automated data exchange between two network enclaves that belong to different security domains. From the WG's perspective one enclave is defined as the high domain, and the other enclave as the low domain.

In an information-exchange scenario involving a high domain and a low domain, also called a cross-domain information exchange, the following threats to the high domain are recognized:

- Leakage of confidential information from the high domain to the low domain;
- Degradation of the integrity or availability of resources in the high-security domain.

Figure A.2 illustrates these threats.

Figure 33 Identification of threats in a cross-domain information exchange

The purpose of the WG is to enable cross-domain information exchange by mediating traffic flows, while offering sufficient protection against the threats mentioned above by enforcing an appropriate security policy. In the case of high-to-low traffic, when information crosses the cross-domain boundary, the information is considered to have been 'released to the low domain'. Note that in the case of an IEG-C deployment, the WG is integrated in the IEG and the cross-domain boundary viewed from the WG's perspective may not coincide with the cross-domain boundary as viewed from the IEG's perspective. For all practical purposes, when this SRS states that information has been "released" by the WG to the low domain, this means that the WG has verified (or ensured) that the information is releasable to the low domain regardless of any potential further processing by other components in the IEG.

A.1.4 Security objective

The security objective of the WG is to protect the confidentiality of information, and the integrity and availability of resources in the high-security domain. The integrity and availability of the high domain is protected by allowing only those messages that have a white-listed message format to pass from the low domain to the high-security domain. In addition, constraints are set on the contents of the message. This is captured in a security policy.

The confidentiality of information is protected when messages pass from the high domain to the low domain by validating the confidentiality metadata label[7] that is bound to the information. Depending on the values contained in the label, the security policy in effect and the WG's functionality/configuration, the WG rejects the release of information, accepts it, or sanitizes the information by removing the parts that are in conflict with the security policy. See Section A.3.5 for an explanation of the data sanitization functionality.

(Note that data sanitization functionality is considered optional functionality for a WG developed based on this SRS.)

[7] *The meaning of the term 'confidentiality metadata label' is defined in [STANAG 4774]. A confidentiality metadata label is also known as a 'sensitivity label'. In this document the simplified term 'label' is also used and is understood to mean 'confidentiality metadata label'.*

A.1.5 Label handling

From the WG's point of view each attempted transfer of data from the high to the low domain is considered a request for information release. In order to make the information-release decision to reject, accept or sanitize, the WG validates a confidentiality metadata label that is bound to the information. The label and the binding mechanism must comply with the ([STANAG 4774], [STANAG 4778]). Depending on the information exchange scenario, the services in the COIs that use the WG to transfer information, and the security policy in effect, the WG can leave the confidentiality metadata label unaltered, remove it, or create a new (potentially modified) label. (Removal of the label is an option if the label will not be processed any further in the low domain. If the WG has sanitized information before release, and the low domain requires released information to be labelled, the WG will have to create a new label and bound it to the information before release.) If digital signatures are used, this means the WG must include the functionality to generate signatures in addition to signature verification.

Note that the way the WG handles labels depends on the labelling profile that is applied by the COIs; the [STANAG 4778] defines a number of labelling profiles and some of them allow for the co-existence of (COI-)application specific labels (that do not conform to [STANAG 4774]) and a label that will only be handled by the WG. In general the WG will not interpret (or modify) any (COI-) application specific labels, and will only handle labels that conform to the [STANAG 4774].

From now on in this document, when the term 'label' is used, it is implied to be a label that conforms to the [STANAG 4774] unless otherwise indicated.

A.2 Scope of the system

A.2.1 HTTP Proxy

To the COI services that make use of the WG (in either the high or the low domain), the WG acts as a hypertext transfer protocol (HTTP) 1.1 proxy [IETF RFC 7230, 2014]. The specific behaviour of the WG with respect to HTTP connectivity however, will also be influenced by the security policy that is enforced by the WG (from now on also referred to as the 'WG security policy'). The WG mediates HTTP traffic between HTTP clients and HTTP servers that reside in the high or low domain. The WG security policy pertains to both directions that HTTP messages can flow. For messages flowing from high to low, the enforcement of the WG security policy is referred to as 'high to low enforcement'. For messages flowing from low to high, it is referred to as 'low to high enforcement', see Figure A.3.

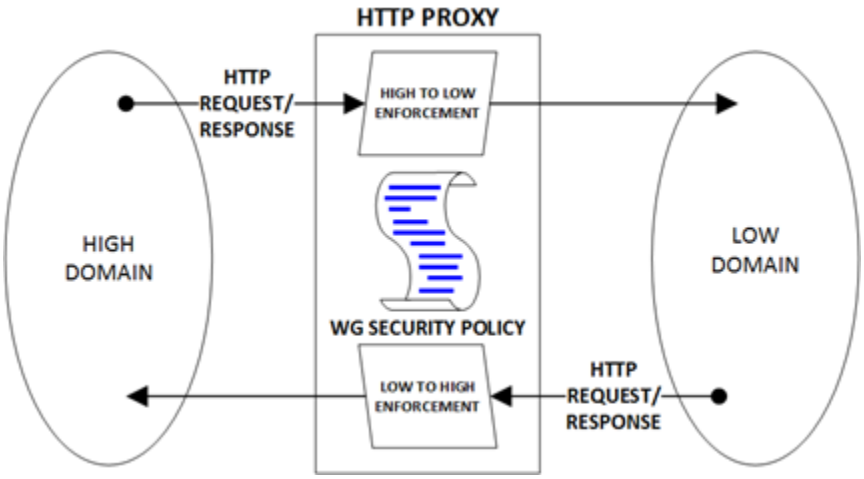

Figure 34 The WG provides HTTP proxy functionality to both domains, and enforces a security policy on traffic flowing in both directions

A.2.2 Types of security policy enforcement

For both directions of traffic flow, the WG security policy determines the security policy enforcement functionality that is enabled. The WG offers the following types of security policy enforcement functionality:

- HTTP header vetting (see [SRS-6-213]);
- Label validation (see [SRS-6-219]), potentially resulting in 'Data sanitization', i.e. removing the parts of the XML-formatted HTTP message body that are in conflict with the WG security policy. (Data sanitization is considered optional functionality for a WG based on the functional requirements in chapter 5.3, see [SRS-6-236]).
- XML schema validation (see [SRS-6-208]).

A.3 WG viewed as access-control mechanism

A.3.1 Access-control functionality

For the purpose of explaining the security policy enforcement functionality of the WG in more detail, this paragraph explains how the WG can be viewed as an access-control mechanism when mediating traffic flows between the high and low domains[8]. Here, it is important to note that the access control decision is made at the domain level, i.e. all initiators and targets are subject to the same domain security policy (based on their domain membership). In the case of high to low enforcement, a request to release information *I_HL* can be viewed as a request to provide the low domain access[9] to *I_HL*. Similarly, an attempt to transfer information *I_LH* from the low to the high domain can be viewed as a request to provide the high domain access to *I_LH*. Taking this point of view, the WG can be viewed as an implementation of a classic access-control mechanism consisting of an access-control policy (i.e. the WG security policy), an access-control decision function (ADF) and an access-control enforcement function (AEF) as shown in Figure A.4. The WG connects the high and low domains and, given the available access-control information (ACI), mediates access requests from initiators to targets located in either of the two domains.

[8] *The type of access control described here is different from user access control; the WG will implement user access control in support of system administration, but it will not implement user*

access control in the sense of taking credentials of a sending or receiving user (in either low or high domain) into account when enforcing the WG security policy.

[9] Whether or not information is actually accessed by a target in the low domain after release (e.g. a low domain user opens a file) is irrelevant to the decision to release the information (which essentially says that any low domain user is authorized to access the information). The act of releasing information to the low domain means that any target in the low domain may now access the information if so desired.

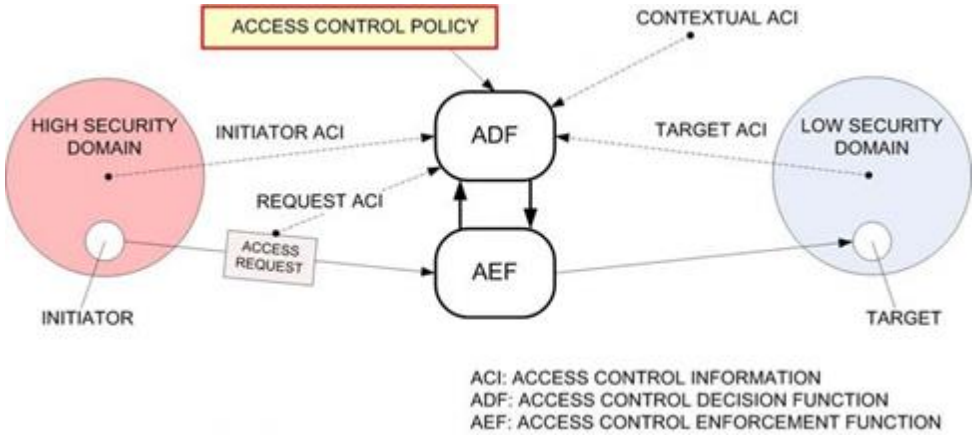

Figure 35 The WG can be viewed as an access-control mechanism connecting two security domains; initiator and target may be located in either domain10 depending on the actual access request

[10] Note that the figure uses the terms 'high security domain' and 'low security domain'. In the text these are referred to as 'high domain' and 'low domain' respectively.

An access request whose initiator is located in the high domain is also called an *information release request*. An access-control decision that grants access to a release request is called a *release of information* or simply a *release*.

A description of the ADF, AEF and ACI for the WG is given below for the types of security policy enforcement functionality for both directions of traffic flow.

A.3.2 HTTP header vetting

The access requests supported by the AEF of the WG are HTTP 1.1 request messages and HTTP response messages.

If the initiator of the access request is in the low domain, only a pre-defined set of HTTP message header lines with corresponding values is allowed. This set is defined in the WG security policy. The ADF tries to match each header line against this set. If it fails, access is denied for the particular header line and it is removed, or the header line is vetted (i.e. rewritten to conform to the WG security policy). As a result of this process an HTTP message with a transformed message header may be forwarded to the high domain.

If the initiator of the access request is in the high domain a similar process takes place. As a result of this process an HTTP message with a transformed message header may be forwarded to the low domain.

A.3.3 XML schema validation

If the initiator of the access request is in the low domain, only permitted XML document types are allowed for HTTP message bodies that are XML. This is defined in the WG security policy in the form of a list of allowed XML schema [W3C WD-xmlschema11-1, 2006] definitions. The ADF performs an XML schema validation. If the validation fails, access is denied for the entire HTTP message.

A.3.4 Label validation

If the initiator is in the high domain, the ACI is in fact a pair consisting of the contents of the HTTP request or response message and also one or more labels. In the context of information release the label provides information about the security-classification levels and categories of the information contained in the body of the HTTP message. For each labelled object in the HTTP message, the WG validates the label by checking its conformance to the [STANAG 4774], verifying the digital signature (if present) and by comparing the security-classification levels and the assigned categories against the WG security policy in order to determine its decision to reject, release or (optionally) sanitize.

A.3.5 Data sanitization

If the initiator is in the high domain, the ADF and AEF can work at a different level of granularity depending on the contents of the HTTP message body. If the HTTP message body is not XML, a single-access decision is made for the entire HTTP message and the decision is to either reject or release the entire HTTP message. However, if the HTTP message body is XML, the NATO labelling standard [STANAG 4778] allows for binding labels to individual information items in the XML infoset [W3C REC-xml-infoset, 2004]. If this is done, the AEF is able to act on every information item individually: individual information items for which the label is such that release to the low side is not allowed by the WG security policy, can be removed so that an HTTP message with a transformed message body results. This process is referred to as ‘data sanitization’. The sanitized HTTP message can then be released to the low domain. Note that it is still possible to reject the entire HTTP message if one of the individual information items cannot be released.

Data sanitization is considered optional functionality for a WG based on the functional requirements in chapter 5.3, see [SRS-6-236]).

A.3.6 Process to determine if a label is in conflict with the WG security policy

The WG security policy expresses the requirements that (the values within) labels must meet in order for the labelled information to be released to the low domain[11]. These requirements are expressed in terms of the values that comprise the clearance level of the low domain. (The clearance level of a domain typically reflects the ownership of the domain, its classification and the coalition that makes use of the domain.) If for a given label *L* these requirements are not met, the information object that is labelled with *L* is rejected or (optionally) sanitized by the WG. The way in which these requirements are captured in the WG security policy as well as the mechanism that is used to verify if a label meets those requirements, can be implemented in different ways.

[11] In theory it is also possible that the WG security policy expresses, for a given label, requirements on the clearance level of the low domain. However, in order to make a release decision for all requests for information release, such an approach would require support for all possible label values and that may not be feasible. Therefore, it is assumed that the WG security policy expresses requirements on the values of the label.

A.4 Common information exchange scenario supported by the WG

A common information exchange scenario that is supported by the WG is referred to as the 'bi-directional cross-domain XML web content' scenario based on HTTP POST. In this scenario, XML-formatted data is transported in the body of HTTP POST requests or associated HTTP response messages. An example of such XML-formatted data are Simple Object Access Protocol (SOAP) messages [W3C Note SOAP, 2000].

In the bi-directional XML web content scenario, the producers and consumers of the web content that are located in either of the two security domains exchange XML-formatted messages over HTTP. The WG acts as an HTTP proxy and the web content producers and consumers have to be configured accordingly. The web content is contained in the body of an HTTP POST message or an HTTP response message.

In this scenario two cases of message processing are distinguished depending on the origin of the HTTP POST request:

- The case in which the HTTP POST request is sent from the low domain is called "low to high web content processing".
- The case in which the HTTP POST request is sent from the high domain is called "high to low web content processing".

The security functionality that is enforced in this scenario is as follows:

- Low to High enforcement:
  - HTTP header vetting;
  - XML schema validation.
- High to Low enforcement:
  - Label validation;
  - HTTP header vetting.

The XML-formatted messages that are sent from the high to the low domain are labelled according to the [STANAG 4774]. Figure 37 shows the data transfers and processing that is involved in the case "low to high web content processing".

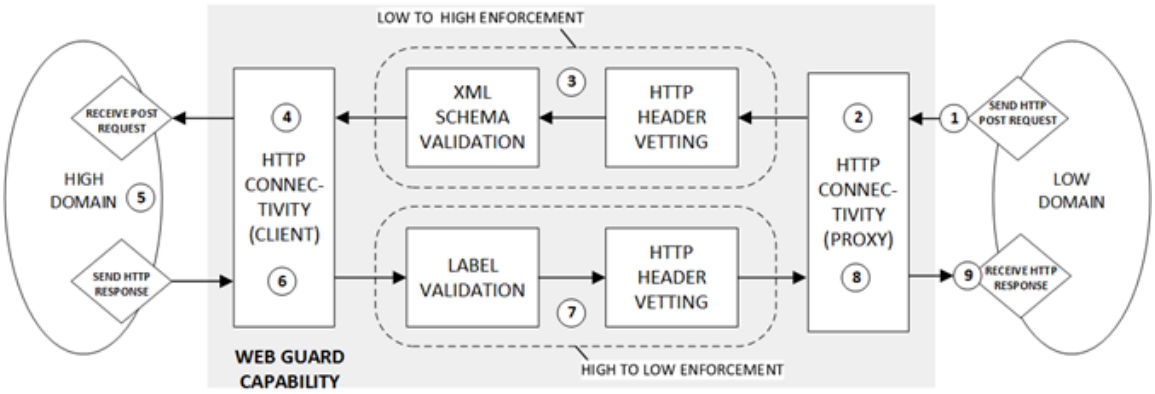

Figure 36 Low to high web content processing based on HTTP POST

The order of processing is as follows (see numbered steps in Figure A.5):

1. A web content consumer located in the low domain initiates the HTTP connection by sending a message in the body of an HTTP POST request message to a web content producer in the high domain.

2. HTTP connectivity (proxy): the HTTP POST request message is mediated by the WG that functions as an HTTP proxy to the web content consumer in the low domain.

3. Low to high enforcement: the WG enforces the WG security policy and performs validation of the messages:

   3.1. HTTP header vetting: the WG checks the HTTP headers for conformance to the WG security policy, and modifies and removes headers if necessary.

   3.2. XML schema validation: the WG checks if message body is XML. If so, it checks the compliance of the message body with predefined XML schemas. If the message body is not XML, the message is rejected.

4. HTTP connectivity (client): on behalf of the web content consumer in the low domain the WG acts as an HTTP client to the web content producer in the high domain.

5. The web content producer located in the high domain receives the HTTP POST request and sends a labelled XML web content message in the body of an HTTP response message to the WG; the target is the web content consumer in the low domain.

6. HTTP connectivity (client): the HTTP response message is received by the WG.

7. High to low enforcement: the WG enforces the WG security policy and performs validation of the messages: this requires the validation of HTTP message body and label.

   7.1. Label validation: the WG validates the label. This includes:

   - The validation of the digital signature of the label;
   - The validation of the conformance of the label (and bindings) to the [STANAG 4774], [STANAG 4778];
   - The validation of the binding(s) of the label to the contents of the HTTP message body;
   - The validation of the values in the label against the metadata policy that governs the information exchange; this policy specifies the label values that can be used, and their allowed usage, and is typically captured in a metadata policy information file (MPIF)[12]. The validation may include processing of an alternative label if the values of the originator label are not supported by the WG (i.e. they are not defined in the MPIF for this information exchange scenario). If neither originator nor alternative label is supported by the WG, the information release request will be rejected;
   - The validation of the conformance of the labelled content to the WG security policy (i.e. whether or not the values of the label imply that release to the low domain is allowed). If the WG security policy is such that the release of the content of the HTTP message body must be denied, the HTTP message is not transferred. If the WG security policy allows for parts of the message body to be released, data sanitization may be executed.

[12] For metadata in the context of sensitivity labels, such an MPIF is also commonly referred to as a security policy information file (SPIF).

7.2. HTTP message header vetting: the WG checks the HTTP headers for conformance to the access-control policy, and modifies or removes headers if necessary.

8. HTTP connectivity (proxy): in its role of HTTP proxy, the WG sends the response message to the web content consumer in the low domain.

9. The low domain web content consumer receives the HTTP response.

Note that the description of steps above assumes that a consumer will request web content from a producer. However, the WG does not distinguish between a consumer or producer when enforcing the WG security policy, hence in the case of “low to high web content processing” the HTTP POST request message can also be initiated by a producer in the low domain if there is a requirement to do so (e.g. push web content). Similar considerations apply to the case ‘high to low web content processing’.

The case ‘high to low web content processing’ contains the same steps and processes as ‘low to high web content processing’, however the traffic flow is in the opposite direction:

- the HTTP connection is initiated in the high domain by sending an HTTP POST request;
- the WG acts an HTTP proxy to the initiator in the high domain;
- Label validation takes place for the message body of the HTTP POST request instead of the HTTP response.

Note that the scenario based on HTTP POST that is described above is an example scenario. Scenarios based on other HTTP methods will be supported by the WG, for which similar steps and diagrams as for Figure A.6 can be developed.

The enforcement of the WG security policy is transparent to producers and consumers of web content. The WG does not authenticate producers or consumers of web content, however the set of producers and consumers that is reachable from either domain can be defined as part of the WG security policy based on a whitelist of URIs.

The sending of HTTP error messages - in case the enforcement of the WG security policy leads to a denial of an HTTP request – is governed by the WG security policy that specifies for a given deployment of the WG whether or not to send error messages, and if so which types are allowed and what the contents of their payload can be.

A.5 WG interfaces and external services

A.5.1 Standard interfaces

The WG offers the following standard interfaces (depicted in Figure A.6):

- WG_IF_NET_HIGH: This is a network interface that connects the WG to a network enclave belonging to the high domain. This interface is also called the ‘high network interface’.
- WG_IF_NET_LOW: This is a network interface that connects the WG to a network enclave belonging to the low domain. This interface is also called the ‘low network interface’.

- WG_IF_LOCAL_MGMT: This interface is intended for local system-administration purposes of the WG.

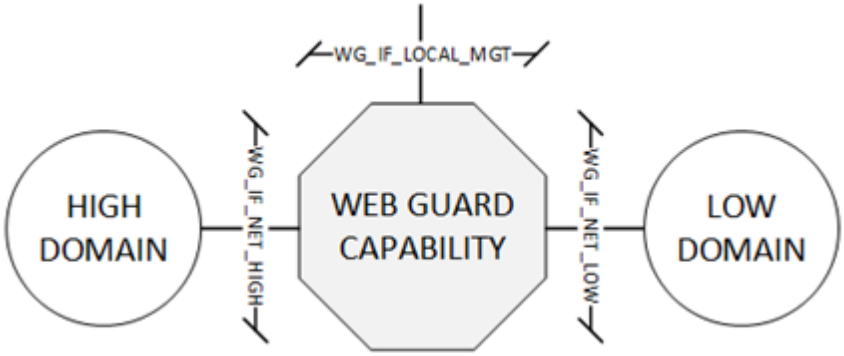

Figure 37 Network and local management interfaces of the WG

Note that depending on the type of deployment of the WG or its integration in the IEG-C, the interfaces in Figure A.6 can be physical or logical interfaces. For example, if the WG is implemented in a virtual machine, WG_IF_LOCAL_MGMT is a logical interface because it will then be accessed through the physical local management interface of the host of the virtual machine. (The physical local management interface consists of a directly attached keyboard and display console.)

A.5.2 Management interface

In addition to the standard interfaces from Section A.5.1, the WG has a (remote) management interface WG_IF_MGMT. The interface WG_IF_MGMT can be a dedicated physical interface, or a logical interface on top of WG_IF_NET_HIGH. (The WG is managed from the administrative high domain or from a dedicated management domain). WG_IF_MGMT supports remote management of the WG, and connections to the following external services:

- The IEG-C Domain Management System (DMS) in order to report on the key performance indicators ‘Availability’, ‘Quality’ and ‘Usage’ [NCIA SMC TA, 2018];
- REST-based Web Services for
    - the retrieval of XML schemas in support of XML schema validation;
    - Information on the metadata policy[13] (i.e. the policy that governs the values of the metadata that comprise the label);
- An OCSP responder provided by E-NPKI for obtaining the revocation status of X.509 digital certificates;
- An LDAP directory service (NATO Enterprise Directory Service (NEDS)) for:
    - The retrieval of X.509 certificates and associated revocation material;
    - Information on the metadata policy[13] (i.e. the policy that governs the values of the metadata that comprise the label);

[13] This information can for example be captured at the WG in the form of a metadata policy information file (MPIF). For metadata in the context of sensitivity labels, such an MPIF is also commonly referred to as a security policy information file (SPIF).

The interface WG_IF_MGMT is visualized in Figure A.7.

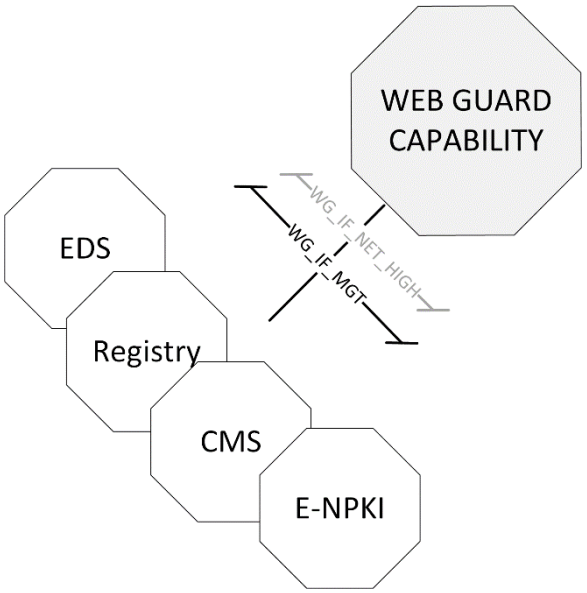

Figure 38 The management interface WG_IF_MGMT can be implemented as a physical interface or a logical interface on top of WG_IF_NET_HIGH; it supports remote management and connections to EDS, Registry, CMS and E-NPKI

A.5.3 Existing Capabilities

An implementation of the WG by NC3A (former NCIA) is operational as a component in an IEG-C at a number of locations. The implementation is referred to as 'NC3A MAXLG' (medium assurance XML-Labelling Guard). The NC3A MAXLG partially provides the functionality of the WG as specified in Chapter 6.3, e.g. the NC3A MAXLG supports an older version of the NATO labelling standard [STANAG 4774].

A.6 Dependencies

A.6.1 Availability of Enterprise NATO PKI

The Enterprise NATO PKI (E-NPKI) must be available to support the information exchange enabled by the WG.

A.6.2 Availability of a malware scanner

A malware scanner helps to protect the integrity and availability of the high domain by implementing specific scanning (such as virus-scanning) for malicious content that can be transmitted from the low domain. Although the WG provides filtering of messages delivered from the low to the high domain based on white listing of message types, it does not provide by itself any protection for the high domain against malicious content that might be injected from the low domain. Therefore, if a malware scanning capability is required for the information exchange scenario supported by the WG, it must be provided separately compliant with [NC3B AC/322-D(2004)0019 (INV), 2004].

A.6.3 Relationship with NC3A MAXLG

The WG is the replacement of the NC3A MAXLG in theatre. The requirements in the WG SRS are based on architecture building blocks (ABBs). The ABBs that are used for the WG are described in [NCIA TR/2016/NSE010871/01, 2016]. In order to understand how the architecture of the NC3A MAXLG relates to the ABBs used for the WG, Figure 39

illustrates this relationship. It shows the system architecture of the NC3A Medium Assurance XML-Labelling Guard (MAXLG) (excluding system management components) with each component in the figure marked according to the accompanying legend which expresses the relationship with the ABBs.

Note that the HTTP connectivity component in the NC3A MAXLG implements both HTTP client and proxy connectivity. It does not implement HTTPS. The Public Key Cryptography Services are implemented in the form of a Public Key Encryption (PKE) module.

The 'WG High to Low Pattern' can be followed through the figure from left to right. Similarly, the 'WG Low to High Pattern' can be followed from right to left.

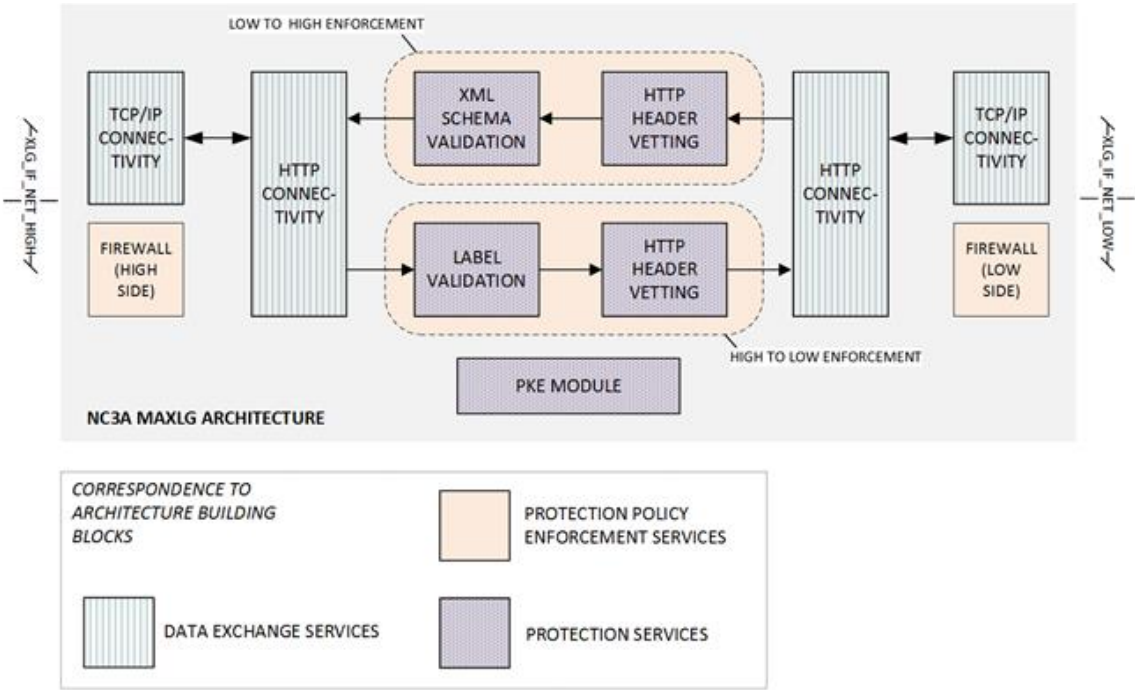

Figure 39 Relationship between NC3A MAXLG system architecture and IEG-C ABBs

APPENDIX B: Service Interface Profiles

B.1 Introduction

NATO communication and information systems (CIS) operate in a heterogeneous environment, with service providers and service consumers operating under multiple different frameworks and application contexts. Systems deployed onto NATO networks are subject to an appropriate security approval and/or accreditation process addressing the confidentiality, integrity and availability of security objectives where different available technologies and mechanisms can be used to apply security.

To ensure interoperability between services, both within NATO, and between NATO and its partners, there is a need to define a standard (and standards-based) profile which will be mandatory for all service operations in the federated mission environment. Service Interface Profiles (SIPs) have been designed to specify new and existing security technologies and mechanisms that offer a security framework that is implementation-independent, and can be used to support interoperability.

SIPs are published as Agency Technical Instructions (INSTR TECH) and are living documents that are periodically reviewed and updated.

In the case were a SIP has not been defined for a specific service, an FMN Service Instructions (SIs), which provides guidance how to implement the service in federated Mission Networks to enable the effective and efficient sharing of information, may be used.

This Appendix defines the SIPs and SIs that are applicable to the IEG-C in order to ensure cross-domain interoperability.

The SIPs and Sis that are applicable to the IEG-C are those that relate to proxies or guards that are hosted within the IEG-C. As identified in section 6.3, Table 10, the following are the initial IEG-C guards and proxies:

- RDP Proxy
- Web Guard
- Web Proxy
- Mail Guard

For services that the IEG-C does not mediate through the use of a proxy or guard, SIPs and SIs are not applicable. For example, the IEG-C may allow the flow of directory information between the High and Low Domains, however the SIP for Enterprise Directory Services is not applicable to the IEG-C as it does not proxy or guard the directory information exchange. Note that the directory services in the High and Low Domains which are exchanging directory information should be compliant with the SIP for Enterprise Directory Services, however this is beyond the scope of this Target Architecture.

B.2 RDP Proxy

There is no current SIP or SI for the remote desktop protocol, and consequently there is no requirement on the RDP proxy.

B.3 Web Guard

The following SIPs are applicable to the IEG-C Web Guard:

1. INSTR TECH 06.02.01 Service Interface Profile for Security Services, 4th February 2015
2. INSTR TECH 06.02.02 Service Interface Profile for REST Security Services, 4th February 2015
3. INSTR TECH 06.02.06 Service Interface Profile for Messaging (SOAP), 4th February 2015
4. INSTR TECH 06.02.07 Service Interface Profile for REST Messaging, 4th February 2015

In particular, these SIPs are applicable to the following interfaces and operations of the IEG-C Data Exchange Services ABB:

- SOA Platform Services HL Interface
    - ReceiveWebContentHL
    - ForwardWebContentHL

- SOA Platform Services LH Interface
    - ReceiveWebContentLH
    - ForwardWebContentLH

B.4 Web Proxy

The following SIPs are applicable to the IEG-C Web Proxy:

1. INSTR TECH 06.02.01 Service Interface Profile for Security Services, 4th February 2015
2. INSTR TECH 06.02.02 Service Interface Profile for REST Security Services, 4th February 2015
3. INSTR TECH 06.02.06 Service Interface Profile for Messaging (SOAP), 4th February 2015
4. INSTR TECH 06.02.07 Service Interface Profile for REST Messaging, 4th February 2015

In particular, these SIPs are applicable to the following interfaces and operations of the IEG-C Data Exchange Services ABB:

- SOA Platform Services HL Interface
    - ReceiveWebContentHL
    - ForwardWebContentHL
- SOA Platform Services LH Interface
    - ReceiveWebContentLH
    - ForwardWebContentLH

B.5 Mail GUARD

The following SI is applicable to the IEG-C Mail Guard:

1. FMN Spiral 1 Service Instructions for Informal Messaging, 18th February 2016

In particular, this SI is applicable to the following interfaces and operations of the IEG-C Data Exchange Services ABB:

- Business Support Service HL Interface
    - ReceiveEmailHL
    - ForwardEmailHL
- Business Support Service LH Interface
    - ReceiveEmailLH
    - ForwardEmailLH

B.6 Future Proxies/Guards

If additional guard and/or proxies are introduced into the IEG-C architecture to support other information exchange requirement, additional SIPs may be applicable.

APPENDIX C: IEG-C Protection Profile

C.1 Security Problem Definition

C.1.1 Threats

Threats	Description	Source
T.ADDRESS_MASQUERADE	A user on one interface may masquerade as a user on another interface to circumvent the TOE policy.	[NCIA TN-1485 v1.1, 2012]
T. ADMIN_ERROR	An administrator may incorrectly install or configure the TOE, or install a corrupted TOE resulting in ineffective security mechanisms.	[NCIA TN-1485 v1.1, 2012]
T.AUDIT_COMPROMISE	An attacker may view audit records, cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a user‘s action.	[NCIA TN-1485 v1.1, 2012]
T.COVERT_CHANNEL	An attacker on the high network may initiate an illicit flow of unauthorised information from the high network enclave to the low network enclave as a result of exploiting a covert channel in the IEG.	[NCIA TN-1485 v1.1, 2012] modified
T.FLAWED_DESIGN	Unintentional or intentional errors in requirements specification or design of the TOE may occur, leading to flaws that may be exploited by an attacker.	[NCIA TN-1485 v1.1, 2012]
T.FLAWED_IMPLEMENTATION	Unintentional or intentional errors in implementation of the TOE may occur, leading to flaws that may be exploited by an attacker.	[NCIA TN-1485 v1.1, 2012]
T.INFORMATION_LEAK	A low network attacker may carry out a network-based attack against the high network enclave in order to obtain unauthorised information.	[NCIA TN-1485 v1.1, 2012] modified
T.MALICIOUS_TSF_COMPROMISE	An attacker may cause TSF data or executable code to be inappropriately accessed (viewed, modified, or deleted).	[NCIA TN-1485 v1.1, 2012]
T.MASQUERADE	An attacker may masquerade as an administrator in order to gain unauthorized access to data or TOE resources.	[NCIA TN-1485 v1.1, 2012]
T.MALWARE_INJECTION	Malicious software, such as viruses and worms, may be introduced into the high domain from the low domain.	[NCIA TN-1485 v1.1, 2012]
T.POOR_TEST	Lack of or insufficient tests to demonstrate that all TOE security functions operate correctly (including in a fielded TOE) may result in incorrect TOE behaviour being undiscovered thereby causing potential security vulnerabilities.	[NCIA TN-1485 v1.1, 2012]
T.RECONNAISSANCE	A low network attacker may obtain unauthorised information about resources (e.g. IP addresses, port numbers, system names, system date/time, products, versions) in the high network enclave e.g. by using network scanning techniques, network traffic monitoring, etc.	[NCIA TN-1485 v1.1, 2012] modified
T.REPLAY	An attacker may gain inappropriate access to the TOE by replaying administrator‘s authentication information, or may cause the TOE to be inappropriately configured by replaying TSF data or IA attributes (e.g., captured as transmitted during the course of legitimate use).	[NCIA TN-1485 v1.1, 2012]
T.RESIDUAL_DATA	A user or process may gain unauthorized access to data through reallocation of TOE resources from one user or process to another.	[NCIA TN-1485 v1.1, 2012]
T.RESOURCE_EXHAUSTION	An attacker may block others from accessing system resources	[NCIA TN-1485 v1.1, 2012]
T.SECURITY_LABEL_TAMPERING	A high network attacker may modify a security label. For example the security label may be modified so that it binds wrong IA attributes to information in such a way that the IA attributes conform to the release level and as a consequence unauthorised information may be illicitly released to the low network enclave.	[NCIA TN-1485 v1.1, 2012] modified
T.SPOOFING	An attacker may misrepresent itself as the TOE to obtain administrator‘s identification and authentication data.	[NCIA TN-1485 v1.1, 2012]
T.UNATTENDED_SESSION	A user may gain unauthorized access to an unattended session.	[NCIA TN-1485 v1.1, 2012]
T.UNAUTHORIZED_ACCESS	A low network attacker may gain access to unauthorised information	[NCIA TN-1485 v1.1, 2012] modified

T.UNIDENTIFIED_ACTIONS	The administrator may not have ability to notice potential security violations, thus limiting the administrator's ability to identify and take action against a possible security breach.	[NCIA TN-1485 v1.1, 2012]
T.UNKNOWN_STATE	When the TOE is initially started or restarted after a failure, the security state of the TOE may be unknown.	[NCIA TN-1485 v1.1, 2012]
T.NETWORK_ATTACK	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may engage in communications with the application software or alter communications between the application software and other endpoints in order to compromise it. A low network attacker may carry out a network-based attack against resources available on the high network thereby compromising the system integrity and availability.	Protection Profile for Application Software Version 1.2 [NIAP PP_APP_V1.2, 2016] Protection Profile for General Purpose Operating Systems [NIAP, PP_OS_V.4.1, 2016] [NCIA TN-1485 v1.1, 2012] modified
T.NETWORK_EAVESDROP	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may monitor and gain access to data exchanged between the application and other endpoints.	Protection Profile for Application Software Version 1.2 [NIAP PP_APP_V1.2, 2016] Protection Profile for General Purpose Operating Systems [NIAP, PP_OS_V.4.1, 2016]
T.LOCAL_ATTACK	An attacker can act through unprivileged software on the same computing platform on which the application executes. Attackers may provide maliciously formatted input to the application in the form of files or other local communications.	Protection Profile for Application Software Version 1.2 [NIAP PP_APP_V1.2, 2016] Protection Profile for General Purpose Operating Systems [NIAP, PP_OS_V.4.1, 2016]
T.PHYSICAL_ACCESS	An attacker may try to access sensitive data at rest.	Protection Profile for Application Software Version 1.2 [NIAP PP_APP_V1.2, 2016]

T.LIMITED_PHYSICAL_ACCESS	An attacker may attempt to access data on the IEG while having a limited amount of time with the physical device.	Protection Profile for General Purpose Operating Systems [NIAP, PP_OS_V.4.1, 2016] modified
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	Threat agents may attempt to gain administrator access to the firewall by nefarious means such as masquerading as an administrator to the firewall, masquerading as the firewall to an administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between the firewall and a network device. Successfully gaining administrator access allows malicious actions that compromise the security functionality of the firewall and the network on which it resides.	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]
T.WEAK_CRYPTOGRAPHY	Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.	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]
T.UNTRUSTED_COMMUNICATION_CHANNELS	Threat agents may attempt to target firewalls that do not use standardized secure tunnelling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the firewall itself.	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]
T.WEAK_AUTHENTICATION_ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g., shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the firewall itself could be compromised.	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]
T.UPDATE_COMPROMISE	Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.	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]
T.UNDETECTED_ACTIVITY	Threat agents may attempt to access, change, and/or modify the security functionality of the firewall without administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the administrator would have no knowledge that the device has been compromised.	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]
T.SECURITY_FUNCTIONALITY_COMPROMISE	Threat agents may compromise credentials and firewall data enabling continued access to the firewall and its critical data. The compromise of credentials include replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the administrator or firewall credentials for use by the attacker.	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]
T.PASSWORD_CRACKING	Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the firewall. Having privileged access to the firewall provides the attacker unfettered access to the network traffic, and may allow them to take advantage of any trust relationships with other network devices.	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]
T.SECURITY_FUNCTIONALITY_FAILURE	A component of the firewall may fail during start-up or during operations causing a compromise or failure in the security functionality of the firewall, leaving the firewall susceptible to attackers.	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]
T.NETWORK_DISCLOSURE	An attacker may attempt to “map” a subnet to determine the machines that reside on the network, and obtaining the IP addresses of machines, as well as the services (ports) those machines are offering. This information could be used to mount attacks to those machines via the services that are exported. Sensitive information on a protected network might be disclosed resulting from disclosure/transmitted information in violation of policy, such as sending unencrypted credit card numbers. The IPS TOE will be capable of inspecting packet payloads for data strings and patterns of characters.	Collaborative Protection Profile for Stateful Traffic Filter Firewalls [NIAP, CPP_FW_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]
T. NETWORK_ACCESS	With knowledge of the services that are exported by machines on a subnet, an attacker may attempt to exploit those services by mounting attacks against those services. An attacker may attempt to gain inappropriate access to one or more networks, endpoints, or services, such as through brute force password guessing attacks, or by transmitting malicious executable code, scripts, or commands. If malicious external devices are able to communicate with devices on the protected network, then those devices may be susceptible to the unauthorized disclosure of information.	Collaborative Protection Profile for Stateful Traffic Filter Firewalls [NIAP, CPP_FW_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]
T.NETWORK_MISUSE	An attacker may attempt to use services that are exported by machines in a way that is unintended by a site’s security policies. For example, an attacker might be able to use a service to “anonymize” the attacker’s machine as they mount attacks against others.	Collaborative Protection Profile for Stateful Traffic Filter Firewalls

	Access to services made available by a protected network might be used counter to Operational Environment policies. Devices located outside the protected network may attempt to conduct inappropriate activities while communicating with allowed public services, (e.g. manipulation of resident tools, SQL injection, phishing, forced resets, malicious zip files, disguised executables, privilege escalation tools, and botnets).	[NIAP, CPP_FW_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]
T.NETWORK_DOS	Attacks against services inside a protected network, or indirectly by virtue of access to malicious agents from within a protected network, might lead to denial of services otherwise available within a protected network. Resource exhaustion may occur in the event of co-ordinate service request flooding from a small number of sources. Though most IPS will provide some protection from DDoS (distributed denial of service) attacks, providing protection against DDoS attacks is not a requirement for conformant TOEs, as this is best counteracted by firewalls, cloud computing and design. Note however that DoS protection is required.	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]
T.ADMIN_ERROR	The security features offered by the TOE may be rendered irrelevant if a malicious or careless administrator configures or operates the TOE in a manner that is inconsistent with the defined security requirements. For example, they may fail to enable encrypted communications, configure an appropriate password policy, or assign excessive administrative privileges to a user who does not require them. While the TSF cannot truly prevent such incidents, the distribution of clear administrative guidance is expected to reduce unintentional errors, and the display of an acceptable use banner (with clearly enumerated consequences for unacceptable use) may deter some malicious activity.	Standard Protection Profile for Enterprise Security Management Policy Management [NIAP, PP_ESM_V.2.1, 2013]
T.EAVES	An Enterprise Security Management architecture will almost certainly require data to be transmitted between remote devices in order to function. The TOE may distribute policies to be enforced to remote Access Control products. It may receive user attributes or session data from elsewhere in the environment, and it may write audit data to a centralized repository that is located remotely. If this data is not protected by a sufficiently secure trusted channel, it may be subject to involuntary disclosure. An attacker with access to this data can use it for reconnaissance purposes or to replay known valid information in an attempt to impersonate a valid user or entity. The Operational Environment will almost certainly require data to be transmitted between remote devices in order to function. The TOE may receive policies to enforce from a remote source. It will receive user attributes or session data from elsewhere in the environment, and it will write audit data to a centralized repository that is located remotely. If this data is not protected by a sufficiently secure trusted channel when in transit, it may be subject to involuntary disclosure. An attacker with access to this data can use it for reconnaissance	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

	purposes or to replay known valid information in an attempt to impersonate a valid user or entity.	[NIAP, PP_ESM_aC_V. 2.1, 2013]
T.UNAUTH	If the TSF does not appropriately identify, authenticate, and authorize its administrators, there will not be assurance that its management functions are being performed appropriately. A poorly designed or implemented authentication function will allow an attacker to illegitimately access the TSF and attempt to perform management functions. A poorly designed or implemented data protection function will allow access control checks to be bypassed allowing for privilege escalation. Regardless of the method by which an attacker gains illegitimate access to the ability to create policies, the resulting compromise of the integrity of the organization's access control policies is the same. The primary purpose of deploying the TOE is to enforce access control against objects that reside in the Operational Environment. It does this by providing mechanisms to intercept subject requests to perform operations against objects and determine whether a defined access control policy should allow the request to occur. If these activities are subverted or bypassed, or if the TOE is incapable of controlling access to the expected level of granularity, then all or some of the Operational Environment will function as if the TOE did not exist. This situation allows for objects being accessed without proper authorization.	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]
T.DISABLE	In order to enforce access control against objects, the TOE must reside in a logical location that will allow it to intercept requests. The types of resources to which access is being controlled may require the TOE to reside locally to these resources. If the TOE is located on an endpoint system, the threat of the TOE being disabled is magnified. This is due to the fact that endpoint systems are less likely to perpetually remain in controlled access environments. When the assurance of physical access control is diminished, the risk of an attacker attempting to access the system is increased. If the TOE runs as a process that can be terminated or if its files can be moved, altered, or removed from the operating system's start-up sequence, a user will have the ability to circumvent access control enforcement.	Standard Protection Profile for Enterprise Security Management Access Control [NIAP, PP_ESM_aC_V. 2.1, 2013]
T.NOROUTE	In cases where the TOE is located remotely from other ESM components, a risk may be present. If connections between the TOE and remote resources are disrupted, the TOE may not be able to properly enforce its security functions. Worse yet, the threat of discontinuity can be realized by denial of service or by simply unplugging physical cables. It can also be very easily performed inadvertently and by individuals far removed from the operation of the TOE itself. Because of this, the TOE must have some way to maintain continuity of operations in the event of a virtually inevitable service outage.	Standard Protection Profile for Enterprise Security Management Access Control [NIAP, PP_ESM_aC_V. 2.1, 2013]
T.FALSIFY	The Policy Management product must communicate with the TOE in order to distribute policies that the TOE will be responsible for enforcing. In order to provide assurance that a policy has been received and will be enforced, the TOE should be able to provide some evidence of policy receipt and consumption to the Policy Management product. However, if the format of this receipt is sufficiently generic or the communications channel is not sufficiently protected from disclosure, an attacker may intercept the distribution of the policy and return a false receipt to the Policy Management product. The result of this is that the TOE does not enforce the correct policy and nothing appears amiss from a management perspective, potentially making the security breach more difficult to detect.	Standard Protection Profile for Enterprise Security Management Access Control [NIAP, PP_ESM_aC_V. 2.1, 2013]
T.WEAKPOL	The Standard Protection Profile for Enterprise Security Management Access Control specifies a variety of technology types and the minimum sets of subjects, objects, operations, and attributes in order to define sufficiently detailed policies for each technology type. A Policy Management product must be capable of creating policies	Standard Protection Profile for Enterprise Security

	that provide the same level of detail that a compatible Access Control product can consume. An insufficiently detailed policy is an ineffective access control mechanism because it either allows unintended activity or incorrectly restricts legitimate usage.	Management Policy Management [NIAP, PP_ESM_V.2.1, 2013]
T.CONTRADICT	An access control policy can potentially contain many different complex rules that permit and forbid access to various objects. A consequence of this is that a policy may contain rules that contradict one another. For example, a rule may exist that allows a particular user the ability to run a particular program on a host while another rule in the same policy may exist that forbids all members of a group that user belongs to from running the same program. If a policy that contains such a contradiction is consumed by an Access Control product, it may create an unpredictable result.	Standard Protection Profile for Enterprise Security Management Policy Management [NIAP, PP_ESM_V.2.1, 2013]
T.FORGE	When an Access Control product receives what appears to be updated policy information from the TOE, the Access Control product must have some assurance of the authenticity of the policy and the identity of the sender. If the communications channel is not sufficiently protected or the mechanism by which the TOE provides a guarantee of a policy's integrity is not sufficiently robust, an attacker who is aware of the syntax used to transmit a policy may be able to forge an arbitrarily fake one and have an Access Control product consume it. If this occurs, an Access Control product may be configured to enforce a permissive fake policy that allows unauthorized access, to enforce a restrictive fake policy that prevents legitimate activities from being performed, or to consume an incorrectly formatted policy and either terminate or allow an attacker access to memory space within the system on which the Access Control product resides. When the TOE receives what appears to be updated policy information, the TOE must have some assurance of the authenticity of the policy and the identity of the sender. If the communications channel is not sufficiently protected or the mechanism by which the TOE validates the identity of the policy's source is not sufficiently robust, an attacker who is aware of the syntax used to transmit a policy may be able to forge an arbitrarily fake one and have the TOE consume it. If this occurs, the TOE may be configured to enforce a permissive fake policy that allows unauthorized access, to enforce a restrictive fake policy that prevents legitimate activities from being performed, or to consume an incorrectly formatted policy.	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]
T.WEAKIA	The ability of the TSF to define administrative privileges does not prevent malicious use if the TSF's authentication function can be subjected to brute force guessing. The TSF must provide sufficient login frustration mechanisms to limit the ability of an attacker to authenticate to the TOE through brute force.	Standard Protection Profile for Enterprise Security Management Policy Management [NIAP, PP_ESM_V.2.1, 2013]
T.MASK	Part of the reason for implementing an Enterprise Security Management solution within an organization is to provide transparency and accountability. Because of this, the TOE is expected to provide the capability to monitor and audit enforcement of its functionality. If an attacker is able to alter audit data or prevent it from being recorded, then they can begin to probe a system for weaknesses with a reduced risk of discovery. Similarly, if the TOE does not identify and audit anomalous or malicious actions taken against the TSF, then the potential exists for its behaviour to be altered without detection. If this were to occur, there would be no assurance that its security functions were operating properly.	Standard Protection Profile for Enterprise Security Management Policy Management [NIAP, PP_ESM_V.2.1, 2013]

	Part of the reason for implementing an ESM solution within an organization is to provide transparency and accountability. Because of this, the TOE is expected to provide the capability to monitor and audit enforcement of its access control policies. If an attacker is able to confound audit data by exploiting previously-discussed attack vectors (impersonating Secure Configuration Management to reconfigure the TOE's audit ability, compromising a trusted channel to any remote audit repository to divert or rewrite data, disabling a part of the TOE responsible for auditing, or deleting or modifying local audit logs), then they can begin to probe a system for policy weaknesses with a reduced risk of discovery. Similarly, if the TOE does not identify and audit anomalous or malicious actions taken against itself, then the potential exists for its behaviour to be altered without detection. If this were to occur, there would be no assurance that its access control enforcement was functioning properly.	Standard Protection Profile for Enterprise Security Management Access Control [NIAP, PP_ESM_aC_V. 2.1, 2013]
T.OFLOWS	The TOE is responsible for accepting input from potentially a variety of sources. If an attacker can replay policy data or modify legitimate policy data in transit, then the TSF may be enforcing an incorrect policy. This presents the attacker an opportunity to access data without authorization.	Standard Protection Profile for Enterprise Security Management Access Control [NIAP, PP_ESM_AC_V .2.1, 2013]

C.1.2 Assumptions

Assumptions	Description	Source
A.CRYPTOGRAPHY_MODULE_VALIDATED	The cryptographic module 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]	[NCIA TN-1485 v1.1, 2012] modified
A.CRYPTOGRAPHY_NATO_APPROVED	The TOE uses NATO approved cryptographic module 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].	[NCIA TN-1485 v1.1, 2012]
A.NO_TOE_BYPASS	Information cannot flow between the high network enclave and the low network enclave without passing through the TOE. Ref: [NAC AC/322-D/0030-REV5]	[NCIA TN-1485 v1.1, 2012]
A.PHYSICAL_ACCESS_MANAGED	The TOE is located in a restricted or monitored environment that provides protection from unmanaged access to the physical components and data interfaces of the TOE. Ref: [NAC C-M(2002)49-COR12, 2015], [NAC AC/35-D/2001-REV2, 2008], [NAC AC/35-D/1030, 2005].	[NCIA TN-1485 v1.1, 2012]
A.PKI_NATO_COMPLIANT	The PKI complies with the NATO directives and guidelines on use of Public-Key Infrastructure, including [NAC C-M(2003)32, 2003], and [NAC AC/322-D(2004)0024-REV3-COR1, 2018].	[NCIA TN-1485 v1.1, 2012]
A.TRUSTED_LABELER	A labeller is trusted to only create security labels in accordance with the NATO policy and respective directives and guidelines with assurance commensurate with the value of the information that he can create labels for. Ref: [NAC C-M(2002)49-COR12, 2015], [NAC AC/35-D/2002-REV4, 2012], [NAC AC/35-D/1032, 2005] [STANAG 4774], [STANAG 4778}.	[NCIA TN-1485 v1.1, 2012]
A.PLATFORM	The TOE relies upon a trustworthy computing platform for its execution. This includes the underlying platform and whatever runtime environment it provides to the TOE. The OS is configured according to relevant NATO guidance and directives [AC/322-D/0048-REV3, 2019]	[NIAP PP_APP_V.1.2, 2016] modified [NIAP PP_OS_V.4.1, 2016] modified

		[NCIA TN-1485 v1.1, 2012] modified
A.PROPER_USER	The user of the IEG is not wilfully negligent or hostile, and uses the functionality provided by the IEG in compliance with NATO policy. At the same time, malicious software could act as the user, so requirements which confine malicious subjects are still in scope.	[NIAP PP_APP_V.1.2, 2016] modified [NIAP PP_OS_V.4.1, 2016] modified
A.TRUSTED_ADMIN	The administrator of the IEG is not careless, wilfully negligent or hostile, and administers the OS within compliance of NATO policy.	[NIAP PP_APP_V.1.2, 2016] modified [NIAP PP_OS_V.4.1, 2016] modified [NIAP CPP_FW_V.1.0, 2015] modified [NIAP CPP_ND_V.1.0, 2015] modified
A.PHYSICAL_PROTECTION	The IEG is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the IEG's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the IEG and the data it contains.	[NIAP CPP_FW_V.1.0, 2015] modified [NIAP CPP_ND_V.1.0, 2015] modified
A.LIMITED_FUNCTIONALITY	The IEG is assumed to provide networking, filtering and guarding functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example the IEG should not provide computing platform for general purpose applications (unrelated to IEG core functionality).	[NIAP CPP_FW_V.1.0, 2015] modified [NIAP CPP_ND_V.1.0, 2015] modified [NCIA TN-1485 v1.1, 2012] modified
A.REGULAR_UPDATES	The IEG firmware and software is assumed to be updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.	[NIAP CPP_FW_V.1.0, 2015] modified [NIAP CPP_ND_V.1.0, 2015] modified
A.ADMIN_CREDENTIALS_SECURE	The administrator's credentials (private key) used to access the firewall are protected by the host platform on which they reside.	[NIAP CPP_FW_V.1.0, 2015] [NIAP CPP_ND_V.1.0, 2015]
A.CONNECTIONS	It is assumed that the TOE is connected to distinct networks in a manner that ensures that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks.	[NIAP PP_NDCP_IPP_EP_V.2.1, 2016]
A.SYSTIME	The TOE will receive reliable time data from the Operational Environment.	[NIAP PP_ESM_V.2.1, 2013] [NIAP PP_ESM_AC_V.2.1, 2013]
A.MANAGE	There will be one or more competent individuals assigned to install, configure, and operate the TOE. The administrators of the IEG-C can be categorised into the following roles: System Administrator: responsible for installation, configuration and maintenance of the IEG-C; Audit Administrator: responsible for regular review of IEG-C audit logs;	[NIAP PP_ESM_V.2.1, 2013] modified [NIAP PP_ESM_AC_V.2.1, 2013] modified

	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 actioning cyber-related tasks; and, SMC Administrator: responsible for monitoring IEG-C services.	

C.1.3 Organizational Security Policies

Organizational Security Policy	Description	Source
P.ACCOUNTABILITY	The authorized users of the TOE shall be held accountable for their actions within the TOE. Reference: [NAC AC/322-D/0048-REV3, 2019]	[NCIA TN-1485 v1.1, 2012]
P.ADMIN_ACCESS	Administrators shall be able to administer the TOE both locally and remotely through protected communications channels. Reference: [NAC AC/322-D/0030-REV5]	[NCIA TN-1485 v1.1, 2012]
P.CLASSIFICATION	The IEG must limit the access to information based on IA attributes included in a label and the information flow control policy as defined in the Protection Policy Enforcement Services. The access rules enforced shall prevent a subject from accessing information which is of higher sensitivity than it is operating at and prevent a subject from causing information from being downgraded to a lower sensitivity. Reference: [NAC AC/35-D/2002-REV4, 2012]	[NCIA TN-1485 v1.1, 2012]
P.CRYPTOGRAPHY	The TOE shall use NATO-approved and validated 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. Reference: [NAC AC/322-D(2007)0002-REV1, 2015]	[NCIA TN-1485 v1.1, 2012]
P.VULNERABILITY_ANALYSIS	The TOE must undergo appropriate independent vulnerability analysis and penetration testing to demonstrate that the TOE is resistant to an attacker possessing a medium attack potential. Reference: [NAC AC/322-D/0048-REV3, 2019]	[NCIA TN-1485 v1.1, 2012]
P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE. Reference: [AC/322-D/0048-REV3, 2019] Appendix 1 Annex 1 page 1-29	[NIAP CPP_FW_V.1.0, 2015] [NIAP PP_ESM_V.2.1, 2013] [NIAP CPP_ND_V.1.0, 2015] [NCIA TN-1485 v1.1, 2012]
P.ANALYZE	Analytical processes and information to derive conclusions about potential intrusions must be applied and appropriate response actions taken.	[NIAP PP_NDCP_IPP_EP_V.2.1, 2016]
P.UPDATEPOL	The organization will exercise due diligence to ensure that the TOE is updated with relevant policy data.	[NIAP PP_ESM_AC_V.2.1, 2013]

C.2 Security Objectives

C.2.1 Security Objectives for the TOE

Security Objective	Description	Source
O.ADMIN_ROLE	The TOE will provide an administrator role to isolate administrative actions, and to make the administrative functions available locally and remotely.	[NCIA TN-1485 v1.1, 2012] (*FMT_SMR.2*)
O.AUDIT_GENERATION	The TOE will provide the capability to detect and create records of security-relevant events associated with users.	[NCIA TN-1485 v1.1, 2012] *(FAU_GEN.1, FAU_GEN.2, FAU_SEL.1, FAU_STG.3,*

		FAU_STG.4(1), FAU_STG.4(2), FIA_USB.1) [NIAP PP_ESM_V.2.1, 2013] - O.AUDIT *(FAU_GEN.1, FAU_SEL.1, FAU_STG_EXT.1, FPT_STM.1)*
O.AUDIT_PROTECTION	The TOE shall provide the capability to protect audit information.	[NCIA TN-1485 v1.1, 2012] *(FAU_SAR.2, FAU_STG.1, FAU_STG.3, FAU_STG.4(1), FAU_STG.4(2), FMT_MOF.1)*
O.AUDIT_REVIEW	The TOE will provide the capability to selectively view audit information, and alert the administrator of identified potential security violations.	[NCIA TN-1485 v1.1, 2012] *(FAU_ARP.1, FAU_ARP.2, FAU_SAA.1, FAU_SAR.1, FAU_SAR.3, FMT_MOF.1(3), FMT_MOF.1(4), FMT_MOF.1(5))*
O.CHANGE_MANAGEMENT	The configuration of, and all changes to, the TOE and its development evidence will be analysed, tracked, and controlled throughout the TOE‘s development.	[NCIA TN-1485 v1.1, 2012]
O.CORRECT_TSF_OPERATION	The TOE will provide a capability to test the TSF to ensure the correct operation of the TSF in its operational environment.	[NCIA TN-1485 v1.1, 2012] *(FPT_TST.1)*
O.DISPLAY_BANNER	The TOE will display an advisory warning regarding use of the TOE.	[NCIA TN-1485 v1.1, 2012] *(FTA_TAB.1)* [NIAP PP_ESM_V.2.1, 2013] – O.BANNER *(FTA_TAB.1)*
O.MAINT_MODE	The TOE shall provide a mode from which recovery or initial start-up procedures can be performed.	[NCIA TN-1485 v1.1, 2012] *(FPT_RCV.2)*
O.MANAGE	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.	[NCIA TN-1485 v1.1, 2012] *(FAU_SAR.1, FAU_SAR.2, FAU_SAR.3, FAU_SEL.1, FAU_STG.1, FAU_STG.3, FAU_STG.4(1), FAU_STG.4(2), FMT_MOF.1(1), FMT_MOF.1(2), FMT_MOF.1(3), FMT_MOF.1(4), FMT_MOF.1(5), FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_MTD.2(1), FMT_MTD.2(2), FMT_MTD.2(3))*

		[NIAP PP_OS_V.4.1, 2016] - O.MANAGEMENT *(FMT_MOF_EXT.1, FTP_TRP.1)* [NIAP PP_NDCP_IPP_EP_V.2.1, 2016] - O.TOE_ADMINISTRATION *(FMT_MOF.1/IPS, FMT_MTD.1/IPS, FMT_SMF.1/IPS, FMT_SMR.2/IPS)* [NIAP PP_ESM_V.2.1, 2013] *(FAU_SEL_EXT.1, FMT_MOF.1, FMT_MOF_EXT.1, FMT_MTD.1, FMT_SMF.1)*
O.MEDIATE_FLOW	The TOE shall mediate the flow of information between the high network interface and the low network interface in accordance with the information flow policy.	[NCIA TN-1485 v1.1, 2012] *(FMT_REV.1(1), FMT_REV.1(2))*
O.MESSAGE_VETTING	The TOE shall control the flow of information from the low network interface to the high network interface and vice versa by only relaying messages that are allowed as part of the TOE security policy.	[NCIA TN-1485 v1.1, 2012] modified
O.MINIMAL_PROXY	The TOE shall provide mechanisms that can be used to limit the amount of information, which is transmitted from the high to the low network enclave in the header or envelope of a transport protocol message.	[NCIA TN-1485 v1.1, 2012] modified
O.REPLAY_DETECTION	The TOE will provide a means to detect and reject the replay of authentication data as well as other TSF data and security attributes.	[NCIA TN-1485 v1.1, 2012] *(FPT_RPL.1)*
O.RESIDUAL_INFORMATION	The TOE will 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.	[NCIA TN-1485 v1.1, 2012] *(FDP_RIP.2)*
O.RESOURCE_SHARING	The TOE shall provide mechanisms that mitigate attempts to exhaust resources provided by the TOE (e.g., resulting in denying access to high network resources).	[NCIA TN-1485 v1.1, 2012] modified *(FMT_MOF.1(5), FMT_MTD.2(2), FMT_MTD.2(3), FRU_RSA.1(1), FRU_RSA.1(2))*
O.REVERSE_PROXY	The TOE shall provide capability to hide unauthorised information attributes like type, address and name of resources of the high network enclave from the low network enclave.	[NCIA TN-1485 v1.1, 2012] modified
O.ROBUST_ADMIN_GUIDANCE	The TOE will provide administrators with the necessary information for secure delivery and management [NAC AC/35-D/1014-REV2, 2006].	[NCIA TN-1485 v1.1, 2012]

O.ROBUST_TOE_ACCESS	The TOE will provide mechanisms that control a user's logical access to the TOE and to explicitly deny access to specific users when appropriate.	[NCIA TN-1485 v1.1, 2012] *(FIA_AFL.1, FIA_ATD.1, FIA_UAU.2, FIA_UID.2, FTA_SSL.1, FTA_SSL.2, FTA_SSL.3, FTA_TSE.1)* [NIAP PP_ESM_V.2.1, 2013] – O.ROBUST *(FIA_AFL.1, FIA_SOS.1, FTA_SSL_EXT.1, FTA_SSL.3, FTA_SSL.4, FTA_TSE.1)*
O.SELF_PROTECTION	The TSF shall maintain a domain for its own execution that protects itself and its resources from external interference, tampering or unauthorized disclosure.	[NCIA TN-1485 v1.1, 2012] *(FTP_ITC.1(1), FTP_ITC.1(2), FTP_TRP.1(1), FTP_TRP.1(2))*
O.SOUND_DESIGN	The TOE will be designed using sound design principles and techniques. The TOE design, design principles and design techniques will be adequately and accurately documented.	[NCIA TN-1485 v1.1, 2012]
O.SOUND_IMPLEMENTATION	The implementation of the TOE will be an accurate instantiation of its design, and is adequately and accurately documented.	[NCIA TN-1485 v1.1, 2012]
O.THOROUGH_FUNCTIONAL_TESTING	The TOE will undergo appropriate security functional testing that demonstrates the TSF satisfies the security functional requirements.	[NCIA TN-1485 v1.1, 2012]
O.TIME_STAMPS	The TOE shall provide reliable time stamps and the capability for the administrator to set the time used for these time stamps.	[NCIA TN-1485 v1.1, 2012] *(FMT_MTD.1, FPT_STM.1)*
O.TRUSTED_PATH	The TOE will 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.	[NCIA TN-1485 v1.1, 2012] *(FTP_ITC.1(1), FTP_ITC.1(2), FTP_TRP.1(1), FTP_TRP.1(2))*
O.VALID_LABEL	The TOE shall validate the origin, integrity and binding [STANAG 4778] of a security label [STANAG 4774] to a data object before it is used.	[NCIA TN-1485 v1.1, 2012] *(FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3))*
O.VULNERABILITY_ANALYSIS	The TOE will 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.	[NCIA TN-1485 v1.1, 2012]
O.ACCOUNTABILITY	An IEG 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.	[NIAP PP_OS_V.4.1, 2016] modified *(FAU_GEN.1)*
O.INTEGRITY	An IEG 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 IEGs provide execution environment-based	[NIAP PP_OS_V.4.1, 2016] modified *(FPT_SBOP_EXT.1,*

	mitigations that increase the cost to attackers by adding complexity to the task of compromising systems. The TOE will contain the ability to assert the integrity of policy data. The TOE will contain the ability to verify the integrity of transferred data from Operational Environment components.	*FPT_ASLR_EXT.1, FPT_TUD_EXT.1, FPT_TUD_EXT.2, FCS_COP.1.1(2), FCS_COP.1.1(3), FCS_COP.1.1(4), FPT_ACF_EXT.1, FPT_SRP_EXT.1, FIA_X509_EXT.2, FPT_TST_EXT.1, FTP_ITC_EXT.1, FPT_W^X_EXT.1.1, FIA_AFL.1, FIA_UAU.5)* [NIAP PP_ESM_V.2.1, 2013] *(FTP_ITC.1)* [NIAP PP_ESM_AC_V.2.1, 2013] *(FTP_ITC.1)*
O.PROTECTED_STORAGE	To address the issue of loss of confidentiality of credentials in the event of loss of physical control of the storage medium, conformant IEGs provide data-at-rest protection for credentials. Conformant IEGs also provide access controls which allow users to keep their files private from other users of the same system.	[NIAP PP_OS_V.4.1, 2016] modified *(FCS_STO_EXT.1, FCS_RBG_EXT.1, FCS_COP.1.1(1), FDP_ACF_EXT.1)*
O.SYSTEM_MONITORING	The IEG must collect and store information about all events that may indicate a policy violation related to misuse, inappropriate access, or malicious activity on monitored networks. For an IEG implemented in the static environment the TOE provides a NATO approved malware scanning capability. Ref: [NC3B AC/322-D(2004)0019 (INV), 2004]	[NIAP PP_NDCP_IPP_EP_V.2.1, 2016] modified *(FAU_ARP.1, FAU_GEN.1/IPS, FAU_SAR.1, FAU_SAR.2, FAU_SAR.3, FAU_STG.1, FAU_STG.4, FRU_RSA)* [NIAP PP_ESM_AC_V.2.1, 2013] – O.MONITOR *(FAU_GEN.1, FAU_SEL.1, FAU_STG.1, FAU_STG_EXT.1)*

		[NCIA TN-1485 v1.1, 2012] modified – OE.MALWARE_SCANNER
O.IPS_ANALYZE	The IEG must apply analytical processes to network traffic data collected from monitored networks and derive conclusions about potential intrusions or network traffic policy violations. For an IEG implemented in the static environment the TOE provides a NATO approved malware scanning capability. Ref: [NC3B AC/322-D(2004)0019 (INV), 2004]	[NIAP PP_NDCP_IPP_EP_V.2.1, 2016] modified *(IPS_ABD_EXT.1, IPS_IPB_EXT.1, IPS_NTA_EXT.1, IPS_SBD_EXT.1, IPS_SBD_EXT.2)* [NCIA TN-1485 v1.1, 2012] modified – OE.MALWARE_SCANNER
O.IPS_REACT	The IEG must respond appropriately to its analytical conclusions about policy violations. For an IEG implemented in the static environment the TOE provides a NATO approved malware scanning capability. Ref: [NC3B AC/322-D(2004)0019 (INV), 2004]	[NIAP PP_NDCP_IPP_EP_V.2.1, 2016] modified *(FAU_ARP.1, IPS_ABD_EXT.1)* [NCIA TN-1485 v1.1, 2012] modified – OE.MALWARE_SCANNER
O.TRUSTED_COMMUNICATIONS	The IEG will ensure that communications between distributed components of the TOE are not subject to unauthorized modification or disclosure.	[NIAP PP_NDCP_IPP_EP_V.2.1, 2016] modified *(FPT_ITT.1)* [NIAP PP_OS_V.4.1, 2016] modified – O.PROTECTED_COMMS *(FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSC_EXT.3, FCS_TLSC_EXT.4, FCS_DTLS_EXT.1, FCS_RBG_EXT.1, FCS_CKM.1(1), FCS_CKM.2(1), FCS_COP.1.1(1), FDP_IFC_EXT.1, FIA_X509_EXT.1, FIA_X509_EXT.*

		2, FTP_ITC_EXT.1) [NIAP PP_ESM_V.2.1, 2013] – O.PROTCOMMS *(FCS_HTTPS_EXT.1, FCS_IPSEC_EXT.1, FCS_SSH_EXT.1, FCS_TLS_EXT.1, FPT_SKP_EXT.1, FTP_ITC.1, FTP_TRP.1)* [NIAP PP_ESM_AC_V.2.1, 2013] modified *(ESM_DSC.1, ESM_EID.2, FDP_ACC.1, FDP_ACF.1, FMT_MOF.1(1), FMT_MOF.1(2), FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, FMT_SMR.1, FTA_TSE.1)*
O.ACCESSID	The TOE will contain the ability to validate the identity of other IEG-C components prior to distributing data to them.	[NIAP PP_ESM_V.2.1, 2013] modified
O.AUTH	The TOE will 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.	[NIAP PP_ESM_V.2.1, 2013] *(ESM_EAU.2, ESM_EID.2, FIA_USB.1, FMT_MOF.1, FMT_SMR.1, FPT_APW_EXT.1, FTP_TRP.1)*
O.CONSISTENT	The TSF will provide a mechanism to identify and rectify contradictory policy data.	[NIAP PP_ESM_V.2.1, 2013]
O.CRYPTO_NATO_APPROVED	The TOE will provide cryptographic primitives that can be used to provide services such as ensuring the confidentiality and integrity of communications. The TOE provides a NATO approved cryptographic module 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). Ref: [NAC AC/322-D(2007)0002-REV1, 2015]	[NIAP PP_ESM_V.2.1, 2013] modified – O.CRYPTO *(FCS_CKM.1, FCS_CKM_EXT.4, FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4), FCS_RBG_EXT.1)*

		[NIAP PP_ESM_AC_V.2.1, 2013] modified – O.CRYPTO *(FCS_CKM.1, FCS_CKM_EXT.4, FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4), FCS_RBG_EXT.1)*
O.DISTRIB	The TOE will provide the ability to distribute policies to trusted IT products using secure channels.	[NIAP PP_ESM_V.2.1, 2013] *(ESM_ACT.1, FTP_ITC.1)*
O.MAINTAIN		[NIAP PP_ESM_AC_V.2.1, 2013] modified *(FPT_FLS_EXT.1, FRU_FLT.1)*
O.OFLOWS	The TOE will be able to recognize and discard invalid or malicious input provided by users.	[NIAP PP_ESM_AC_V.2.1, 2013]
O.UPDATES	The TOE firmware and software is updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.	[NIAP CPP_FW_V.1.0, 2015] – OE.UPDATES [NIAP CPP_ND_V.1.0, 2015] - OE.UPDATES

C.2.2 Security Objectives for the Operational Environment

Security Objective	Description	Source
OE.ADMIN_NO_EVIL	Sites using the TOE will ensure that administrators are aware of the security policies and procedures of their organization, are trained and competent to follow the manufacturer‘s guidance and documentation, and correctly configure and operate the TOE in accordance with those policies and procedures.	[NCIA TN-1485 v1.1, 2012]
OE.MALWARE_SCANNER	For an IEG implemented in the deployed environment the OE provides a NATO approved malware scanning capability. Ref: [NC3B AC/322-D(2004)0019 (INV), 2004]	[NCIA TN-1485 v1.1, 2012] modified
OE.NO_TOE_BYPASS	Information cannot flow between the high network enclave and the low network enclave without passing through the TOE. Ref: [NAC AC/322-D/0030-REV5]	[NCIA TN-1485 v1.1, 2012]
OE.PHYSICAL_ACCESS_MANAGED	The TOE is located in a restricted or monitored environment that provides protection from unmanaged access to the physical components and data interfaces of the TOE. Ref: [NAC C-M(2002)49-COR12, 2015], [NAC AC/35-D/2001-REV2, 2008], [NAC AC/35-D/1030, 2005].	[NCIA TN-1485 v1.1, 2012]
OE.TRUSTED_LABELLER	A labeller is trusted to only create security labels in accordance with the NATO policy and respective directives and guidelines. The assurance of the label creation process must be commensurate with the value of the information that the labels are created for. Ref: [NAC C-M(2002)49-COR12, 2015], [NAC AC/35-D/2002-REV4, 2012], [NAC AC/35-D/1032, 2005], [NAC AC/322-D(2004)0021 (INV) 2004], [NAC AC/322-D(2004)0022 (INV), 2004].	[NCIA TN-1485 v1.1, 2012]

OE.PLATFORM	The TOE relies upon a trustworthy computing platform for its execution. This includes the underlying operating system and any discrete execution environment provided to the TOE. The OS relies on being installed on trusted hardware.	[NIAP PP_APP_V.1.2, 2016] [NIAP PP_OS_V.4.1, 2016]
OE.PROPER_USER	The user of the IEG is not wilfully negligent or hostile, and uses the software within compliance of the applied NATO policy.	[NIAP PP_APP_V.1.2, 2016] modified [NIAP PP_OS_V.4.1, 2016] modified
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the operational environment.	[NIAP CPP_FW_V.1.0, 2015] modified [NIAP CPP_ND_V.1.0, 2015] modified
OE.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all guidance documentation in a trusted manner.	[NIAP CPP_FW_V.1.0, 2015] [NIAP CPP_ND_V.1.0, 2015] [NIAP PP_ESM_V.2.1, 2013]
OE.UPDATES	The TOE firmware and software is updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.	[NIAP CPP_FW_V.1.0, 2015] [NIAP CPP_ND_V.1.0, 2015]
OE.ADMIN_CREDENTIALS_SECURE	The administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.	[NIAP CPP_FW_V.1.0, 2015] [NIAP CPP_ND_V.1.0, 2015]
OE.CONNECTIONS	TOE administrators will ensure that the TOE is installed in a manner that will allow the TOE to effectively enforce its policies on network and application traffic of monitored networks.	[NIAP PP_NDCP_IPP_EP_V.2.1, 2016] modified
OE.ADMIN	There will be one or more administrators of the Operational Environment that will be responsible for managing the TOE.	[NIAP PP_ESM_V.2.1, 2013]
OE.PROTECT	The Operational Environment will protect the TOE from unauthorized modifications and access to its functions and data.	[NIAP PP_ESM_V.2.1, 2013] [NIAP PP_ESM_AC_V.2.1, 2013]
OE.ROBUST	The Operational Environment will provide mechanisms to reduce the ability for an attacker to impersonate a legitimate user during authentication.	[NIAP PP_ESM_V.2.1, 2013]
OE.SYSTIME	The Operational Environment will provide reliable time data to the TOE.	[NIAP PP_ESM_V.2.1, 2013] [NIAP PP_ESM_AC_V.2.1, 2013]

APPENDIX D: Component Detailed Specifications

D.1 Firewalls

D.1.1 Palo Alto Networks PA-3260 with redundant AC power supplies

#	Part Number	Specification	Quantity
1.	PAN-PA-3260	Palo Alto Networks PA-3260 with redundant AC power supplies	1
2.	PAN-SVC-PREM-3260	Premium support year 1, PA-3260	1

D.2 Network Switches

D.2.1 Dell Networking N1124T Switch

#	Item	Specification	Quantity
1.	Configuration	• DELL N1124T-ON Switch • 24x 10/100/1000Mbps half/full duplex RJ45 ports • 4x SFP/SFP+ 1/10GbE ports • 1 RU switch form factor • User Guide • Power cord 250V, 2 M, C13/14	1
2.	Support	• 5 Years Basic Hardware Warranty Repair	1

D.2.2 Dell Networking S3048 Switch

#	Item	Specification	Quantity
1.	Configuration	• DELL S3048 Switch • 48x 1GbE, 4x SFP+ 10GbE, 1x AC PSU • User Guide • Power Supply, 200w, PSU S3048-ON • Jumper cord 250V, 12A, 2 M, C13/C14	1
2.	Support	• Lifetime limited Warranty NBD 5 Year • ProSupport NBD Onsite 5 Year • ProSupport 7X24 HW/SW Tech Support 5 Year	1

D.2.3 Dell Networking S3124F Switch

#	Item	Specification	Quantity
1	210-AIMS	Dell Networking S3124F, L3, 24x 1GbE SFP, 2xCombo, 2x 10GbE SFP+ fixed ports, Stacking, IO to PSU air, 1x AC PSU	2
2	407-BBDB	Dell Networking, Transceiver, SFP, 1000BASE-SX, 850nm Wavelength, 550m Reach	6
3	450-AART	Rack Power Cord 2M, C13/C14, 12A	2
4	470-AAPT	Stacking Cable, for Dell Networking N2000/N3000/S3100 series switches (no cross-series stack), 1m	2
5	709-14075	S3124P,S3124F,S3124 Base Warranty	2
6	709-14076	S3124P,S3124F,S3124 Limited Lifetime Hardware Warranty Minimum Warranty	2

7	709-14077	S3124P,S3124F,S3124 90 Days Software Support (Bug Fixes), Software Media Replacement	2
8	865-11154	S3124P,S3124F,S3124 3Yr ProSupport and 4hr Mission Critical	2

D.2.4 Dell Networking S3148P Switch

#	Item	Specification	Quantity
1	210-AIMP	Dell Networking S3148P, L3, PoE+, 48x 1GbE, 2x Combo, 2x 10GbE SFP+ fixed ports, Stacking, IO to PSU air, 1x 1100w AC PS	2
2	450-ADXF	European 250V C15 Power Cord for N20xxP/N30xxP	2
3	450-AFHX	Power Supply, 1100w, S3148P, Required for more than 900 watts of POE+, or for redundancy	2
4	470-AAPT	Stacking Cable, for Dell Networking N2000/N3000/S3100 series switches (no cross-series stack), 1m	2
5	709-14107	S3148,S3148P Base Warranty	2
6	709-14108	S3148P Limited Lifetime Hardware Warranty - Minimum Warranty	2
7	709-14109	S3148P 90 Days Software Support (Bug Fixes), Software Media Replacement	2
8	865-11486	S3148,S3148P 3Yr ProSupport and 4hr Mission Critical	2

D.3 Rack

D.3.1 Server Equipment Cabinet

#	Item	Specification	Quantity
1.	5500009 / MODNL	Network rack 800x2000x1200mm	1
2.		Cabinet based on TS-IT	1
3.		Size 800x2000x1200mm (WxHxD) 42HE	1
4.		Color RAL 7035 (light gray) cabinet frame and plate parts Color RAL 9005 (black) interior design	1
5.		Cabinet will be provided with:	
6.		Perforated, vertically divided, front door,	1
7.		(vented surface area approx. 85% perforated)	1
8.		Doors equipped with single-cylinder comfort handle with cylinder locks 3524E and 180 ° hinges	1
9.		Perforated, vertically divided, rear door, (vented surface area approx. 85% perforated)	1
10.		Doors equipped with single-cylinder comfort handle with cylinder locks 3524E and 180 ° hinges	1
11.		Base open	1
12.		Two 482.6 mm (19") mounting sections front and rear, variably mounted on support strips with quick-release fasteners, HE coding on all 19"	1
13.		profiles, statically loadable up to 1500kg	1
14.		Air baffle plates around the 19 inch as a partition between the hot and cold sides, including 6x 1HE blanking panel	1
15.		Roof plate, multi-piece, removable, with side cable entry in the depth	1
16.		and covered cut-out for fan mounting plate	1
17.		shipped on pallet.	1
18.		Loose provided in the cabinet:	
19.		component shelf DK 5501685, depth adjustable 600-900mm (loadable up to 50kg)	1

D.3.2 UPS

#	Item	Specification	Quantity
1	SMC1500I-2U	UPS SMC1500I-2U APC Smart-UPS C 1500VA 2U Rack mountable LCD 230V	1

D.3.3 Power Distribution Unit

#	Item	Specification	Quantity
1	IP-BA-C09SH00010	Powerstrip Conteg 19” 1U Basic PDU, plug IEC 320 C14, power cord 2.8m, Outlets - 9x Schuko, power rating 10A	2

D.5 Management Workstation

D.5.1 Hardware

D.5.1.1 Dell Optiplex 5070 SFF

#	Item	Minimum Requirements
1.	Form Factor	SFF
2.	Microsoft Licences	MS Windows 10 Pro OEM 64bit no-media
3.	Performance	i5- 9500, office productivity of 1073
4.	Processor	6 cores
5.	Graphics	Intel UHD Graphics 630, Performance: at least 917@ 1024x600 in ComputeMark v2.14, Triple Display Capable (1920x1200@60Hz on each display minimum); Compatible with DirectX 12 (Feature Level 12.0) and OpenGL 4.5; HDMI 1.4 and Displayport
6.	Memory	8GB
7.	Storage	Size: min. 240GB, Speed: min. 450MB/sec sequential read and min. 250MB/sec sequential write durability: 72TBW, supported functions: TCG Opal, IEEE-1667, FDE AES-256
8.	I/O Ports	10x USB (5x 3.1 & 5x 2.0) 2x DP 1.2 1x UAJ front incl. audio jack split adapter
9.	Network	On-board Gigabit Ethernet controller 1000BASE-T (RJ-45 interface port)
10.	Network	100Base-FX or 1000BASE-SX, LC connector, Wake-On-LAN, PXE
11.	Drive Bays	1x slim line external bay
12.	Expansion Slots	1x PCIe x16 & 1x PCIe x4, both low profile
13.	Security	Trusted Platform Module (TPM) 2.0 chip on the motherboard; AES New Instructions (AES-NI), SecureKey, BIOS Guard, OS Guard or equivalent; PnP and BIOS setup/boot password/system configuration protection
14.	Lock	Kensington supervisor lock included
15.	HDD cage	Optional Hard Disk Cage with Lock for 2,5" SATA Disk

D.5.1.2 Dell P2419H Monitor

#	Item	Minimum Requirements
1.	Size – diagonal	23.8” screen with ultrathin bezel
2.	Contrast	1000:1
3.	Brightness	250 nits
4.	Standards	TCO certified Displays 7.0
5.	Connections	Yes, 1 x VGA, 1 x HDMI, 1 x DP 1.2 standard ports
6.	Native refresh rate	60Hz
7.	Horizontal/vertical viewing angle	178 degrees horizontally and vertically
8.	Native resolution	FHD resolution 1920 x 1080 with 82% sRGB coverage or CIE 1931 value of >= 72%
9.	Speakers	Dell AC 511M Soundbar with 2x1,25 W speakers included
10.	Tilt and Swivel	Tilt: +21deg/-5deg Swivel: 90deg
11.	Appearance	Black colour
12.	Power supply and cords	1x Power cord included
13.	Cabling	1x DisplayPort cable (cable length 1.8m) included
14.	Lock	Kensington lock slot included

D.5.1.3 Dell KB216 Multimedia Keyboard

#	Item	Minimum Requirements
1.	Device	US QWERTY keyboard

2.	Compatibility	Microsoft Windows 10 Enterprise
3.	Connectors	USB
4.	Additional Features	Low profile keys
5.	Cabling	Length: 1.5m

D.5.1.4 Dell 6 Button Laser Mouse

#	Item	Minimum Requirements
1.	Device	Ergonomic keyboard US QWERTY
2.	Compatibility	Microsoft Windows 10
3.	Connectors	USB
4.	Additional Features	Low profile keys
5.	Cabling	Length: 1.0m

APPENDIX E: Named Elements

Common components acronyms used within the named elements

ACRONYM	DESCRIPTION
AV	Attachment Validation
BS	Business support
CIP	Content Inspection Policy
CIPE	Content Inspection Policy Enforcement
CIS	Content Inspection Services
COI	Community of Interest
DEX	Data Exchange services
EV	Envelope Validation
FLOT	First Line Of Text
HL	High-to-Low
IEG-FS	Information Exchange Gateway Functional Services
IFCPE	Information Flow Control Policy Enforcement
IFP	Information Flow control Policy
LH	Low-to-High
LV	Label Validation
MG	Mail guard component
PKCS	Public Key Cryptographic Services
SOA	Service Oriented Architecture
SV	Schema Validation
WG	Web guard component

Interfaces can be identified by the use of the “IF_” component. This component is generally prefixed by the related component, Web Guard (WG) or Mail Guard (MG).

NAME	DESCRITPION
IEG-C_IF_MGMT	Overall IEG-C Management Network Interface
IEG-C_IF_NET_HIGH	Overall IEG-C High Domain Network Interface
IEG-C_IF_NET_LOW	Overall IEG-C Low Domain Network Interface
MG_IF_LOCAL_MGMT	Mail Guard Local Management Interface
MG_IF_MGMT	Mail Guard (Remote) Management Network Interface
MG_IF_NET_HIGH	Mail Guard High Domain Network Interface
MG_IF_NET_LOW	Mail Guard Low Domain Network Interface
WG_IF_LOCAL_MGMT	Web Guard Local Management Interface
WG_IF_MGMT	Web Guard (Remote) Management Network Interface
WG_IF_NET_HIGH	Web Guard High Domain Network Interface
WG_IF_NET_LOW	Web Guard Low Domain Network Interface

Rulesets are prefixed with ‘’RULESET_”

NAME	DESCRIPTION
RULESET_MG_IFCPE-CA_HL_IN	Mail Guard Communications Access High to Low Inbound
RULESET_MG_IFCPE-CA_HL_OUT	Mail Guard Communications Access High to Low Outbound
RULESET_MG_IFCPE-CA_LH_IN	Mail Guard Communications Access Low to High Inbound
RULESET_MG_IFCPE-CA_LH_OUT	Mail Guard Communications Access Low to High Outbound
RULESET_MG_IFCPE-MGMT_IN	Mail Guard Management Inbound
RULESET_MG_IFCPE-MGMT_OUT	Mail Guard Management Outbound
RULESET_WG_CIS_HV-HL	Web Guard Header Validation High to Low
RULESET_WG_CIS_HV-LH	Web Guard Header Validation Low to Hugh
RULESET_WG_CIS_LV	Web Guard Label Validation
RULESET_WG_CIS_HV	Web Guard Header Validation
RULESET_WG_CIS_SV	Web Guard Schema Validation
RULESET_WG_CIS_MD	Web Guard Malware Detection
RULESET_WG_IFCPE-CA_HL_IN	Web Guard Communications Access High to Low Inbound
RULESET_WG_IFCPE-CA_HL_OUT	Web Guard Communications Access High to Low Outbound
RULESET_WG_IFCPE-CA_LH_IN	Web Guard Communications Access Low to High Inbound
RULESET_WG_IFCPE-CA_LH_OUT	Web Guard Communications Access Low to High Outbound
RULESET_WG_IFCPE-MGMT_IN	Web Guard Management Inbound
RULESET_WG_IFCPE-MGMT_OUT	Web Guard Management Outbound

Variables are prefixed with a keyword representing the type of data they are to hold:

- ACTIONS_: A set of actions.
- BOOL_: A boolean.
- LIST_ : A list of values.
- NUM_ : An integer
- STR_ : An array of characters

NAME	COMMENT
BOOL_MG_CIS_LV_CB	Indicates whether a Cryptographic Binding is required
LIST_MG_CIS_AV_DIRTYWORDS	Mail Guard Dirty Words (Attachment Validation)

NAME	COMMENT
LIST_MG_CIS_AV_MALWARE_DEFINITIONS	list of definitions/signatures of currently known malware
LIST_MG_CIS_AV_TYPES	Mail Guard Attachment Types (Attachment Validation)
LIST_MG_CIS_EV_ORIG	List of allowable SMTP originator
LIST_MG_CIS_EV_RECIPS	List of allowable SMTP recipients
LIST_MG_CIS_LV_FLOT	List of valid FLOT markings;
LIST_MG_CIS_LV_KEYWORDS	List of valid keywords.
LIST_MG_CIS_LV_TP	List of trust points (e.g. trusted root certificates).
LIST_MG_CIS_LV-CRL	List of certificate revocation lists
LIST_MG_CIS_LV-DM	List of allowable digest method algorithms
LIST_MG_CIS_LV-SM	List of allowable signature method algorithms
LIST_MG_CIS_LV-SPIF	List of allowable security policies (including classifications and categories)
LIST_WG_CIS_LV-CM	List of Canonicalization Methods.
LIST_WG_CIS_LV-CRL	List of certificate revocation lists
LIST_WG_CIS_LV-TP	List of trust points (e.g. trusted root certificates).
LIST_WG_CIS_LV-XS	List of XML Schemas (Label Validation)
LIST_WG_CIS_SV-NS	List of valid namespaces
LIST_WG_CIS_SV-XS	List of XML schemas (Schema Validation)
NUM_MG_CIS_AV_ATTACHMENTS	The maximum number of attachments
STR_MG_CIS_LV_FLOT_PREFIX	Prefix to identify a FLOT in a message
STR_MG_CIS_LV_KEYWORD_HEADER	SMTP header field which contains keywords
LIST_WG_CIS_LV-DM	List of Digest Methods
LIST_WG_CIS_LV-SM_HMAC	List of HMAC Signature Methods
LIST_WG_CIS_LV-SM_PKI	List of PKI Signature Methods

Outcomes are prefixed with “O_”.

NAME	COMMENT
O_MG_CIS_AV	Outcome of Mail Guard attachment validation
O_MG_CIS_EV	Outcome of Mail Guard envelope validation
O_MG_CIS_LV	Outcome of Mail Guard label validation
O_MG_CIPE_HL	Outcome of Mail Guard Content Inspection High to Low
O_MG_CIPE_LH	Outcome of Mail Guard Content Inspection Low to High
O_MG_CIS	Outcome of Mail Guard Content Inspection Service
O_MG_IFCPE	Outcome of Mail Guard Information Flow Control Policy
O_WG_CIPE_HL	Outcome of Web Guard Content Inspection High to Low
O_WG_CIPE_LH	Outcome of Web Guard Content Inspection Low to High
O_WG_CIS	Outcome of Web Guard Content Inspection Service
O_WG_IFCPE	Outcome of Web Guard Information Flow Control Policy