



**ASSURANCE MAINTENANCE REPORT MR1
(supplementing Certification Report No. CRP261)**

**McAfee Firewall Enterprise
Version 7.0.1.03**

running on

Models S1104, S2008, S3008, S4016, S5032, S6032, S7032-04, S7032-08, S7032-16,
S7032-32, 1100E, 2150E, 4150E, FW-410F, FW-510F, FW-1100F, FW-2100F,
FW-2150F, FW-4150F, FW-2150F-VX04, and RM700F;
also VMware vSphere Hypervisor (ESXi) version 4.0,
and Riverbed Steelhead 250-H, 550-H,
1050-H and 2050-H appliances

Issue 1.0

November 2011

© Crown Copyright 2011 – All Rights Reserved

Reproduction is authorised, provided
that this report is copied in its entirety.

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:	McAfee Inc.	Developer:	McAfee Inc.
Product and Version:	MR1 Derived: McAfee Firewall Enterprise, Version 7.0.1.03 Original: McAfee Firewall Enterprise, Version 7.0.1.02HW02		
Platforms:	Models S1104, S2008, S3008, S4016, S5032, S6032, S7032-04, S7032-08, S7032-16, S7032-32, 1100E, 2150E, 4150E, FW-410F, FW-510F, FW-1100F, FW-2100F, FW-2150F, FW-4150F, FW-2150F-VX04, and RM700F; also VMware vSphere Hypervisor (ESXi) version 4.0, and Riverbed Steelhead 250-H, 550-H, 1050-H and 2050-H appliances		
Description:	McAfee Firewall Enterprise is a firewall and access control security platform for the enterprise, providing access control of communication and information flow between two or more networks using application-level proxy and packet filtering technology.		
CC Version:	Version 3.1 Revision 3		
CC Part 2:	Extended	CC Part 3:	Conformant
EAL:	EAL 4 augmented by ALC_FLR.3		
PP Conformance:	U.S. Government Protection Profile for Application-level Firewall in Basic Robustness Environments [PP]		
Related CC Certificates:	P261 and P261 Maintenance Addendum 1		
Date Maintained:	11 November 2011		
FIPS 140-2 Validation	Crypto module validation is covered by FIPS 140-2 validation certificates numbers <i>(TBD)</i> .		
<p>The evaluation and maintenance was performed in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme as described in United Kingdom Scheme Publication 01 [UKSP01] and 02 [UKSP02P1], [UKSP02P2]. The Scheme has established the CESG Certification Body, which is managed by CESG on behalf of Her Majesty’s Government.</p> <p>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.</p> <p>The issue of an Assurance Maintenance Report and Certificate Maintenance Addendum is a confirmation that the evaluation process has been performed properly and that no <i>exploitable</i> vulnerabilities have been found in the evaluated configuration of the TOE. It is not an endorsement of the product.</p>			




 <p>122</p>	<p>The CESG Certification Body of the UK IT Security Evaluation and Certification Scheme is accredited by the United Kingdom Accreditation Service (UKAS) to <i>EN 45011:1998 (ISO/IEC Guide 65:1996)</i> to provide product conformity certification as follows:</p> <p>Category: Type Testing Product Certification of IT Products and Systems.</p> <p>Standards:</p> <ul style="list-style-type: none"> • Common Criteria for Information Technology Security Evaluation (CC) EAL1 - EAL7; and • Information Technology Security Evaluation Criteria (ITSEC) E1 - E6. <p>Details are provided on the UKAS website (www.ukas.org).</p>
	<p>Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (CCRA), May 2000</p> <p>The CESG Certification Body is a Participant to the above Arrangement [CCRA]. The Participants to the Arrangement are detailed on the Common Criteria Portal (www.commoncriteriaportal.org). The mark (left) confirms that the Common Criteria certificate has been authorised by a Participant to the above Arrangement and it is the Participant’s statement that the certificate has been issued in accordance with the terms of the above Arrangement. Upon receipt of the certificate, the vendor(s) may use the mark in conjunction with advertising, marketing and sales of the IT product for which the certificate is issued.</p>
	<p>Mutual Recognition Agreement of Information Technology Security Evaluation Certificates (SOGIS MRA), Version 3.0</p> <p>The CESG Certification Body is a Participant to the above Agreement [MRA]. The current Participants to the Agreement are Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The mark (left) confirms that the conformant certificate has been authorised by a Participant to the above Agreement and it is the Participant’s statement that the certificate has been issued in accordance with the terms of the above Agreement. The judgments contained in the certificate and in this associated Certification Report are those of the compliant Certification Body which issued them and of the Evaluation Facility which performed the evaluation. Use of the mark does not imply acceptance by other Participants of liability in respect of those judgments or for loss sustained as a result of reliance placed upon those judgments by a third party.</p>

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	7
TOE Identification	8
TOE Scope and TOE Configuration	8
TOE Documentation	8
TOE Environment	8
III. TOE TESTING	9
Vulnerability Analysis	9
TOE Testing	9
IV. SUMMARY, CONCLUSIONS AND DISCLAIMERS	11
Summary	11
Conclusions	11
Disclaimers	11
V. REFERENCES	13
VI. ABBREVIATIONS	16

I. INTRODUCTION

Overview

1. This Assurance Maintenance Report (MR¹) [MR1] states the outcome of the Common Criteria (CC) [CC] Assurance Continuity [AC] process for *McAfee Firewall Enterprise, Version 7.0.1.03*, as summarised on page 2 ‘Certification Statement (Addendum)’ 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 original CC evaluation of *McAfee Firewall Enterprise, Version 7.0.1.02HW02*. That version was certified to CC EAL 4 augmented by ALC_FLR.3, in January 2011. See [ST], [CR] and [PP] for full details.
3. Prospective consumers are advised to read this document [MR1] in conjunction with the following documents (available on the CESG and CC websites):
 - a) the Security Target [ST] for the original certified Target of Evaluation (TOE), which specifies the functional, environmental and assurance requirements for the evaluation;
 - b) the Certification Report [CR] for the original certified TOE, to which this report is an Addendum;
 - c) the updated Security Target [ST1] for the latest maintained derivative.
4. The Developer of the certified TOE, and the derived maintained version, is detailed on page 2 ‘Certification Statement (Addendum)’ of this report and elaborated further on the CESG website (www.cesg.gov.uk).

Maintained Versions

5. The version of the product originally evaluated was:
 - *McAfee Firewall Enterprise, Version 7.0.1.02HW02*, running on S1104, FW-410F, FW-510F, FW-1100F, FW-2100F, FW-2150F, FW-4150F, FW-2150F-VX04, and RM700F; also VMware vSphere Hypervisor (ESXi) version 4.0 and onwards, and Riverbed Steelhead 250, 550, and 1050 appliances.
6. The latest derived version of the product for which assurance is maintained is:
 - *McAfee Firewall Enterprise, Version 7.0.1.03*, running on Models S1104, S2008, S3008, S4016, S5032, S6032, S7032-04, S7032-08, S7032-16, S7032-32, 1100E, 2150E, 4150E, FW-410F, FW-510F, FW-1100F, FW-2100F, FW-2150F, FW-4150F, FW-2150F-VX04, and RM700F; also VMware vSphere Hypervisor (ESXi) version 4.0, and Riverbed Steelhead 250-H, 550-H, 1050-H and 2050-H appliances.

¹ Assurance Maintenance Report (AMR) is often abbreviated to Maintenance Report (MR).

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

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 UK specific aspects are presented in [UKSP03P2].

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 *McAfee Firewall Enterprise, Version 7.0.1.03*, the IAR [IAR1] has been examined by the CESG Certification Body (CB), who produced this Maintenance Report No. 1 [MR1].

10. The Developer, McAfee Inc., has carried out retesting on *McAfee Firewall Enterprise, Version 7.0.1.03* as documented in [Test_Map], [Test_Rep] and [Vul_Rep]; 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 Chapter II of this report [MR1], 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 *McAfee Firewall Enterprise, Version 7.0.1.02HW02*, to *McAfee Firewall Enterprise, Version 7.0.1.03*, and provides the Assurance Continuity rationale for the maintained TOE on the stated platforms. [IAR1] conforms to the Assurance Continuity requirements specified in [AC], in particular Chapters 4 and 5.

13. No major changes that could cause a security impact on the TOE were made between the certified version and the derived version. As described in Chapter 2 of [IAR1], all security relevant changes were either bug fixes, which ensured that the security functions specified in the Security Target [ST1] were implemented correctly, or were product enhancements that did not impact on the security functionality of the TOE.

14. One significant change to the TOE development environment since the certified version was the move from the Action Request (AR) System from Remedy Corporation to the Bugzilla tracking tool. However, the security impact of this change is *Minor* since the Remedy and Bugzilla tools offer similar features for the tracking of issues from entry into the system to closure and the bug/flare tracking procedures have not changed. There were no changes that directly impacted the *ALC_FLR.3* augmentation since there were no changes to any of the deliverables that provided input into the associated evaluation activity.

15. The TOE changes and their impact and effect on the evaluation deliverables are described in Chapter 3 of [IAR1], which shows that *for all changes*:

- a) The impact of change is determined to be *Minor* or *None*.
- b) The effect on evaluation deliverables is determined to be *Minor* or *None*.
- c) The action required for resolution is determined to be *None* (since evaluation deliverables have already been updated).

16. Note that:

- a) Only minor generic changes were required to the Security Target [ST], to reflect TOE version changes, platform changes and correction of typographical errors; resulting in [ST1].
- b) Some platforms that were in the original *McAfee Firewall Enterprise, Version 7.0.1.02HW02*, evaluation have been removed from the TOE Scope and this clearly has no impact on the security of the remaining platforms.
- c) Some additional platforms have been included in the TOE Scope of the Assurance Continuity for *McAfee Firewall Enterprise, Version 7.0.1.03*:

- (i) S2008, S3008, S4016, S5032, S6032;

CRP261 MR1 – McAfee Firewall Enterprise 7.0.1.03

- (ii) S7032-04, S7032-08, S7032-16 and S7032-32 – these are the same base appliance, but with a differing number of NICs (indicated by the last 2 digits of the appliance identifier) and memory;
 - (iii) 1100E, 2150E, 4150E;
 - (iv) Riverbed Steelhead 250-H, 550-H, 1050-H and 2050-H.
- d) The above additional platforms are similar to the certified platforms and only differ in the following attributes: Chassis, Form Factor, CPU, Memory, Hard Disk, RAID, NICs, Out of Band Mgmt/Remote Access, Optical Drive. The variation of these attributes over the additional platforms does not affect the security functionality of the Security Target [ST1] in relation to [ST].
- e) Some of the changes to the product were related to application protocols which were not included within the scope of the original evaluation of *McAfee Firewall Enterprise, Version 7.0.1.02HW02*, and hence were considered to be outside the scope of the Assurance Continuity for *McAfee Firewall Enterprise, Version 7.0.1.03*. For example, support for SNMPv3 has been added to the MFE product as stated in Section 2.1 of [IAR1] but the use of SNMP is excluded from the TOE as stated in Section 2.3.2 and Section 5.1.11, covering FDP_IFF.1.5(1) part f), of [ST1].
- f) Some of the changes were related to aspects of the product in general, which were not related to any Security Functional Requirements (SFRs), and hence were considered to be out of scope of the TOE. These are stated in Section 2.1 of [IAR1] as customer support for upgrading, third party tool support, GUI fixes/corrections, changes to High Availability (HA) functionality and fixes/updates to drivers.

17. The crypto module validation is covered by FIPS 140-2 [FIPS 140-2] validation certificate numbers (*TBD*²).

Changes to Developer Evidence

18. Chapter 3 of [IAR1] shows that the *only* evaluation documentation deliverables that were updated for *McAfee Firewall Enterprise, Version 7.0.1.03*, were as follows:

- McAfee Firewall Enterprise Security Target [ST1].
- McAfee Firewall Enterprise Functional Specification [FS1]
- McAfee Firewall Enterprise TDS [TDS1]
- McAfee Firewall Enterprise Source files [SF1]

² This document [MR1] will be update with respect to the outcome of the latest FIPS 140-2 validation of the cryptographic module used by MFE 7.0.1.03 when it completes in the CMVP.

- McAfee Firewall Enterprise Configuration List [CL1]
- McAfee Firewall Enterprise Test coverage and depth mapping [Test_Map]
- McAfee Firewall Enterprise Test Report [Test_Rep]
- *(New for Assurance Maintenance)* Vulnerability Analysis [Vul_Rep]
- Common Criteria Evaluated Configuration Guide [ECG1]
- McAfee Firewall Enterprise Administration Guide [AG1]
- McAfee Firewall Enterprise Release Notes [RN1]

19. All updates in the above documents were classified as Minor.

TOE Identification

20. The maintained TOE is uniquely identified as:

- **McAfee Firewall Enterprise, Version 7.0.1.03** running on Models S1104, S2008, S3008, S4016, S5032, S6032, S7032-04, S7032-08, S7032-16, S7032-32, 1100E, 2150E, 4150E, FW-410F, FW-510F, FW-1100F, FW-2100F, FW-2150F, FW-4150F, FW-2150F-VX04, and RM700F; also VMware vSphere Hypervisor (ESXi) version 4.0, and Riverbed Steelhead 250-H, 550-H, 1050-H and 2050-H appliances.

TOE Scope and TOE Configuration

21. The TOE scope is described in Section 2.3 *Physical and Logical Boundaries* of [ST1] and the latest Evaluated Configuration is defined in [ST1] Section 2.3 and [ECG1].

TOE Documentation

22. The Installation, Configuration and Guidance documents have changed as described in Paragraph 17.

TOE Environment

23. The defined environment is defined in [ST1] and the only change has been described above in Paragraph 14.

III. TOE TESTING

Vulnerability Analysis

24. In order to assess whether any vulnerabilities had been introduced into the product between *McAfee Firewall Enterprise, Version 7.0.1.02HW02*, and *McAfee Firewall Enterprise, Version 7.0.1.03*, the Developer performed an analysis of the Bugzilla flaw reporting/tracking tool, as well as public domain vulnerabilities. The same level of vulnerability analysis, in accordance with EAL4 requirements, was performed for the re-assessment as was performed for the original evaluation. The information assessed also contained details of generic vulnerabilities, so any generic vulnerabilities relevant to *McAfee Firewall Enterprise* were automatically included in the analysis.

25. Chapter 2 of [IAR1] describes the enhancements and fixes to flaws or bugs within the scope of the maintained TOE between Version 7.0.1.02HW02 and Version 7.0.1.03.

26. During the original evaluation, the vulnerability analysis was based on a search of public domain sources primarily based on <http://cve.mitre.org> and <http://nvd.nist.gov>. That search was repeated on 6 October 2011 leading to the creation of [Vul_Rep] which shows the Status of all listed vulnerabilities as *Closed*, with a Resolution rating of *Fixed*, as a result of the testing activity described below.

27. Chapter 4 of [IAR1] refers to [Vul_Rep] for a summary of the Developer's search for vulnerabilities performed on public domain sources (key security websites) in order to assess whether any vulnerabilities had been introduced into the product between *McAfee Firewall Enterprise, Version 7.0.1.02HW02*, and *McAfee Firewall Enterprise, Version 7.0.1.03*.

28. In summary, no vulnerabilities were found between the certified version of the TOE (*McAfee Firewall Enterprise, Version 7.0.1.02HW02*) and the maintained version of the TOE (*McAfee Firewall Enterprise, Version 7.0.1.03*).

TOE Testing

29. As explained in Chapter 4 of [IAR1], the Quality Assurance team within McAfee Inc. executed the predefined Developer's QA test plan for *McAfee Firewall Enterprise, Version 7.0.1.03*. The test plan covered new feature testing (for CAC, OCSP, SNMPV3 and HA reboot), regression testing (for bug fixes) and upgrades testing (from 7.0.1.02HW02 to 7.0.1.03).

30. The evaluator tests used for *McAfee Firewall Enterprise, Version 7.0.1.02HW02*, were assessed for any impact caused by modified functionality in *McAfee Firewall Enterprise, Version 7.0.1.03*. The affected tests were rerun on the TOE software, hosted on a representative subset of the appliances identified in [ST1]. In order to ensure consistency, the identified tests were performed on a virtual appliance (ESX4.0) and on a new S-model, the S5032 appliance.

31. Tests were run on the TOE corresponding to the Bugzilla entries [Vul_Rep], to demonstrate the resolution of the identified public domain vulnerabilities. For each Bugzilla entry, the developer only declares the issue "Closed" once the related testing has achieved a Pass verdict.



32. The testing performed for the evaluation of *McAfee Firewall Enterprise, Version 7.0.1.02HW02*, was manual and was controlled by a set of test scripts.

33. 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. The Developer holds developer test scripts, which have been updated. The Developer only holds evaluator test scripts in terms of the Evaluation Technical Report (ETR), and as such does not update those test scripts.

34. The tests for *McAfee Firewall Enterprise, Version 7.0.1.03*, were run on a representative sample of all of the platforms included within the scope of the maintenance. All of those tests passed and the results did not reveal any inconsistencies or concerns.

35. Thus confidence is established that *McAfee Firewall Enterprise, Version 7.0.1.03*, provides the claimed security functionality in the same manner as *McAfee Firewall Enterprise, Version 7.0.1.02HW02*.

IV. SUMMARY, CONCLUSIONS AND DISCLAIMERS

Summary

36. The analyses in [IAR1] show that no major changes have been made to the TOE between *McAfee Firewall Enterprise, Version 7.0.1.02HW02*, and *McAfee Firewall Enterprise, Version 7.0.1.03*. The only changes have been bug-fixes, which have been categorised as having a **Minor** impact and hence CC EAL 4 augmented by ALC_FLR.3 assurance has been maintained.

Conclusions

37. The 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**.

38. The Certification Body has therefore determined that EAL 4 augmented by ALC_FLR.3, as outlined in Certification Report P261 [CR], has been maintained for the latest derived version, *McAfee Firewall Enterprise, Version 7.0.1.03*, running on Models S1104, S2008, S3008, S4016, S5032, S6032, S7032-04, S7032-08, S7032-16, S7032-32, 1100E, 2150E, 4150E, FW-410F, FW-510F, FW-1100F, FW-2100F, FW-2150F, FW-4150F, FW-2150F-VX04, and RM700F; also VMware vSphere Hypervisor (ESXi) version 4.0, and Riverbed Steelhead 250-H, 550-H, 1050-H and 2050-H appliances. These conclusions are summarised in the ‘Certification Statement (Addendum)’ on Page 2.

39. Prospective consumers of *McAfee Firewall Enterprise, Version 7.0.1.03*, 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.

40. 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 P261 [CR].

Disclaimers

41. 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 Certification Body’s view at the time of certification.

42. 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.



43. 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.

44. 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, Senior Officials Group – Information Systems Security (SOGIS), Version 3.0, 8 January 2010 (effective April 2010).

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.
- [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] McAfee Firewall Enterprise v7.0.1.02 Security Target,
McAfee Inc.,
Issue 1.3, 8 November 2010.
- [CR] Common Criteria Certification Report No. CRP261, McAfee Firewall Enterprise,
Version 7.0.1.02HW02,
CESG Certification Body,
Issue 1.0, January 2011.
- [PP] U.S. Government Protection Profile for Application-level Firewall in Basic
Robustness Environments,
Version 1.1, July 25, 2007.

First Derived Version

- [ST1] McAfee Firewall Enterprise v7.0.1.03 Security Target,
McAfee Inc.,
Version 1.1, 31 October 2011.
- [ECG1] Common Criteria Evaluated Configuration Guide, McAfee® Firewall Enterprise
(Sidewinder®), version 7.0.1.03,
McAfee Inc.,
Part number 700-3113A00, November 2011.
- [FS1] McAfee Firewall Enterprise v7.0.1.03 Functional Specification
McAfee Inc.,
Version 1.0, August 2011.
- [TDS1] McAfee Firewall Enterprise v7.0.1.03 TDS
McAfee Inc.,
Version 1.0, August 2011.
- [SF1] Source files (7.0.1.03 branch of CVSSERV.SCUR.COM)
McAfee Inc.,
(Please note that 7.0.1.03 is the unique identifier for the source files.)

CRP261 MR1 – McAfee Firewall Enterprise 7.0.1.03

- [IAR1] McAfee Enterprise Firewall (MFE) Version 7.0.1.03, Impact Analysis Report, McAfee Inc.,
Version 1.1, 31 October 2011.
- [RN1] Release Notes, McAfee® Firewall Enterprise (Sidewinder®), version 7.0.1.03
McAfee Inc.
Part number 700-3292A00, 2011.
- [AG1] McAfee® Firewall Enterprise (Sidewinder®) Administration Guide, version
7.0.1.03
McAfee Inc.
Part number 700-3108A00, June 2011.
- [CL1] McAfee Firewall Enterprise 7.0.1.03 Configuration List
McAfee Inc.
Version 1.2, 31 October 2011
- [MR1] (*this document*)

Test Documents

- [Test_Map] McAfee Firewall Enterprise v7.0.1.03, Test coverage and depth mapping,
McAfee Inc.,
Version 1.0, August 2011.
- [Test_Rep] McAfee Firewall Enterprise v7.0.1.03 Test Report,
McAfee Inc.,
Version 1.1, 28 October 2011.
- [Vul_Rep] McAfee Firewall Enterprise v7.0.1.03 Vulnerability Test Report,
McAfee Inc.,
Version 1.0, 06-Oct-11.

FIPS Documents

- [FIPS 140-2] Security Requirements for Cryptographic Modules,
Federal Information Processing Standard Publication,
FIPS PUB 140-2, 25 May 2001.

VI. ABBREVIATIONS

This list of abbreviations is specific to the TOE. It therefore excludes: general IT abbreviations (e.g. GUI, HTML, LAN, PC) or standard Common Criteria abbreviations (e.g. TOE, TSF) covered in CC Part 1 [CC1]) and UK Scheme abbreviations (e.g. CESG, CLEF) covered in [UKSP00]).

AR	Action Request
CAC	Common Access Card
HA	High Availability
MFE	McAfee Firewall Enterprise
OCSP	Online Certificate Status Protocol
SNMP	Simple Network Management Protocol