Nexor Sentinel 3E Filtering System
Common Criteria Security Target

connect transform protect

Bell House, Nottingham Science & Technology Park, University Boulevard, Nottingham, NG7 2RL, UK

Tel: +44 (0)115 952 0500, Fax: +44 (0) 115 952 0519, Enquiries: info@Nexor.com

NEXOR®

www.nexor.com

Copyright/Trademarks

This document is copyrighted and all rights are reserved by Nexor. The distribution and sale of this document is intended solely for use by those licensed to do so. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical including photocopying or stored on a retrieval system for any purpose other than the original use, without the express written consent of Nexor.

Copyright© Nexor Limited 2012

Nexor is a trademark of Nexor Limited

All other trademarks mentioned herein are acknowledged.

Nexor reserve the right to modify any of the information contained within this document without notice.

Document reference: NEX2764ENG v23

Last updated: 18th December 2012

Copyright Nexor Limited © 2012, All rights reserved

Contents

COPYRIGHT/TRADEMARKS ..... **I**

CONTENTS ..... **II**

TABLE OF FIGURES AND TABLES III

1 INTRODUCTION **1**

1.1 IDENTIFICATION 1

1.2 TARGET OF EVALUATION OVERVIEW 1

1.2.1 TOE Usage *1*

1.2.2 Major Security Features *2*

1.2.3 Non-TOE Hardware/Software/Firmware *2*

1.3 RELATED DOCUMENTS 3

1.4 SECURITY TARGET ORGANISATION 3

1.5 HIGH ASSURANCE MAIL GUARD 4

1.5.1 Application *4*

1.5.2 TOE Description *5*

1.5.3 Physical Scope *7*

1.5.4 Logical Scope *7*

2 COMMON CRITERIA CONFORMANCE CLAIMS **9**

3 SECURITY PROBLEM DEFINITION **10**

3.1 THREATS 10

3.2 ORGANISATIONAL SECURITY POLICIES 10

3.3 ASSUMPTIONS 11

4 OBJECTIVES **12**

4.1 SECURITY OBJECTIVES FOR THE TOE 12

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT 13

5 IT SECURITY REQUIREMENTS **14**

5.1 TOE SECURITY FUNCTIONAL REQUIREMENTS 14

5.1.1 User Data Protection (FDP) *16*

5.1.2 Identification and Authentication (FIA) *18*

5.1.3 Security Management (FMT) *19*

5.2 TOE SECURITY ASSURANCE REQUIREMENTS 20

6 TOE SUMMARY SPECIFICATION **21**

6.1 MESSAGE FILTERING 21

6.2 CONFIGURATION 22

7 RATIONALE **23**

7.1 SECURITY OBJECTIVES RATIONALE 23

7.2 SECURITY REQUIREMENTS RATIONALE 24

7.3 SECURITY ASSURANCE RATIONALE 26

8 APPENDIX – GLOSSARY OF ACRONYMS AND TERMINOLOGY **27**

Copyright Nexor Limited © 2012, All rights reserved

Table of Figures and Tables

FIGURE 1 - NEXOR SENTINEL 3.3 HIGH ASSURANCE MAIL GUARD IN ITS SINGLE-BOX APPLIANCE 1
TABLE 1 – NON-TOE HARDWARE/SOFTWARE/FIRMWARE 2
FIGURE 2 – NEXOR SENTINEL 3.3 HIGH ASSURANCE MAIL GUARD 4
TABLE 2 - PHYSICAL BOUNDARY OF THE TOE 7
TABLE 3 - THREATS 10
TABLE 4 - ORGANISATIONAL SECURITY POLICIES 10
TABLE 5 - ASSUMPTIONS 11
TABLE 6 - SECURITY OBJECTIVES FOR THE TOE 12
TABLE 7 - SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT 13
TABLE 8 - TOE SECURITY FUNCTIONAL REQUIREMENTS 15
TABLE 9 - EAL4+ ASSURANCE REQUIREMENTS 20
TABLE 10 - SECURITY OBJECTIVES RATIONALE 23
TABLE 11 - SECURITY REQUIREMENTS RATIONALE 24
TABLE 12 - SECURITY OBJECTIVES MET BY SFRS 25
TABLE 13 - ASSURANCE EVIDENCE 26

Copyright Nexor Limited © 2012, All rights reserved

1 Introduction

1.1 Identification

TOE Identification: Nexor Sentinel 3E Filtering System

ST Identification: Nexor Sentinel 3E Filtering System Security Target

ST Version: NEX2764ENG version 23

Date: 18th December 2012

ST Author: Nexor Ltd

Registration: NSCIB-CC-12-34853

Keywords: Guard, Multi-Level Security, Secure Messaging, Message Filter, Security Label and Security Target

1.2 Target of Evaluation Overview

This Security Target (ST) describes the Nexor Sentinel 3E Filtering System.

Figure 1 - Nexor Sentinel 3.3 High Assurance Mail Guard in its single-box appliance

The Target of Evaluation (TOE) is a portion of the Nexor Sentinel 3.3 high assurance mail guard, specifically the Filtering Engine, together with the Nexor Sentinel Manager Web Application and the SELinux policy which enforces the trusted path.

The high assurance mail guard is a single-box appliance designed to protect an organisation by validating that inbound and outbound electronic messages conform to the security policy of the protected domain.

1.2.1 TOE Usage

The high assurance mail guard will be delivered to the customer's site with all the software, including the TOE, installed and tested. The appliance is delivered with a Quality Checklist containing information such as default passwords and an instruction advising the customer to change the passwords as soon as possible. A CD is also shipped which will allow reinstallation of the software should it be required.

The TOE in the high assurance mail guard and the underlying secure platform ensure network separation of the connected domains by ensuring messages can only pass from one domain to the other via a trusted path. Filters are applied to the messages while on this trusted path to check whether they conform to the defined security policy. Non-conformant messages are rejected, preventing the potential damage caused by outbound data loss or data that does not meet an organisational security policy.

The TOE is used to prevent unintentional mistakes from users that violate organisational security policies.

Copyright Nexor Limited © 2012, All rights reserved

1.2.2 Major Security Features

The TOE:

- Provides the following filters that provide Security Enforcing Functions on emails:
  - Allowed attachment types
  - Prohibited words
  - Allowed security labels.
- Provides the following capabilities that are not Security Enforcing Functions on emails (outside the scope of the evaluation):
  - Virus scanning
  - Allow SMTP messages
  - Allow X.400 messages
  - Allow notifications
  - Allow delivery reports
  - Allow delivery report return of content
  - Allow signed receipt requests
  - Allow signed receipts
  - Allow Exchange public folder messages
  - Allow Exchange replication messages
  - Optionally send copies of rejected messages to a journal address
  - Optionally send rejected messages to a quarantine facility.
- Allows administrators to configure each filter.

1.2.3 Non-TOE Hardware/Software/Firmware

The TOE in its evaluated configuration requires the hardware and operating system listed in Table 1.

Component	Name and version
19” rack computer	HP ProLiant hardware that can run the OS. The DL360 range is used and the current version is G7.
Operating System	EAL4+ certified Red Hat Enterprise Linux 5 Operating System hardened using the Certifiable Linux Integration Platform (CLIP) according to the NSA guidelines: Director of Central Intelligence Directive 6/3 “Protecting Sensitive Compartmented Information within Information Systems” (DCID 6/3) Protection Level 4 (PL4). From the baseline CLIP target, packages have been removed when they are not required, such as those providing support for printing. Packages have been added where needed, for example to support X Windows or to address security vulnerabilities. SELinux policies have also been amended to provide control around the functionality of the high assurance mail guard. The initial system will be delivered with Red Hat security fixes rolled up and included. Subsequent security patches will be packaged by Nexor and should be installed by customers.
Non-TOE portions of the high assurance mail guard	Nexor Sentinel 3.3

Table 1 – Non-TOE Hardware/Software/Firmware

Copyright Nexor Limited © 2012, All rights reserved

The installation CDs include the TOE and non-TOE portions of the high assurance mail guard and the Red Hat Enterprise Linux 5 operating system. By performing the installation both the TOE and the underlying dependencies are installed and configured securely.

The high assurance mail guard delivers the following services to the TOE. The TOE can use these services to process signed and encrypted email messages.

- IETF S/MIME v3 RFC 3369 Cryptographic Message Syntax (CMS) and RFC 2634 Enhanced Security Services (ESS) specifications, to enable messages that use ESS security features, for example signed receipts, security labels, secure mail list information, and signing certificate attributes.

1.3 Related Documents

This Security Target is aligned with:

- Common Criteria (CC) Version 3.1 Release 3 (ISO/IEC 15408 Evaluation Criteria for Information Technology Security; Part 1: Introduction and general model, Part 2: Security functional requirements, and Part 3: Security assurance requirements)
- Common Methodology for Information Security Evaluation (CEM) Version 3.1 Release 3.

1.4 Security Target Organisation

The main Sections of the ST are the TOE Description, Security Problem Definition, Objectives, IT Security Requirements, TOE Summary Specification and Rationale.

Section 1.5.2, the TOE Description, provides general information about the TOE, serves as an aid to understanding its security requirements, and provides context for the ST's evaluation.

The Security Problem Definition in Section 3 describes security aspects of the environment in which the TOE is to be used and the manner in which it is to be employed. The TOE security environment includes:

a. The assets that are to be protected

b. Threats relevant to secure TOE operation

c. Organisational security policies with which the TOE must comply

d. Assumptions about the operational environment.

Section 4 contains the security objectives that reflect the stated intent of the ST. The objectives define how the TOE will counter identified threats and how it will cover identified organisational security policies and assumptions. Each security objective is categorised as being for the TOE or for the environment.

Section 5 contains the applicable Security Requirements taken from the Common Criteria, with appropriate refinements. The requirements are provided in separate subsections for the TOE and its environment. The IT security requirements are subdivided as follows:

a. TOE Security Functional Requirements

b. TOE Security Assurance Requirements.

Section 6 contains the TOE Summary Specification.

The Rationale in Section 7 presents evidence that the ST is a complete and cohesive set of requirements and that a conformant TOE would provide an effective set of IT security countermeasures within the security environment. The Rationale is in three main parts. Firstly, a Security Objectives Rationale demonstrates that the stated security objectives are traceable to all of the aspects identified in the TOE security environment and are suitable to cover them. Then, a Security Requirements Rationale demonstrates that the security requirements (TOE and environment) are traceable to the security objectives and are suitable to meet them. Finally a TOE Summary Specification Rationale summarises why all of the IT Security Functions in the TOE Summary Specification are necessary. A glossary of acronyms and terms used in the ST is provided in the Appendix (Section 8).

Copyright Nexor Limited © 2012, All rights reserved

1.5 High Assurance Mail Guard

The TOE – Nexor Sentinel 3E Filtering System – is a portion of the high assurance mail guard, specifically the Filtering Engine, together with the Nexor Sentinel Manager Web Application and the SELinux policy which enforces the trusted path.

Figure 2 depicts Nexor Sentinel 3.3 high assurance mail guard.

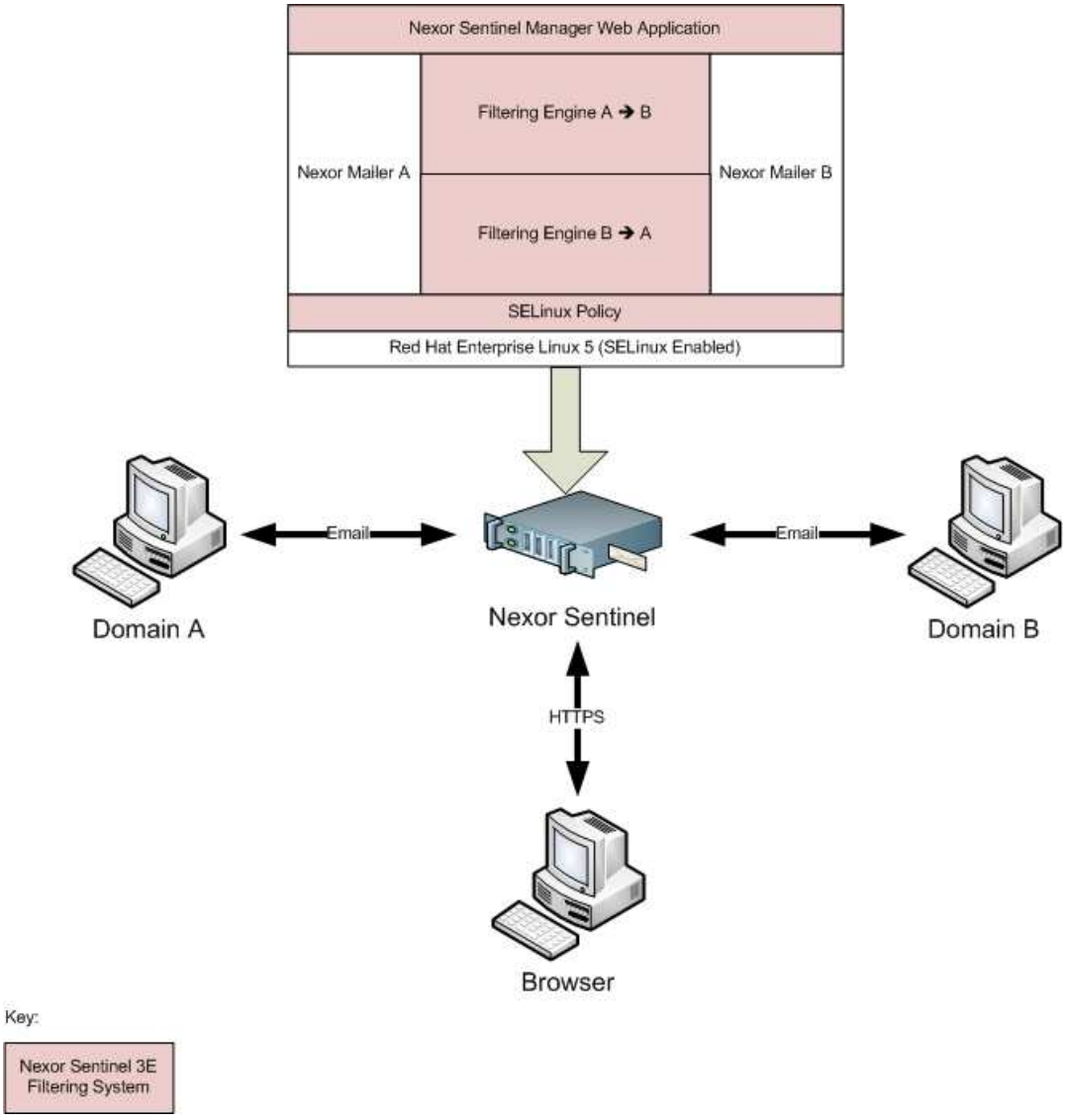

Figure 2 – Nexor Sentinel 3.3 High Assurance Mail Guard

1.5.1 Application

The high assurance mail guard on a single-box appliance is designed to protect an organisation by validating that inbound and outbound electronic messages conform to the security policy of the protected domain. The underlying secure platform ensures network separation of the connected domains by ensuring messages can only pass from one domain to the other via a trusted path. The Secure Messaging Filters are applied to the messages while on this trusted path to check whether they conform to the defined security policy. Non-conformant messages are rejected, preventing the potential damage caused by outbound data loss or data that does not meet the organisational security policy.

Copyright Nexor Limited © 2012, All rights reserved

1.5.2 TOE Description

The TOE consists of the Filtering Engine together with the Nexor Sentinel Manager Web Application and the SELinux policy which enforces the trusted path. User data is considered to be mail messages transiting the TOE and the security attributes of each mail message. The TOE supports the following message types: SMTP, X.400 (both P22 and P772) and the secure versions, Secure X.400 and Secure MIME (S/MIME). The four filters within the Filtering Engine that comprise the TSF are:

1. Dirty Word Searching Filter
2. Security Label for Domain Filter (Unstructured)
3. Security Label for Domain Filter (Structured)
4. Allowed Attachment Types Filter.

These four filters support the following security policies within the mail guard:

P.PROHIBITEDWORDS – The TSF enforces the P.PROHIBITEDWORDS security policy by not allowing Mail messages with contents[1] (including header, body and any attachments including attached messages) that exceed the threshold for prohibited words using the ASCII character set. Prohibited words will only be found if they are present as stand-alone words and not as part of longer words. The filter that implements this policy is:

- Dirty Word Searching filter

Processing of emails with attachments involves the following:

- A specific set of container file types is supported. Supported container types will be recursively handled
- All supported file types, whether extracted from a supported container type or attached directly, are converted to a textual representation of the file type. Files can contain information that is not converted and therefore not processed (e.g. pictures or embedded items)
- For the non-supported file types all printable strings are extracted
- For all file types, the extracted textual form is used in the processing.

P.LABELFILTER – The TSF enforces the P.LABELFILTER security policy by only allowing Mail messages marked at one of the configured security labels. The filters that implement this policy are:

- Security Label for Domain Filter (Unstructured)
- Security Label for Domain Filter (Structured)

Processing of emails with attachments involves the following:

- A specific set of container file types is supported. Supported container types will be recursively handled
- All supported file types, whether extracted from a supported container type or attached directly, are converted to a textual representation of the file type. Files can contain information that is not converted and therefore not processed (e.g. pictures or embedded items)
- For the non-supported file types all printable strings are extracted
- For all file types, the extracted textual form is used in the processing.

[1] Excludes envelope and email addresses

Copyright Nexor Limited © 2012, All rights reserved

P.ATTACHMENT – The TSF enforces the P.ATTACHMENT security policy by only allowing Mail messages to have an attachment if the attachment type is allowed and the attachment is identified as that type. Certain specific container file types will be expanded and further checks will be made on attachments embedded within. The filter that implements this policy is:

- Allowed Attachment Types Filter.

Processing of emails with attachments involves the following:

- A specific set of container file types is supported. Supported container types will be recursively handled
- Attachments that have been extracted from a supported container type or attached directly are used in the processing
- Attachments embedded in other attachments (except for supported container types) will not be checked.

For a detailed list of supported container file types, supported file types and supported information locations, refer to Nexor Sentinel 3E Filtering System – Operational Environment Guidance, document reference NEX2817ENG.

The configuration is used to define the security policy to be enforced. It governs which filters are to be implemented on different message types and controls the detail of the filters to be performed. For example, the configuration can define a list of prohibited words, a list of valid security labels and a list of attachment types to be permitted. As each Nexor Sentinel 3.3 high assurance mail guard can support multiple connected domains, the configuration is specific to each pair of domains.

The Nexor Sentinel Manager Web Application manages the configuration of the Sentinel 3.3 high assurance mail guard. It is accessed using HTTPS from a web browser which is on a trusted network and which can only connect to the Nexor Sentinel 3.3 high assurance mail guard. It must not be used to connect to any untrusted web servers.

Nexor Sentinel 3.3 high assurance mail guard uses the SELinux capability of Red Hat Enterprise Linux by delivering a strict SELinux policy to provide a trusted path which controls the flow of information crossing the guard.

SELinux provides mandatory access controls, checking for allowed operations on top of the standard Linux discretionary access controls. The controls are applied using a security policy that is acted on in the Linux kernel to mediate requests for access to objects. In Nexor Sentinel 3.3 high assurance mail guard, every object is labelled and type enforcement is used to ensure that only defined users or processes are allowed to access each object. This process allows the message flow to be controlled by ensuring that messages cannot be sent across the mail guard without going through the necessary steps, specifically the Filtering Engine.

Copyright Nexor Limited © 2012, All rights reserved

1.5.3 Physical Scope

The physical boundary of the TOE is shown in Table 2.

Type	Identification	Version	Media
Software	Nexor Sentinel 3E Filtering System	Version 3E[2] for NATO customers	CD[3]. Packages to be itemised in the Nexor Sentinel 3E Filtering System – Operational Environment Guidance
Software	Nexor Sentinel 3E Filtering System	Version 3E[4] for non-NATO customers	CD[5]. Packages to be itemised in the Nexor Sentinel 3E Filtering System – Operational Environment Guidance
Manual	Nexor Sentinel 3.3 Administration Guide, document reference NEX2812MAN	Version 04	PDF on Nexor Sentinel documentation CD
Manual	Nexor Sentinel 3E Filtering System – Operational Environment Guidance, document reference NEX2817ENG	Version 10	PDF on Nexor Sentinel documentation CD
Manual	Nexor Sentinel 3E Filtering System-TOE Identification, document reference NEX2814ENG	Version 16	PDF on Nexor Sentinel documentation CD
Letter	Sentinel 3 Delivery Customer Letter, document reference NEX2818CON		Paper as part of delivery
Letter	NSENT3CCC Customer Sentinel 3.30 Seals Check	Version 01	Email

Table 2 - Physical Boundary of the TOE

1.5.4 Logical Scope

The major security features of the TOE are

- Filtering Engine, including four filters:
  - Dirty Word Searching Filter

[2] This version number is also part of the identification
[3] There are two versions of the CD package. The CDs for NATO customers contain 3 versions of the label filter libraries. These libraries provide support for different unstructured security label grammars.
[4] This version number is also part of the identification
[5] There are two versions of the CD package. The CDs for non-NATO customers contain 2 versions of the label filter libraries. These libraries provide support for different unstructured security label grammars.

Copyright Nexor Limited © 2012, All rights reserved

  - Security Label for Domain Filter (Unstructured)
  - Security Label for Domain Filter (Structured)
  - Allowed Attachment Types Filter.
- Nexor Sentinel Manager Web Application with which the contents of the filters can be defined and the flow direction between two domains can be set
- The identification and authentication of the Nexor Sentinel Manager Web Application administrator user.

Copyright Nexor Limited © 2012, All rights reserved

2 Common Criteria Conformance Claims

The TOE and the ST claim conformance with Common Criteria (CC) Version 3.1R3 (ISO/IEC 15408 Evaluation Criteria for Information Technology Security; Part 1: Introduction and general model, Part 2: Security functional requirements, and Part 3: Security assurance requirements).

The ST claims to be:

- Part 2 Conformant, and
- Part 3 Conformant.

This ST conforms to no Protection Profile.

This ST conforms to EAL4 augmented with ALC_FLR.2, and to no other packages.

Copyright Nexor Limited © 2012, All rights reserved

3 Security Problem Definition

The main purpose of the TOE is to determine whether messages are to be passed through. The TOE determines this by checking the message contents against the configuration of the TOE filters. The TOE filter configuration specifies whether messages must be passed or blocked. Only the administrator, through an HTTPS web interface, can modify the TOE filter configuration.

The assets protected by the TOE are:

- The determination of whether messages are to be passed through and the TOE filter configuration data upon which this is decided
- The identification and authentication of the administrator and the TOE configurations data against which this is checked.

3.1 Threats

Table 3 defines and describes each of the threats related to the assets identified above.

Threat	Description
T.TOO_MANY_DIRTY_WORDS	A (trusted) member of the organisation employing the TOE accidentally sends an email with contents which should not be transferred from one domain to another due to it containing too many dirty (prohibited) words using the ASCII character set, which indicates that transferring the message may be a leak of sensitive information.
T.SECURITY_LABEL	A (trusted) member of the organisation employing the TOE accidentally sends an email from one domain to another that fails to include an appropriate security label, indicating that transferring the message may be a leak of sensitive information.
T.ILLEGAL_ATTACHMENT	A (trusted) member of the organisation employing the TOE accidentally sends an email from one domain to another containing one or more attachments of a type considered a security risk.
T.AUTHENTICATE	A user who is not properly identified and authenticated as an administrator is able to make unauthorised changes to the TOE filter configuration.

Table 3 - Threats

3.2 Organisational Security Policies

Table 4 identifies the relevant organisational security policies.

Policy	Description
OSP.CONFIGURE_FILTERS	The TOE shall provide a (HTTPS based) interface that enables configuration of the filters.

Table 4 - Organisational Security Policies

Copyright Nexor Limited © 2012, All rights reserved

3.3 Assumptions

Table 5 defines and describes each of the assumptions.

Assumption	Description
Installation	
A.UNDERLYING_PLATFORM	The TOE shall be installed on Red Hat Enterprise Linux (RHEL). RHEL contains SELinux that provides the mandatory access controls that are applied using a security policy that is acted on in the Linux kernel. It is assumed that the Red Hat-supplied binaries and libraries behave correctly.
A.PHYSICAL_LOCATION	The TOE shall be installed in a physically secure location. All remote access other than via the GUI uses SSH2 which is secure, with strong passwords enforced.
A.IT-NETWORK	The TOE is connected to 2 or more network domains. The IT network employed shall be such that for messages the TOE is the only path between these network domains.
Usage	
A.MANAGEMENT_STATIONS	The TOE shall be managed by workstations that cannot connect to un-trusted HTTP(S) servers (such as on the internet). This includes any workstations that can view the TOE configuration.
A.TRUSTED_USE	For the TOE there shall be two types of TOE-deploying organisation internal users: • Those who administer the TOE • Those who send/receive messages through the TOE. It is assumed that: • both types of users are trustworthy and that they will not abuse their privileges • the users' IT equipment used for emailing is trusted.

Table 5 - Assumptions

Copyright Nexor Limited © 2012, All rights reserved

4 Objectives

4.1 Security Objectives for the TOE

Table 6 defines and describes each of the Security Objectives for the TOE.

Security Objective	Description
O.WORD_CHECKING	The TOE shall • Check the content of all messages (excluding envelope and email addresses) for the presence of a configured list of words or phrases using the ASCII character set • Not allow a message to pass through if the threshold for these words or phrases is exceeded.
O.SECURITY_LABEL	The TOE shall: • Check that each appropriate message contains a structurally valid security label and that the security label is appropriate for the message destination network • Allow only those appropriate messages with a security label that is structurally valid and appropriate for the message destination network to pass through • Check that each appropriate message contains a valid unstructured security label and that the security label is appropriate for the message destination network • Allow only those appropriate messages with an unstructured security label that is valid and appropriate for the message destination network to pass through.
O.ATTACHMENT_CHECKING	The TOE shall • Only allow messages with permitted attachment types to pass through • Only allow attachments to pass through if the claimed type of the attachment matches the detected type.
O.CONFIGURE_FILTERS	The TOE shall • Allow only an authenticated administrator to configure the filters • Use initial secure values for configuration parameters.
O.AUTHENTICATE	The TOE shall • Require an administrator to authenticate through a username and password.

Table 6 - Security Objectives for the TOE

Copyright Nexor Limited © 2012, All rights reserved

4.2 Security Objectives for the Operational Environment

Table 7 defines and describes each of the Security Objectives for the Operational Environment.

Security Objective	Objective Description
Installation	
OE.UNDERLYING_PLATFORM	The TOE shall be installed on Red Hat Enterprise Linux (RHEL). RHEL contains SELinux that provides the mandatory access controls that are applied using a security policy that is acted on in the Linux kernel. The Red Hat-supplied binaries and libraries behave correctly.
OE.PHYSICAL_LOCATION	The TOE shall be installed in a physically secure location. All remote access other than via the GUI uses SSH2 which is secure, with strong passwords enforced.
OE.IT-NETWORK	The TOE is connected to 2 or more network domains. The IT network employed shall be such that for messages the TOE is the only path between these network domains.
Usage	
OE.MANAGEMENT_STATIONS	The TOE shall be managed by workstations that cannot connect to un-trusted HTTP(S) servers (such as on the internet). This includes any workstations that can view the TOE configuration.
OE.TRUSTED_USE	For the TOE there shall be two types of TOE-deploying organisation internal users: • Those who administer the TOE • Those who send/receive messages through the TOE. It is assumed that: • both types of users are trustworthy and that they will not abuse their privileges • the users' IT equipment used for emailing is trusted.

Table 7 - Security Objectives for the Operational Environment

Copyright Nexor Limited © 2012, All rights reserved

5 IT Security Requirements

This Section defines the TOE security functional requirements and assurance requirements. All requirements are from the CC Parts 2 and 3.

The CC permits four functional component operations: assignment, iteration, refinement, and selection to be performed on functional requirements. These operations are defined in Common Criteria, Part 1, Section 4.4.1.3.2, as:

- Assignment: allows the specification of an identified parameter
- Refinement: allows the addition of details or the narrowing of requirements
- Selection: allows the specification of one or more elements from a list
- Iteration: allows a component to be used more than once with varying operations.

This ST indicates which text is affected by each of these operations in the following manner:

- Assignments and Selections specified by the ST author are in ***italicised bold text***
- Refinements are identified with ***italicised bold and underlined text***
- *Iterations* are identified with a letter "(n)". These follow the short family name and allow components to be used more than once with varying operations. “(*)” refers to all iterations of a component
- Application notes provide additional information for the reader, but do not specify requirements. Application notes are denoted by *italicised text.*

5.1 TOE Security Functional Requirements

This Section defines the TOE security functional requirements. A list of the requirements is provided in Table 8. All SFRs are from CC Part 2; there are no explicitly stated requirements. The full text of the security functional requirements is contained below. Note that all TOE security functional requirements are iterated, as indicated in the text in Table 8.

SFR Component	Description	Dependencies
FDP_IFC.1(1)	Subset information flow control – P.PROHIBITEDWORDS	FDP_IFF.1(1) Simple security attributes – P.PROHIBITEDWORDS
FDP_IFC.1(2)	Subset information flow control – P.LABELFILTER	FDP_IFF.1(2) Simple security attributes – P.LABELFILTER
FDP_IFC.1(3)	Subset information flow control – P.ATTACHMENT	FDP_IFF.1(3) Simple security attributes – P.ATTACHMENT
FDP_IFF.1(1)	Simple Security Attributes – P.PROHIBITEDWORDS	FDP_IFC.1(1) Subset information flow control – P.PROHIBITEDWORDS FMT_MSA.3(1) Static attribute initialisation – P.PROHIBITEDWORDS
FDP_IFF.1(2)	Simple Security Attributes – P.LABELFILTER	FDP_IFC.1(2) Subset information flow control – P.LABELFILTER FMT_MSA.3(2) Static attribute initialisation – P.LABELFILTER
FDP_IFF.1(3)	Simple Security Attributes – P.ATTACHMENT	FDP_IFC.1(3) Subset information flow control – P.ATTACHMENT FMT_MSA.3(3) Static attribute initialisation – P.ATTACHMENT

Copyright Nexor Limited © 2012, All rights reserved

SFR Component	Description	Dependencies
FIA_UAU.2	User authentication before any action	FIA_UID.1. FIA_UID.2 is hierarchical to FIA_UID.1
FIA_UID.2	User identification before any action	No dependencies
FMT_MSA.1	Management of security attributes	FDP_IFC.1[6] Subset information flow control FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_MSA.3(1)	Static attribute initialisation – P.PROHIBITEDWORDS	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MSA.3(2)	Static attribute initialisation – P.LABELFILTER	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MSA.3(3)	Static attribute initialisation – P.ATTACHMENT	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_SMF.1	Specification of management functions	No dependencies
FMT_SMR.1	Security roles	FIA_UID.1. FIA_UID.2 is hierarchical to FIA_UID.1

Table 8 - TOE Security Functional Requirements

The TOE/TSF supports three Information Flow Control Security Function Policies that are included in the mail guard:

P.PROHIBITEDWORDS[7] – The TSF enforces the P.PROHIBITEDWORDS security policy by not allowing Mail messages[8] with contents[9] (including header, body and any attachments including attached messages) that exceed the threshold for prohibited words using the ASCII character set. Prohibited words will only be found if they are present as stand-alone words and not as part of longer words.

Processing of emails with attachments involves the following:

- A specific set of container file types is supported. Supported container types will be recursively handled
- All supported file types, whether extracted from a supported container type or attached directly, are converted to a textual representation of the file type. Files can contain information that is not converted and therefore not processed (e.g. pictures or embedded items)
- For the non-supported file types all printable strings are extracted.

For all file types, the extracted textual form is used in the processing.

P.LABELFILTER[10] – The TSF enforces the P.LABELFILTER security policy by only allowing Mail messages[11] marked at one of the configured security labels.

[6] It is not necessary to define FDP_IFC.1 for the policy P.ACCESS_CONTROL as the policy is fully defined through its definition (see section 5.1) and its use in FMT_MSA.1. In addition: FDP_IFC.1 relates to a controlled information flow which is not applicable for P.ACCESS_CONTROL.
[7] This policy relates to the SFRs for the Dirty Word Searching filter.
[8] Mail messages that cannot be decrypted by the TOE are blocked. Mail messages with attachments that are password-protected container files (e.g. ZIP files) are blocked. The contents of encrypted attachments are ignored by the TOE.
[9] Excludes envelope and email addresses
[10] This policy relates to the SFRs for the Security Label for Domain Filters
[11] See footnote 8.

Copyright Nexor Limited © 2012, All rights reserved

Processing of emails with attachments involves the following:

- A specific set of container file types is supported. Supported container types will be recursively handled
- All supported file types, whether extracted from a supported container type or attached directly, are converted to a textual representation of the file type. Files can contain information that is not converted and therefore not processed (e.g. pictures or embedded items)
- For the non-supported file types all printable strings are extracted
- For all file types, the extracted textual form is used in the processing.

P.ATTACHMENT[12] – The TSF enforces the P.ATTACHMENT security policy by only allowing Mail messages[13] to have an attachment if the attachment type is allowed and the attachment is identified as that type. Certain specific container file types will be expanded and further checks will be made on attachments embedded within.

Processing of emails with attachments involves the following:

- A specific set of container file types is supported. Supported container types will be recursively handled
- Attachments that have been extracted from a supported container type or attached directly are used in the processing
- Attachments embedded in other attachments (except for supported container types) will not be checked.

For a detailed list of supported container file types, supported file types and supported information locations, refer to Nexor Sentinel 3E Filtering System – Operational Environment Guidance, document reference NEX2817ENG.

The TOE/TSF supports one Access Control Security Function Policy that is included in the mail guard:

P.ACCESS_CONTROL – The TSF enforces the P.ACCESS_CONTROL security policy by only allowing an administrator to configure the filters

5.1.1 User Data Protection (FDP)

FDP_IFC.1(1) Subset information flow control – P.PROHIBITEDWORDS

Hierarchical to: No other components

FDP_IFC.1.1(1) The TSF shall enforce the ***P.PROHIBITEDWORDS information flow control SFP*** on ***Subjects: mail messages; Information: message content; Operations: processing of mail messages through the TOE filters***.

Dependencies: FDP_IFF.1(1) Simple security attributes – P.PROHIBITEDWORDS

FDP_IFF.1(1) Simple security attributes – P.PROHIBITEDWORDS

Hierarchical to: No other components

FDP_IFF.1.1(1) The TSF shall enforce the ***P.PROHIBITEDWORDS information flow control SFP*** based on the following types of subject and information security attributes: ***Subjects: mail messages; Information: message content***[14] ***(including header, body and any attachments including attached messages); Security attributes of messages: message subject and content***.

[12] This policy relates to the SFRs for the Allowed Attachment Types Filter
[13] See footnote 8.
[14] Excludes envelope and email addresses

Copyright Nexor Limited © 2012, All rights reserved

FDP_IFF.1.2(1) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

1) ***The message must not exceed the threshold for prohibited words using the ASCII character set.***

FDP_IFF.1.3(1) The TSF shall enforce ***no additional rules within the P.PROHIBITEDWORDS information flow control SFP.***

FDP_IFF.1.4(1) The TSF shall explicitly authorise an information flow based on the following rules: ***the administrator can force the TOE to pass the SMTP message after it was rejected.***

FDP_IFF.1.5(1) The TSF shall explicitly deny an information flow based on the following rules: ***no additional rules within the P.PROHIBITEDWORDS information flow control SFP.***

Dependencies: FDP_IFC.1(1) Subset information flow control – P.PROHIBITEDWORDS, FMT_MSA.3(1) Static attribute initialisation – P.PROHIBITEDWORDS

FDP_IFC.1(2) Subset information flow control – P.LABELFILTER

Hierarchical to: No other components

FDP_IFC.1.1(2) The TSF shall enforce the ***P.LABELFILTER information flow control SFP*** on ***Subjects: mail messages; Information: message content; Operations: processing of mail messages through the TOE filters***.

Dependencies: FDP_IFF.1(2) Simple security attributes – P.LABELFILTER

FDP_IFF.1(2) Simple security attributes - P.LABELFILTER

Hierarchical to: No other components

FDP_IFF.1.1(2) The TSF shall enforce the ***P.LABELFILTER information flow control SFP*** based on the following types of subject and information security attributes: ***Subjects: mail messages; Information: message content; Security attributes of messages: Security Label.***

FDP_IFF.1.2(2) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

1) ***The message must contain a valid Security Label***

2) ***The Security Label defined for the message must be allowed to flow from the source network interface to the destination network interface as defined by the filter configuration.***

FDP_IFF.1.3(2) The TSF shall enforce ***no additional rules within the P.LABELFILTER information flow control SFP.***

FDP_IFF.1.4(2) The TSF shall explicitly authorise an information flow based on the following rules: ***the administrator can force the TOE to pass the SMTP message after it was rejected.***

FDP_IFF.1.5(2) The TSF shall explicitly deny an information flow based on the following rules: ***no additional rules within the P.LABELFILTER information flow control SFP.***

Dependencies: FDP_IFC.1(2) Subset information flow control – P.LABELFILTER, FMT_MSA.3(2) Static attribute initialisation – P.LABELFILTER

FDP_IFC.1(3) Subset information flow control – P.ATTACHMENT

Hierarchical to: No other components

FDP_IFC.1.1(3) The TSF shall enforce the ***P.ATTACHMENT information flow control SFP*** on ***Subjects: mail messages; Information: message content; Operations: processing of mail messages through the TOE filters***.

Dependencies: FDP_IFF.1(3) Simple security attributes – P.ATTACHMENT

FDP_IFF.1(3) Simple security attributes - P.ATTACHMENT

Hierarchical to: No other components

 Copyright Nexor Limited © 2012, All rights reserved

FDP_IFF.1.1(3) The TSF shall enforce the ***P.ATTACHMENT information flow control SFP*** based on the following types of subject and information security attributes: ***Subjects: mail messages; Information: message content; Security attributes of messages: Message Attachments type.***

FDP_IFF.1.2(3) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

1) Only attachment types that are specifically listed will be allowed. Attachment types will be identified by checking file extensions and other techniques.

FDP_IFF.1.3(3) The TSF shall enforce ***no additional rules within the P.ATTACHMENT information flow control SFP.***

FDP_IFF.1.4(3) The TSF shall explicitly authorise an information flow based on the following rules: ***the administrator can force the TOE to pass the SMTP message after it was rejected.***

FDP_IFF.1.5(3) The TSF shall explicitly deny an information flow based on the following rules: ***no additional rules within the P. ATTACHMENT information flow control SFP.***

Dependencies: FDP_IFC.1(3) Subset information flow control – P.ATTACHMENT, FMT_MSA.3(3) Static attribute initialisation – P.ATTACHMENT

5.1.2 Identification and Authentication (FIA)

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: FIA_UID.1 Timing of identification

FIA_UID.2: User identification before any action

Hierarchical to: FIA_UID.1

FIA_UID.2.1 - The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies

Copyright Nexor Limited © 2012, All rights reserved

5.1.3 Security Management (FMT)

FMT_MSA.1 Management of security attributes – P.ACCESS_CONTROL

Hierarchical to: No other components.

FMT_MSA.1.1 The TSF shall enforce the ***P.ACCESS_CONTROL access control SFP*** to restrict the ability to ***modify*** the security attributes ***filter configuration for the Dirty Word Searching Filter, the Security Label for Domain Filter (Unstructured and Structured) and the Allowed Attachment Types Filter*** to the ***administrator***.

Dependencies: FDP_IFC.1[15] Subset information flow control, FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles

FMT_MSA.3(1) Static attribute initialisation – P.PROHIBITEDWORDS

Hierarchical to: No other components.

FMT_MSA.3.1(1) The TSF shall enforce the ***P.PROHIBITEDWORDS information flow control SFP*** to provide ***restrictive*** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(1) The TSF shall allow ***no one*** to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1 Management of security attributes, FMT_SMR.1 Security roles

FMT_MSA.3(2) Static attribute initialisation – P.LABELFILTER

Hierarchical to: No other components.

FMT_MSA.3.1(2) The TSF shall enforce the ***P.LABELFILTER information flow control SFP*** to provide ***restrictive*** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(2) The TSF shall allow ***no one*** to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1 Management of security attributes, FMT_SMR.1 Security roles

FMT_MSA.3(3) Static attribute initialisation – P.ATTACHMENT

Hierarchical to: No other components.

FMT_MSA.3.1(3) The TSF shall enforce the ***P.ATTACHMENT information flow control SFP*** to provide ***restrictive*** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(3) The TSF shall allow ***no one*** to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1 Management of security attributes, FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: ***TSF configuration data management***.

Dependencies: No Dependencies

FMT_SMR.1 Security roles

Hierarchical to: No other components

FMT_SMR.1.1 The TSF shall maintain the roles ***administrator***.

[15] It is not necessary to define FDP_IFC.1 for the policy P.ACCESS_CONTROL as the policy is fully defined through its definition (see section 5.1) and its use in FMT_MSA.1. In addition: FDP_IFC.1 relates to a controlled information flow which is not applicable for P.ACCESS_CONTROL.

Copyright Nexor Limited © 2012, All rights reserved

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

5.2 TOE Security Assurance Requirements

The Security Assurance Requirements for the TOE are the assurance components of Evaluation Assurance Level 4 (EAL4) taken from Part 3 of the Common Criteria, augmented with ALC_FLR.2 (Flaw Remediation). EAL4 was selected because the TOE requires a moderate level of independently assured security and requires a thorough investigation of the TOE and its development without substantial re-engineering. ALC_FLR.2 was chosen to provide assurance in Nexor's flaw remediation process. None of the assurance components is refined. The assurance components are listed in Table 9.

Assurance Class	SAR Component	Description
Development	ADV_ARC.1	Security Architecture
	ADV_FSP.4	Functional Specification
	ADV_IMP.1	Implementation Representation
	ADV_TDS.3	TOE Design
Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures
Life Cycle Support	ALC_CMC.4	Configuration Management Capabilities
	ALC_CMS.4	Configuration Management Scope
	ALC_DEL.1	Delivery
	ALC_DVS.1	Development Security
	ALC_LCD.1	Life-Cycle Definition
	ALC_TAT.1	Tools and Techniques
	ALC_FLR.2	Flaw reporting procedures
Security Target Evaluation	ASE_CCL.1	Conformance Claims
	ASE_ECD.1	Extended Components Definition
	ASE_INT.1	ST Introduction
	ASE_OBJ.2	Security Target – Security Objectives
	ASE_REQ.2	Security Requirements
	ASE_SPD.1	Security Problem Definition
	ASE_TSS.1	TOE Summary Specification
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: high-level design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability Assessment	AVA_VAN.3	Independent vulnerability analysis

Table 9 - EAL4+ Assurance Requirements

Copyright Nexor Limited © 2012, All rights reserved

6 TOE Summary Specification

This section describes the TOE security functionality showing how each of the SFRs described in Section 5.1 TOE Security Functional Requirements above is realised.

6.1 Message Filtering

The TOE only forwards messages if those messages are allowed to pass by all of its filters (and their configuration). The TOE encompasses several filters:

- **Dirty Word Searching filter** – This filter will check each message against a modifiable list of dirty words or phrases defined as sensitive. This list can contain words or phrases using the ASCII character set, although the filter can check messages even if they have other character sets present within them. The dirty word filter carries out a case insensitive search of message contents[16] (including header, body and any attachments including attached messages) for entered words or phrases. Prohibited words will only be found if they are present as stand-alone words and not as part of longer words. Each word or phrase is weighted. When a message is scanned the weighting for the first occurrence of a word or phrase in the dirty words list is added to a cumulative total. If a word or phrase in the dirty words list occurs more than once it is not counted again. If this total exceeds a specified limit the message will be rejected. Certain specific container file types will be expanded and further checks will be made on attachments embedded within. The administrator can force the TOE to pass a rejected SMTP message.

  This realises FDP_IFC.1(1) and FDP_IFF.1(1).

- **Security Label for Domain Filter (Unstructured)** – Unstructured security labels in an appropriate message will be checked that they are cleared for the target domain, and if the check fails the message will not be allowed through the Nexor Sentinel 3E Filtering System. This filter will be applied to selected messages and attachments based on the selected configuration settings. Certain specific container file types will be expanded and further checks will be made on attachments embedded within. The administrator can force the TOE to pass a rejected SMTP message.

- **Security Label for Domain Filter (Structured)** – Structured security labels in an appropriate message will be checked that they are cleared for the target domain, and if the check fails the message will not be allowed through the Nexor Sentinel 3E Filtering System. This filter will be applied to selected messages based on the selected configuration settings. The administrator can force the TOE to pass a rejected SMTP message.

  This realises FDP_IFC.1(2) and FDP_IFF.1(2).

- **Allowed Attachment Types Filter** – The Allowed File Types list contains a list of acceptable file extensions e.g. “.doc” for Word documents. The Administrator may define a file extension without the period, for example, "doc". Only types that are listed and where the content is correctly associated with the extension will be allowed to pass through Nexor Sentinel 3E Filtering System. By default the list is empty and no non-text body parts will be allowed to pass, that is, messages with attachments sent through the Nexor Sentinel 3E Filtering System will fail the filter. Certain specific container file types will be expanded and further checks will be made on attachments embedded within. The administrator can force the TOE to pass a rejected SMTP message.

  This realises FDP_IFC.1(3) and FDP_IFF.1(3).

[16] Excludes envelope and email addresses

Copyright Nexor Limited © 2012, All rights reserved

6.2 Configuration

The TOE is managed through an HTTPS web interface. A user first has to login using a username and password combination (FIA_UID.2 and FIA_UAU.2). Once logged in as an administrator the user can modify the configuration of the filters (FMT_MSA.1, FMT_SMF.1, FMT_SMR.1). Multiple connected domains are supported, and configuration is specific to each pair of domains. The initial configuration of the filters is secure in the following ways (FMT_MSA.3(*)):

- **Dirty Word Searching Filter** – this filter has no initial list of words, and so will not reject any messages with its initial configuration. However the filter will run on each message by default
- **Security Label for Domain Filter (Unstructured)** – In the initial configuration, all messages reaching this filter will be blocked, until an administrator makes changes to the configuration
- **Security Label for Domain Filter (Structured)** – In the initial configuration, all messages reaching this filter will be blocked, until an administrator uploads a Security Policy Information File (SPIF) and configures the filter
- **Allowed Attachment Types Filter** – In the initial configuration, all messages with attachments will be blocked, until an administrator explicitly allows specific attachment types.

Copyright Nexor Limited © 2012, All rights reserved

7 Rationale

7.1 Security Objectives Rationale

Table 10 shows the mapping between SPD and objectives.

Objectives \ SPD	T.TOO_MANY_DIRTY_WORDS	T.SECURITY_LABEL	T.ILLEGAL_ATTACHMENT	OSP.CONFIGURE_FILTERS	T.AUTHENTICATE	A.UNDERLYING_PLATFORM	A.PHYSICAL_LOCATION	A.IT-NETWORK	A.MANAGEMENT_STATIONS	A.TRUSTED_USE
For the TOE:										
O.WORD_CHECKING	√									
O.SECURITY_LABEL		√								
O.ATTACHMENT_CHECKING			√							
O.CONFIGURE_FILTERS				√						
O.AUTHENTICATE					√					
For the environment:										
OE.UNDERLYING_PLATFORM						√				
OE.PHYSICAL_LOCATION							√			
OE.IT-NETWORK								√		
OE.MANAGEMENT_STATIONS									√	
OE.TRUSTED_USE										√

Table 10 - Security Objectives Rationale

The Security Objectives Rationale is:

- Threat T.TOO_MANY_DIRTY_WORDS is completely removed by O.WORD_CHECKING.
- Threat T.SECURITY_LABEL is completely removed by O.SECURITY_LABEL.
- Threat T.ILLEGAL_ATTACHMENT is completely removed by O.ATTACHMENT_CHECKING
- Threat T.AUTHENTICATE is completely removed by O.AUTHENTICATE.
- Policy OSP.CONFIGURE_FILTERS is enforced by O.CONFIGURE_FILTERS
- Assumption A.UNDERLYING_PLATFORM is completely upheld by OE.UNDERLYING_PLATFORM
- Assumption A.PHYSICAL_LOCATION is completely upheld by OE.PHYSICAL_LOCATION
- Assumption A.IT-NETWORK is completely upheld by OE.IT-NETWORK
- Assumption A.MANAGEMENT_STATIONS is completely upheld by OE.MANAGEMENT_STATIONS
- Assumption A.TRUSTED_USE is completely upheld by OE.TRUSTED_USE

Copyright Nexor Limited © 2012, All rights reserved

7.2 Security Requirements Rationale

Table 11 shows the tracing between SFRs and Security Objectives.

SFRs / Objectives for the TOE	FDP_IFC.1(1)	FDP_IFC.1(2)	FDP_IFC.1(3)	FDP_IFF.1(1)	FDP_IFF.1(2)	FDP_IFF.1(3)	FMT_MSA.1	FMT_MSA.3(*)	FMT_SMF.1	FMT_SMR.1	FIA_UID.2	FIA_UAU.2
O.WORD_CHECKING	√			√								
O.SECURITY_LABEL		√			√							
O.ATTACHMENT_CHECKING			√			√						
O.CONFIGURE_FILTERS							√	√	√	√		
O.AUTHENTICATE											√	√

Table 11 - Security Requirements Rationale

Table 12 shows how each of the Security Objectives is met by the SFRs.

Security Objective	Rationale
O.WORD_CHECKING The TOE shall • Check the content of all messages (excluding envelope and email addresses) for the presence of a configured list of words or phrases using the ASCII character set • Not allow a message to pass through if the threshold for these words or phrases is exceeded.	The objective is met by: • FDP_IFC.1(1) that enforces the P.PROHIBITEDWORDS filtering policy • FDP_IFF.1(1) that allows a message to pass if and only if it meets the P.PROHIBITEDWORDS filtering policy.
O.SECURITY_LABEL The TOE shall: • Check that each appropriate message contains a structurally valid security label and that the security label is appropriate for the message destination network • Allow only those appropriate messages with a security label that is structurally valid and appropriate for the message destination network to pass through • Check that each appropriate message contains a valid unstructured security label and that the security label is appropriate for the message destination network • Allow only those appropriate messages with an unstructured security label that is valid and appropriate for the message destination network to pass through.	The objective is met by: • FDP_IFC.1(2) that enforces the P.LABELFILTER filtering policy • FDP_IFF.1(2) that allows a message to pass if and only if it meets the P.LABELFILTER filtering policy.

Copyright Nexor Limited © 2012, All rights reserved

O.ATTACHMENT_CHECKING The TOE shall: • Only allow messages with permitted attachment types to pass through • Only allow attachments to pass through if the claimed type of the attachment matches the detected type.	The objective is met by: • FDP_IFC.1(3) that enforces the P.ATTACHMENT filtering policy • FDP_IFF.1(3) that allows a message to pass if and only if it meets the P.ATTACHMENT filtering policy.
O.CONFIGURE_FILTERS The TOE shall • Allow only an authenticated administrator to configure the filters • Use initial secure values for configuration parameters.	The objective is met by: • FMT_MSA.1 that enforces the P.ACCESS_CONTROL policy to allow only the administrator to change the filter configuration • FMT_MSA.3(1) that enforces the P.PROHIBITEDWORDS policy with initial secure values • FMT_MSA.3(2) that enforces the P.LABELFILTER policy with initial secure values • FMT_MSA.3(3) that enforces the P.ATTACHMENT policy with initial secure values • FMT_SMF.1 that enforces that only the administrator can change the filter configuration • FMT_SMR.1 that enforces the administrator role.
O.AUTHENTICATE The TOE shall • Require an administrator to authenticate through a username and password.	The objective is met by: • FIA_UAU.2 that forces a user to first identify themself • FIA_UID.2 that forces a user to authenticate themself before any other actions are allowed

Table 12 - Security Objectives Met by SFRs

All dependencies of the SFRs have been satisfied; therefore a rationale is not required.

Copyright Nexor Limited © 2012, All rights reserved

7.3 Security Assurance Rationale

EAL4+ was selected as the assurance level for the TOE as it is applicable in those circumstances where developers or users require a moderate to high level of independently assured security in the TOEs. It also provides assurance through the use of development environment controls and additional TOE configuration management including automation, and evidence of secure delivery procedures.

EAL4 represents a meaningful increase in assurance from EAL3 by requiring more design description, a subset of the implementation, and improved mechanisms and/or procedures that provide confidence that the TOE will not be tampered with during development or delivery.

ALC_FLR.2 was included to provide assurance in Nexor's flaw remediation process.

Appropriate assurance measures will be employed to satisfy the security assurance requirements. The evaluation confirms whether the assurance measures are sufficient to satisfy the assurance requirements. The assurance measures consist of the set of evaluation evidence listed in Table 13 below. The documents listed in the table are used to satisfy EAL4+ evaluation requirements.

Assurance Requirement	Evidence
ADV_ARC.1	Design documentation
ADV_FSP.4	Design documentation
ADV_IMP.1	Source code
ADV_TDS.3	Design documentation
AGD_OPE.1	User guidance documentation
AGD_PRE.1	User guidance documentation
ALC_CMC.4	Life Cycle documentation
ALC_CMS.4	Life Cycle documentation
ALC_DEL.1	Life Cycle documentation
ALC_DVS.1	Life Cycle documentation
ALC_FLR.2	Life Cycle documentation
ALC_LCD.1	Life Cycle documentation
ALC_TAT.1	Life Cycle documentation
ASE_CCL.1	Security Target
ASE_ECD.1	Security Target
ASE_INT.1	Security Target
ASE_OBJ.2	Security Target
ASE_REQ.2	Security Target
ASE_SPD.1	Security Target
ASE_TSS.1	Security Target
ATE_COV.2	Test documentation
ATE_DPT.1	Test documentation
ATE_FUN.1	Test documentation
ATE_IND.2	N/A
AVA_VAN.3	N/A

Table 13 - Assurance Evidence

Copyright Nexor Limited © 2012, All rights reserved

8 Appendix – Glossary of Acronyms and Terminology

Acronym	Definition
ASCII	American Standard Code for Information Interchange
CC	Common Criteria
CEM	Common Methodology for Information Security Evaluation
CLIP	Certifiable Linux Integration Platform
DCID 6/3	Directory of Central Intelligence Directive 6/3 “Protecting Sensitive Compartmented Information within Information Systems”
DR	Delivery Report
DSN	Delivery Status Notification
EAL	Evaluation Assurance Level
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IETF	Internet Engineering Task Force
MDN	Message Disposition Notification
MIME	Multipurpose Internet Mail Extensions
MTA	Message Transfer Agent
NSA	National Security Agency – an agency of the US Department of Defense
PL	Protection Level
PP	Protection Profile
P22	Interpersonal Messaging Protocol – X.400 (88)
P772	Military Message Protocol, compliant with STANAG 4406 and ACP 123
SAR	Security Assurance Requirement
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
S/MIME	Secure/Multipurpose Internet Mail Extensions
SMTP	Simple Mail Transfer Protocol
SPD	Security Problem Definition
SPIF	Security Policy Information File
Structured Security Label	A security label as defined by the X.411 standard
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
Unstructured Security Label	A security label in free-form text in the body of a message
X.400	A suite of ITU-T Email standards
X.411	One of the X.400 suite of Email standards. Defines, amongst other things, the structure of a security label

Copyright Nexor Limited © 2012, All rights reserved