122-B

ASSURANCE MAINTENANCE REPORT MR1
(supplementing Certification Report No. CRP249)

StoneGate Firewall/VPN

Version 4.2.2 Build 5708.cc.3.1

**running on the StoneGate appliance models FW-310,
FW-1020, FW-1030, FW-1050, FW-1200, FW-5000 and FW-5100**

Issue 1.0

March 2010

CESG Certification Body
IACS Delivery Office, CESG
Hubble Road, Cheltenham
Gloucestershire, GL51 0EX
United Kingdom

CERTIFICATION STATEMENT (ADDENDUM)

The product detailed below has been certified under the terms of the UK IT Security Evaluation and Certification Scheme and has met the specified Common Criteria requirements. The scope of the certification and the assumed usage environment are specified in the body of this report.

Sponsor	Stonesoft Corporation
Developer	Stonesoft Corporation
Product and Version	StoneGate Firewall/VPN Version 4.2.2 Build 5708.cc.3.1
Platform	StoneGate appliance models FW-310, FW-1020, FW-1030, FW-1050, FW-1200, FW-5000 and FW-5100.
Description	The Stonesoft StoneGate Firewall/VPN is a high-availability firewall and Virtual Private Networking solution for securing data communication channels and enabling continuous network connectivity.
CC Part 2	Extended with FAU_STG.NIAP-0414
CC Part 3	Conformant
EAL	EAL4 augmented by ALC_FLR.1
PP Conformance	None
Related CC Certificates	CRP249
Date Maintained	23 March 2010

The evaluation and maintenance was carried out in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme as described in United Kingdom Scheme Publication 01 [UKSP01], 02 [UKSP02P1], [UKSP02P2] and 03 [UKSP03P1], [UKSP03P2]. The Scheme has established a Certification Body, which is managed by CESG on behalf of Her Majesty's Government.

The purpose of the evaluation and maintenance was to provide assurance about the effectiveness of the TOE in meeting its Security Target [ST1], which prospective consumers are advised to read. To ensure that the Security Target gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated and maintained against this baseline. Both parts of the evaluation were performed in accordance with CC Part 1 [CC1] and 3 [CC3], the Common Evaluation Methodology [CEM] and relevant Interpretations.

The issue of a Certification Report and Addendum is a confirmation that the evaluation process has been carried out properly and that no *exploitable* vulnerabilities have been found in the evaluated configuration of the TOE. It is not an endorsement of the product.

ARRANGEMENT ON THE RECOGNITION OF COMMON CRITERIA CERTIFICATES IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY

The Certification Body of the UK IT Security Evaluation and Certification Scheme is a member of the above Arrangement [CCRA] and, as such, this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement.

The judgements[1] contained in the certificate and in this report are those of the Qualified Certification Body which issued them and of the Evaluation Facility which performed the evaluation. There is no implication of acceptance by other Members of the Arrangement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed by a third party upon those judgements.

MUTUAL RECOGNITION AGREEMENT OF INFORMATION TECHNOLOGY SECURITY EVALUATION CERTIFICATES

The SOG-IS MRA logo which appears below:

- confirms that the certificate has been issued under the authority of a party to an international Mutual Recognition Agreement (MRA) [MRA] designed to ensure that security evaluations are performed to high and consistent standards;
- indicates that it is the claim of the evaluating party that its evaluation and certification processes meet all the conditions of the MRA.

The judgements[1] contained in the certificate, Certification Report and in this Maintenance Report are those of the Qualified Certification Body which issued them and of the Evaluation Facility which performed the evaluation. Use of the logo of this Agreement does not imply acceptance by other Members of liability in respect of those judgements or for loss sustained as a result of reliance placed by a third party upon those judgements.

CCRA logo **CC logo** **SOG-IS MRA logo**

[1] All judgements contained in this Maintenance Report, excluding the ALC_FLR.1 component, are covered by the CCRA [CCRA] and the MRA [MRA].

TABLE OF CONTENTS

CERTIFICATION STATEMENT (ADDENDUM) 2

TABLE OF CONTENTS 3

I. INTRODUCTION 4

Overview 4
Maintained Versions 4
Assurance Continuity Process 5
General Points 5

II. ASSURANCE MAINTENANCE 6

Analysis of Changes 6
Changes to Developer Evidence 6
TOE Identification 7
TOE Scope and TOE Configuration 7
TOE Documentation 7
TOE Environment 7

III. TOE TESTING 8

Vulnerability Analysis 8
TOE Testing 8

IV. SUMMARY, CONCLUSIONS AND DISCLAIMERS 9

Summary 9
Conclusions 9
Disclaimers 9

V. REFERENCES 11

VI. ABBREVIATIONS 13

I. INTRODUCTION

Overview

1. This Maintenance Report (MR) states the outcome of the Common Criteria (CC) [CC] Assurance Continuity process for StoneGate Firewall/VPN Version 4.2.2, Build 5708.cc.3.1, as summarised in the 'Certification Statement (Addendum)' on page 2 of this report, and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

2. The baseline for this Assurance Continuity (also known as Assurance Maintenance) report was the Common Criteria evaluation and certification, to the EAL4 Evaluation Assurance Level, of StoneGate Firewall/VPN Version 4.2.2, Build 5708.cc.3.1. That version was certified to CC EAL4, augmented with ALC_FLR.1, in March 2009. See [ST], [ETR] and [CR] for full details.

3. Prospective consumers are advised to read this report [MR1] in conjunction with the following documents (which are available on the CESG and CC websites):

- the Certification Report CRP249 [CR] for the EAL4 evaluation of the original certified Target of Evaluation (TOE), to which this report is an Addendum;
- the Security Target [ST] of the certified TOE, which specifies the functional, environmental and assurance requirements for the evaluation;
- the updated Security Target [ST1] of the latest maintained derivative.

Maintained Versions

4. The version of the product originally evaluated and certified was:

- StoneGate Firewall/VPN Version 4.2.2, Build 5708.cc.3.1

5. The first and latest derived version (which is in fact unchanged with respect to the certified version) of the product for which assurance has been maintained is:

- StoneGate Firewall/VPN Version 4.2.2, Build 5708.cc.3.1

6. The maintenance of the latest derived version is described in this report [MR1], which provides a summary of the incremental changes from the certified version.

7. The Developer of the Certified TOE and derived versions is detailed in the 'Certification Statement (Addendum)' on page 2 of this report and elaborated in further detail on the CESG website.

Assurance Continuity Process

8. The Common Criteria Recognition Arrangement (CCRA) [CCRA] has been established as a basis for the mutual recognition of the results of Common Criteria evaluations. The process of Assurance Continuity within the Common Criteria is defined in the document 'Assurance Continuity: CCRA Requirements' [AC] and is detailed in [UKSP03P2] for the UK Scheme.

9. The Assurance Continuity process is based on an Impact Analysis Report (IAR) produced by the Developer. The IAR describes all the changes made to the product, together with the updated evaluation evidence, and assesses the security impact of each change. For the assurance maintenance of StoneGate Firewall/VPN Version 4.2.2, Build 5708.cc.3.1, [IAR1] has been examined by the CESG Certification Body, who produced this Maintenance Report No. 1 [MR1].

10. The Developer, Stonesoft Corporation, has carried out full retesting on the assurance maintained StoneGate Firewall/VPN Version 4.2.2, Build 5708.cc.3.1, and has considered all the assurance aspects detailed in 'Assurance Continuity: CCRA Requirements' [AC].

General Points

11. Assurance Continuity addresses the security functionality claimed in the Security Target [ST1] with reference to the assumed environment specified. The assurance maintained TOE configurations and platform environments are as specified by the modifications detailed in this Report [MR1] (see 'TOE Identification' and 'TOE Environment') in conjunction with the original Certification Report [CR]. Prospective consumers are advised to check that this matches their identified requirements.

II. ASSURANCE MAINTENANCE

Analysis of Changes

12. [IAR1] provides the Impact Analysis Report from certified StoneGate Firewall/VPN Version 4.2.2, Build 5708.cc.3.1 to the assurance maintained Version 4.2.2, Build 5708.cc.3.1, and provides the Assurance Continuity rationale for Version 4.2.2, Build 5708.cc.3.1 on an additional platform (FW-1030), as well as the original set of platforms (FW-310, FW-1020, FW-1050, FW-1200, FW-5000 and FW-5100). [IAR1] conforms to the Assurance Continuity requirements specified in [AC], in particular Chapters 4 and 5.

13. No ***Major*** changes were made between the certified StoneGate Firewall/VPN Version 4.2.2, Build 5708.cc.3.1 and the assurance maintained Version 4.2.2, Build 5708.cc.3.1. The only change was the addition of a hardware appliance (FW-1030) to the original list of appliances, as described in [IAR1]. No changes were made to the development environment and there were no changes that impacted the ALC_FLR.1 augmentation, since there were no changes to any of the deliverables that provided input into the associated evaluation activity.

14. The TOE changes and their impact and effect on the evaluation deliverables are described in [IAR1] and evaluated in [ETR1]. This shows that *for all changes*:

- The "Impact of Change" is determined to be "***Minor***".
- The "Effect on evaluation deliverables" is determined to be "***None***".
- The "Action" required for resolution is determined to be "***None***".

15. Note that:

- Only ***Minor*** generic changes were required to the Security Target [ST], to reflect the addition of FW-1030, resulting in [ST1].

Changes to Developer Evidence

16. [IAR1] shows that the only evaluation documentation deliverables that were updated for the assurance maintained StoneGate Firewall/VPN Version 4.2.2, Build 5708.cc.3.1 were as follows:

- Security Target [ST1], updated from [ST];
- GRD23046 - Configuration List;
- GRD23045 - Test Documentation Configuration List;
- Common Criteria Hardware List;
- GRD11084 - Observed Security Flaws;

- Common Criteria Certification User's Guide - StoneGate Firewall/VPN 4.2 and SMC 4.2;

- GRD23059 - Appliance Model Test Mapping;

- StoneGate FWVPN ATF CC environment;

- Environment setup and general usage.

17. All updates in the above documents were classified as ***Minor***.

TOE Identification

18. The assurance maintained TOE is uniquely identified as:

- Stonesoft Corporation StoneGate Firewall/VPN Version 4.2.2, Build 5708.cc.3.1 running on StoneGate appliance models FW-310, FW-1020, FW-1030, FW-1050, FW-1200, FW 5000 and FW-5100.

TOE Scope and TOE Configuration

19. The TOE scope is unchanged and is described in [ST1] Section 2.3. The latest Evaluated Configuration is defined in [ST1] Section 2.3.

TOE Documentation

20. The Installation, Configuration and Guidance documents have changed, as described in Paragraph 16.

TOE Environment

21. The defined environment has not changed and is defined in [ST1].

III. TOE TESTING

Vulnerability Analysis

22. In order to assess whether any vulnerabilities had been introduced into the product between the certified Version 4.2.2, Build 5708.cc.3.1 and the assurance maintained Version 4.2.2, Build 5708.cc.3.1, an analysis was made of the Stonesoft Corporation Flaw Reporting Knowledge Base and public domain vulnerabilities. The same level of vulnerability analysis was performed during Assurance Maintenance as was performed for the original evaluation. The information that was assessed also contained details of generic vulnerabilities, so any generic vulnerabilities that were relevant to StoneGate Firewall/VPN were automatically included in the analysis.

23. [IAR1] showed that there had been no flaws or bugs logged that required changes within the scope of the TOE between the certified Version 4.2.2, Build 5708.cc.3.1 and the maintained Version 4.2.2, Build 5708.cc.3.1.

24. During the original evaluation, the vulnerability analysis was based on a search of public domain sources. That search was repeated on 3 February 2010 and it was found that no new vulnerabilities had been reported. As the scope of the TOE and the deliverables were unchanged, the mitigation of these vulnerabilities was unchanged from that reported in [ETR].

25. Therefore, no vulnerabilities were found between the certified version of the TOE and the maintained version of the TOE.

TOE Testing

26. The testing performed during the original evaluation of StoneGate Firewall/VPN Version 4.2.2, Build 5708.cc.3.1 was manual and was controlled by a set of test scripts. The testing performed for the assurance maintained StoneGate Firewall/VPN Version 4.2.2, Build 5708.cc.3.1 was performed by Stonesoft Corporation.

27. The manual test scripts examined during the original evaluation have been appropriately updated. However the actual tests themselves have not significantly changed and they test exactly the same security functionality in the same manner.

28. All test scripts that were used for testing the certified StoneGate Firewall/VPN Version 4.2.2, Build 5708.cc.3.1 were run on all StoneGate appliance models FW-310, FW-1020, FW-1030, FW-1050, FW-1200, FW 5000 and FW-5100 included within the scope of the Assurance Maintenance activity and all of those tests passed. The results were exactly the same as the results of the tests performed during the original evaluation and did not reveal any inconsistencies or concerns.

29. Thus confidence can be gained that the assurance maintained StoneGate Firewall/VPN Version 4.2.2, Build 5708.cc.3.1 provides the claimed security functionality in the same manner as the certified StoneGate Firewall/VPN Version 4.2.2, Build 5708.cc.3.1.

IV. SUMMARY, CONCLUSIONS AND DISCLAIMERS

Summary

30. The analyses in [IAR1] show that no ***Major*** changes have been made to the TOE between the certified StoneGate Firewall/VPN Version 4.2.2, Build 5708.cc.3.1 and the assurance maintained StoneGate Firewall/VPN Version 4.2.2, Build 5708.cc.3.1. The only change has been the introduction of an additional hardware appliance which has not resulted in any changes to the source code. Thus all changes are categorised as having a ***Minor*** impact and hence CC EAL4, augmented with ALC_FLR.1, assurance has been maintained.

Conclusions

31. The CESG Certification Body accepts the decisions detailed in [IAR1], which has assessed each change as being of ***Minor*** impact, and concludes that the overall impact of all the changes is ***Minor***.

32. The CESG Certification Body has therefore determined that EAL4, augmented with ALC_FLR.1 assurance, as outlined in Certification Report P249 [CR], has been maintained for the latest derived version, StoneGate Firewall/VPN Version 4.2.2, Build 5708.cc.3.1 running on StoneGate appliance models FW-310, FW-1020, FW-1030, FW-1050, FW-1200, FW 5000 and FW-5100. These conclusions are summarised in the 'Certification Statement (Addendum)' on Page 2 of this report.

33. Prospective consumers of the assurance maintained StoneGate Firewall/VPN Version 4.2.2, Build 5708.cc.3.1 should understand the specific scope of the certification by reading this report in conjunction with the Security Target [ST1]. The TOE should be used in accordance with the environmental assumptions specified in the Security Target. Prospective consumers are advised to check that the SFRs and the evaluated configuration match their identified requirements, and to give due consideration to the recommendations and caveats of this report.

34. The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration. A number of recommendations relating to the secure receipt, installation, configuration and operation of the TOE are included in Certification Report P249 [CR].

Disclaimers

35. The Assurance Continuity process is *not* a guarantee of freedom from security vulnerabilities. There remains a small probability (smaller with higher Evaluation Assurance Levels) that exploitable vulnerabilities may be discovered after the Assurance Continuity process has been completed. This Maintenance Report reflects the CESG Certification Body's view at the time of certification.

36. Existing and prospective consumers should check regularly for themselves whether any security vulnerabilities have been discovered since this Report was issued and, if appropriate,

should check with the vendor to see if any patches exist for the product and whether those patches have further assurance.

37. The installation of patches for security vulnerabilities, whether or not those patches have further assurance, should improve the security of the TOE. However, note that unevaluated patching will invalidate the certification of the TOE, unless the TOE has undergone a formal re-certification or is covered under an approved Assurance Continuity process by a CCRA certificate-authorising Scheme.

38. All product or company names used in this report are for identification purposes only and may be trademarks of their respective owners.

V. REFERENCES

Common Criteria Documents

[CC] Common Criteria for Information Technology Security Evaluation,
(comprising Parts 1, 2, 3: [CC1], [CC2], [CC3]).

[CC1] Common Criteria for Information Technology Security Evaluation,
Part 1, Introduction and General Model,
Common Criteria Maintenance Board,
CCMB-2009-07-001, Version 3.1 R3, July 2009

[CC2] Common Criteria for Information Technology Security Evaluation,
Part 2, Security Functional Components,
Common Criteria Maintenance Board,
CCMB-2009-07-002, Version 3.1 R3, July 2009.

[CC3] Common Criteria for Information Technology Security Evaluation,
Part 3, Security Assurance Components,
Common Criteria Maintenance Board,
CCMB-2009-07-003, Version 3.1 R3, July 2009.

[CEM] Common Methodology for Information Technology Security Evaluation,
Evaluation Methodology,
Common Criteria Maintenance Board,
CCMB-2009-07-004, Version 3.1 R3, July 2009.

[CCRA] Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security,
Participants in the Arrangement Group,
May 2000.

[AC] Assurance Continuity: CCRA Requirements,
Common Criteria Interpretation Management Board,
CCIMB-2004-02-009, Version 1.0, February 2004.

[MRA] Mutual Recognition Agreement of Information Technology Security Evaluation Certificates,
Management Committee of Agreement Group,
Senior Officials Group – Information Systems Security,
Version 2.0, April 1999.

UK IT Security Evaluation and Certification Scheme Documents

[UKSP00] Abbreviations and References,
UK IT Security Evaluation and Certification Scheme,
UKSP 00, Issue 1.6, December 2009.

[UKSP01] Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 6.3, December 2009.

[UKSP02P1] CLEF Requirements - Startup and Operations,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part I, Issue 4.2, December 2009.

[UKSP02P2] CLEF Requirements - Conduct of an Evaluation,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part II, Issue 2.4, December 2009.

[UKSP03P1] Sponsor’s Guide – General Introduction,
UK IT Security Evaluation and Certification Scheme,
UKSP 03: Part I, Issue 2.2, December 2009.

[UKSP03P2] Sponsor’s Guide - Assurance Continuity,
UK IT Security Evaluation and Certification Scheme,
UKSP 03: Part II, Issue 1.0, December 2009.

Evaluated Version (Original)

[ST] Security Target - StoneGate Firewall/VPN Version 4.2.2, Build 5708.cc.3.1,
Stonesoft Corporation,
Version 1.0, 23 January 2009.

[ETR] Evaluation Technical Report,
BT CLEF,
LFS/T536/ETR, Issue 1.0, 4 March 2009.

[CR] Certification Report No. CRP249,
UK IT Security Evaluation and Certification Scheme,
CRP249, Issue 1.0, March 2009.

Latest Derived Version (1st Derived Version)

[ST1] Security Target - StoneGate Firewall/VPN Version 4.2.2, Build 5708.cc.3.1,
Stonesoft Corporation,
Version 1.3, 19 February 2010.

[IAR1] Impact Analysis Report for FW-1030,
Stonesoft Corporation,
GRD23060, Version 5, 17 February 2010.

[ETR1] Evaluation Technical Report,
SiVenture CLEF,
STLZ-TR-0001, Version 1-1, 22 March 2010.

[MR1] *(this document)*

VI. ABBREVIATIONS

This list does not include well-known IT terms (such as GUI, HTML, LAN, PC) or standard Common Criteria abbreviations (such as TOE, TSF; see Common Criteria Part 1 [CC1]) or Scheme abbreviations (such as CESG, CLEF; see [UKSP00]).

Term	Meaning
MR	Maintenance Report
VPN	Virtual Private Network

This page is intentionally blank.