For a given SMTP message *M*:

- Subject *M* to policy enforcement; and
- If *M* violates the MG security policy: generate (but not send) the appropriate SMTP error message.

Let the '*MG processing time of an SMTP message*' or simply '*SMTP message processing time*' (notation: *T_MG_Proc*) be the time measured in order for the MG to complete the sequence '*SMTP message processing*' above.

When it is written that the 'MG processes an SMTP message', this means the same as subjecting an SMTP message to '*SMTP message processing*'. Therefore, the time it takes for the MG to process an SMTP message is equal to *T_MG_Proc*.

Let the '*MG processing times*' be the processing times that the MG is able to offer.

Throughput

Let the '*MG throughput*', or simply '*throughput'* be the number of SMTP messages that the MG can process per given time period.

Forwarding time

Let the '*MG forwarding time of an SMTP message*' or simply '*SMTP message forwarding time*' (notation: *T_MG_Forward*) be the time measured in order for the MG to complete the following sequence:

For a given SMTP message *M*:

- Receive *M* at MG_IF_NET_HIGH or MG_IF_NET_LOW;
- If necessary queue *M*; and then
- Execute '*SMTP message processing*' for *M*;
- Then, if *M* did not violate the MG policy:
  - If necessary queue *M;* and then
  - Forward *M* onto the low domain or high domain respectively.
- Else, if *M* did violate the MG policy:
  - If necessary queue the associated SMTP error message; and then
  - Forward the SMTP error message onto the high domain or low domain, as required.

When it is written that the '*MG forwards an SMTP message*', this means the same as completing the sequence above.

The '*SMTP message forwarding time*' is equal to the '*SMTP message processing time*' plus the time it takes to receive, queue and forward SMTP messages. (The 'SMTP message forwarding time' is similar to the concept of 'response time' (i.e. 'processing time' + 'queueing time').)

Let the '*MG forwarding times*' be the forwarding times that the MG is able to offer.

5.4.1.2.2 Message size categories

Througput, processing time and forwarding time depend on message size. Therefore this SRS distinguishes a number of message size cagetories for the MG.

Let the following terminology denote size categories for SMTP messages. The size categories are determined by the size of the encoded SMTP (MIME) body.

- Small SMTP messages: *0 KB < SMTP body size <= 100 KB*;
- Medium SMTP messages: *100 MB < SMTP body size <= 500 KB*;
- Large SMTP message: 500 KB < *SMTP body size <= 10 MB*;

5.4.1.2.3 'Normal load' and 'peak load'

Normal load

In this SRS the '*normal load'* is the load on the MG (in terms of SMTP messages to be forwarded) that can be assumed to exist under normal traffic conditions. This SRS defines a 'normal load' for each size category from 5.4.1.2.2, which is referred to as the '*size category normal load*' (*SCNL*). Then, the '*total normal load*' (notation *TNL*) is the sum of all size category normal loads that the MG can be subjected to simultaneously.

The following '*load characteristics*' are distinguished in order to characterize the traffic that comprises the normal load (note that not all load characteristics have to apply to a normal load simultaneously):

- *Average message size*;
- *Maximum message* size; (For the *size category normal load* this is bound by the maximum message size in the category. For the *TNL* this is bound by the maximum message size of the 'very large SMTP messages' category.)
- *Number of messages per time unit;*
- *Message size distribution*;
- *Message type distribution.*

When it is written that the MG '**supports a normal load**', this means that the *MG throughput*, the *MG processing times* and the *MG forwarding times* are such that the MG is able to support a continuous normal load without degradation in performance.

Peak load

Let '*peak load*' be a multiple of the normal load (in terms of its load characterisitcis), during a limited period of time.

5.4.1.2.4 Requirements for MG forwarding times, throughput and processing times

Requirement ID: [SRS-5-217]

The MG SHALL support[1] a total normal load, *TNL*, with the following normal loads per message size category:

- Small SMTP messages: a *SCNL* of 22 SMTP messages per minute with average message size 70 KB.
- Medium SMTP messages: a *SCNL* of 4 SMTP messages per minute with average message size 250 KB.
- Large SMTP messages: a *SCNL* of 1 SMTP messages per minute with average message size 1 MB.

[1] When it is written that the MG 'supports a normal load', this means that the *MG throughput*, the *MG processing times* and the *MG forwarding times* are such that the MG is able to support a continuous normal load without degradation in performance.

Requirement ID: [SRS-5-218]

The MG SHALL support the total normal load *TNL* with the following constraints on the *TNL* characteristics:

- *TNL* average message size < 250 KB;
- *TNL* maximum message size <= 10 MB;
- *TNL* message size distribution: 80% of *TNL* < 100 KB; 95% of *TNL* < 500 KB; 98% of *TNL* < 2.5 MB.

Requirement ID: [SRS-5-219]

Per size category the average *SMTP message processing time T_MG_Proc-Average* SHALL meet the following constraints under the size category normal loads from [SRS-5-217]:

- Small SMTP messages: *T_MG_Proc-Average* < 200 milliseconds;
- Medium SMTP messages: *T_MG_Proc-Average* < 3000 milliseconds;
- Large SMTP messages: *T_MG_Proc-Average* < 15000 milliseconds;

Requirement ID: [SRS-5-220]

The MG SHALL meet the requirements on *SMTP message processing time* in [SRS-5-219] under a total normal load *TNL* with the following constraints on the *TNL* characteristics:

- *TNL* average message size < 250 KB;
- *TNL* maximum message size <= 1 MB;
- *TNL* message size distribution: 80% of *TNL* < 100 KB; 95% of *TNL* < 500 KB; 98% of *TNL* < 2.5 MB.

Requirement ID: [SRS-5-221]

If an SMTP message *M* is processed by the MG that is too large for the category ‘Large SMTP messages’, the MG SHALL:

- continue to operate;
- be responsive to commands issued by a System Administrator;
- meet the requirements in [SRS-5-219] under the total normal load *TNL*;
- and MAY terminate the processing of *M* in order to do so.

5.4.1.2.5 Requirements for peak load

The following 3 requirements specify the extent to which a peak load may impact the MG throughput, processing times or forwarding times. The peak loads are based on the normal loads from requirement [SRS-5-217]. Each requirement is followed by a rationale.

Requirement ID: [SRS-5-222]

If, while under the total normal load *TNL*, a peak load occurs for one of the size categories, the average *MG throughput* for that size category SHALL meet the following constraints for the peak load stated, while not rejecting SMTP traffic:

- Small SMTP messages: for a peak load of 2 times the number of messages in the *SCNL* with a duration of 300 seconds, the average *throughput* SHALL decrease at most 10% when compared to the *SCNL*.
- Medium SMTP messages: for a peak load of 2 times the number of messages in the *SCNL* with a duration of 300 seconds, the average *throughput* SHALL decrease at most 10% when compared to the *SCNL*.
- Large SMTP messages: for a peak load of 2 times the number of messages in the *SCNL* with a duration of 300 seconds, the average *throughput* SHALL decrease at most 10% when compared to the *SCNL*.

Rationale behind [SRS-5-222]: A peak load may require the MG to divert part of its resources to peak load handling, e.g. managing messages queues, potentially affecting resources dedicated to throughput. This requirement aims to limit the impact of a peak load on the MG's throughput. (Because of the temporary nature of a peak load, it may be possible to temporarily make additional system resources available to handle the overhead introduced by the peak load.)

Requirement ID: [SRS-5-223]

If, while under the total normal load *TNL*, a peak load occurs for one of the size categories, the average *SMTP message forwarding time T_MG_Forward-Average* for that size category SHALL satisfy the following conditions for the peak load stated, while not rejecting SMTP traffic:

- Small SMTP messages: for a peak load of 2 times the number of messages in the *SCNL* with a duration of 300 seconds, *T_MG_Forward-Average* SHALL increase at most 20% when compared to the *SCNL*.
- Medium SMTP messages: for a peak load of 2 times the number of messages in the *SCNL* with a duration of 300 seconds, *T_MG_Forward-Average* SHALL increase at most 30% when compared to the *SCNL*.
- Large SMTP messages: for a peak load of 2 times the number of messages in the *SCNL* with a duration of 300 seconds, *T_MG_Forward-Average* SHALL increase at most 40% when compared to the *SCNL*.

Rationale behind [SRS-5-223]0: A peak load implies longer message queues and hence an increase in forwarding time. This requirement aims to limit the impact on the forwarding times. (Because of the temporary nature of a peak load, it may be possible to temporarily make resources available to increase throughput such that an increase in forwarding time can be limited.)

Requirement ID: [SRS-5-224]

If, while under the total normal load *TNL*, a peak load occurs for one of the size categories, the average *SMTP message processing time T_MG_Proc-Average* for that size category SHALL satisfy the following conditions for the peak load stated, while not rejecting SMTP traffic:

- Small SMTP messages: for a peak load of 2 times the number of messages in the *SCNL* with a duration of 300 seconds, *T_MG_Proc-Average* SHALL increase at most 10% compared to normal load.
- Medium SMTP messages: for a peak load of 2 times the number of messages in the *SCNL* with a duration of 300 seconds, *T_MG_Proc-Average* SHALL increase at most 20% compared to normal load.
- Large SMTP messages: for a peak load of 2 times the number of messages in the *SCNL* with a duration of 300 seconds, *T_MG_Proc-Average* SHALL increase at most 30% compared to normal load.

Requirement ID: [SRS-5-225]

During peak loads that are larger in size or longer in duration than those specified in [SRS-5-222], [SRS-5-223] and [SRS-5-224], the MG SHALL continue to operate and be responsive to commands issued by a System Administrator, and MAY reject SMTP traffic in order to do so.

Requirement ID: [SRS-5-226]

If peak loads for multiple size categories take place simultaneously, the MG SHALL continue to operate and be responsive to commands issued by a System Administrator, and MAY reject SMTP traffic in order to do so.

Requirement ID: [SRS-5-227]

It SHALL be possible to configure an upper message size limit, L, such that the MG SHALL reject messages that exceed the size limit L.

5.4.1.2.6 Requirements on impact of logging

Requirement ID: [SRS-5-228]

The impact of logging by the MG on its performance SHALL remain within the following limits, for the following syslog severity levels [RFC 5424]:

- For severity levels ‘Emergency’ (0), ‘Alert’ (1), ‘Critical’ (2), ‘Error’ (3), ‘Warning’ (4): no impact on performance;
- For severity levels ‘Notice’ (5) and ‘Informational’ (6): a decrease in throughput of at most 40%.
- For severity level ‘Debug’ (7): a decrease in throughput of at most 80%.

5.4.1.3 Scalability

Requirement ID: [SRS-5-229]

The MG SHALL be scalable such that when an increase in traffic occurs, capacity can be increased in order to keep meeting the requirements on Time Behaviour in 5.4.1.2.

Requirement ID: [SRS-5-230]

The MG architecture SHALL support horizontal scalability and allow for multiple instances of the MG to be deployed on multiple machines, supporting the information exchange requirements and MG policy in concert.

Requirement ID: [SRS-5-231]

The MG SHALL be vertically scalable, i.e. the MG SHALL be able to adapt its performance characteristics by having additional system resources added such as processing power, memory, disk capacity, or network capacity.

Requirement ID: [SRS-5-232]

In order to keep meeting the requirements on Time Behaviour in 5.4.1.2 it SHALL be possible to apply horizontal scalability without disrupting the services offered by any active MG.

Requirement ID: [SRS-5-233]

The horizontal scaling of the MG SHALL NOT introduce any additional MG management overhead.

Requirement ID: [SRS-5-328]

The MG SHALL be dimensioned and configured to be able to scale in performance and support the following per year, for three years, without degradation of performance as specified in section 5.4.1.2:

- a 100% increase in the SCNL (normal load for each SMTP message size category);
- a 50% increase in message size.

5.4.2 Usability

5.4.2.1 Usability

The extent to which an interactive system can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use.

Requirement ID: [SRS-5-234]

The MG SHALL have a high degree of learnability, making it very easy to use for System Administrators even the first time.

Requirement ID: [SRS-5-235]

The MG SHALL score above 80% in user success rate without external support, for System Administrators that have received standard training.

5.4.3 Reliability

5.4.3.1 Fault Tolerance

Requirement ID: [SRS-5-236]

The MG SHALL continue to receive and queue messages in the event of unavailability of recipient side networking.

Requirement ID: [SRS-5-237]

The MG SHALL continue to dequeue and send messages in the event of unavailability of originator side networking.

5.4.4 Security

5.4.4.1 Audit and Accountability

5.4.4.1.1 Log Configuration

Requirement ID: [SRS-5-238]

The MG SHALL notify a System Administrator by e-mail when the audit log reaches 75% of its maximum permitted size.

Requirement ID: [SRS-5-239]

The MG SHALL provide a configuration option to set the maximum permitted size of the audit log.

5.4.4.2 Integrity

Requirement ID: [SRS-5-240]

The MG SHALL contain residual information protection mechanisms to ensure that purged information is no longer accessible.

Requirement ID: [SRS-5-241]

The MG SHALL ensure that newly created objects do not contain information that has been purged.

5.4.5 Maintainability

5.4.5.1 Analysability

The degree of effectiveness and efficiency with which it is possible to assess the impact on a product or system of an intended change to one or more of its parts, or to diagnose a product for deficiencies or causes of failures, or to identify parts to be modified.

NOTE Implementation can include providing mechanisms for the product or system to analyse its own faults and provide reports prior to a failure or other event.

The system shall be effective and efficient in the possibility to assess the impact on a product or system of an intended change to one or more of its parts, or to diagnose a product for deficiencies or causes of failures, or to identify parts to be modified.

Requirement ID: [SRS-5-242]

Alert messages triggered by the MG (e.g., error, warning, notification and informational messages) SHALL contain initiating module information, context sensitive help or directives on where to find answers and solutions.

Requirement ID: [SRS-5-243]

MG log messages SHALL contain initiating module information, Date/Time(Z), system instance, (log) message, category/severity, user (invoker of function), context information (for example, mission/session, service/function, parameters, and trace-log).

5.4.6 Portability

The portability is defined as the capability of the software product to be transferred from one environment to another.

5.4.6.1 Installability

The degree of effectiveness and efficiency with which a product or system can be successfully installed and/or uninstalled in a specified environment.

Requirement ID: [SRS-5-507]

A MG System Administrator SHALL be able to successfully deploy (i.e., install and configure) the MG within a time frame of one (1) working day after receiving a maximum of five (5) days of training.

6 Web Guard Functional Requirements

6.1 Background

6.1.1 Introduction

This chapter describes the functional requirements for a 'Web Guard Capability' (WG)[4]. For a general system description of the WG, including a common information exchange scenario supported by the WG, see APPENDIX A. The functional requirements are described in terms of interfaces and operations that have been defined for the IEG-C ABBs (see [NCIA TR/2016/NSE010871/01, 2017]). The ABBs, interfaces and operations that together comprise a Web Guard capability are captured in WG patterns. The patterns are described in Section 6.3. In each pattern the WG enforces a number of policies. An overview of the policies is provided in Section 6.2.

[4] Note that the abbreviation 'WG' stands for the capability, and not necessarily for a single (physical or virtual) system; in other words, a Web Guard Capability may be composed of more than one system.

Due to the choice for an IEG-C architecture based on a DMZ, and the WG being part of that DMZ, the operations at the external interfaces of the WG are not identical to those at the external interfaces of the IEG-C. This distinction is important to note in order to correctly interpret the WG patterns. The next section explains the use of the interfaces and operations for the WG and IEG-C.

6.1.2 Domains, interfaces and operations

The IEG-C TA [NCIA TR/2016/NSE010871/01, 2017] assumes a DMZ architecture. Figure 10 shows the logical placement of the WG in the DMZ, the interfaces of IEG and WG, and the domains to which the IEG-C and WG interface. The WG interfaces to the high side of the DMZ at WG_IF_NET_HIGH, and to the low side of the DMZ at WG_IF_NET_LOW.

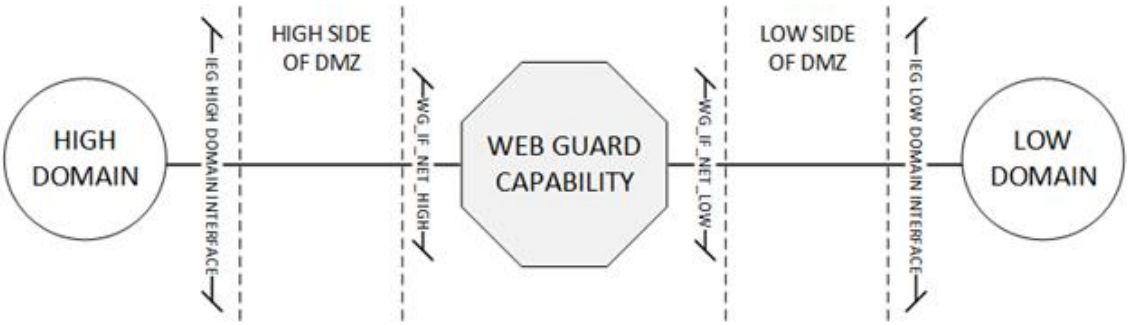

Figure 10 WG in DMZ architecture: domains and interfaces

Note that the WG is not aware of the DMZ configuration; a release of information to the low side of the DMZ is considered a release to the low domain, and an import from the high side of the DMZ is considered an import from the high domain.

The interfaces WG_IF_NET_HIGH and WG_IF_NET_LOW offer TCP/IP over Ethernet network connectivity. Both interfaces support a subset of the logical interfaces offered by the IEG-C ABB 'Data Exchange Services'. Table 6 provides an overview.

Table 8 Subset of logical IEG-C ABB interfaces supported by WG interfaces

WG interfaces (Section A.5)	**Supported subset of logical interfaces from IEG-C ABB 'Data Exchange Services'**	**Note on security domains**
WG_IF_NET_HIGH	- Communications Access Services HL Interface - Communications Access Services LH Interface - SOA Platform Services HL Interface - SOA Platform Services LH Interface	From the point of view of the WG, the high side DMZ and the high domain are the same security domain referred to as 'high domain'.
WG_IF_NET_LOW	- Communications Access Services HL Interface - Communications Access Services LH Interface - SOA Platform Services HL Interface - SOA Platform Services LH Interface.	From the point of view of the WG, the low side DMZ and the low domain are the same security domain referred to as 'low domain'.
WG_IF_MGMT (Not shown in Figure 10.)	Management interface	The management interface can be implemented as a logical interface on top of WG_IF_NET_HIGH in which

		case – from the point of view of the WG - the management domain is equal to the high domain. If the management interface is implemented as a separate physical interface, then – from the point of view of the WG – the management domain is considered a separate security domain referred to as 'management domain'.

In the DMZ architecture in Figure 10, the external networks are those represented by the low and high domains; the internal networks are those represented by the high side and low side of the DMZ. From the point of view of the WG however, both sides of the DMZ are external domains. This point of view has no consequence on the selection of logical interfaces that apply to the WG as shown in Table 6. However, the operations that are defined for the logical interface 'Communications Access Services' do distinguish between internal and external networks, where the point of view taken is that of the IEG-C. These operations are 'ReceiveExternalNetwork', 'ReceiveInternalNetwork', 'ForwardInternalNetwork' and 'ForwardExternalNetwork' (see section A.3.3.1 of [NCIA TR/2016/NSE010871/01, 2017]). So even though both sides of the DMZ are external to the WG, the operations that apply to the WG are 'ReceiveInternalNetwork' and 'ForwardInternalNetwork'.

Figure 11 illustrates the logical interface 'Communications Access Services HL interface' and its operations supporting the traffic flow from the high domain to the low domain.

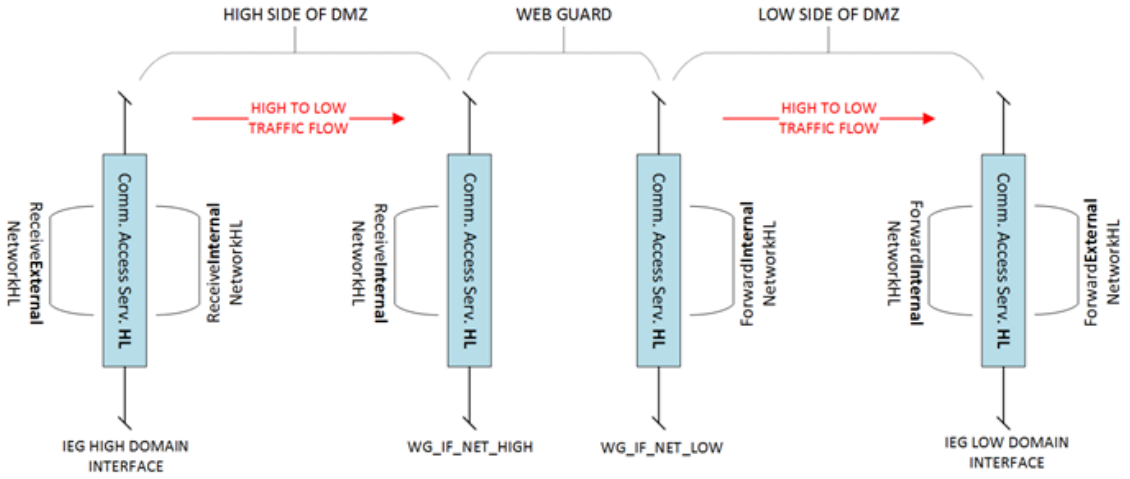

Figure 11 Operations at instances of the interface 'Communication Access Services HL' for traffic flowing from the high to the low domain

Figure 12 illustrates the logical interface 'Communications Access Services LH interface' and its operations supporting the traffic flow from the low domain to the high domain.

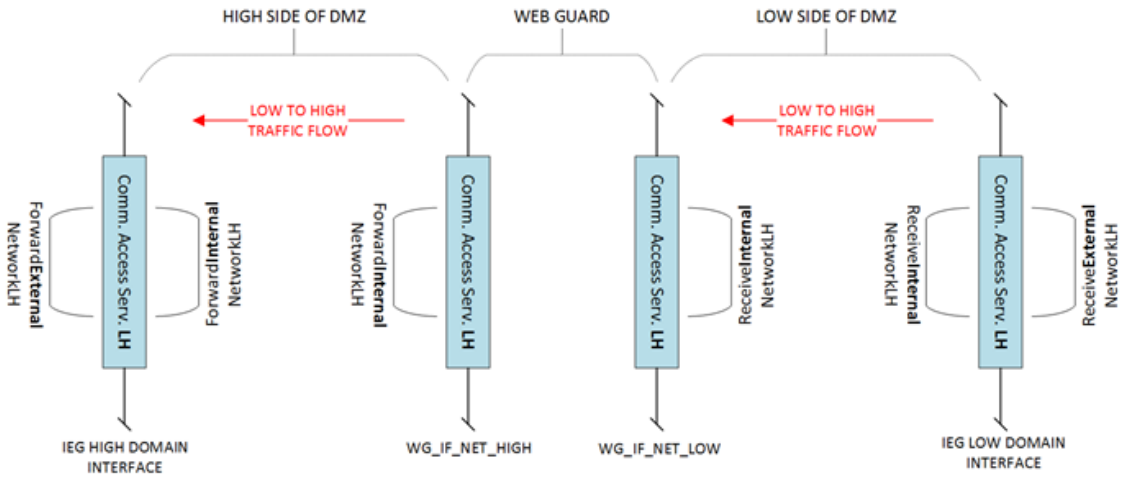

Figure 12 Operations at instances of the interface 'Communication Access Services LH' for traffic flowing from the low to the high domain

6.2 WG Policy Enforcement

6.2.1 WG security policy

The WG enforces a security policy. This policy is referred to as the 'WG security policy' (see Section A.2.1). Regarding the enforcement of the WG security policy on low-to-high and high-to-low traffic[5] (Figure A.3), the WG security policy is composed of two types of policies:

[5] Note that the WG also needs to enforce a security policy with respect to local access control (in support of system administration, system audit and self-protection (see 6.8)). The local access control policy is considered a part of the WG security policy, however may be administered separately from the policies listed in 6.2.

- Information flow control policies (Section 6.2.2);
- Content inspection policies (Section 6.2.3).

6.2.2 WG information flow control policies

The information flow control policy (IFP) that is enforced by the WG is referred to as 'WG_IFP'. The policy WG_IFP is the union of three sub-policies:

- The sub-policy that pertains to high-to-low traffic, referred to as 'WG_IFP_HL';
- The sub-policy that pertains to low-to-high traffic, referred to as 'WG_IFP_LH'; and
- The sub-policy that pertains to management traffic, referred to as 'WG_IFP_MGMT'.

All three policies can be broken down further into sub-polices. Table 7 provides an overview of all IFPs and their scope; each IFP is covered in Section 6.5.2.

Table 9 IFPs enforced by WG and their scope

Policy	Union of sub-policies	Scope
WG_IFP	WG_IFP_HL	High to low traffic
	WG_IFP_LH	Low to high traffic
	WG_IFP_MGMT	Management traffic (related to management of the WG itself).
WG_IFP_MGMT	WG_IFP_MGMT_IN	Management traffic destined for WG
	WG_IFP_MGMT_OUT	Management traffic leaving WG
WG_IFP_HL	WG_IFP_CA_HL	High to low HTTP traffic
	WG_IFP_SOA_HL	HTTP messages transferred from high to low
WG_IFP_LH	WG_IFP_CA_LH	Low to high HTTP traffic
	WG_IFP_SOA_LH	HTTP messages transferred from low to high
WG_IFP_CA_HL	WG_IFP_CA_HL_IN	Transfer-in high to low HTTP traffic for processing by WG
	WG_IFP_CA_HL_OUT	Transfer-out high to low HTTP traffic processed by WG
WG_IFP_CA_LH	WG_IFP_CA_LH_IN	Transfer-in low to high HTTP traffic for processing by WG
	WG_IFP_CA_LH_OUT	Transfer-out low to high HTTP traffic processed by WG

6.2.3 WG content inspection policies

The content inspection policy (CIP) that is enforced by the WG is referred to as ‘WG_CIP’. The policy WG_CIP is the union of the policies ‘WG_CIP_HL’ and ‘WG_CIP_LH’, see Table 8.

Table 10 WG content inspection policies

Policy	Union of sub-policies	Scope
WG_CIP	WG_CIP_HL	HTTP messages transferred from high to low
	WG_CIP_LH	HTTP messages transferred from low to high

Note that the outcome of the enforcement of IFPs WG_IFP_SOA_HL and WG_IFP_SOA_LH depends on the outcome of the enforcement of WG_CIP in the sense that WG_IFP_SOA_HL and WG_IFP_SOA_LH will not permit traffic flow when traffic violates WG_CIP (see requirements [SRS-6-136] and [SRS-6-137]).

Section 6.6.1 specifies the functional requirements of the WG for the ABB ‘Content Inspection Services’. The enforcement functionality of the WG related to this ABB is:

- XML schema validation;
- HTTP header vetting;
- label validation; and
- detection of malware.

The enforcement of XML schema validation, HTTP header vetting, and label validation is referred to as the ‘common WG information exchange scenario, see A.2.2. However, this chapter adds malware detection as required enforcement functionality.

The WG provides the enforcement functionality through the application of content filters that enforce the content inspection policies WG_CIP_HL and WG_CIP_LH. In order to

be able to group functional requirements per WG functionality, WG_CIP_HL and WG_CIP_LH are split into sub-policies as per Table 9; each CIP is described in Section 6.5.4. The selection of sub-policies depends on the information exchange scenario that will be supported. The sub-policies in Table 9 assume the common WG information exchange scenario that is described in A.4, augmented with malware detection.

Table 11 Further breakdown of WG content inspection policies in support of the common WG information exchange scenario (described in A.4), augmented with malware detection

Policy	Union of sub-policies	Scope	WG functionality
WG_CIP_HL	WG_CIP_HL_LV	HTTP message body	Label validation
	WG_CIP_HL_HV	HTTP message headers	HTTP header vetting
WG_CIP_LH	WG_CIP_LH_SV	HTTP message body	XML schema validation
	WG_CIP_LH_HV	HTTP message headers	HTTP header vetting
	WG_CIP_LH_MD	HTTP message headers and body	Malware detection

6.2.4 Support for enforcement of WG_CIP_LH_LV, WG_CIP_HL_SV, and WG_CIP_HL_MD

Sections 6.5.3 and Section 6.6.1 cover the policies from Table 11. Information exchange scenarios that require the WG functionalities label validation, XML schema validation, or malware detection in the direction opposite to the one covered in Table 11, can be supported by implementing policy enforcement for the associated sub-policies WG_CIP_LH_LV, WG_CIP_HL_SV, and WG_CIP_HL_MD respectively. Functional requirements that describe policy enforcement based on WG_CIP_LH_LV, WG_CIP_HL_SV, and WG_CIP_HL_MD are not included in this document, however can be formulated in a similar fashion to those that cover the enforcement of the policies in Table 11.

6.3 WG Patterns

6.3.1 Main Patterns

Three main patterns comprise the WG. Each pattern is a combination of two sub-patterns, see Table 10.

Table 12 Patterns that comprise the WG

Pattern	Combination of sub-patterns	Depicted in
WG High to Low Pattern	WG High to Low Node Self Protection Pattern	Figure 13
	WG High to Low Cross Domain Information Exchange Pattern	
WG Low to High Pattern	WG Low to High Node Self Protection Pattern	Figure 15
	WG Low to High Cross Domain Information Exchange Pattern	
WG Management pattern	WG Management Self Protection Pattern	Figure 17
	WG Element Management Services Pattern	Figure 18

The WG patterns enforce the information flow control and content inspection policies that are described in Sections 6.2.2 and 6.2.3. Therefore it shall be noted that support for the enforcement of additional policies (6.2.4) may require a modification to the patterns.

6.3.2 WG High to Low Pattern

The policy WG_IFP_HL is enforced in the WG High to Low Pattern (depicted in Figure 13). The pattern is composed of the following ABBs, interfaces and operations (sub-policies that are enforced are shown [between brackets]):

(In order to clarify the sequence of the pattern, the following formatting is used: interfaces are underlined and *operations* are in italic.)

- [START] Data Exchange Services -> Communications Access Services HL -> *ReceiveInternalNetworkHL*
- Protection Policy Enforcement Services -> IFCPE Services High to Low -> *Enforce HL Communications IFCPE* [IFP: WG_IFP_CA_HL_IN]
- Data Exchange Services -> SOA Platform Services HL -> *ReceiveWebContentHL*
- Protection Services -> Public Key Cryptographic Services -> *Verify / Decrypt*
- (Required if TLS connection is used or content is digitally signed)
- Protection Policy Enforcement Services -> IFCPE Services High to Low -> *Enforce HL SOA Platform IFCPE* [IFP: WG_IFP_SOA_HL]
- Protection Policy Enforcement Services -> CIPE Services High to Low -> *Enforce HL SOA CIPE* [CIP: WG_CIP_HL]
- Protection Services -> Content Inspection Services -> *Initialize / Filter / Halt*
- Protection Services -> Public Key Cryptographic Services -> *Verify*
- (Required if digital signature must be verified)
- Data Exchange Services -> SOA Platform Services HL -> *ForwardWebContentHL*
- Protection Services -> Public Key Cryptographic Services -> *Encrypt/Sign*
- (Required if TLS connection is used or if content is to be signed by the WG)
- Protection Policy Enforcement Services -> IFCPE Services High to Low -> *Enforce HL Communications IFCPE* [IFP: WG_IFP_CA_HL_OUT]
- Data Exchange Services -> Communications Access Services HL -> *ForwardInternalNetworkHL* [END]

Note that the pattern starts with the operation ‘ReceiveInternalNetworkHL’ and ends with the operation ‘ForwardInternalNetworkHL’; this is in line with Figure 11.

Traffic will follow the pattern from [START] to [END] if no policy violation occurs. In case a policy violation occurs, traffic flow is interrupted according to Figure 13:

- If enforcement of WG_IFP_CA_HL_IN or WG_IFP_CA_HL_OUT results in a policy violation, traffic will be rejected and an action shall be executed as specified in [SRS-6-116].
- If enforcement of WG_IFP_SOA_HL results in a policy violation, an HTTP error message may be generated according to [SRS-6-138]. Note that [SRS-6-138] includes the option to silently drop traffic. Figure 13 however assumes an HTTP error message is generated.

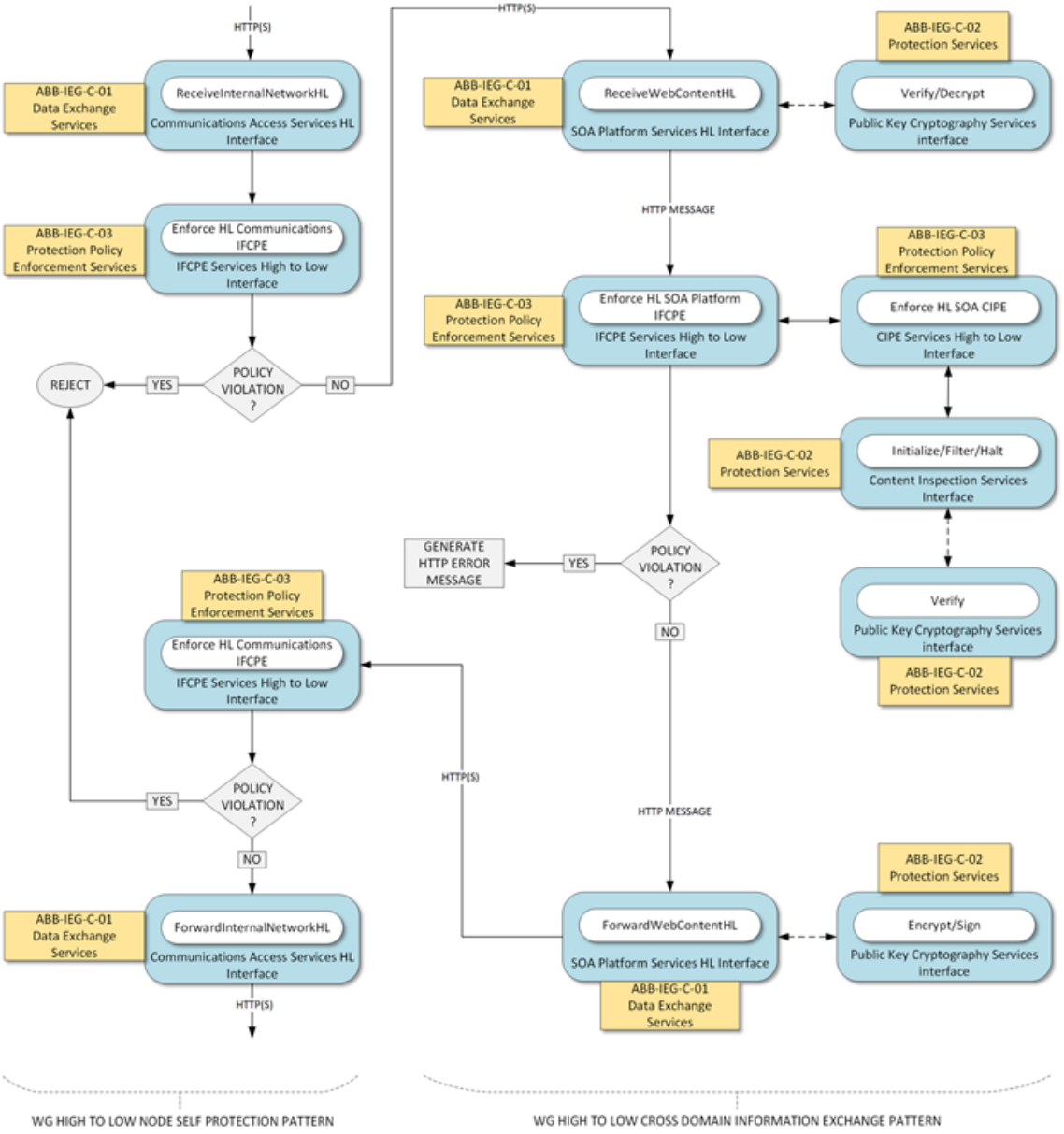

Figure 13 WG High to Low Pattern (combination of 'WG High to Low Node Self Protection Pattern' and 'WG High to Low Cross Domain Information Exchange pattern')

HTTP error messages are sent as response messages, therefore they will not continue to follow the WG High to Low Pattern. Instead they will follow part of the WG Low to High Pattern. The WG Low to High Pattern is depicted in full in Figure 15; the part that is relevant to the sending of HTTP error messages is included as a sub-pattern in Figure 14.

Figure 14 shows the composed pattern for the generation and sending of HTTP error messages that occur during high to low traffic flow processing. The pattern is composed of two sub-patterns: a WG High to Low sub-pattern in which the error message is generated, and a WG Low to High sub-pattern in which the error message is sent.

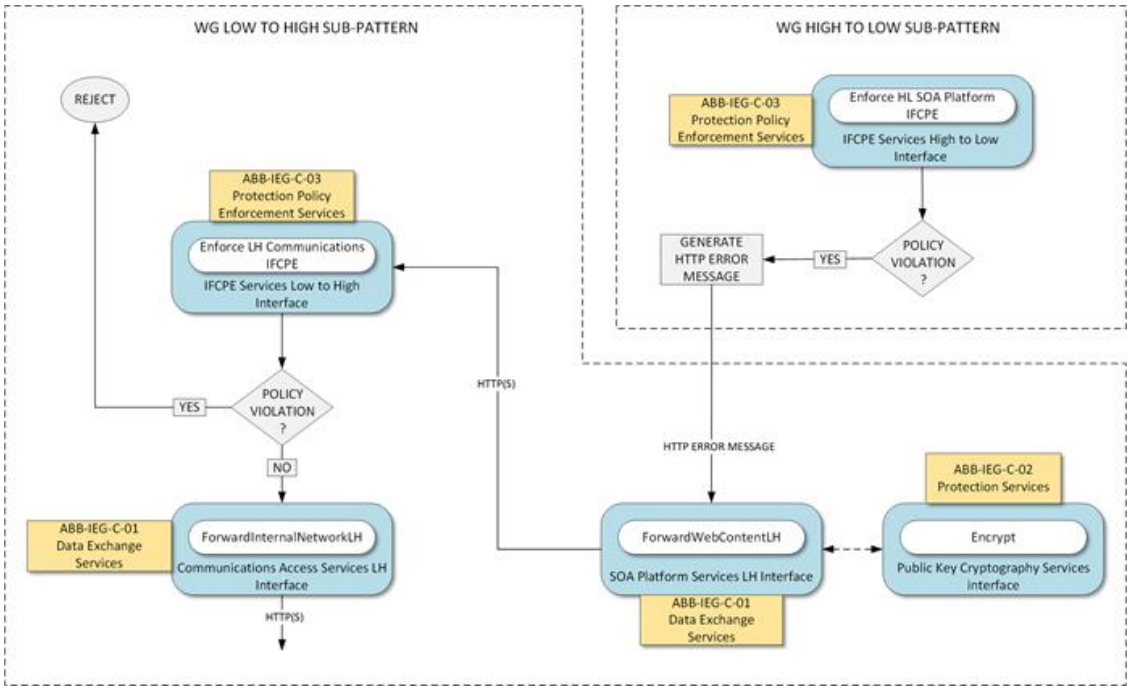

Figure 14 Pattern for generation and sending of HTTP error messages that occur during high to low traffic flow processing

6.3.3 WG Low to High Pattern

The policy WG_IFP_LH is enforced in the WG Low to High Pattern (depicted in Figure 15). The pattern is composed of the following ABBs, interfaces and operations (sub-policies that are enforced are shown [between brackets]):

(In order to clarify the sequence of the pattern, the following formatting is used: interfaces are underlined and *operations* are in italic.)

- [START] Data Exchange Services -> Communications Access Services LH -> *ReceiveInternalNetworkLH*
- Protection Policy Enforcement Services -> IFCPE Services Low to High -> *Enforce LH Communications IFCPE* [IFP: WG_IFP_CA_LH_IN]
- Data Exchange Services -> SOA Platform Services LH -> *ReceiveWebContentLH*
- Protection Services -> Public Key Cryptographic Services -> *Verify / Decrypt*

(Required if TLS connection is used or content is digitally signed)

- Protection Policy Enforcement Services -> IFCPE Services Low to High -> *Enforce LH SOA Platform IFCPE* [IFP: WG_IFP_SOA_LH]
- Protection Policy Enforcement Services -> CIPE Services Low to High -> *Enforce LH SOA CIPE* [CIP: WG_CIP_LH]
- Protection Services -> Content Inspection Services -> *Initialize / Filter / Halt*
- Data Exchange Services -> SOA Platform Services LH -> *ForwardWebContentLH*
- Protection Services -> Public Key Cryptographic Services -> *Encrypt*
- (Required if TLS connection is used)
- Protection Policy Enforcement Services -> IFCPE Services Low to High -> *Enforce LH Communications IFCPE* [IFP: WG_IFP_CA_LH_OUT]
- Data Exchange Services -> Communications Access Services LH -> *ForwardInternalNetworkLH* [END]

Note that the pattern starts with the operation ‘ReceiveInternalNetworkLH’ and ends with the operation ‘ForwardInternalNetworkLH’; this is in line with Figure 12.

Traffic will follow the pattern from [START] to [END] if no policy violation occurs. In case a policy violation occurs, traffic flow is interrupted according to Figure 15:

- If enforcement of WG_IFP_CA_LH_IN or WG_IFP_CA_LH_OUT results in a policy violation, traffic will be rejected and an action shall be executed as specified in [SRS-6-116].
- If enforcement of WG_IFP_SOA_LH results in a policy violation, an HTTP error message may be generated according to [SRS-6-138]. Note that [SRS-6-138] includes the option to silently drop traffic. Figure 15 however assumes an HTTP error message is generated.

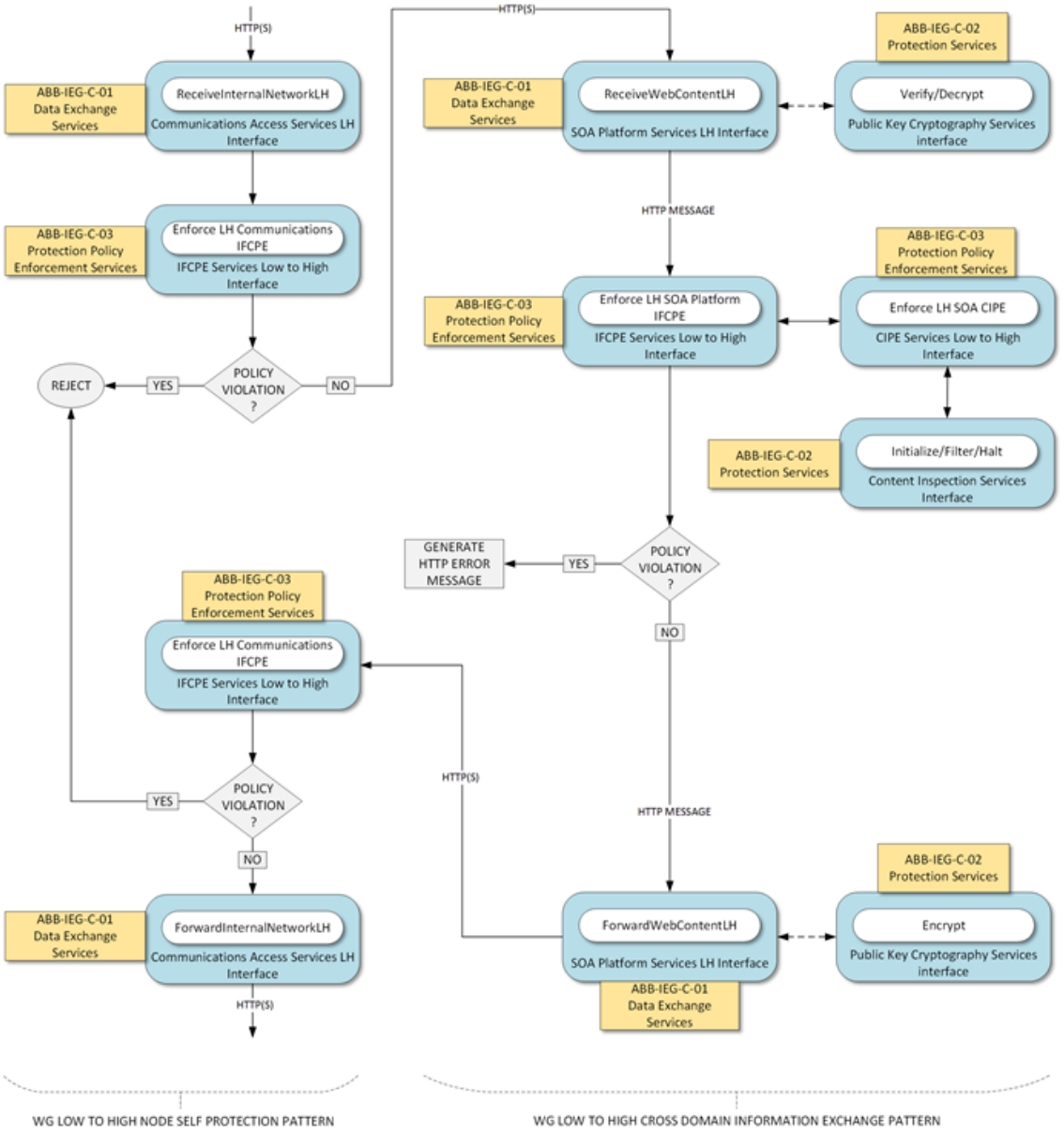

Figure 15 WG Low to High Pattern (combination of 'WG Low to High Node Self Protection Pattern' and 'WG Low to High Cross Domain Information Exchange Pattern')

HTTP error messages are sent as response messages, therefore they will not continue to follow the WG Low to High Pattern. Instead they will follow part of the WG High to Low. The WG High to Low Pattern is depicted in full in Figure 13; the part that is relevant to the sending of HTTP error messages is included as a sub-pattern in Figure 16

Figure 16 shows the composed pattern for the generation and sending of HTTP error messages that occur during low to high traffic flow processing. The pattern is composed of two sub-patterns: a WG Low to High sub-pattern in which the error message is generated, and a WG High to Low sub-pattern in which the error message is sent.

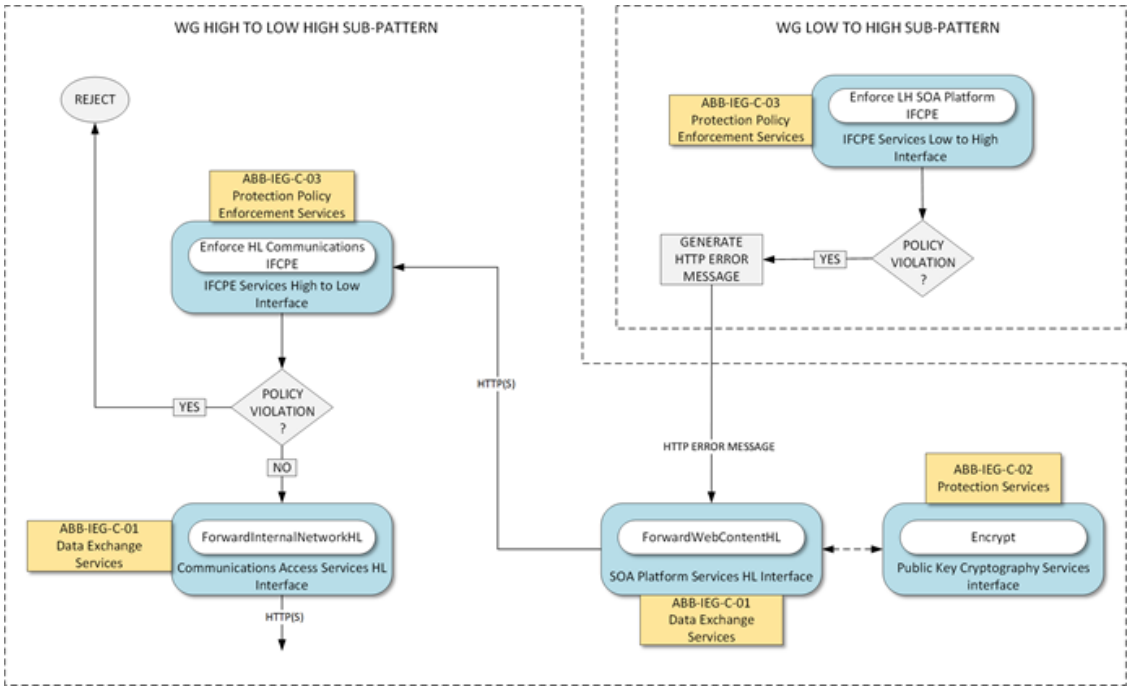

Figure 16 Pattern for generation and sending of HTTP error messages that occur during low to high traffic flow processing

6.3.4 WG Management Pattern

The WG Management Pattern is composed of the 'WG Management Self Protection Pattern' (Figure 17) and the 'WG Element Management Services Pattern' (Figure 18). The 'WG Management Self Protection Pattern' enforces the policy WG_IFP_MGMT, and the 'WG Element Management Services Pattern' enables management of the operating system and the WG ABBs. Management services at the WG are offered by the ABB 'Element Management Services' (see 6.7). The WG Management Pattern also applies to management traffic initiated at the WG with external destination (related to the operations described in Sections 6.7.7 and 6.7.8).

6.3.4.1 WG Management Self Protection Pattern

Figure 17 shows the 'WG Management Self Protection Pattern'. The pattern forwards incoming management traffic to the 'WG Element Management Services Pattern'. Traffic that is output by the 'WG Element Management Services Pattern' is picked up again by the 'WG Management Self Protection Pattern'. It is composed of the following ABBs, interfaces and operations (sub-policies that are enforced are shown [between brackets]):

(In order to clarify the sequence of the pattern, the following formatting is used: interfaces are underlined and *operations* are in italic.)

- [START] Data Exchange Services -> Communications Access Services Management -> ReceiveNetworkManagement
- Protection Policy Enforcement Services -> IFCPE Services Management -> EnforceManagemenCommunicationstIFCPE [IFP: WG_IFP_MGMT_IN] -> 'WG Element Management Services Pattern'
- Processing by 'WG Element Management Services Pattern' (Figure 18)

- 'WG Element Management Services Pattern' -> Protection Policy Enforcement Services -> IFCPE Services Management -> EnforceManagementCommunicationsIFCPE [IFP: WG_IFP_MGMT_OUT]
- Data Exchange Services -> Communications Access Services Management -> ForwardNetworkManagement [END]

Traffic will follow the pattern from [START] to [END] if no policy violation occurs. If enforcement of WG_IFP_MGMT_IN or WG_IFP_MGMT_OUT results in a policy violation, traffic will be rejected and an action shall be executed as specified in [SRS-6-116].

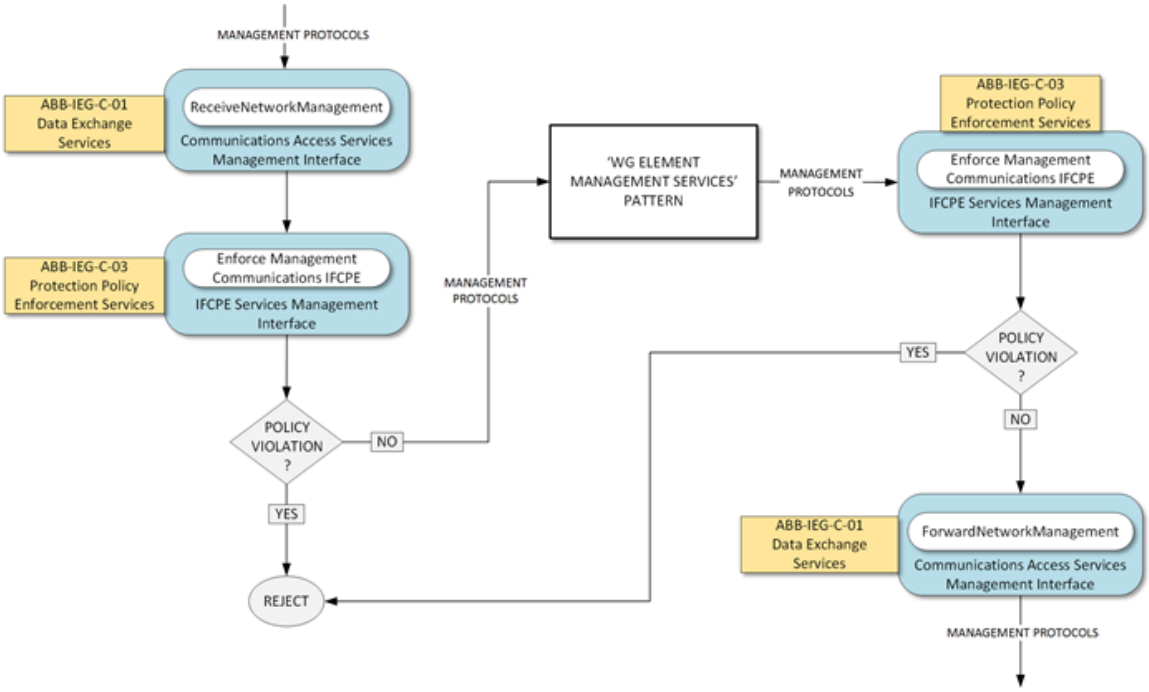

Figure 17 WG Management Self Protection Pattern; this pattern is connected to the pattern 'WG Element Management Services' and enforces an IFP on incoming and outgoing management traffic

6.3.4.2 WG Element Management Services Pattern

The 'WG Element Management Services Pattern' takes input from and outputs to the 'WG Management Self Protection Pattern'. It is composed of the following ABBs, interfaces and operations (sub-policies that are enforced are shown [between brackets]):

(In order to clarify the sequence of the pattern, the following formatting is used: interfaces are underlined and *operations* are in italic.)

- 'WG Management Self Protection Pattern' - > [START] Data Exchange Services -> Core Services Management -> ReceiveManagementContent
- Protection Services -> Public Key Cryptographic Services -> Verify / Decrypt (Required if SSH or TLS connection is used, or content is digitally signed)
- Element Management Services -> CIS Security -> Manage Protection Policies / Review / Manage Public Key Material

OR:

- Element Management Services -> SMC Configuration Management -> Configure OS / Configure Protection Policy Enforcement Services / Configure Data Exchange Services / Configure Protection Services

OR:

- Element Management Services -> Event Management -> Log / Alert / Report

OR:

- Element Management Services -> Cyber Defence -> Assess / Response / Recover

OR:

- Element Management Services -> Performance Management -> Monitor / Meter / Track Messages
- Data Exchange Services -> Core Services Management -> ForwardManagementContent
- Protection Services -> Public Key Cryptographic Services -> Encrypt
- (Required if SSH or TLS connection is used)
- [END] -> ‘WG Management Self Protection Pattern’

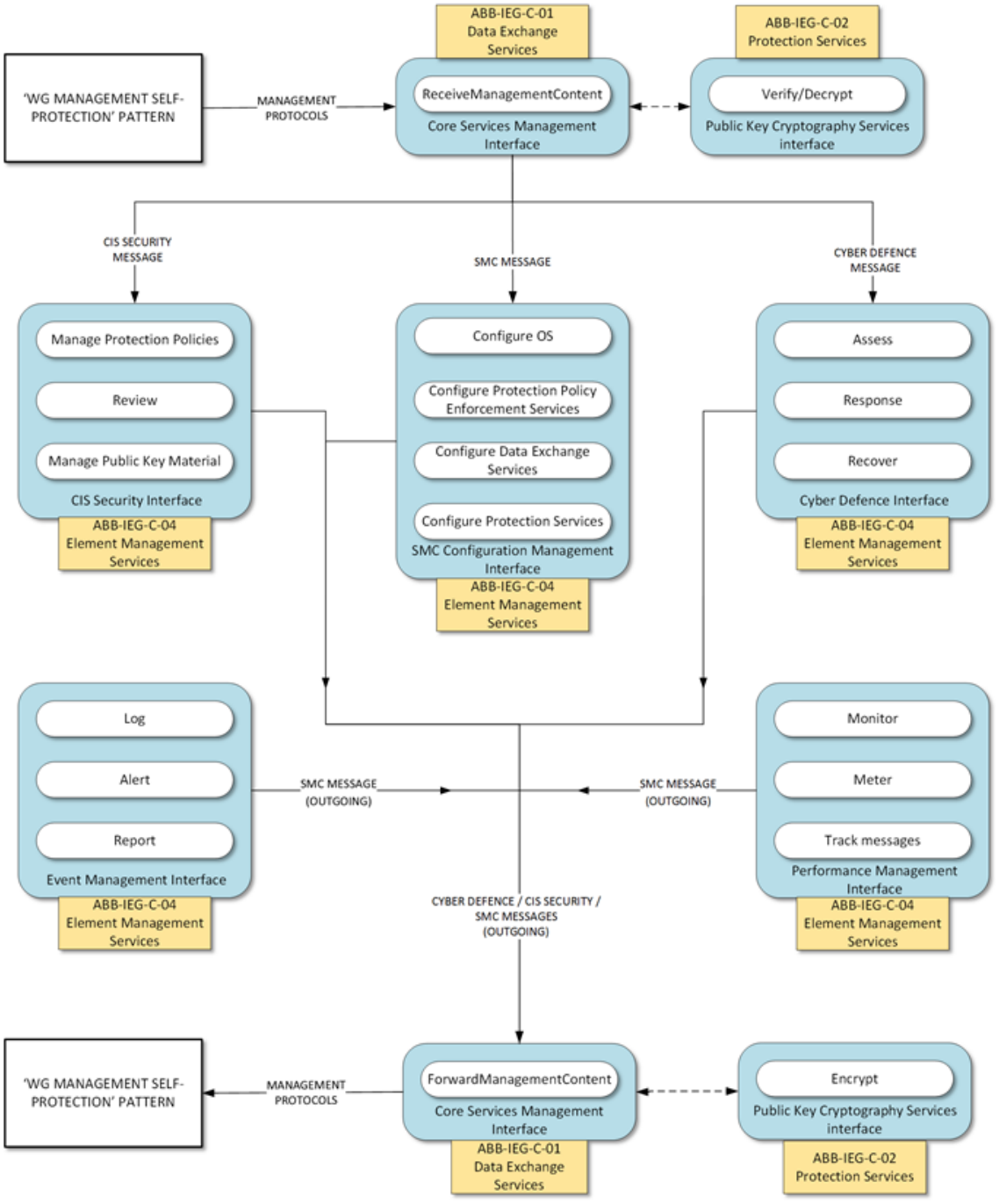

Figure 18 WG Element Management Services Pattern; this pattern takes input from and outputs to the 'WG Management Self Protection Pattern'

6.3.4.3 Types of management content

Note that the payload (i.e. the management content) of the management protocols that are processed at the interface 'Core Services Management' is referred to as a 'management message'. There are three types of management message:

- CIS Security message;
- SMC message; or
- Cyber Defence message.

All the management messages that are delivered to one of the interfaces of ‘Element Management Services’ are referred to as ‘incoming management messages’. The incoming management messages are processed by one of the operations of ‘Element Management Services’. The result of the processing is a management message of the same type; these are referred to as ‘outgoing management messages’. At the interface ‘Core Services Management’ the outgoing management messages are forwarded as payload of the appropriate management protocol by the operation ‘ForwardManagementContent’.

Note that operations of ‘Element Management Services’ can also generate outgoing management messages that have not been preceded by an incoming management messages.

The next sections group the functional requirements for the WG per IEG-C ABB and assume the WG patterns from Section 6.5. Note that in Section 6.3 the terms ‘high domain’ and ‘low domain’ are to be interpreted according to Table 6.

6.4 Data Exchange Services

6.4.1 Data Exchange Services

6.4.1.1 WG_DEX

Requirement ID: [SRS-6-1]

The WG MUST provide a data exchange capability WG_DEX that facilitates the mediation of data between the high domain and the low domain.

6.4.1.2 WG_IF_NET_HIGH

Requirement ID: [SRS-6-2]

WG_DEX MUST offer a physical network interface WG_IF_NET_HIGH that provides Ethernet connectivity to the high domain.

Requirement ID: [SRS-6-3]

WG_IF_NET_HIGH MUST support an operation 'ReceiveHigh' that receives (transfer-in) data from the high domain for processing by the WG.

Requirement ID: [SRS-6-4]

WG_IF_NET_HIGH MUST support an operation 'ForwardHigh' that forwards (transfer-out) data that has been processed by the WG to the high domain.

6.4.1.3 WG_IF_NET_LOW

Requirement ID: [SRS-6-5]

WG_DEX MUST offer a physical network interface WG_IF_NET_LOW that provides Ethernet connectivity to the low domain.

Requirement ID: [SRS-6-6]

WG_IF_NET_LOW MUST support an operation 'ReceiveLow' that receives (transfer-in) data from the low domain for processing by the WG.

Requirement ID: [SRS-6-7]

WG_IF_NET_LOW MUST support an operation 'ForwardLow' that forwards (transfer-out) data that has been processed by the WG to the low domain.

6.4.1.4 WG_IF_MGMT

Requirement ID: [SRS-6-8]

WG_DEX SHOULD offer a physical network interface WG_IF_MGMT that provides Ethernet connectivity to the management domain.

Requirement ID: [SRS-6-9]

If WG_DEX does not offer a physical network interface WG_IF_MGMT, it MUST offer a logical network interface WG_IF_MGMT on top of WG_IF_NET_HIGH.

Requirement ID: [SRS-6-10]

WG_IF_MGMT MUST support an operation 'ReceiveManagement' that receives data from the management domain for processing by the WG.

Requirement ID: [SRS-6-11]

WG_IF_MGMT MUST support an operation 'ForwardManagement' that forwards data that has been processed by the WG to the management domain.

6.4.2 Communications Access Services

6.4.2.1 Communications Access Services HL

Requirement ID: [SRS-6-12]

WG_DEX MUST offer a TCP/IP [IETF RFC 791, 1981], [IETF RFC 2460, 1998], [IETF RFC 7414, 2015] over Ethernet interface 'Communications Access Services HL' on top of WG_IF_NET_HIGH and WG_IF_NET_LOW.

6.4.2.1.1 ReceiveInternalNetworkHL

Requirement ID: [SRS-6-13]

The interface 'Communications Access Services HL' MUST support an operation 'ReceiveInternalNetworkHL' on top of WG_IF_NET_HIGH that provides TCP/IP connectivity on the high domain by receiving IP traffic for processing by the WG.

Requirement ID: [SRS-6-14]

The operation 'ReceiveInternalNetworkHL' MUST support error handling as specified in [IETF RFC 7414, 2015].

6.4.2.1.2 ForwardInternalNetworkHL

Requirement ID: [SRS-6-15]

The interface 'Communications Access Services HL' MUST support an operation 'ForwardInternalNetworkHL' on top of WG_IF_NET_LOW that forwards IP traffic to the low domain.

Requirement ID: [SRS-6-16]

The operation 'ForwardInternalNetworkHL' MUST support error handling as specified in [IETF RFC 7414, 2015].

6.4.2.2 Communications Access Services LH

Requirement ID: [SRS-6-17]

WG_DEX MUST offer a TCP/IP [IETF RFC 791, 1981], [IETF RFC 2460, 1998], [IETF RFC 7414, 2015] over Ethernet interface 'Communications Access Services LH' on top of WG_IF_NET_LOW and WG_IF_NET_HIGH.

6.4.2.2.1 ReceiveInternalNetworkLH

Requirement ID: [SRS-6-18]

The interface 'Communications Access Services LH' MUST support an operation 'ReceiveInternalNetworkLH' on top of WG_IF_NET_LOW that provides TCP/IP connectivity on the low domain by receiving IP traffic for processing by the WG.

Requirement ID: [SRS-6-19]

The operation 'ReceiveInternalNetworkLH' MUST support error handling as specified in [IETF RFC 7414, 2015].

6.4.2.2.2 ForwardInternalNetworkLH

Requirement ID: [SRS-6-20]

The interface 'Communications Access Services LH' MUST support an operation 'ForwardInternalNetworkLH' on top of WG_IF_NET_HIGH that forwards IP traffic to the high domain.

Requirement ID: [SRS-6-21]

The operation 'ForwardInternalNetworkLH' MUST support error handling as specified in [IETF RFC 7414, 2015].

6.4.3 SOA Platform Services

6.4.3.1 SOA Platform Services HL

Requirement ID: [SRS-6-22]

WG_DEX MUST offer a HyperText Transport Protocol (HTTP) v1.1 and v2, [IETF RFC 7230, 2014], [IETF RFC 7540, 2014] interface 'SOA Platform Services HL' on top of 'Communications Access Services HL'.

Requirement ID: [SRS-6-23]

The interface 'SOA Platform Services HL' and its operations SHALL be conformant to the following service interface profiles (SIPs), see Appendix A.3:

- Service Interface Profile for Security Services;
- Service Interface Profile for REST Security Services;
- Service Interface Profile for Messaging (SOAP);
- Service Interface Profile for REST Messaging.

6.4.3.1.1 ReceiveWebContentHL

Requirement ID: [SRS-6-24]

The interface 'SOA Platform Services HL' MUST support an operation 'ReceiveWebContentHL' that provides HTTP connectivity on the high domain.

Requirement ID: [SRS-6-25]

The operation 'ReceiveWebContentHL' MUST support Transport Layer Security (TLS, [IETF RFC 8446, 2018]).

Requirement ID: [SRS-6-26]

The operation 'ReceiveWebContentHL' MUST support the invocation of the operations 'Verify' (6.6.2.2.3) and 'Decrypt' (6.6.2.2.5) at the interface 'Public Key Cryptographic Services' ([SRS-6-239]) provided by WG_PKCS (6.6.2.1).

Requirement ID: [SRS-6-27]

After receiving an HTTP message, the operation 'ReceiveWebContentHL' SHALL pass the HTTP message to the interface 'IFCPE Services High to Low' ([SRS-6-71]) for further processing.

Requirement ID: [SRS-6-28]

The operation 'ReceiveWebContentHL' SHALL persist the HTTP TCP/IP connection from an HTTP client in the high domain until:

- an HTTP Response is received at the interface ‘SOA Platform Services LH’ (6.4.3.2) and processed by the operation ‘ForwardWebContentLH’ (6.4.3.2.3); or
- the HTTP TCP/IP connection is timed out by the HTTP client.

Requirement ID: [SRS-6-29]

In support of the use of HTTP persistent connections, the WG SHALL be able to correlate HTTP request and response messages that belong to the same HTTP connection initiated in the high domain.

Requirement ID: [SRS-6-30]

The operation 'ReceiveWebContentHL' MUST support error handling as specified in [IETF RFC 7231, 2014].

6.4.3.1.2 ForwardWebContentHL

Requirement ID: [SRS-6-31]

The interface 'SOA Platform Services HL' MUST support an operation 'ForwardWebContentHL' that provides HTTP connectivity on the low domain.

Requirement ID: [SRS-6-32]

After receiving an HTTP Request message from the interface 'IFCPE Services High to Low', the operation 'ForwardWebContentHL' SHALL initiate a new HTTP connection - including the HTTP message - to an HTTP server on the low domain. The new HTTP connection SHALL not use the stateful HTTP protocol attributes associated with the connection in [SRS-6-28].

Requirement ID: [SRS-6-33]

After receiving an HTTP Response message from the interface 'IFCPE Services High to Low', the operation 'ForwardWebContentHL' SHALL forward the HTTP message to the low domain using the persisted HTTP connection ([SRS-6-43]).

Requirement ID: [SRS-6-34]

The operation 'ForwardWebContentHL' MUST support Transport Layer Security (TLS, [IETF RFC 8446, 2018]).

Requirement ID: [SRS-6-35]

The operation 'ForwardWebContentHL' MUST support the invocation of the operation 'Encrypt' (6.6.2.2.4) at the interface 'Public Key Cryptographic Services' ([SRS-6-239]) provided by WG_PKCS (6.6.2.1).

Requirement ID: [SRS-6-36]

The operation 'ForwardWebContentHL' MUST support error handling as specified in [IETF RFC 7231, 2014].

6.4.3.2 SOA Platform Services LH

Requirement ID: [SRS-6-37]

WG_DEX MUST offer a HyperText Transport Protocol (HTTP), v1.1 and v2, [IETF RFC 7230, 2014], [IETF RFC 7540, 2014] interface 'SOA Platform Services LH' on top of 'Communications Access Services LH'.

Requirement ID: [SRS-6-38]

The interface 'SOA Platform Services LH' and its operations SHALL be conformant to the following service interface profiles (SIPs), see Appendix A.3:

- Service Interface Profile for Security Services;
- Service Interface Profile for REST Security Services;
- Service Interface Profile for Messaging (SOAP);
- Service Interface Profile for REST Messaging.

6.4.3.2.1 ReceiveWebContentLH

Requirement ID: [SRS-6-39]

The interface 'SOA Platform Services LH' MUST support an operation 'ReceiveWebContentLH' that provides HTTP connectivity on the low domain.

Requirement ID: [SRS-6-40]

The operation 'ReceiveWebContentLH' MUST support Transport Layer Security (TLS, [IETF RFC 8446, 2018]).

Requirement ID: [SRS-6-41]

The operation 'ReceiveWebContentLH' MUST support the invocation of the operations 'Verify' (6.6.2.2.3) and 'Decrypt' (6.6.2.2.5) at the interface 'Public Key Cryptographic Services' ([SRS-6-239]) provided by WG_PKCS (6.6.2.1).

Requirement ID: [SRS-6-42]

After receiving an HTTP message, the operation 'ReceiveWebContentLH' SHALL pass the HTTP message to the interface 'IFCPE Services Low to High' (6.5.1.2.2) for further processing.

Requirement ID: [SRS-6-43]

The operation 'ReceiveWebContentLH' SHALL persist the HTTP TCP/IP connection from an HTTP client in the high domain until:

- an HTTP Response is received at the interface ‘SOA Platform Services HL’ ([SRS-6-22]) and processed by the operation ‘ForwardWebContentHL’ (6.4.3.1.3); or
- the HTTP TCP/IP connection is timed out by the HTTP client.

Requirement ID: [SRS-6-44]

In support of the use of HTTP persistent connections, the WG SHALL be able to correlate HTTP Request and Response messages that belong to the same HTTP connection initiated in the low domain.

Requirement ID: [SRS-6-45]

The operation 'ReceiveWebContentLH' MUST support error handling as specified in [IETF RFC 7231, 2014].

6.4.3.2.2 ForwardWebContentLH

Requirement ID: [SRS-6-46]

The interface 'SOA Platform Services LH' MUST support an operation 'ForwardWebContentLH' that provides HTTP connectivity on the high domain.

Requirement ID: [SRS-6-47]

After receiving an HTTP Request message from the interface 'IFCPE Services Low to High', the operation 'ForwardWebContentLH' SHALL initiate a new HTTP connection - including the HTTP message - to an HTTP server on the high domain. The new HTTP connection SHALL not use the stateful HTTP protocol attributes associated with the connection in [SRS-6-43].

Requirement ID: [SRS-6-48]

After receiving an HTTP Response message from the interface 'IFCPE Services Low to High', the operation 'ForwardWebContentLH' SHALL forward the HTTP message to the high domain using the persisted HTTP connection ([SRS-6-43]).

Requirement ID: [SRS-6-49]

The operation 'ForwardWebContentLH' MUST support Transport Layer Security (TLS, [IETF RFC 8446, 2018]).

Requirement ID: [SRS-6-50]

The operation 'ForwardWebContentLH' MUST support the invocation of the operation 'Encrypt' (6.6.2.2.4) at the interface 'Public Key Cryptographic Services' ([SRS-6-239]) provided by WG_PKCS (6.6.2.1).

Requirement ID: [SRS-6-51]

The operation 'ForwardWebContentLH' MUST support error handling as specified in [IETF RFC 7231, 2014].

6.4.4 Communications Access Services Management

6.4.4.1 Communications Access Services Management

Requirement ID: [SRS-6-52]

WG_DEX MUST offer UDP [IETF RFC 768, 1980] and IPv4 and IPv6, [IETF RFC 791, 1981], [IETF RFC 8200, 2017] over Ethernet interface 'Communications Access Services Management' on top of WG_IF_MGMT.

6.4.4.1.1 ReceiveNetworkManagement

Requirement ID: [SRS-6-53]

The interface 'Communications Access Services Management' MUST support an operation 'ReceiveNetworkManagement' that provides TCP/IP connectivity on the management domain by receiving IP traffic for processing by the WG.

Requirement ID: [SRS-6-54]

The operation 'ReceiveNetworkManagement' MUST support error handling as specified in [IETF RFC 7414, 2015].

6.4.4.1.2 ForwardNetworkManagement

Requirement ID: [SRS-6-55]

The interface 'Communications Access Services Management' MUST support an operation 'ForwardNetworkManagement' that forwards IP traffic to the management domain.

Requirement ID: [SRS-6-56]

The operation 'ForwardNetworkManagement' MUST support error handling as specified in [IETF RFC 7414, 2015].

6.4.5 Core Services Management

6.4.5.1 Core Services Management

Requirement ID: [SRS-6-57]

WG_DEX MUST offer an interface 'Core Services Management' on top of 'Communications Access Services Management'.

Requirement ID: [SRS-6-58]

The interface 'Core Services Management' MUST support the following management protocols:

- Transport Layer protocol [IETF RFC 4251, 2006];
- Simple Network Management Protocol (SNMP) Version 3 [IETF RFC 3410 – 3418, 2002];
- Syslog;
- Network Time Protocol;
- Intelligent Platform Management Interface (IPMI) [IPMI V2.0, 2013];
- Hyper-Text Transport Protocol (HTTP) v1.1 Web interface [IETF RFC 7230, 2014] [IETF RFC 7231, 2014]; Hyper-Text Transport Protocol (HTTP) v2 Web interface, [IETF RFC 7540, 2014]
- Remote Desktop (RDP).

Requirement ID: [SRS-6-59]

The interface 'Core Services Management' MAY support the following management protocol:

- Remote Procedure Call (RPC).
- Keyboard, video and mouse (KVM) over Ethernet;
- Command Line interface (CLI) via Secure Shell (SSH)

6.4.5.2 ReceiveManagementContent

Requirement ID: [SRS-6-60]

The interface 'Core Services Management' MUST support an operation 'ReceiveManagementContent' that receives external management traffic for further processing.

Requirement ID: [SRS-6-61]

The operation 'ReceiveManagementContent' MUST support Transport Layer Security (TLS, [IETF RFC 8446, 2018]).

Requirement ID: [SRS-6-62]

The operation 'ReceiveManagementContent' MUST support the Secure Shell Protocol (SSH) [IETF RFC 4251, 2006].

Requirement ID: [SRS-6-63]

The operation 'ReceiveManagementContent' MUST support the invocation of the operations 'Verify' (6.6.2.2.3) and 'Decrypt' (6.6.2.2.5) at the interface 'Public Key Cryptographic Services' ([SRS-6-239]) provided by WG_PKCS (6.6.2.1).

Requirement ID: [SRS-6-64]

The operation 'ReceiveManagementContent' SHALL pass management content in the form of a management message to the appropriate interface offered by WG_MGMT ([SRS-6-252]) for further processing.

6.4.5.3 ForwardManagementContent

Requirement ID: [SRS-6-65]

The interface 'Core Services Management' MUST support an operation 'ForwardManagementContent' that accepts outgoing management messages for further processing.

Requirement ID: [SRS-6-66]

After receiving a management message from one of the interfaces offered by WG_MGMT ([SRS-6-252]), the operation 'ForwardManagementContent' SHALL forward the management message, as payload of the appropriate management protocol, to the management domain.

Requirement ID: [SRS-6-67]

The operation 'ForwardManagementContent' MUST support Transport Layer Security (TLS, [IETF RFC 8446, 2018]).

Requirement ID: [SRS-6-68]

The operation 'ForwardManagementContent' MUST support the Secure Shell Protocol (SSH) [IETF RFC 4251, 2006].

Requirement ID: [SRS-6-69]

The operation 'ForwardManagementContent' MUST support the invocation of the operation 'Encrypt' (6.6.2.2.4) at the interface 'Public Key Cryptographic Services' ([SRS-6-239]) provided by WG_PKCS (6.6.2.1).

6.5 Protection Policy Enforcement Services

6.5.1 Information Flow Control Policy (IFP) Enforcement

6.5.1.1 WG_IFCPE

Requirement ID: [SRS-6-70]

The WG MUST provide an information flow control policy enforcement (IFCPE) capability WG_IFCPE that enables the WG to:

- Mediate the flow of information between WG_IF_NET_HIGH and WG_IF_NET_LOW in accordance with the WG information flow policy WG_IFP;
- Control incoming and outgoing management traffic at WG_IF_MGMT in accordance with the WG information flow policy WG_IFP.

Requirement ID: [SRS-6-71]

The design of WG_IFCPE SHALL be such that the enforcement of policies WG_CIP_LH_LV and WG_CIP_HL_SV can be supported (see 6.2.4).

6.5.1.2 IFCPE Services High to Low

Requirement ID: [SRS-6-72]

For the flow of information from WG_IF_NET_HIGH to WG_IF_NET_LOW, WG_IFCPE MUST offer an interface 'IFCPE Services High to Low' that accepts information for further processing.

6.5.1.2.1 Enforce HL Communications IFCPE

Requirement ID: [SRS-6-73]

The interface 'IFCPE Services High to Low' MUST support an operation 'Enforce HL Communications IFCPE' that enforces the policy WG_IFP_CA_HL.

Requirement ID: [SRS-6-74]

The operation 'Enforce HL Communications IFCPE' SHALL enforce the policy WG_IFP_CA_HL_IN on the following information flow:

- Source: Communications Access Services HL Interface -> ReceiveInternalNetworkHL;
- Destination: SOA Platform Services HL Interface -> ReceiveWebContentHL;
- Information: HTTP(S) traffic;

- Operation: pass HTTP(S) traffic by ensuring the following conditions:
    - WG_IFP_CA_HL_IN permits information flow.

Requirement ID: [SRS-6-75]

The operation 'Enforce HL Communications IFCPE' SHALL enforce the policy WG_IFP_CA_HL_OUT on the following information flow:

- Source: SOA Platform HL Interface -> ForwardWebContentHL;
- Destination: Communications Access Services HL Interface -> ForwardNetworkHL;
- Information: HTTP(S) traffic;
- Operation: pass HTTP(S) traffic by ensuring the following conditions:
    - WG_IFP_CA_HL_OUT permits information flow.

Requirement ID: [SRS-6-500]

If WG_IFP_CA_HL_IN or WG_IFP_CA_HL_OUT do not permit information flow, the WG SHALL execute the actions specified in WG_IFP_CA_HL.

Requirement ID: [SRS-6-76]

For every action taken, the operation 'Enforce HL Communications IFCPE' SHALL invoke the operation 'Log' 6.7.7.1.1) at the interface 'Event Management' (6.7.7.1) and log the action.

Requirement ID: [SRS-6-77]

If WG_IFP_CA_HL does not permit the release of information due to a policy violation, the WG SHALL invoke the operation 'Log' (6.7.7.1.1) at the interface 'Event Management' (6.7.7.1) and log the outcome O_WG_IFCPE (6.6.2.4).

Requirement ID: [SRS-6-78]

The WG SHALL ensure that no illicit information flows exist to circumvent the enforcement of WG_IFP_CA_HL

6.5.1.2.2 Enforce HL SOA Platform IFCPE

Requirement ID: [SRS-6-79]

The interface 'IFCPE Services High to Low' MUST support an operation 'Enforce HL SOA Platform IFCPE' that enforces the policy WG_IFP_SOA_HL.

Requirement ID: [SRS-6-80]

Prior to enforcing WG_IFP_SOA_HL, WG_IFCPE SHALL completely reassemble all chunks of an HTTP message-body that was received with chunked transfer encoding.

Requirement ID: [SRS-6-81]

The operation 'Enforce HL SOA Platform IFCPE' SHALL enforce the policy WG_IFP_SOA_HL on the following information flow:

- Source: SOA Platform Services HL Interface->ReceiveWebContentHL;
- Destination: SOA Platform Services HL Interface >ForwardWebContentHL;
- Information: HTTP Messages;
- Operation: pass HTTP Messages from source to destination ensuring the following conditions:
  - the HTTP Message has been processed by the WG content inspection policy enforcement capability WG_CIPE (6.5.3.1) based on the content inspection policy WG_CIP_HL ([SRS-6-144]);
  - Based on the outcome of processing by WG_CIPE, WG_IFP_SOA_HL permits the release of the HTTP Message to the low domain.
  - In case of an HTTP response message, pass message only if it was preceded by an HTTP request message that was passed as part of the enforcement of WG_IFP_SOA_LH ([SRS-6-97]).

Requirement ID: [SRS-6-82]

The operation 'Enforce HL SOA Platform IFCPE' MUST support the invocation of the operation 'Enforce HL SOA CIPE' at the interface 'CIPE Services High to Low' (6.5.3.2). The operation 'Enforce HL SOA CIPE' SHALL take as input:

- The HTTP message that is being processed;
- The policy WG_CIP_HL.

Requirement ID: [SRS-6-83]

If WG_IFP_SOA_HL does not permit the release of information, the WG SHALL execute the actions specified in WG_IFP_SOA_HL.

Requirement ID: [SRS-6-84]

For every action taken, the operation 'Enforce HL SOA Platform IFCPE' SHALL invoke the operation 'Log' (6.7.7.1.1) at the interface 'Event Management' ([SRS-6-342]) and log the action.

Requirement ID: [SRS-6-85]

If WG_IFP_SOA_HL does not permit the release of information due to a policy violation, the WG SHALL invoke the operation 'Log' (6.7.7.1.1) at the interface 'Event Management' ([SRS-6-342]) and log the outcome O_WG_IFCPE ([SRS-6-115]).

Requirement ID: [SRS-6-86]

The WG SHALL ensure that no illicit information flows exist to circumvent the enforcement of WG_IFP_SOA_HL.

6.5.1.3 IFCPE Services Low to High

Requirement ID: [SRS-6-87]

For the flow of information from WG_IF_NET_LOW to WG_IF_NET_HIGH, WG_IFCPE MUST offer an interface 'IFCPE Services Low to High' that accepts information for further processing.

6.5.1.3.1 Enforce LH Communications IFCPE

Requirement ID: [SRS-6-88]

The interface 'IFCPE Services Low to High' MUST support an operation 'Enforce LH Communications IFCPE' that enforces the policy WG_IFP_CA_LH.

Requirement ID: [SRS-6-89]

The operation 'Enforce LH Communications IFCPE' SHOULD enforce the policy WG_IFP_CA_LH_IN on the following information flow:

- Source: Communications Access Services LH Interface -> ReceiveInternalNetworkLH;
- Destination: SOA Platform Services LH Interface -> ReceiveWebContentLH;
- Information: HTTP(S) traffic;
- Operation: pass HTTP(S) traffic by ensuring the following conditions:
  - WG_IFP_CA_LH_IN permits information flow.

Requirement ID: [SRS-6-90]

The operation 'Enforce LH Communications IFCPE' SHOULD enforce the policy WG_IFP_CA_LH_OUT on the following information flow:

- Source: SOA Platform LH Interface -> ForwardWebContentLH;
- Destination: Communications Access Services LH Interface -> ForwardNetworkLH;
- Information: HTTP(S) traffic;
- Operation: pass HTTP(S) traffic by ensuring the following conditions:
  - WG_IFP_CA_LH_OUT permits information flow.

Requirement ID: [SRS-6-91]

If WG_IFP_CA_LH_IN or WG_IFP_CA_LH_OUT do not permit information flow, the WG SHALL execute the actions specified in WG_IFP_CA_LH.

Requirement ID: [SRS-6-92]

For every action taken, the operation 'Enforce LH Communications IFCPE' SHALL invoke the operation 'Log' (6.7.7.1.1) at the interface 'Event Management' ([SRS-6-342]) and log the action.

Requirement ID: [SRS-6-93]

If WG_IFP_CA_LH does not permit the release of information due to a policy violation, the WG SHALL invoke the operation 'Log' (6.7.7.1.1) at the interface 'Event Management' ([SRS-6-342]) and log the outcome O_WG_IFCPE ([SRS-6-115]).

Requirement ID: [SRS-6-94]

The WG SHALL ensure that no illicit information flows exist to circumvent the enforcement of WG_IFP_CA_LH.

6.5.1.3.2 Enforce LH SOA Platform IFCPE

Requirement ID: [SRS-6-95]

The interface 'IFCPE Services Low to High' MUST support an operation 'Enforce LH SOA Platform IFCPE' that enforces the policy WG_IFP_SOA_LH.

Requirement ID: [SRS-6-96]

Prior to enforcing WG_IFP_SOA_LH, WG_IFCPE SHALL completely reassemble all chunks of an HTTP message-body that was received with chunked transfer encoding.

Requirement ID: [SRS-6-97]

The operation 'Enforce LH SOA Platform IFCPE' SHALL enforce the policy WG_IFP_SOA_LH on the following information flow:

- Source: SOA Platform Services LH Interface->ReceiveWebContentLH;
- Destination: SOA Platform Services LH Interface >ForwardWebContentLH;
- Information: HTTP Messages;
- Operation: pass HTTP Messages from source to destination ensuring the following conditions:
  - the HTTP Message has been processed by the WG content inspection policy enforcement capability WG_CIPE (6.5.3.1) based on the content inspection policy WG_CIP_LH ([SRS-6-151]).
  - Based on the outcome of processing by WG_CIPE, WG_IFP_SOA_LH permits the import of the HTTP Message to the high domain.
  - In case of an HTTP response message, pass message only if it was preceded by an HTTP request message that was passed as part of the enforcement of WG_IFP_SOA_HL ([SRS-6-81]).

Requirement ID: [SRS-6-98]

The operation 'Enforce LH SOA Platform IFCPE' MUST support the invocation of the operation 'Enforce LH SOA CIPE' at the interface 'CIPE Services Low to High' (6.5.3.2). The operation 'Enforce LH SOA CIPE' SHALL take as input:

- The HTTP message that is being processed;
- The policy WG_CIP_LH.

Requirement ID: [SRS-6-99]

If WG_IFP_SOA_LH does not permit the release of information, the WG SHALL execute the actions specified in WG_IFP_SOA_LH.

Requirement ID: [SRS-6-100]

For every action taken, the operation 'Enforce LH SOA Platform IFCPE' SHALL invoke the operation 'Log' (6.7.7.1.1) at the interface 'Event Management' ([SRS-6-342]) and log the action.

Requirement ID: [SRS-6-101]

If WG_IFP_SOA_LH does not permit the release of information due to a policy violation, the WG SHALL invoke the operation 'Log' (6.7.7.1.1) at the interface 'Event Management' ([SRS-6-342]) and log the outcome O_WG_IFCPE ([SRS-6-115]).

Requirement ID: [SRS-6-102]

The WG SHALL ensure that no illicit information flows exist to circumvent the enforcement of WG_IFP_SOA_LH.

6.5.1.4 IFCPE Services Management

Requirement ID: [SRS-6-103]

For incoming and outgoing management traffic at WG_IF_MGMT, WG_IFCPE MUST offer an interface 'IFCPE Services Management' that accepts information for further processing.

6.5.1.4.1 Enforce Management Communications IFCPE

Requirement ID: [SRS-6-104]

The interface 'IFCPE Services Management' MUST support an operation 'Enforce Management Communications IFCPE' that enforces the policy WG_IFP_MGMT.

Requirement ID: [SRS-6-105]

The operation 'Enforce Management Communications IFCPE' SHOULD enforce the policy WG_IFP_MGMT_IN on the following information flow:

- Source: Communications Access Services Management Interface -> ReceiveNetworkManagement
- Destination: Core Services Management Interface -> ReceiveManagementContent
- Information: Management traffic.
- Operation: pass management traffic by ensuring the following conditions:
    - WG_IFP_MGMT_IN permits information flow.

Requirement ID: [SRS-6-106]

The operation 'Enforce Management Communications IFCPE' SHOULD enforce the policy WG_IFP_MGMT_OUT on the following information flow:

- Source: Core Services Management Interface -> ForwardManagementContent
- Destination: Communications Access Services Management Interface -> ForwardNetworkManagement
- Information: Management traffic.
- Operation: pass management traffic by ensuring the following conditions:
    - WG_IFP_MGMT_OUT permits information flow.

Requirement ID: [SRS-6-107]

If WG_IFP_MGMT_IN or WG_IFP_MGMT_OUT do not permit information flow, the WG SHALL execute the action specified in WG_IFP_MGMT.

Requirement ID: [SRS-6-108]

For every action taken, the operation 'Enforce Management Communications IFCPE' SHALL invoke the operation 'Log' (6.7.7.1.1) at the interface 'Event Management' ([SRS-6-342]) and log the action.

Requirement ID: [SRS-6-109]

If WG_IFP_MGMT does not permit the release of information due to a policy violation, the WG SHALL invoke the operation 'Log' (6.7.7.1.1) at the interface 'Event Management' ([SRS-6-342]) and log the outcome O_WG_IFCPE ([SRS-6-115]).

Requirement ID: [SRS-6-110]

The WG SHALL ensure that no illicit information flows exist to circumvent the enforcement of WG_IFP_MGMT.

6.5.2 Information flow control policies

Requirement ID: [SRS-6-111]

WG_IFP SHALL be configurable.

Requirement ID: [SRS-6-112]

WG_IFP SHALL specify the actions ACTIONS that need to be executed by WG_IFCPE.

Requirement ID: [SRS-6-113]

For each action in ACTIONS it SHALL be possible to:

- Enable or disable the action.
- Instruct WG_IFCPE to ignore the outcome of the execution of the action.
- If the outcome O_WG_IFCPE of the execution of the action is negative (e.g. verification or validation fails, or a policy violation was determined): instruct WG_IFCPE to continue the enforcement of WG_IFP, or to stop.

Requirement ID: [SRS-6-114]

It SHALL be possible to enable or disable the enforcement of each of the following sub-policies:

- WG_IFP_CA_LH_IN;
- WG_IFP_CA_LH_OUT;
- WG_IFP_CA_HL_IN;
- WG_IFP_CA_HL_OUT;
- WG_IFP_MGMT_IN;
- WG_IFP_MGMT_OUT;
- WG_IFP_SOA_LH;
- WG_IFP_SOA_HL.

Requirement ID: [SRS-6-115]

WG_IFP SHALL specify the level of granularity of the outcome O_WG_IFCPE. It SHALL be possible for WG_IFCPE to distinguish within O_WG_IFCPE:

- The sub-policy ([SRS-6-114]) that was enforced when a policy violation was determined;
- Identification of the action that led to the policy violation;
- Reason for policy violation.

Requirement ID: [SRS-6-116]

The policies WG_IFP_CA_HL, WG_IFP_CA_LH and WG_IFP_MGMT SHALL specify:

- That an information flow (as described in 6.5.1.2.2, 6.5.1.3.2 and 6.5.1.4.2 respectively) is not permitted if the outcome O_WG_IFCPE constitutes a policy violation;
- The action the WG shall take in case information flow is not permitted. The possible actions SHALL include:
  - Silently drop traffic;
  - Reset the TCP/IP connection.

Requirement ID: [SRS-6-117]

The policy WG_IFP_CA_HL_IN SHALL specify the actions ACTIONS_WG_CA_HL_IN that the operation 'Enforce HL Communications IFCPE' SHALL execute for the information flow described in ([SRS-6-74]).

Requirement ID: [SRS-6-118]

ACTIONS_WG_CA_HL_IN SHALL include the following actions:

- Filter traffic based on the ruleset RULESET_WG_IFCPE-CA_HL_IN.

Requirement ID: [SRS-6-119]

The policy WG_IFP_CA_HL_OUT SHALL specify the actions ACTIONS_WG_CA_HL_OUT that the operation 'Enforce HL Communications IFCPE' SHALL execute for the information flow described in ([SRS-6-75]).

Requirement ID: [SRS-6-120]

ACTIONS_WG_CA_HL_OUT SHALL include the following actions:

- Filter traffic based on the ruleset RULESET_WG_IFCPE-CA_HL_OUT.

Requirement ID: [SRS-6-121]

The policy WG_IFP_CA_LH_IN SHALL specify the actions ACTIONS_WG_CA_LH_IN that the operation 'Enforce LH Communications IFCPE' SHALL execute for the information flow described in ([SRS-6-89]).

Requirement ID: [SRS-6-122]

ACTIONS_WG_CA_LH_IN SHALL include the following actions:

- Filter traffic based on the ruleset RULESET_WG_IFCPE-CA_LH_IN.

Requirement ID: [SRS-6-123]

The policy WG_IFP_CA_LH_OUT SHALL specify the actions ACTIONS_WG_CA_LH_OUT that the operation 'Enforce LH Communications IFCPE' SHALL execute for the information flow described in ([SRS-6-90]).

Requirement ID: [SRS-6-124]

ACTIONS_WG_CA_LH_OUT SHALL include the following actions:

- Filter traffic based on the ruleset RULESET_WG_IFCPE-CA_LH_OUT.

Requirement ID: [SRS-6-125]

The policy WG_IFP_MGMT_IN SHALL specify the actions ACTIONS_WG_MGMT_IN that the operation 'Enforce Management Communications IFCPE' SHALL execute for the information flow described in [SRS-6-105].

Requirement ID: [SRS-6-126]

ACTIONS_WG_MGMT_IN SHALL include the following actions:

- Filter traffic based on the ruleset RULESET_WG_IFCPE-MGT_IN.

Requirement ID: [SRS-6-127]

The policy WG_IFP_MGMT_OUT SHALL specify the actions ACTIONS_WG_MGMT_OUT that the operation 'Enforce Management Communications IFCPE' SHALL execute for the information flow described in [SRS-6-106].

Requirement ID: [SRS-6-128]

ACTIONS_WG_MGMT_OUT SHALL include the following actions:

- Filter traffic based on the ruleset RULESET_WG_IFCPE-MGT_OUT.

Requirement ID: [SRS-6-129]

The policy WG_IFP_CA_HL SHALL specify RULESET_WG_IFCPE-CA_HL_IN and RULESET_WG_IFCPE-CA_HL_OUT.

Requirement ID: [SRS-6-130]

RULESET_WG_IFCPE-CA_HL_IN and RULESET_WG_IFCPE-CA_HL_OUT SHALL be configurable.

Requirement ID: [SRS-6-131]

The policy WG_IFP_CA_LH SHALL specify RULESET_WG_IFCPE-CA_LH_IN and RULESET_WG_IFCPE-CA_LH_OUT.

Requirement ID: [SRS-6-132]

RULESET_WG_IFCPE-CA_LH_IN and RULESET_WG_IFCPE-CA_LH_OUT SHALL be configurable.

Requirement ID: [SRS-6-133]

The policy WG_IFP_MGMT SHALL specify RULESET_WG_IFCPE-MGT_IN and RULESET_WG_IFCPE-MGT_OUT.

Requirement ID: [SRS-6-134]

RULESET_WG_IFCPE-MGT_IN and RULESET_WG_IFCPE-MGT_OUT SHALL be configurable.

Requirement ID: [SRS-6-135]

Each of the rulesets RULESET_WG_IFCPE-CA_HL_IN, RULESET_WG_IFCPE-CA_HL_OUT, RULESET_WG_IFCPE-CA_LH_IN, RULESET_WG_IFCPE-CA_LH_OUT, RULESET_WG_IFCPE-MGT_IN, RULESET_WG_IFCPE-MGT_OUT SHALL include:

- Identification of traffic flow that is allowed or disallowed based on source and destination IP addresses;
- Identification of traffic that is allowed or disallowed based on protocols and ports;
- Identification of traffic that is allowed or disallowed based on values of protocol fields.

Requirement ID: [SRS-6-136]

The policy WG_IFP_SOA_HL SHALL specify:

- That a release of information to the low domain is not permitted if O_WG_CIPE_HL ([SRS-6-148]) constitutes a policy violation;

- The action the WG shall take in case of a policy violation, see [SRS-6-138].

Requirement ID: [SRS-6-137]

The policy WG_IFP_SOA_LH SHALL specify:

- That an import of information to the high domain is not permitted if O_WG_CIPE_LH ([SRS-6-155]) constitutes a policy violation;
- The action the WG shall take in case of a policy violation, see [SRS-6-138].

Requirement ID: [SRS-6-138]

The policies WG_IFP_SOA_HL and WG_IFP_SOA_LH SHALL specify the action the WG shall take in case of a policy violation. The possible actions SHALL include:

- Silently drop traffic;
- Send an HTTP error response of a specific type;
  - The type of HTTP error message SHALL be configurable.
- Send a custom HTTP error message;
  - The contents of the custom HTTP error message SHALL be configurable.
  - It SHALL be possible to include the items in [SRS-6-163].

6.5.3 Content Inspection Policy (CIP) Enforcement

6.5.3.1 WG_CIPE

Requirement ID: [SRS-6-139]

The WG MUST provide a content inspection policy enforcement (CIPE) capability WG_CIPE that enables the WG to manage and schedule the routing of content through content filters (by WG_CIS ([SRS-6-190])) in accordance with the WG content inspection policy WG_CIP.

Requirement ID: [SRS-6-140]

The design and functionality of WG_CIPE MUST conform to the NATO CIPE functional specification in [NC3A TN-1486, 2012].

Requirement ID: [SRS-6-141]

WG_CIPE SHALL ensure that no illicit information flows exist to circumvent the enforcement of WG_CIP.

Requirement ID: [SRS-6-142]

WG_CIPE SHALL ensure that enforcement actions are executed in the order as specified in WG_CIP ([SRS-6-159]).

6.5.3.2 CIPE Services High to Low

Requirement ID: [SRS-6-143]

For the flow of information from WG_IF_NET_HIGH to WG_IF_NET_LOW, WG_CIPE MUST offer an interface 'CIPE Services High to Low' that accepts information for further processing.

6.5.3.2.1 Enforce HL SOA CIPE

Requirement ID: [SRS-6-144]

The interface 'CIPE Services High to Low' MUST support an operation 'Enforce HL SOA CIPE' that enforces the policy WG_CIP_HL.

Requirement ID: [SRS-6-145]

The operation 'Enforce HL SOA CIPE' MUST support the invocation of the following operations at the interface 'Content Inspection Services' ([SRS-6-194]) provided by WG_CIS ([SRS-6-190]):

- Operation ‘Initialize’ ([SRS-6-199]) that takes as input an identifier CIPE_CF_ID that identifies a content filter in WG_CIS;
- Operation ‘Filter’ ([SRS-6-201]) that takes as input a data object CIPE_DATA and a set of rules CIPE_DATA_RULES for processing CIPE_DATA;
- Operation ‘Halt’ ([SRS-6-203]) that takes as input an attribute CIPE_CF_ID that identifies a content filter in WG_CIS.

Requirement ID: [SRS-6-146]

WG_CIPE SHALL determine CIPE_CF_ID, CIPE_DATA and CIPE_DATA_RULES based on the policy WG_CIP_HL.

Requirement ID: [SRS-6-147]

For every action taken, the operation 'Enforce HL SOA CIPE' SHALL invoke the operation 'Log' (6.7.7.1.1) at the interface 'Event Management' ([SRS-6-342]) and log the action.

Requirement ID: [SRS-6-148]

WG_CIPE SHALL inform WG_IFCPE of the outcome O_WG_CIPE_HL of the enforcement of WG_CIP_HL based on WG_CIP ([SRS-6-163]).

Requirement ID: [SRS-6-149]

WG_CIPE SHALL invoke the operation 'Log' (6.7.7.1.1) at the interface 'Event Management' ([SRS-6-342]) and log O_WG_CIPE_HL.

6.5.3.3 CIPE Services Low to High

Requirement ID: [SRS-6-150]

For the flow of information from WG_IF_NET_LOW to WG_IF_NET_HIGH, WG_CIPE MUST offer an interface 'CIPE Services Low to High' that accepts information for further processing.

6.5.3.3.1 Enforce LH SOA CIPE

Requirement ID: [SRS-6-151]

The interface 'CIPE Services Low to High' MUST support an operation 'Enforce LH SOA CIPE' that enforces the policy WG_CIP_LH.

Requirement ID: [SRS-6-152]

The operation 'Enforce LH SOA CIPE' MUST support the invocation of the following operations at the interface 'Content Inspection Services' ([SRS-6-194]) provided by WG_CIS ([SRS-6-190]):

- Operation ‘Initialize’ ([SRS-6-199]) that takes as input an identifier CIPE_CF_ID that identifies a content filter in WG_CIS;
- Operation ‘Filter’ ([SRS-6-201]) that takes as input a data object CIPE_DATA and a set of rules CIPE_DATA_RULES for processing CIPE_DATA;
- Operation ‘Halt’ ([SRS-6-203]) that takes as input an attribute CIPE_CF_ID that identifies a content filter in WG_CIS.

Requirement ID: [SRS-6-153]

WG_CIPE SHALL determine CIPE_CF_ID, CIPE_DATA and CIPE_DATA_RULES based on the policy WG_CIP_LH.

Requirement ID: [SRS-6-154]

For every action taken, the operation 'Enforce LH SOA CIPE' SHALL invoke the operation 'Log' (6.7.7.1.1) at the interface 'Event Management' ([SRS-6-342]) and log the action.

Requirement ID: [SRS-6-155]

WG_CIPE SHALL inform WG_IFCPE of the outcome O_WG_CIPE_LH of the enforcement of WG_CIP_LH based on WG_CIP ([SRS-6-163]).

Requirement ID: [SRS-6-156]

WG_CIPE SHALL invoke the operation 'Log' (6.7.7.1.1) at the interface 'Event Management' ([SRS-6-342]) and log O_WG_CIPE_LH.

6.5.4 Content inspection policies

Requirement ID: [SRS-6-157]

WG_CIP SHALL be configurable.

Requirement ID: [SRS-6-158]

WG_CIP SHALL specify the actions ACTIONS that need to be executed by WG_CIS.

Requirement ID: [SRS-6-159]

WG_CIP SHALL specify the order in which ACTIONS need to be executed.

Requirement ID: [SRS-6-160]

For each action in ACTIONS it SHALL be possible to:

- Enable or disable the action.
- Instruct WG_CIPE to ignore the outcome of the execution of the action by WG_CIS (as received from WG_CIS ([SRS-6-206])).
- If the outcome of the execution of the action by WG_CIS is a policy violation: instruct WG_CIPE to continue the enforcement of WG_CIP, or to stop.

Requirement ID: [SRS-6-161]

It SHALL be possible to group ACTIONS per the following sub-policies:

- WG_CIP_LH_SV;
- WG_CIP_LH_HV;
- WG_CIP_LH_MD;
- WG_CIP_HL_HV;
- WG_CIP_HL_LV.

Requirement ID: [SRS-6-162]

It SHALL be possible to enable or disable the enforcement of each sub-policy in ([SRS-6-161]).

Requirement ID: [SRS-6-163]

WG_CIP SHALL specify the level of granularity of the outcomes O_WG_CIS ([SRS-6-205]), O_WG_CIPE_HL ([SRS-6-148]) and O_WG_CIPE_LH ([SRS-6-155]). It SHALL be possible for WG_CIS to distinguish within O_WG_CIS, O_WG_CIPE_HL and O_WG_CIPE_LH:

- The WG_CIS capability that determined a policy violation (WG_CIS_SV ([SRS-6-208]), WG_CIS_HV ([SRS-6-213]), WG_CIS_LV ([SRS-6-219]), and WG_CIS_MD ([SRS-6-508]);
- Identification CIPE_CF_ID of the content filter that determined the policy violation;
- Identification of the action that led to policy violation;
- Reason for policy violation.

Requirement ID: [SRS-6-164]

The policy WG_CIP_LH_SV SHALL specify the actions ACTIONS_WG_LH_SV that need to be performed by WG_CIS_SV.

Requirement ID: [SRS-6-165]

ACTIONS_WG_LH_SV SHALL include the following actions:

- Check the HTTP message body for XML well-formedness;
- Validate the HTTP message body against a list of W3C XML Schemas LIST_WG_CIS_SV-XS;
  - Select LIST_WG_CIS_SV-XS based on the URI in the HTTP message startline.
- Check that the namespace of the root node belongs to a list of allowed namespaces LIST_WG_CIS_SV-NS;
  - Select LIST_WG_CIS_SV-NS based on the URI in the HTTP message startline.

Requirement ID: [SRS-6-166]

WG_CIP_LH_SV SHALL specify LIST_WG_CIS_SV-XS.

Requirement ID: [SRS-6-167]

LIST_WG_CIS_SV-XS SHALL be configurable.

Requirement ID: [SRS-6-168]

WG_CIP_LH_SV SHALL include the option to specify a LIST_WG_CIS_SV-XS for a given URI.

Requirement ID: [SRS-6-169]

WG_CIP_LH_SV SHALL specify LIST_WG_CIS_SV-NS.

Requirement ID: [SRS-6-170]

LIST_WG_CIS_SV-NS SHALL be configurable.

Requirement ID: [SRS-6-171]

WG_CIP_LH_SV SHALL include the option to specify a LIST_WG_CIS_SV-NS for a given URI.

Requirement ID: [SRS-6-172]

The policy WG_CIP_HL_HV SHALL specify the actions ACTIONS_WG_HL_HV that need to be performed by WG_CIS_HV.

Requirement ID: [SRS-6-173]

ACTIONS_WG_HL_HV SHALL include the following actions based on RULESET_WG_CIS_HV-HL:

- Verify the information attributes in [SRS-6-214] ;
- Add or rewrite a header line;
- Remove a header line;
- Add or rewrite a value;
- Remove a value;
- Translate a URI to another value;
- Normalize the URIs in header lines of an HTTP message (i.e. remove all unneeded or escaped characters from a URI and ensure sure all characters that require escaping are escaped).

Requirement ID: [SRS-6-174]

WG_CIP_HL_HV SHALL specify RULESET_WG_CIS_HV-HL.

Requirement ID: [SRS-6-175]

RULESET_WG_CIS_HV-HL SHALL be configurable.

Requirement ID: [SRS-6-176]

The policy WG_CIP_LH_HV SHALL specify the actions ACTIONS_WG_LH_HV that need to be performed by WG_CIS_HV.

Requirement ID: [SRS-6-177]

ACTIONS_WG_LH_HV SHALL include the following actions based on RULESET_WG_CIS_HV-LH:

- Verify the information attributes in [SRS-6-214] ;
- Add or rewrite a header line;
- Remove a header line;
- Add or rewrite a value;
- Remove a value;
- Translate a URI to another value;
- Normalize the URIs in header lines of an HTTP message (i.e. remove all unneeded or escaped characters from a URI and ensure sure all characters that require escaping are escaped).

Requirement ID: [SRS-6-178]

WG_CIP_LH_HV SHALL specify RULESET_WG_CIS_HV-LH.

Requirement ID: [SRS-6-179]

RULESET_WG_CIS_HV-LH SHALL be configurable.

Requirement ID: [SRS-6-180]

Each of the rulesets RULESET_WG_CIS_HV-HL and RULESET_WG_CIS_HV-LH SHALL include:

- Whitelist of allowed values for the information attributes in [SRS-6-214] ;
- Whitelist of allowed header lines;

- Header lines that shall be present in the message header;
- Header lines that shall not be present in the message header;
- Rules on the start line:
  - Format MUST be according to [IETF RFC 7230, 2014], or [IETF RFC 7540, 2014], depending on the version;
  - Allowed values for the scheme;
  - Allowed values for HTTP version;
  - All case-insensitive parts MUST be lowercase;
  - Maximum length of URI;
  - Maximum number of arguments in URI;
  - Whitelist of allowed URIs;
  - Value to translate a given URI to;
  - Unneeded whitespace SHALL not be present;
  - Allowed values for 'Status Codes;
  - Allowed values for 'Reason String''.
- Rules on the header lines:
  - Remove headers that are not on the whitelist;
  - Remove values that are not on the whitelist;
  - Values that must be added (or rewritten) if not present;
  - Value to translate a given URI to;
  - Maximum length of header;
  - Whitelist of allowed character sets;
  - All case-insensitive parts MUST be lowercase;
  - Host header line: MUST match hostname in start-line URI;
  - Content-Length header line: value MUST be correct.

Requirement ID: [SRS-6-181]

The policy WG_CIP_HL_LV SHALL specify the actions ACTIONS_WG_HL_LV that need to be performed by WG_CIS_LV.

Requirement ID: [SRS-6-182]

ACTIONS_WG_HL_LV SHALL include the following actions:

- Verify that the syntax of the confidentiality metadata label conforms to ADatP-4774 "Confidentiality Metadata Label Syntax" [STANAG 4774];
- Verify that the binding mechanism used conforms to ADatP-4778 "Metadata Binding Mechanism" [STANAG 4778];
- Verify that the binding profile that is applied conforms to "XML Signature Cryptographic Artefact Profile" in [STANAG 4778 SRD.2];
- Validate the *BindingInformation* element (see [STANAG 4778]) against a list of W3C XML Schemas LIST_WG_CIS_LV-XS.
- Verify that the value of any *TransformAlgorithm* attribute is allowed according to a list of allowed values LIST_WG_CIS_LV-TR as specified in [STANAG 4778 SRD.2];
- Verify that the value of any *CanonicalizationMethodAlgorithm* attribute is allowed according to a list of allowed values LIST_WG_CIS_LV-CM as specified in [STANAG 4778 SRD.2];

- Verify that the value of any *DigestMethodAlgorithm* attribute is allowed according to a list LIST_WG_CIS_LV-DM as specified in [STANAG 4778 SRD.2];
- Verify that the value of any *SignatureMethodAlgorithm* attribute used for a digital signature is allowed according to a list LIST_WG_CIS_LV-SM_PKI as specified in [STANAG 4778 SRD.2];
- Verify that the value of any *SignatureMethodAlgorithm* attribute used for a keyed-hash message authentication code (HMAC) is allowed according to a list LIST_WG_CIS_LV-SM_HMAC as specified in [STANAG 4778 SRD.2];
- Check the validity of certificates against a certificate revocation list LIST_WG_CIS_LV-CRL or by using OCSP;
- Evaluate the binding according to [STANAG 4778] and [STANAG 4778 SRD.2]. Evaluation SHALL include:
    - Identify the complete set of data objects *S* that are labelled (i.e. for each data object *DO* in *S* there is a confidentiality metadata label *CL* identified that is bound to *DO*).
    - For each data object *DO* in *S*, associate the information attributes in ([SRS-6-233]) with *DO*.
- For each data object *DO* in *S*, verify the values of the information attributes in ([SRS-6-233]) against a Metadata Policy Information File (MPIF) MPIF_NATO;
- For each data object *DO* in *S*, verify that *DO* can be released to the low domain based on RULESET_WG_CIS_LV;
- Sanitize the body of the HTTP message based on RULESET_WG_CIS_LV; (Note that the rule set RULESET_WG_CIS_LV will specify whether or not data sanitization shall take place.)
- In the case of sanitization of a file for which a filename has been specified of the form <FILENAME.EXTENSION>, modify the filename to '<FILENAME-SANITIZED_STRING-TIMESTAMP.EXTENSION>' with 'SANITIZED_STRING' and 'TIMESTAMP' as defined in RULESET_WG_CIS_LV.
- Modify BindingInformation for *DO* based on RULESET_WG_CIS_LV;
- Before release of a data object *DO* to the low domain, apply a canonicalization-without-comments [W3C Canonical XML Version 1,1, 2008] transform to *DO*.

Requirement ID: [SRS-6-183]

WG_CIP_HL_LV SHALL specify the lists:

- LIST_WG_CIS_LV-XS;
- LIST_WG_CIS_LV-TR;
- LIST_WG_CIS_LV-CM;
- LIST_WG_CIS_LV-DM;
- LIST_WG_CIS_LV-SM_PKI;
- LIST_WG_CIS_LV-SM_HMAC;
- LIST_WG_CIS_LV-CRL.

Requirement ID: [SRS-6-184]

All lists in [SRS-6-183] SHALL be configurable.

Requirement ID: [SRS-6-185]

WG_CIP_HL_LV SHALL specify the metadata policy information file MPIF_NATO.

Requirement ID: [SRS-6-187]

WG_CIP_HL_LV SHALL specify RULESET_WG_CIS_LV.

Requirement ID: [SRS-6-188]

RULESET_WG_CIS_LV SHALL be configurable.

Requirement ID: [SRS-6-189]

RULESET_WG_CIS_LV SHALL specify:

- The clearance level of the low domain (based on the classification level of the low domain and the clearance levels of the actors in the low domain) in accordance with [STANAG 4774];
- One or more additional (alternative) clearance levels of the low domain, if required.
- The clearance level of the high domain (based on the classification level of the high domain and the clearance levels of the actors in the high domain);
- One or more additional (alternative) clearance levels of the high domain, if required.
- Given a data object *DO* to which a confidentiality metadata label *CL* is bound, the requirements *R* that the values of the information attributes in CL ([SRS-6-233]) must meet in order for *DO* to be releasable from the high domain to the low domain.
    - *R* SHALL be expressed in terms of values of the information attributes in *CL* ([SRS-6-233]) and values that comprise the clearance levels of the low and the high domain;
    - It SHALL be possible to express *R* in terms of a series of AND and OR statements.
- Rules for releasing a data object for which the binding is granular (as defined in [STANAG 4778]);
- Rules for releasing a data object that has an alternative confidentiality metadata label bound to it;
- Whether or not a confidentiality metadata label and associated binding information for *DO* shall be removed before release of *DO*.
- Whether or not signatures shall be removed before release of *DO*.
- Whether or not data sanitization shall be applied;
- If data sanitization shall be applied: