defence Administrator: responsible for monitoring and performing cyber-related tasks; and,
- SMC Administrator: responsible for monitoring IEG-C services.
- Local SMC Administrator: responsible for monitoring a subset of IEG-C's services and components.

3.5 Patterns

The IEG-C ABBs can be combined into patterns which describe re-useable solutions (or components) to:

- support the mediation of any type of data over any type of protocol;
- enforce the protection policy required for that information exchange requirement; and,
- centrally and locally manage the IEG-C.

From a generic approach, patterns for combining the ABBs can be put together as shown in the IEG-C TA [TR/2016/NSE010871/01, 2016] APPENDIX B (listed below for reference):

- High to Low Node Protection Pattern
- High to Low Cross Domain Information Exchange Pattern
- Low to High Node Protection Pattern
- Low to High Cross Domain Information Exchange Pattern
- Management Pattern

However, the interfaces offered and the functionality provided by each of the composite ABBs and how the ABBs are combined are dependent upon the information exchange requirement (IER) that the IEG-C is required to support and the organizational policy to be enforced. As such, the patterns described in [TR/2016/NSE010871/01, 2016]

Appendix B have been tailored to specifically support the information exchange requirements that are required to be supported by the IEG-C (as listed below):

- Communications Access Services Pattern;
- SOA Platform Web Services Pattern;
- Business Support Services Email Pattern;
- Business Support Services Chat Pattern;
- Infrastructure Remote Desktop Access Pattern;
- SOA Platform High to Low Web Browsing Pattern;
- CIS Security Management Pattern; and,
- Service Management and Control (SMC) pattern.

These specific patterns are documented in Section 5.4.1 of the IEG-C TA [TR/2016/NSE010871/01, 2016] and are used as the basis for defining the requirements for the IEG-C components, the system interfaces offered by the IEG-C components and how the IEG-C components are integrated as specified in Section 4.

4 IEG-C Components, Interfaces and Integration

4.1 General

4.1.1 Components

Requirement ID: [SRS-4-1]

The IEG-C (depending upon the IERs and protection policies to be enforced for the CIS interconnection) SHALL consist of the following components:

- Firewalls;
- Network Switches;
- RDP Proxy;
- Web Proxy;
- Mail Guard; and,
- Web Guard.

Requirement ID: [SRS-4-2]

Only those IEG-C components, hence only the protocols, network services, and the information or data flows, required to support the information exchange requirements SHALL be configured and used through the interconnection.

Requirement ID: [SRS-4-3]

The IEG-C architecture and all of its components SHALL be compliant with "INFOSEC Technical and Implementation Directive for the Interconnection of Communications and Information Systems (CIS)" [NAC, AC/322-D/0030-REV5.

Requirement ID: [SRS-4-4]

The IEG-C and all of its components SHALL be configured in accordance with the “Technical and Implementation Directive for CIS Security” [NAC AC/322-D/0048-REV3, 2019].

Requirement ID: [SRS-4-225]

Unless otherwise identified during the Site Survey [SOW-673], the IEG-C and all of its components SHALL be certified to TEMPEST Level C, as defined in [SDIP-27/2].

Requirement ID: [SRS-4-5]

All IEG-C components SHALL gracefully shut down on notification from the Uninterruptible Power Supply (UPS).

Requirement ID: [SRS-4-226]

It SHALL be possible to trigger the graceful shut down from the central and local management solution.

Table 3 specifies the high level IEG-C TA ABBs (refer to Section 3.4) provided by each of the IEG-C components.

Table 3 IEG-C TA ABB mapping to IEG-C components

	Data Exchange Services	**Protection Services**	**Policy Protection Services**	**Element Management Services**
Firewall	X		X	X
Network Switch	X			X
RDP Proxy	X			X
Web Proxy	X	X	X	X
Mail Guard	X	X	X	X
Web Guard	X	X	X	X

Figure 7 illustrates the association between the patterns identified in Section 3.5 and the IEG-C components required to support those patterns.

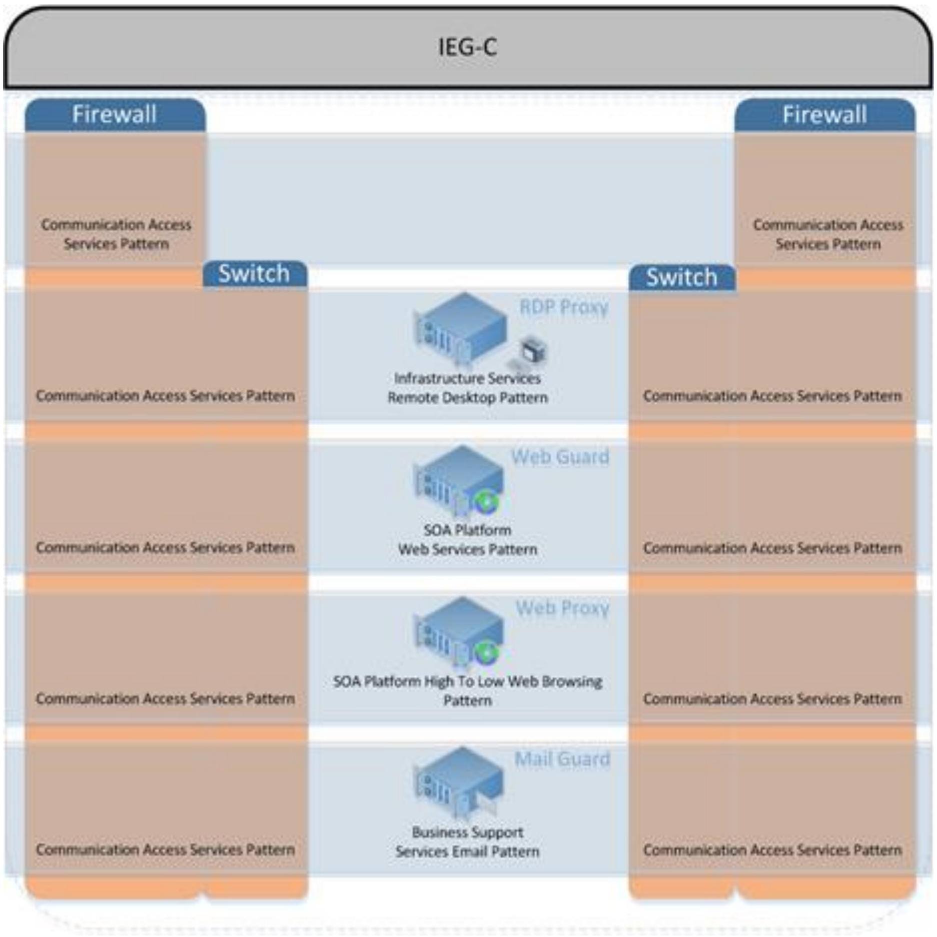
IEG-C
Firewall
Firewall
Communication Access Services Pattern
Communication Access Services Pattern
Switch
Switch
RDP Proxy
Infrastructure Services Remote Desktop Pattern
Communication Access Services Pattern
Communication Access Services Pattern
Web Guard
SOA Platform Web Services Pattern
Communication Access Services Pattern
Communication Access Services Pattern
Web Proxy
SOA Platform High To Low Web Browsing Pattern
Communication Access Services Pattern
Communication Access Services Pattern
Mail Guard
Business Support Services Email Pattern
Communication Access Services Pattern
Communication Access Services Pattern

Figure 7 IEG-C components associated with the patterns

Requirement ID: [SRS-4-6]

The IEG-C SHALL provide supporting components required for the composition of an IEG-C (see Section 4.7.2).

4.1.2 System Interfaces

Figure 8[1] below provides the system interfaces illustrating how the IEG-C components are connected based on the physical interfaces (see Section 3.2) offered by the IEG-C in order to support up a mission.

[1] *Note that this figure illustrates how future proxies or guards can be integrated into the IEG-C to support future information exchange requirements.*

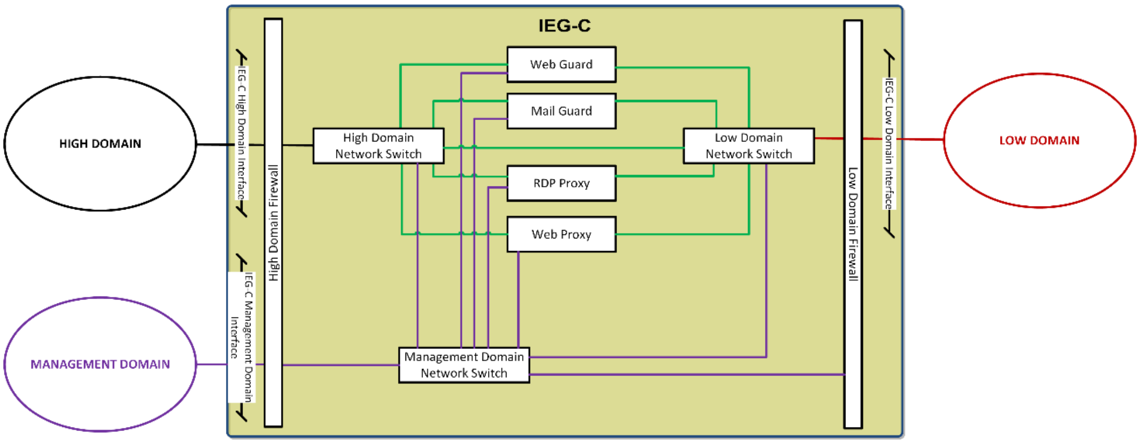
IEG-C
HIGH DOMAIN
LOW DOMAIN
MANAGEMENT DOMAIN
IEG C High Domain Interface
IEG C Management Domain Interface
IEG-C Low Domain Interface
High Domain Firewall
Low Domain Firewall
Web Guard
Mail Guard
High Domain Network Switch
Low Domain Network Switch
RDP Proxy
Web Proxy
Management Domain Network Switch

Figure 8 IEG-C Network Level System Interface

The IEG-C_DEX physical network interfaces (IEG-C High Domain Interface, IEG-C Low Domain Interfaces and Management Interface) depicted in Figure 5 above are further sub-divided into system (logical) interfaces provided by the Data Exchange Services (see Section 3.4.1) supporting connectivity to the high and low domains dependent upon the protocol being mediated across the IEG-C.

Table 4 shows a list of the application and management (SMC Service) protocols that will be arbitrated by the IEG-C, together with the primary component that will mediate the information using the protocol.

Table 4: Protocols Supported by the IEG-C

Protocol	**Name**	**IEG-C Component**	**Service**
DNS	Domain Name Services	Firewall	Domain Name Services
OCSP	Online Certificate Status Protocol	Firewall	PKI
LDAP	Lightweight Directory Access Protocol	Firewall	PKI
			Global Address List
			Identity and Access Management
HTTP	Hyper Text Transfer Protocol	Web Proxy	Web browsing from NS to MS
			Operational Planning information
			C2 Information
			Reporting Information
			Geographic Information Services
			Common Operational Picture
			JISR Replication
			SMC
		Web Guard	Web Service
			File Transfer
			Database Replication/Synchronization Data
			Friendly Force Tracking Exchange
			JISR Replication
			Geographic Information Services
			Common Operational Picture

Protocol	Name	IEG-C Component	Service
			SMC
SMTP	Simple Mail Transfer Protocol	Mail Guard	Email Exchange (with attachment)
			Formal Messaging (NMS)
			Operational Planning information
			C2 Information
			Reporting Information
			File Transfer
XMPP	eXtensible Message and Presence Protocol	Web Guard	Instant Messaging
RDP	Remote Desktop Protocol	RDP Proxy	Remote Desktop
			SMC
RTP	Real Time Protocol	Firewall	Full Motion Video
RTCP	Real Time Control Protocol	Firewall	Full Motion Video
Link 1	Link 1	Web Guard	Tactical Data Links
Link 11	Link 11	Web Guard	Tactical Data Links
Link 16	Link 16	Web Guard	Tactical Data Links
Link 22	Link 22	Web Guard	Tactical Data Links
JREAP	Joint Range Extension Applications Protocol	Firewall	Tactical Data Links
OTH-GOLD	Over-The-Horizon GOLD	Web Guard	Tactical Data Links
FFTS	Friendly Force Tracking Systems	Web Guard	Tactical Data Links
NTP	Network Time Protocol	Firewall	SMC
SYSLOG	Syslog	Firewall	SMC
SNMP	Simple Network Management Protocol	Firewall	SMC
SSH	Secure Shell	Firewall	SMC
FTP	File Transport Protocol	Firewall	SMC
TELNET	Telnet	Firewall	SMC
RPC	Remote Procedure Call	Firewall	SMC
IPMI	Intelligent Platform Management Interface	Firewall	SMC
SCOM	System Center Operations Manager	Firewall	SMC
SCCM	System Center Configuration Manager	Firewall	SMC
WSUS	Window Server Update Services	Firewall	SMC

Protocol	Name	IEG-C Component	Service
CMDBf	Configuration Management Database Federation	Firewall	SMC
SMS	System Management Server	Firewall	SMC
EPO	Mc-Afee e-Policy Orchestrator	Firewall	SMC
AP	Adobe Patching	Firewall	SMC

Requirement ID: [SRS-4-7]

IEG-C_DEX SHALL offer User Datagram Protocol (UDP) [IETF RFC 768, 1980] and Internet Protocol (IP), IPv4 and IPv6, [IETF RFC 791, 1981], [IETF RFC 8200, 2017] over Ethernet interfaces 'Communications Access Services HL' and 'Communications Access Services LH' on top of IEG-C_IF_NET_HIGH and IEG-C_IF_NET_LOW, respectively.

Requirement ID: [SRS-4-224]

The IEG-C_DEX SHALL preserve the Differentiated Services field (DS Field) [IETF RFC 2474, 1998] in the IPv4 and IPv6 Headers.

Requirement ID: [SRS-4-8]

IEG-C_DEX SHALL offer HyperText Transport Protocol (HTTP), v1.1 and v2, [IETF RFC 7230, 2014], [IETF RFC 7540, 2014] interface 'SOA Platform Services HL' on top of 'Communications Access Services HL' and HyperText Transport Protocol (HTTP), v1.1 and v2. [IETF RFC 7230, 2014],[IETF RFC 7540, 2014] interface 'SOA Platform Services LH' on top of 'Communications Access Services LH'.

Requirement ID: [SRS-4-9]

The 'SOA Platform Services HL' and 'SOA Platform Services LH' interfaces SHALL support Transport Layer Security (TLS, [IETF RFC 8446, 2018]).

Requirement ID: [SRS-4-101]

The TLS Server identity (X.509 PKIX version 3.0 certificate, [IETF RFC 5280, 2008]) SHALL be validated, as per Section 6 of [IETF RFC 6125, 2011] following the best current practices documented in the "Recommendations for Secure Use of TLS and DTLS" [IETF RFC 7525, 2015(IETF)].

Requirement ID: [SRS-4-10]

IEG-C_DEX SHALL offer Simple Mail Transfer Protocol (SMTP) [IETF RFC 5321, 2008] interface 'Business Support Services HL' on top of 'Communications Access Services HL' and Simple Mail Transfer Protocol (SMTP) [IETF RFC 5321, 2008] interface 'Business Support Services LH' on top of 'Communications Access Services LH'.

Requirement ID: [SRS-4-11]

IEG-C_DEX SHALL offer Remote Desktop Protocol (RDP) [RDP Overview, 2019] interface 'Infrastructure Services HL' on top of 'Communications Access Services HL'.

Requirement ID: [SRS-4-102]

IEG-C_DEX SHALL offer an interface “Core Services” on top of 'Communications Access Services Management' that SHALL support the following protocols:

- DNS [IETF RFC 1035, 1987]
- OCSP [IETF RFC 6960, 2013]
- LDAP [IETF RFC 4510-4519, 2006]
- RTP [IETF RFC 3350, 2003]
- RTCP [IETF RFC 3350, 2003]
- JREAP [STANAG 5518]

Requirement ID: [SRS-4-12]

IEG-C_DEX SHALL offer UDP [IETF RFC 768, 1980] and IPv4 and IPv6, [IETF RFC 791, 1981], [IETF RFC 8200, 2017] over Ethernet interface 'Communications Access Services Management' on top of IEG-C_IF_MGMT.

Requirement ID: [SRS-4-13]

IEG-C_DEX SHALL offer an interface 'Core Services Management' on top of 'Communications Access Services Management' that SHALL support the following management protocols:

- Keyboard, video and mouse (KVM) over Internet Protocol (IP);
- Command Line interface (CLI) via Secure Shell (SSH) Transport Layer protocol [IETF RFC 4251, 2006];
- Simple Network Management Protocol (SNMP) Version 3 [IETF RFC 3410 – 3418, 2002];
- Syslog [IETF RFC 5424, 2009];
- Secure Shell (SSH, [IETF RFC 4253, 2006]);
- Network Time Protocol (NTP, [IETF RFC 5905, 2010]);
- Intelligent Platform Management Interface (IPMI, [IPMI V.2.0, 2013]);
- Hyper-Text Transport Protocol (HTTP) v1.1 Web interface [IETF RFC 7230, 2014] [IETF RFC 7231, 2014]
- Hyper-Text Transport Protocol (HTTP) v2 Web interface [IETF RFC 7540, 2014] ;
- Remote Desktop (RDP [RDP Overview, 2019];
- Remote Procedure Call (RPC, [IETF RFC 5531, 2009]).
- System Center Operations Manager
- Systems Center Configuration Manager
- Windows Server Update Services
- McAfee e-Policy Orchestrator
- Adobe Patching
- File Transfer Protocol [IETF RFC 959, 1985]
- Telnet [IETF RFC 854, 1983]

Table 4 below identifies the IEG-C_DEX Data Exchange Services interfaces offered by each of the IEG-C components.

Table 5 Data Exchange Services offered by IEG-C components

IEG-C Component	Data Exchange Services Interface	IEG-C TA Reference
Firewall	Communications Access Services Interface Communications Access Management Services Interface Core Services Management Interface	Section A.3.3.1 Section A.3.3.2 Section A.3.3.6
Network Switch	Communications Access Services Interface Communications Access Management Services Interface Core Services Management Interface	Section A.3.3.1 Section A.3.3.2 Section A.3.3.6
RDP Proxy	Communications Access Services Interface Infrastructure Services Interface Communications Access Management Services Interface Core Services Management Interface	Section A.3.3.1 Section A.3.3.3 Section A.3.3.2 Section A.3.3.6
Web Proxy	Communications Access Services Interface SOA Platform Services Interface Communications Access Management Services Interface Core Services Management Interface	Section A.3.3.1 Section A.3.3.4 Section A.3.3.2 Section A.3.3.6
Mail Guard	Communications Access Services Interface Business Support Services Interface Communications Access Management Services Interface Core Services Management Interface	Section A.3.3.1 Section A.3.3.5 Section A.3.3.2 Section A.3.3.6
Web Guard	Communications Access Services Interface SOA Platform Services Interface Communications Access Management Services Interface Core Services Management Interface	Section A.3.3.1 Section A.3.3.4 Section A.3.3.2 Section A.3.3.6

4.1.3 Integration

The IEG-C is a separate security domain from both the high domain and the low domain.

Requirement ID: [SRS-4-14]

Installation guidelines for “Selection and Installation of Equipment for the Processing of Classified Information“ [SDIP-29/2] regarding equipment separation and installation requirements SHALL be adhered to.

Requirement ID: [SRS-4-15]

The IEG-C SHALL support a network architecture containing a de-militarized zone (DMZ).

The IEG-C Firewall is physically separated as a High Domain Firewall and a Low Domain Firewall.

Requirement ID: [SRS-4-17]

To support connectivity of the proxies and the guards to the high domain and the low domains the High Network Domain Switch and a Low Domain Network Switch SHALL be provided, respectively.

Requirement ID: [SRS-4-18]

The High Domain Switch SHALL be connected to the High Domain Firewall.

Requirement ID: [SRS-4-19]

The Low Domain Switch SHALL be connected to the Low Domain Firewall.

Requirement ID: [SRS-4-20]

The RDP Proxy SHALL be connected to the High Domain Firewall (via the High Domain Network Switch) and the Low Domain Firewall (via the Low Domain Network Switch) using separate physical network interfaces.

Requirement ID: [SRS-4-21]

The Web Proxy SHALL be connected to the High Domain Firewall (via the High Domain Network Switch) and the Low Domain Firewall (via the Low Domain Firewall) using separate physical network interfaces.

Requirement ID: [SRS-4-22]

The Mail Guard SHALL be connected to the High Domain Firewall (via the High Domain Network Switch) and the Low Domain Firewall (via the Low Domain Network Switch) using separate physical network interfaces.

Requirement ID: [SRS-4-23]

The Web Guard SHALL be connected to both the High Domain Firewall (via the High Domain Network Switch) and the Low Domain Firewall (via the Low Domain Network Switch) via separate physical interfaces.

Requirement ID: [SRS-4-24]

The IEG-C shall include secure remote management capabilities providing the ability to monitor and control all IEG-C components remotely from central NATO management premises.

Requirement ID: [SRS-4-227]

The IEG-C shall include secure remote management capabilities providing the ability to integrate the monitoring all IEG-C components into a local NATO monitoring solution.

Requirement ID: [SRS-4-228]

The IEG-C shall include secure remote management capabilities providing the ability to manage all IEG-C components locally in case of loss of connectivity with the central management system.

Requirement ID: [SRS-4-25]

To support the (remote) management of the IEG-C, a Management Domain Network Switch SHALL be provided.

Requirement ID: [SRS-4-28]

The Management Domain Network Switch SHALL be connected to the High Domain Firewall.

Requirement ID: [SRS-4-29]

All IEG-C components SHALL have a connection to the Management Domain Switch.

Requirement ID: [SRS-4-30]

The IEG-C wired infrastructure for connecting IEG-C components (that are required to be connected together to support the information exchange requirements for the CIS interconnection) SHALL be based on Ethernet running over fibre optic and copper cables.

Requirement ID: [SRS-4-200

The IEG-C wired infrastructure for connecting IEG-C components (that are required to be connected together to support the information exchange requirements for the CIS interconnection) SHALL support VLANs.

4.1.4 External Interfaces

Figure 9 illustrates the external interfaces, server-to-server, across the IEG-C, together with the associated IEG-C components that mediate the information exchange.

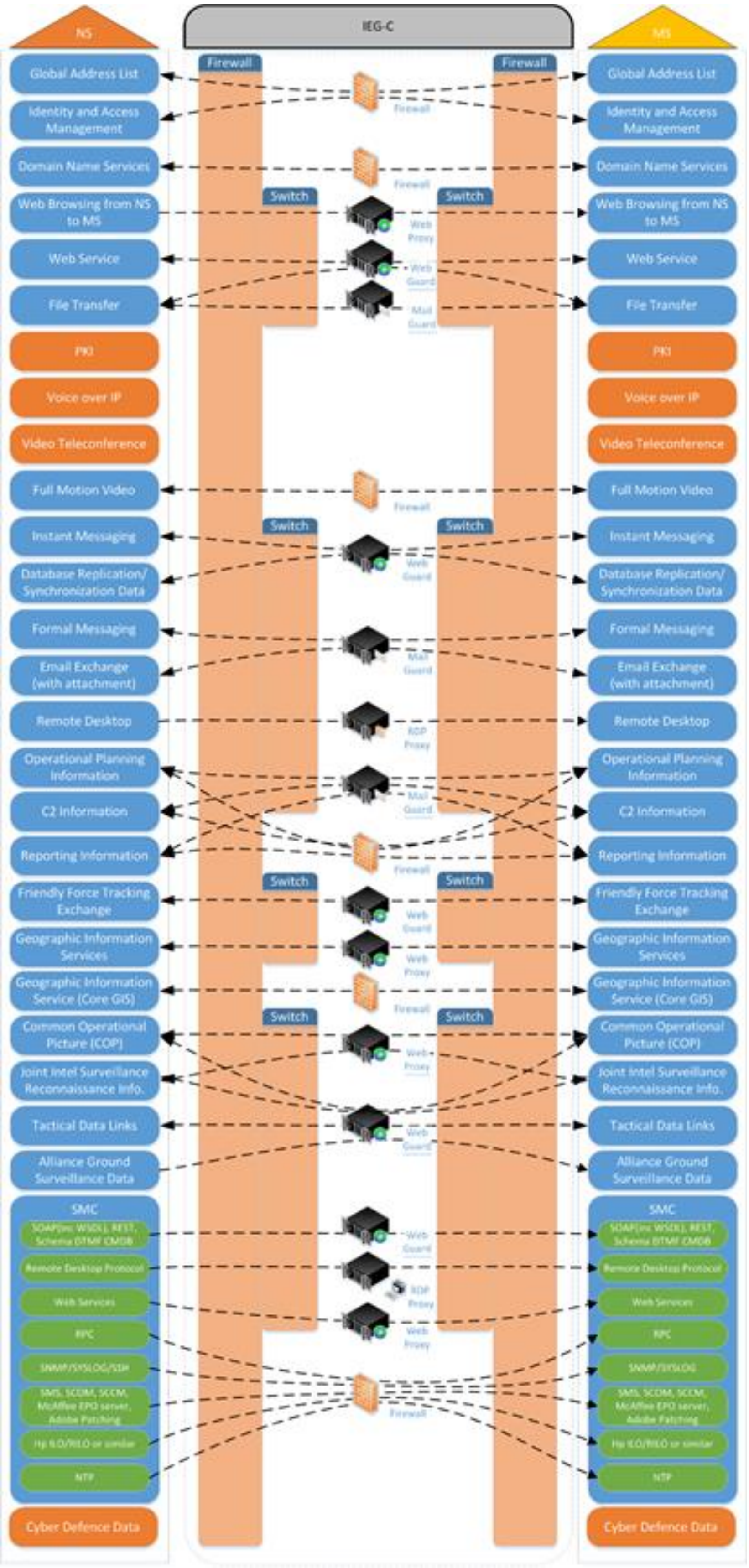
NS
IEG-C
MS
Firewall
Firewall
Global Address List
Global Address List
Identity and Access Management
Identity and Access Management
Firewall
Domain Name Services
Domain Name Services
Firewall
Switch
Switch
Web Browsing from NS to MS
Web Browsing from NS to MS
Web Proxy
Web Service
Web Service
Web Guard
File Transfer
File Transfer
Mail Guard
PKI
PKI
Voice over IP
Voice over IP
Video Teleconference
Video Teleconference
Full Motion Video
Full Motion Video
Firewall
Switch
Switch
Instant Messaging
Instant Messaging
Web Guard
Database Replication/ Synchronization Data
Database Replication/ Synchronization Data
Formal Messaging
Formal Messaging
Mail Guard
Email Exchange (with attachment)
Email Exchange (with attachment)
Remote Desktop
Remote Desktop
RDP Proxy
Operational Planning Information
Operational Planning Information
Mail Guard
C2 Information
C2 Information
Reporting Information
Reporting Information
Firewall
Switch
Switch
Friendly Force Tracking Exchange
Friendly Force Tracking Exchange
Web Guard
Geographic Information Services
Geographic Information Services
Web Proxy
Geographic Information Service (Core GIS)
Geographic Information Service (Core GIS)
Firewall
Switch
Switch
Common Operational Picture (COP)
Common Operational Picture (COP)
Web Proxy
Joint Intel Surveillance Reconnaissance Info.
Joint Intel Surveillance Reconnaissance Info.
Tactical Data Links
Tactical Data Links
Web Guard
Alliance Ground Surveillance Data
Alliance Ground Surveillance Data
SMC
SMC
SOAP(inc WSDL), REST, Schema DTMF CMDB
SOAP(inc WSDL), REST, Schema DTMF CMDB
Web Guard
Remote Desktop Protocol
Remote Desktop Protocol
RDP Proxy
Web Services
Web Services
Web Proxy
RPC
RPC
SNMP/SYSLOG/SSH
SNMP/SYSLOG
SMS, SCOM, SCCM, McAffee EPO server, Adobe Patching
SMS, SCOM, SCCM, McAffee EPO server, Adobe Patching
Firewall
Hp ILO/RILO or similar
Hp ILO/RILO or similar
NTP
NTP
Cyber Defence Data
Cyber Defence Data

Figure 9 External interfaces, server-to-server, across the IEG-C

Requirement ID: [SRS-4-31]

The IEG-C SHALL be conformant with the service interface profiles (SIPs) and NATO Interoperability Standards and Profiles (NISPs) listed in APPENDIX B.

Requirement ID: [SRS-4-32]

The IEG-C SHALL interface and function correctly with the NATO General Purpose Segment Communications System (NGCS) network, the NATO Communications Infrastructure (NCI) network and security infrastructure.

Requirement ID: [SRS-4-33]

The IEG-C SHALL interface and function correctly with the NATO Computer Incident Response Capability (NCIRC).

Requirement ID: [SRS-4-34]

The IEG-C SHALL interface and function correctly with the NATO Enterprise Service Management and Control (SMC) capability.

Requirement ID: [SRS-4-35]

The IEG-C SHALL interface and function correctly with the NATO Public Key Infrastructure (NPKI) capability.

Requirement ID: [SRS-4-36]

The IEG-C SHALL interface and function correctly with the NATO Enterprise Directory Services (NEDS) capability.

Requirement ID: [SRS-4-37]

The IEG-C SHALL interface and function correctly with the ON AIS and MS AIS Active Directory Domain Services (ADDS) capability.

Requirement ID: [SRS-4-38]

The IEG-C SHALL interface and function correctly with the Operational Network (ON) Automated Information System (AIS) and Mission Secret (MS) AIS mail exchange capability.

Requirement ID: [SRS-4-39]

The IEG-C SHALL interface and function correctly with the ON AIS and MS AIS Domain Name Services (DNS) capability.

Requirement ID: [SRS-4-40]

The IEG-C SHALL use fully qualified domain names (FQDN, [IETF RFC 1983, 1996]) for identifying all hosts, unless specifically requested not to.

Requirement ID: [SRS-4-41]

The IEG-C SHALL interface and function correctly with the ON AIS and MS AIS web client and server capability providing SOAP-based and REST-based web services.

Requirement ID: [SRS-4-42]

The IEG-C SHALL interface and function correctly with the ON AIS and MS AIS web client and server capability providing web browsing.

Requirement ID: [SRS-4-43]

The IEG-C SHALL interface and function correctly with the ON AIS and MS AIS Collaboration Services capability providing audio, voice and video services.

Requirement ID: [SRS-4-44]

The IEG-C SHALL interface and function correctly with the ON AIS Information Exchange Gateway Functional Services (IEG-FS) Extensible Messaging and Presence Protocol (XMPP) capability for exchanging text-based collaboration services messages.

Requirement ID: [SRS-4-45]

The IEG-C SHALL interface and function correctly with the ON AIS Information Exchange Gateway Functional Services (IEG-FS) Tactical Data Link (TDL) capability for exchanging TDL-formatted messages.

Requirement ID: [SRS-4-46]

The IEG-C SHALL interface and function correctly with the ON AIS Information Exchange Gateway Functional Services (IEG-FS) Friendly Force Tracking (FFT) capability for exchanging FFT-formatted messages.

Requirement ID: [SRS-4-48]

The IEG-C SHALL interface and function correctly with the authoritative ON AIS Network Time Protocol (NTP) source.

4.2 Firewall

4.2.1 General

Requirement ID: [SRS-4-49]

The IEG-C Firewall components (High Domain Firewall and Low Domain Firewall) SHALL be the:

- Palo Alto Networks PA-3260 with redundant AC power supplies

A detailed description of this component is provided in Appendix D.

Requirement ID: [SRS-4-221]

The Firewall components SHALL support 10GbE.

Requirement ID: [SRS-4-222]

The Firewall components SHALL handle at least 90Gb throughput per 24 hour period.

Requirement ID: [SRS-4-223]

The Firewall components SHALL be able to sustain, on average, at least 6Gb/s throughput.

Requirement ID: [SRS-4-201]

The selected IEG-C High Domain and Low Domain Firewalls components SHALL include compatible rack mount kits and power cords.

Requirement ID: [SRS-4-51]

The IEG-C High Domain Firewall component Network Time Protocol (NTP) server SHALL be synchronized to a designated NTP server in the ON AIS domain.

Requirement ID: [SRS-4-52]

The IEG-C High Domain Firewall component SHALL be configured as the Authoritative Network Time Protocol (NTP) source for all IEG-C components (including the Low Domain Firewall) that require to be time synchronised.

4.2.2 Data Exchange Services

Requirement ID: [SRS-4-53]

The IEG-C High Domain Firewall and IEG-C Low Domain Firewall components SHALL enable the capability to support only those Data Exchange Services as specified in Table 4 (for that component).

Requirement ID: [SRS-4-202]

The IEG-C High Domain Firewall and IEG-C Low Domain Firewall components SHALL mediate all Data Exchange Services that transition the IEG-C.

4.2.3 Protection Policy Enforcement Services

Requirement ID: [SRS-4-54]

The IEG-C High Domain Firewall and Low Domain Firewall components SHALL be configurable to support the enforcement of the following IEG-C IFPs (see Section 3.4.4):

- IEG-C_IFP_CA_HL - Communications Access Services High to Low IFP;
- IEG-C_IFP_CA_LH - Communications Access Services Low to High IFP; and,

- IEG-C_IFP_CS_MGMT - Core Services Management Services IFP

Requirement ID: [SRS-4-55]

The IEG-C High Domain Firewall and Low Domain Firewall components SHALL enable the capability to configure the IEG-C_IFP_CA_HL and IEG-C_IFP_CA_LH IFPs to allow only authorized systems/hosts to exchange data between the high domain and the low domain.

Requirement ID: [SRS-4-56]

The IEG-C High Domain Firewall and Low Domain Firewall components SHALL enable the capability to configure the IEG-C_IFP_CA_HL and IEG-C_IFP_CA_LH IFPs in order to allow only those protocols and ports required to support the information exchange requirements for the high domain - low domain interconnection.

Requirement ID: [SRS-4-203]

The IEG-C High Domain Firewall and Low Domain Firewall components SHALL enable the capability to configure the IEG-C_IFP_CA_HL and IEG-C_IFP_CA_LH IFPs in order to allow only those application layer protocols and applications that are required to support the information exchange requirements for the high domain - low domain interconnection.

Requirement ID: [SRS-4204]

The IEG-C High Domain Firewall and Low Domain Firewall components SHALL identify application layer protocols and applications through application protocol inspection, which SHALL be based on the use of application signatures, application protocol decoding, and heuristics.

Requirement ID: [SRS-4-57]

The IEG-C High Domain Firewall and Low Domain Firewall components SHALL enable the capability to configure the IEG-C_IFP_SOA_HL and the IEG-C_IFP_SOA_LH IFPs in order to route authorised HTTP(S) application-level traffic to the appropriate IEG-C guard or proxy component (through the High Side Switch or appropriate Low Side Switch depending upon the source and destination of the HTTP(S) application-level traffic) in the DMZ.

Requirement ID: [SRS-4-58]

The IEG-C High Domain Firewall and Low Domain Firewall components SHALL enable the capability to configure the IEG-C_IFP_BS_HL and the IEG-C_IFP_BS_LH IFPs in order to route authorised SMTP application-level traffic to the IEG-C Mail Guard component (through the High Side Switch or appropriate Low Side Switch depending upon the source and destination of the SMTP application-level traffic) in the DMZ.

Requirement ID: [SRS-4-59]

The IEG-C High Domain Firewall and Low Domain Firewall components SHALL enable the capability to configure the IEG-C_IFP_IS_HL IFP in order to route authorised RDP application-level traffic to the IEG-C RDP Proxy component (through the High Side

Switch depending upon the source and destination of the RDP application-level traffic) in the DMZ.

Requirement ID: [SRS-4-60]

The IEG-C High Domain Firewall and Low Domain Firewall components SHALL enable the capability to configure the IEG-C_IFP_CS_MGMT IFP in order to route authorised management traffic to the appropriate IEG-C component (through the Management Switch) in the DMZ.

Requirement ID: [SRS-4-61]

The IEG-C High Domain Firewall and Low Domain Firewall components SHALL enforce the IEG-C IFPs configured (depending upon the information exchange requirements and protection policy enforced for the CIS interconnection) for the IEG-C.

4.2.4 Element Management Services

Requirement ID: [SRS-4-62]

The IEG-C High Domain Firewall and Low Domain Firewall components SHALL be enabled and configured with the capability for being managed as specified in Section 9.

Requirement ID: [SRS-4-205]

The IEG-C High Domain Firewall and Low Domain Firewall components SHALL be managed from the Service Operation Centre (SOC) using the current management tools (i.e. Palo Alto Networks Panorama).

4.2.5 Hardware and Software

Requirement ID: [SRS-4-63]

The IEG-C High Domain Firewall component SHALL be configured to have at least three network interfaces (NICs: one for the network connection to the high domain; one for the network connection to the High Domain Switch; and, one for the network connection to the Management Domain Switch).

Requirement ID: [SRS-4-64]

The IEG-C High Domain Firewall component network interfaces to the high domain SHALL be 1000BASE-SX gigabit Ethernet interfaces.

Requirement ID: [SRS-4-65]

The IEG-C High Domain Firewall component network interfaces to the High Domain Switch SHALL be 1000BASE-SX gigabit Ethernet interfaces.

Requirement ID: [SRS-4-66]

The IEG-C High Domain Firewall component network interface to the Management Domain Switch SHALL be a 1000-Base-SX gigabit Ethernet interface.