Certification Report

Nexor Sentinel 3E Filtering System

Sponsor and developer: ***Nexor***
Bell House, Nottingham Science and Technology Park
Nottingham, NG7 2RL
United Kingdon

Evaluation facility: ***Brightsight***
Delftechpark 1
2628 XJ Delft
The Netherlands

Report number: **NSCIB-CC-12-34853-CR**

Report version: **1**

Project number: **NSCIB-CC-12-34853**

Author: **Denise Cater**

Date: **December 19 2012**

Number of pages: **17**

Number of appendices: **0**

Head office Apeldoorn:
Boogschutterstraat 11A
P.O. Box 541
7300 AM Apeldoorn
The Netherlands
Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

Location Apeldoorn::
Vissenstraat 6
P.O. Box 541
7300 AM Apeldoorn
The Netherlands
Tel. +31 (0)88 888 7 888
Fax +31 (0) 88 888 7 879

Location Enschede:
Josink Esweg 10
P.O. Box 337
7500 AH Enschede
The Netherlands
Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 859

TÜV Rheinland Nederland B.V. is a registered company with the Amsterdam Chamber of Commerce under number 27288788
info@nl.tuv.com
www.tuv.com/nl

Certificate

Standard	Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 3 (ISO/IEC 15408)
Certificate number	**PC 4603055**

TÜV Rheinland Nederland B.V. certifies:

Certificate holder and developer	**Nexor Ltd.** **Located in Bell House Nottingham Science and Technology Park, University Boulevard, NG7 2RL, Nottingham, United Kingdom**
Product and assurance level	**Nexor Sentinel 3E Filtering System,** Assurance Package: ▪ EAL4 augmented ALC_FLR.2
Project number	**NSCIB-CC-12-34853-CR**
Evaluation facility	**Brightsight BV located in Delft, the Netherlands** Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 3 (ISO/IEC 18045)

Common Criteria Recognition Arrangement for components up to EAL4

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using the Common Methodology for IT Security Evaluation version 3.1 Revision 3 for conformance to the Common Criteria for IT Security Evaluation version 3.1 Revision 3. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report. The evaluation has been conducted in accordance with the provisions of the Netherlands scheme for certification in the area of IT security *[NSCIB]* and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by TÜV Rheinland Nederland B.V. or by other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Rheinland Nederland B.V. or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Validity

Date of issue : **21-12-2012**

Certificate expiry : **21-12-2022**

Registration number
Notified Body 0336

PRODUCTS
RvA C078
Accredited by the Dutch Council for Accreditation

Managing Director
TÜV Rheinland Nederland B.V.
P.O. Box 541
7300 AM Apeldoorn
The Netherlands

www.tuv.com/nl

TÜVRheinland®
Precisely Right.

TÜVRheinland®
Precisely Right.

CONTENTS:

TÜVRheinland®
Precisely Right.

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TÜV Rheinland Nederland B.V. has the task of issuing certificates for IT security products.

A part of the procedure is the technical examination (evaluation) of the product according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TÜV Rheinland Nederland B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TÜV Rheinland Nederland B.V. to perform Common Criteria evaluations; a significant requirement for such a license is accreditation to the requirements of ISO Standard 17025, General requirements for the accreditation of calibration and testing laboratories.

By awarding a Common Criteria certificate, TÜV Rheinland Nederland B.V. asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

TÜVRheinland®
Precisely Right.

Recognition of the certificate

The Common Criteria Recognition Arrangement and SOG-IS logos are printed on the certificate to indicate that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS agreement

The CCRA has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL4. The current list of signatory nations and approved certification schemes can be found on: http://www.commoncriteriaportal.org.

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA) version 3 effective from April 2010 provides mutual recognition of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (resp. E3-basic) is provided for products related to specific technical domains. This agreement was initially signed by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOGIS-MRA in December 2010. The current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies can be found on: http://www.sogisportal.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the Nexor Sentinel 3E Filtering System. The developer of the Nexor Sentinel 3E Filtering System is Nexor located in Nottingham, UK and they also act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

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.

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.

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 supporting the security policies 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.

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

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands and was completed on December 19 2012 with the delivery of *[ETR]*. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]* and in accordance with *[NSP6]*. The certification was completed on December 19 2012 with the preparation of this Certification Report. It should be noted that the certification results only apply to the specific version of the product as evaluated.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the Nexor Sentinel 3E Filtering System, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the Nexor Sentinel 3E Filtering System are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report *[ETR]*[1] for this product provide sufficient evidence that it meets the EAL4 augmented (EAL4(+)) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_FLR.2 (Flaw Reporting Procedures).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3 *[CEM]*, for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 3 *[CC]*.

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the Nexor Sentinel 3E Filtering System evaluation meets all the conditions for international recognition of Common Criteria

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

Certificates and that the product will be listed on the NSCIB Certified Products list. It should be noted that the certification results only apply to the specific version of the product as evaluated.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the Nexor Sentinel 3E Filtering System from Nexor located in Nottingham, UK.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Software (CD-ROM)	Nexor Sentinel 3E Filtering System	Version 3E[2] for NATO customers
Software (CD-ROM)	Nexor Sentinel 3E Filtering System	Version 3E[3] for non-NATO customers

The installation CD-ROMs 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.

To ensure secure usage a set of guidance documents is provided together with the Nexor Sentinel 3E Filtering System. Details can be found in section 2.5 of this report. For details of how to confirm which version of the TOE is installed (NATO/non-NATO), see section 2.7 of this report.

2.2 Security Policy

There are three security filtering policies in the Filtering Engine (implemented by 4 filtering engines, identified in ***bold italics***). These are:

P.PROHIBITEDWORDS –The ***Dirty Word Searching Filter*** enforces the P.PROHIBITEDWORDS security policy by not allowing Mail messages with contents that exceed the threshold for prohibited words.

- Prohibited words are only found when the word uses 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.
- Prohibited words will be found in the email header and email body.
- Prohibited words will not be found in envelope and email addresses.
- Prohibited words will be found in limited set of locations in attachments. The exact list of location in the attachments where prohibited words will be found is provided in the user guidance *Nexor Sentinel 3E Filtering System – Operational Environment Guidance* (see section 2.5 of this report).

P.LABELFILTER – The ***Security Label for Domain Filter (Unstructured)*** and the ***Security Label for Domain Filter (Structured)*** enforce the P.LABELFILTER security policy by only allowing Mail messages marked with the structured or unstructured security labels when these labels are in line with the configuration of the TOE.

[2] 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.

[3] The CDs for non-NATO customers contain 2 versions of the label filter libraries. These libraries provide support for different unstructured security label grammars.

- Structured labels added to the email envelopes and/or the security signatures and/or P772 content.
- Unstructured labels must be present in the email body. Unstructured labels in attachments or attached email will be checked whether their classification is dominant over the unstructured label in the FLOT of the email body.
- Unstructured labels will be found in limited set of locations in attachments. The exact list of location in the attachments where unstructured labels will be found is provided in the user guidance *Nexor Sentinel 3E Filtering System – Operational Environment Guidance* (see section 2.5 of this report).

P.ATTACHMENT – The ***Allowed Attachment Types Filter*** enforces the P.ATTACHMENT security policy by only allowing Mail messages having an attachment of which the file type is in the white list of the TOE configuration.

- Certain specific container types will be expanded and further checks will be made on attachments embedded within. The exact list of supported container types is provided in the user guidance *Nexor Sentinel 3E Filtering System – Operational Environment Guidance* (see section 2.5 of this report).
- Other embedded attachments will not be checked. An example would be a PowerPoint presentation with an embedded MP3 file.
- Also the Dirty Word Searching filter and the Security Label for Domain filter (Unstructured) will not perform any checks on attachments embedded in other attachments.

In addition, the following policy is the access control policy for the TOE administrators.

P.ACCESS_CONTROL – The Nexor Sentinel Manager Web Application enforces the P.ACCESS_CONTROL security policy by only allowing an administrator to configure the filters after entering a correct login name and a password.

- 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.
- To ensure that unauthorised users are not able to administer or configure the Nexor Sentinel or to view its configuration, authorised users must log out of the Nexor Sentinel Manager Web Application when they have finished using it.

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.

2.3 Assumptions and Clarification of Scope

2.3.1 Usage assumptions

Detailed information on the assumption and threats can be found in the *[ST]* sections 3.1 and 3.3 respectively. Detailed information on the security objectives that must be fulfilled by the TOE environment can be found in section 4.1 of the *[ST]*.

2.3.2 Environmental assumptions

The following assumption about the environmental aspects defined by the Security Target has to be met (for the detailed and precise definition of the assumption refer to the *[ST]*, chapter 3.3):

- **A.MANAGEMENT_STATIONS**: The TOE shall be managed by workstations that cannot connect to un-trusted web servers (such as on the internet).
- **A.TRUSTED_USE**: It is assumed that both administrators and those who send/receive messages through the TOE are trustworthy and will not abuse their privileges.

Furthermore, the following organisational security policy relates to the environment in which the TOE shall be operated (for the detailed and precise definition of the organisational security policy refer to the *[ST]*, chapter 3.2):

- **OSP.CONFIGURE_FILTERS**: The TOE shall provide a secure web-based interface that enables configuration of the filters.

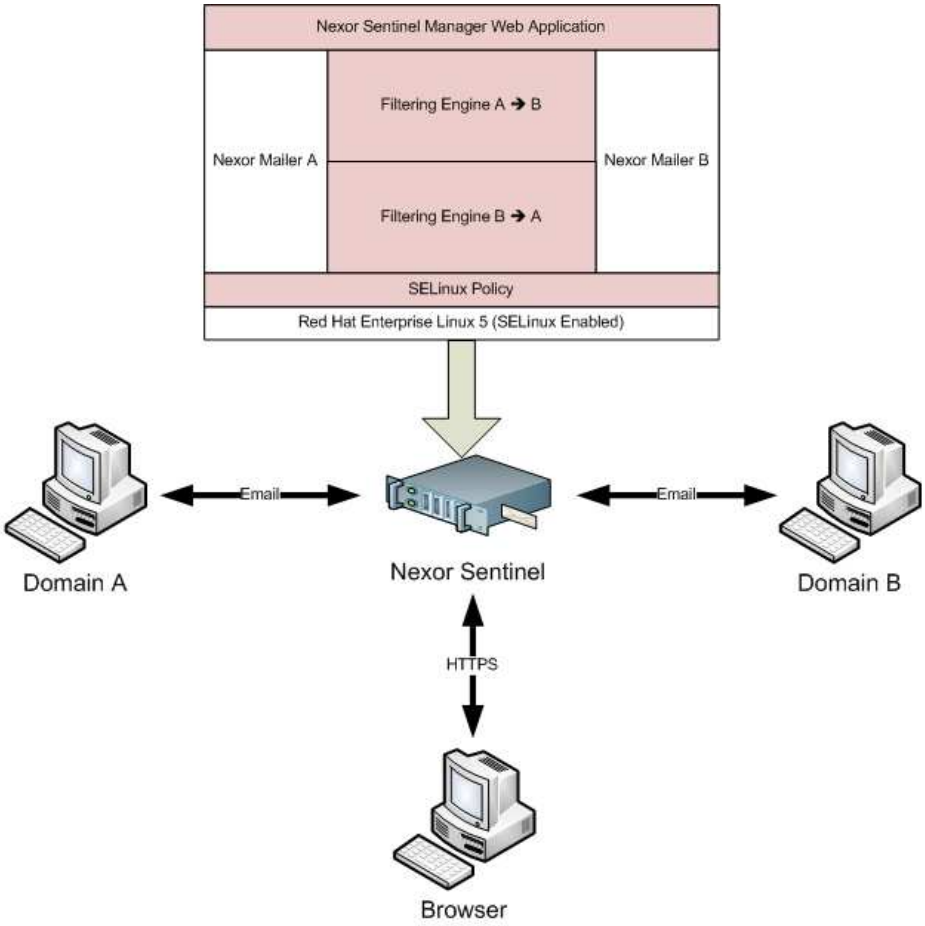
2.3.3 Clarification of scope

The TOE filtering of emails is limited to the policies, as summarised in Section 2.2 above and detailed in the Security Objectives for the TOE in *[ST]* section 4.1 and the definition of Information Flow Control Security Function Policies in *[ST]* Section 5.1. In particular:

- The TOE relies on the user (message recipient/sender) being trustworthy and not maliciously attempting to hide information in email messages. For example:
  - The message content search for dirty words is limited to ASCII words. Only message content (message content (including header, body and any attachments including attached messages) is searched for dirty words;
  - The message envelope, email addresses and attachment filenames are excluded from this search.
  - Only whole words are checked; the filter does not consider sub-strings.
  - Special locations of attachments are not searched (for example, document property, Word Art, embedded tables).
- The attachment filter only recursively handles supported container file types to unpack files for inspection (attachments embedded in other non-container types or unsupported container types will not be checked).

2.4 Architectural Information

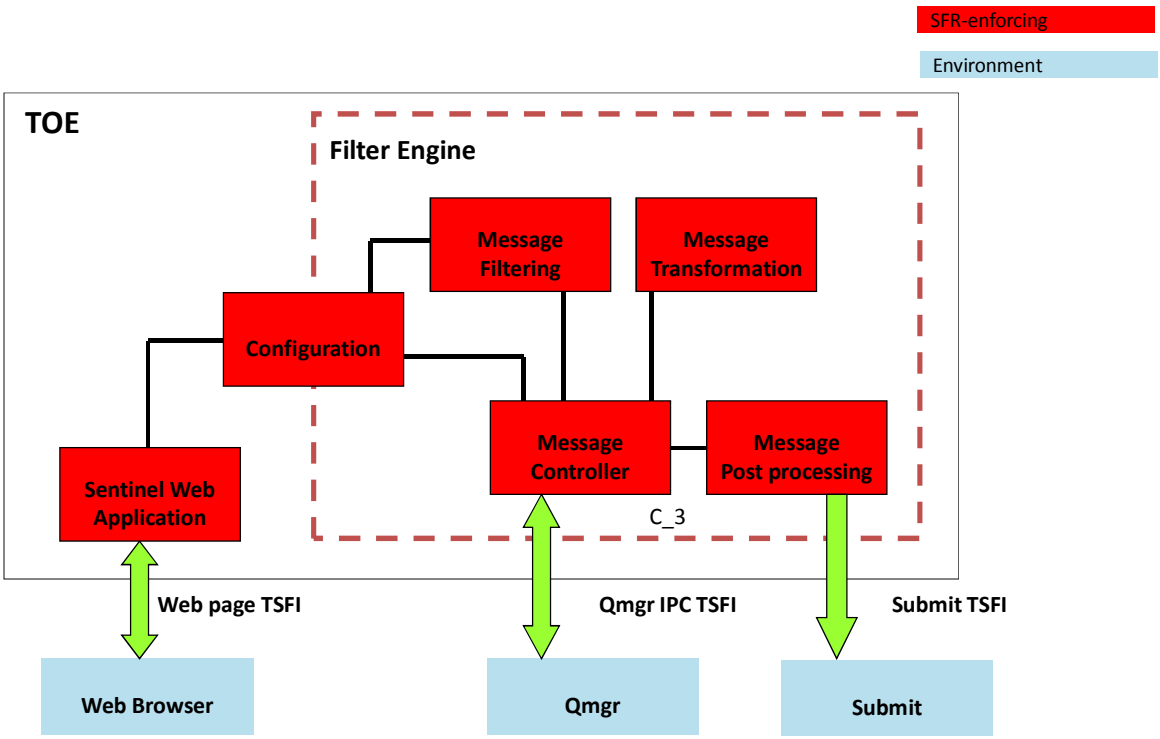
The following diagram depicts the TOE - Nexor Sentinel 3E Filtering System - in the context of the Nexor Sentinel 3.3 High Assurance Mail Guard.



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 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. This ensures network separation of the connected domains by ensuring messages can only pass from one domain to the other via a trusted path. 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.

The TOE 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.

The subsystems of the TOE shown in the diagram below.



The subsystems relating to the filter engine are iterated for each filter engine configured (up to a maximum of 56 engines (pairs between a maximum of 8 interconnected networks).

2.5 Documentation

The following documentation is provided with the product by the developer to the customer:

Identifier	Version
Nexor Sentinel 3.3 Administration Guide, document reference NEX2812MAN	Version 04
Nexor Sentinel 3E Filtering System – Operational Environment Guidance, document reference NEX2817ENG	Version 10
Nexor Sentinel 3E Filtering System-TOE Identification, document reference NEX2814ENG	Version 16
Sentinel 3 Delivery Customer Letter, document reference NEX2818CON	Letter
NSENT3CCC Customer Sentinel 3.30 Seals Check	Version 01

2.6 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

2.6.1 Testing approach and depth

Developer testing of the engine filters and configuration of the Sentinel was performed using (perl) scripting to generate and send messages of different types and perform necessary configuration changes. Login related tests were performed manually using a web browser.

The developer performed at least one test case to demonstrate the behaviour of each TSFI and each SFR. The developer testing also demonstrated the expected behaviour of each subsystem, tested from the TSFI interfaces.

The independent evaluator testing was comprised of:

- Sample testing (2:ATE_IND.2-4) to validate the developer testing by repeating/witnessing of all developer tests;
- Independent testing (2:ATE_IND.2-6) was performed based on (15) new tests defined by the evaluator for the validation of the correct enforcement of all SFRs.

2.6.2 Independent Penetration Testing

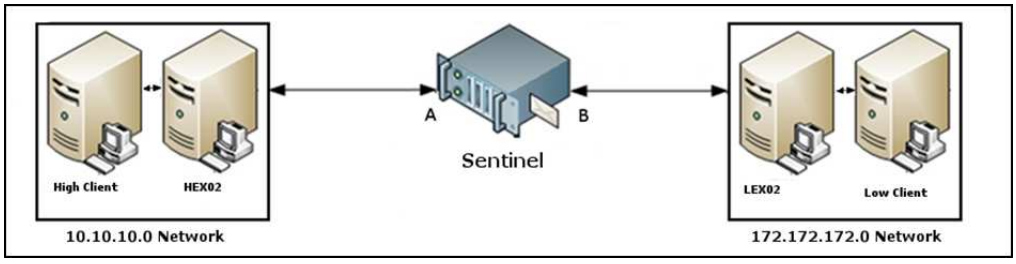
The evaluator independent penetration tests were conducted according to the following testing approach:

- During evaluation of the ADV, ATE and AGD classes the evaluators hypothesized possible vulnerabilities. This resulted in a shortlist of possible vulnerabilities to be further analysed in AVA using the design knowledge gained. This resulted in a shortlist of potential vulnerabilities to be tested.
- The evaluators used CEM Annex B.2 as an additional source for possible vulnerabilities and penetration tests.
- The evaluators conducted a search of the public domain to identify any relevant vulnerabilities relating to the TOE and to components of the TOE. This resulted in a shortlist of possible vulnerabilities to be further analysed in AVA using the design knowledge gained. This resulted in a shortlist of potential vulnerabilities to be tested.

As a result of the vulnerability analysis conducted (19) penetration tests were performed to determine whether any potential vulnerabilities could be exploited in the operational environment.

2.6.3 Test Configuration

The developer and evaluator tested the TOE in the *[ST]* configuration, as delivered to a customer. The following diagram and table of test components detail the evaluator test setup:



Identifier	Details
HEX02 VM	VM using a windows operating system. A Microsoft exchange server is installed. This will connect to MTA-A of the Sentinel appliance.
High Client VM	VM using a windows operating system with outlook installed with user mailboxes on HEX02. This client also has installed python for sending more test specific emails.
LEX02 VM	VM using a windows operating system. A Microsoft exchange server is installed. This will connect to MTA-B of the Sentinel appliance.
Low Client VM	VM using a windows operating system with outlook installed with user mailboxes on LEX02.
Sentinel HW	HP ProLiant hardware that can run the OS. The DL360 range is used and the version is G7.
Sentinel OS	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).

The following tools were used by the evaluator when testing the TOE:

- 2 standard PCs
- Backtrack and Windows as Operating System on 2 PCs
- VMware workstation
- Microsoft exchange server
- Outlook
- Python scripting language (sending SMTP email)
- WireShark for analysing network protocols. It can be used to capture network traffic and interactively browse the network packets and to unpack ASN.1.

2.6.4 Testing Results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

From the set of (15) evaluator independent functional tests and (19) evaluator independent penetration tests it was determined that (4) of the functional test cases and (2) of the penetration test cases were not relevant to the claims in *[ST]*, which led to clarification of *[ST]*.

With the revision of the evaluator independent functional and penetration test case sets to remove the invalid test cases, the developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its *[ST]* and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

2.7 Evaluated Configuration

The TOE is defined uniquely by its name and version number Nexor Sentinel 3E Filtering System. The consumer can verify whether they have the NATO or non-NATO version by checking the number of label filter libraries the directory `/usr/local/nexor/shlib`., as detailed in the guidance document *Nexor Sentinel 3E Filtering System-TOE Identification*.

2.8 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]*[4] which references several Intermediate Reports and other evaluator documents. The verdict of each claimed assurance requirement is given in the following tables:

Development		**Pass**
Security architecture	ADV_ARC.1	Pass
Functional specification	ADV_FSP.4	Pass
Implementation representation	ADV_IMP.1	Pass
TOE design	ADV_TDS.3	Pass

Guidance documents		**Pass**
Operational user guidance	AGD_OPE.1	Pass
Preparative procedures	AGD_PRE.1	Pass

Life-cycle support		**Pass**
Configuration Management capabilities	ALC_CMC.4	Pass
Configuration Management scope	ALC_CMS.4	Pass

[4] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

Delivery	ALC_DEL.1	Pass
Development security	ALC_DVS.1	Pass
Flaw Remediation	ALC_FLR.2	Pass
Life-cycle definition	ALC_LCD.1	Pass
Tools and techniques	ALC_TAT.1	Pass

Security Target		**Pass**
Conformance claims	ASE_CCL.1	Pass
Extended components definition	ASE_ECD.1	Pass
ST introduction	ASE_INT.1	Pass
Security objectives	ASE_OBJ.2	Pass
Security requirements	ASE_REQ.2	Pass
Security problem definition	ASE_SPD.1	Pass
TOE summary specification	ASE_TSS.1	Pass

Tests		**Pass**
Coverage	ATE_COV.2	Pass
Depth	ATE_DPT.1	Pass
Functional tests	ATE_FUN.1	Pass
Independent testing	ATE_IND.2	Pass

Vulnerability assessment		**Pass**
Vulnerability analysis	AVA_VAN.3	Pass

Based on the above evaluation results the evaluation lab concluded the Nexor Sentinel 3E Filtering System-TOE Identification to be **CC Part 2 conformant, CC Part 3 conformant**, and to meet the requirements of **EAL 4 augmented by ALC_FLR.2**. This implies that the product satisfies the security technical requirements specified in Security Target *Nexor Sentinel 3E Filtering System Common Criteria Security Target*, version 23, dated 18th December 2012.

2.9 Evaluator Comments/Recommendations

2.9.1 Obligations and hints for the developer

None.

2.9.2 Recommendations and hints for the customer

The customer must/shall follow the provided guidance documentation, as detailed in Section 2.5. In particular the implementation of the following policies:

- P.PROHIBITEDWORDS security policy - Non-text attachments, Word Matching, Supported Information Locations, Supported File Types;
- P.ATTACHMENTS security policy - Embedded Attachments, Supported Container File Types, Supported File Types;
- P.LABELFILTER security policy - Supported Information Locations, Embedded Attachments, Supported File Types.

3 Security Target

The Security Target *Nexor Sentinel 3E Filtering System Common Criteria Security Target*, version 23, dated 18th December 2012 is included here by reference.

4 Definitions

This list of Acronyms and the glossary of terms contains elements that are not already defined by the CC or CEM:

ASN.1	Abstract Syntax Notation One
IT	Information Technology
ITSEF	IT Security Evaluation Facility
NSCIB	Nederlands Schema voor Certificatie op het gebied van IT-Beveiliging
SE Linux	Security Enhanced Linux
TOE	Target of Evaluation

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report:

[CC]	Common Criteria for Information Technology Security Evaluation, Parts I version 3.1 revision 1, and Part II and III, version 3.1 revision 3.
[CEM]	Common Methodology for Information Technology Security Evaluation, version 3.1, Revision 3, July 2009.
[ETR]	Brightsight, Evaluation Technical Report Nexor Sentinel 3E Filtering System – EAL4+, Version 4.0, Issue Date December 19, 2012.
[NSCIB]	Nederlands Schema for Certification in the Area of IT Security, Version 2.0, 1 July 2011.
[NSP6]	NSCIB Scheme Procedure #6, Medium Assurance Evaluations, Version 1.0, June 1st, 2012
[ST]	Nexor Sentinel 3E Filtering System Common Criteria Security Target, version 23, dated 18th December 2012

(This is the end of this report).