122-B

CERTIFICATION REPORT No. CRP261

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

Issue 1.0

January 2011

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

CERTIFICATION STATEMENT

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

Sponsor:	McAfee Inc.	Developer:	McAfee Inc.
Product and Version:	McAfee Firewall Enterprise Version 7.0.1.02HW02		
Platform:	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		
Description:	McAfee Firewall 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:	EAL4 augmented by ALC_FLR.3		
PP Conformance:	U.S. Government Protection Profile for Application-level Firewall in Basic Robustness Environments [PP]		
CLEF:	Logica		
CC Certificate:	CRP261	Date Certified:	21 January 2011

The evaluation was performed in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme as described in UK 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.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [ST], 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 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 is a confirmation that the evaluation process has been performed 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 CESG 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 SOGIS MRA logo which appears below confirms that the conformant certificate has been authorised by a Participant to this Agreement and it is the Participant's statement that the certificate has been issued in accordance with the terms of this Agreement.

The judgments[1] contained in the certificate and this Certification Report are those of the compliant Certification Body which issued them and of the Evaluation Facility which carried out the evaluation. Use of the logo 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.

CCRA logo **CC logo** **SOGIS MRA logo**

[1] All judgements contained in this Certification Report, are covered by the CCRA [CCRA] and the MRA [MRA].

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria (CC) security evaluation of McAfee Firewall Enterprise Version 7.0.1.02HW02 to the Sponsor, McAfee Inc., as summarised on page 2 'Certification Statement' 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. Prospective consumers are advised to read this report in conjunction with the Security Target [ST][2], which specifies the functional, environmental and assurance requirements.

Evaluated Product and TOE Scope

3. The following product completed evaluation to CC **EAL4** augmented by ALC_FLR.3 on 31 December 2010:

   - **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**

4. The Developer was McAfee Inc.

5. The evaluated configuration of this product is described in this report as the Target of Evaluation (TOE). Details of the TOE Scope, its assumed environment and the evaluated configuration are given in Chapter III 'Evaluated Configuration' of this report.

6. An overview of the TOE and its product architecture can be found in Chapter IV 'Product Architecture' of this report. Configuration requirements are specified in Section 2.3 of [ST] and in the Evaluated Configuration Guide [ECG].

Protection Profile Conformance

7. The Security Target [ST] is certified as achieving conformance to the following protection profile:

   - U.S. Government Protection Profile for Application-level Firewall in Basic Robustness Environments [PP].

8. The Security Target [ST] also includes objectives and Security Functional Requirements (SFRs) additional to those of the protection profile.

[2] Note that the Security Target [ST] uses the phrase "VMware (3.5 or 4) ESX Server"; however this platform reference was subsequently determined by the Sponsor to be outdated. Therefore, this Certification Report uses the correct platform reference, which is "VMware vSphere Hypervisor (ESXi) version 4.0 and onwards". It was not considered necessary to update the Security Target for just this change.

Security Claims

9. The Security Target [ST] fully specifies the TOE's Security Objectives, the Threats which these Objectives counter, the Organisational Security Policies (OSPs) that should be met and the Security Functional Requirements (SFRs) that achieve the Objectives. Most of the SFRs are taken from CC Part 2 [CC2]; use of this standard facilitates comparison with other evaluated products.

10. The TOE security policies are detailed in the ST [ST]. The OSPs that must be met are specified in [ST] Section 3.3.

11. The environmental assumptions related to the operating environment are detailed in Chapter III (in 'Environmental Requirements') of this report.

Evaluation Conduct

12. The CESG Certification Body monitored the evaluation which was performed by the Logica Commercial Evaluation Facility (CLEF). The evaluation addressed the requirements specified in the Security Target [ST]. The results of this work, completed in December 2010, were reported in the Evaluation Technical Report [ETR] and Supplement [SUPP].

Conclusions and Recommendations

13. The conclusions of the CESG Certification Body are summarised on page 2 'Certification Statement' of this report.

14. Prospective consumers of McAfee Firewall Enterprise Version 7.0.1.02HW02 should understand the specific scope of the certification by reading this report in conjunction with the Security Target [ST] and [PP]. 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.

15. The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration. Chapter II 'TOE Security Guidance' of this report includes a number of recommendations regarding the secure receipt, installation, configuration and operation of the TOE.

16. The Evaluators did not have any additional comments and recommendations to make, all observations and recommendations having been duly addressed by the Developer during the course of the evaluation. The Sponsor intends to add the following sentence to the Maintenance section on page 13 of the Evaluated Configuration Guide [ECG]:

- "Administrators should take appropriate steps to safeguard any configuration backup files against unauthorised access, and should consider using the optional encryption feature as an additional protective measure."

Disclaimers

17. This report is only valid for the evaluated TOE. This is specified in Chapter III 'Evaluated Configuration' of this report.

18. Certification 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 an evaluation has been completed. This report reflects the CESG Certification Body's view at the time of certification.

19. Existing and prospective consumers should check regularly for themselves whether any security vulnerabilities have been discovered since the ETR 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.

20. 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.

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

II. TOE SECURITY GUIDANCE

Introduction

22. The following sections provide guidance that is of particular relevance to purchasers of the TOE.

Delivery

23. On receipt of the TOE, the consumer is recommended to check that the evaluated version has been supplied, and to check that the security of the TOE has not been compromised during delivery.

24. In particular, the procedures detailed in the section *Verifying a secure delivery* in [ECG] must be followed. These include:

a) Visual inspection of packages and their contents for evidence of tampering or attempted masquerade.

b) Examination of shipping and tracking information for unexpected timing or routing details.

c) Confirmation that the correct CD version has been received (i.e. version 7.0.1.02HW02).

d) Download of the correct ISO image file from the McAfee Technical Support Service Portal, in the event of the CD version being incorrect.

e) Verification of CD contents against shipping information and MD5 signature verification.

Installation and Guidance Documentation

25. The Installation and Secure Configuration documentation is as follows:

- [ECG];
- [SUG];
- [VPAG].

26. The User Guide and Administration Guide documentation is as follows:

- [AG].

III. EVALUATED CONFIGURATION

TOE Identification

27. The TOE is McAfee Firewall Enterprise Version 7.0.1.02HW02, which consists of the firewall application and the SecureOS operating system, running on a dedicated McAfee appliance platform or virtual appliance. The TOE also includes the Admin Console client software (the McAfee Firewall Enterprise (Sidewinder) Admin Console version 4.10).

TOE Documentation

28. The relevant guidance documentation for the evaluated configuration is identified in Chapter II (in 'Installation and Guidance Documentation') of this report.

TOE Scope

29. The TOE Scope is defined in the Security Target [ST] Section 2. Functionality that is outside the TOE Scope is defined in [ST] Section 2.3.3.

TOE Configuration

30. The evaluated configuration of the TOE is defined in Section 2.3 of [ST] and in [ECG].

Environmental Requirements

31. The environmental assumptions for the TOE are stated in Section 3.1 of the Security Target [ST].

32. The TOE was evaluated 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.

33. Further details on IT environment requirements are provided in the Security Target [ST] Section 2.3.4.

Test Configuration

34. The Developers used the configuration illustrated in the diagram below for their testing, for which the following points should be noted:

    a) The firewall was installed and connected to networks designated as either Internal or External as illustrated in the diagram.

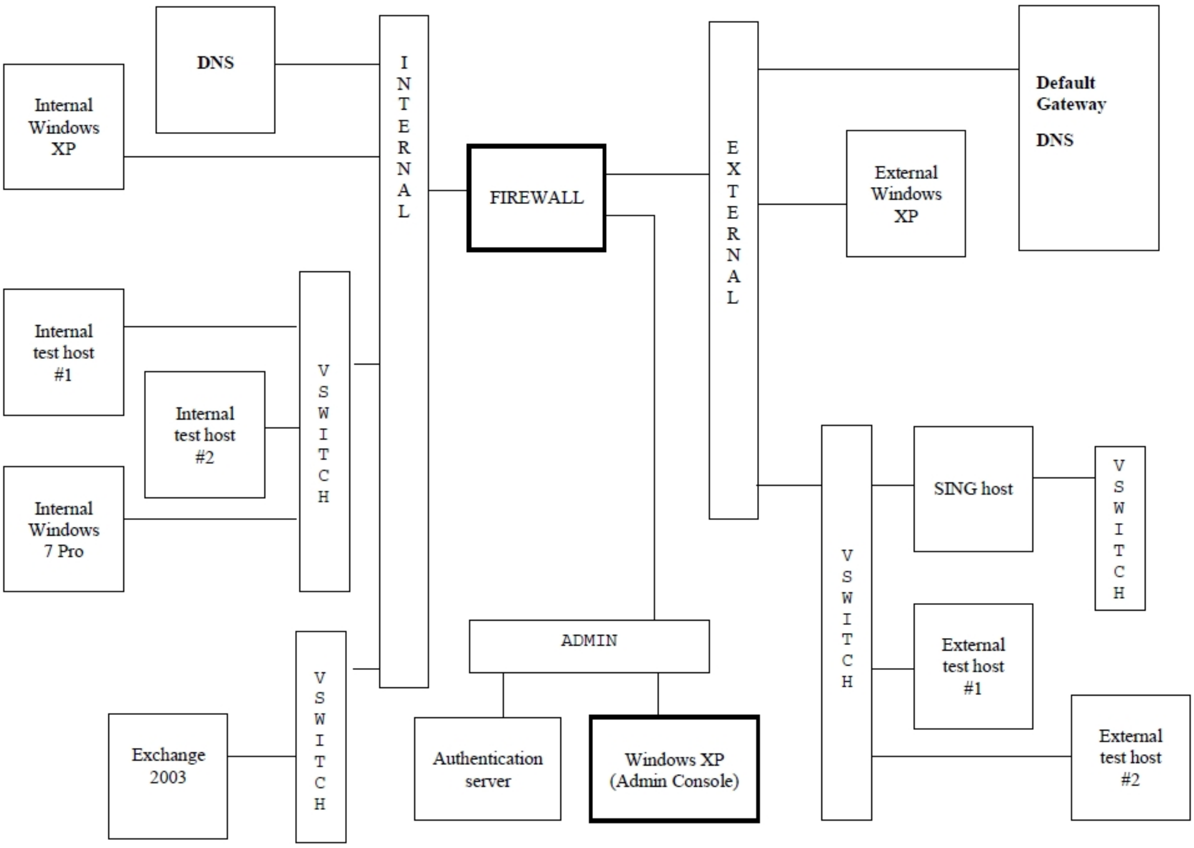
    b) The firewall was managed from a Windows XP PC running Admin Console client software version 4.10. (The PC met the minimum requirements as specified in the Security Target [ST] Section 2.3.4.1).

c) Unless otherwise specified (i.e. Windows hosts), the external and internal test hosts are all Unix-based (FreeBSD 7.2), and were used for firewall policy testing (typically using FTP or Telnet, or specific test scripts to generate traffic).

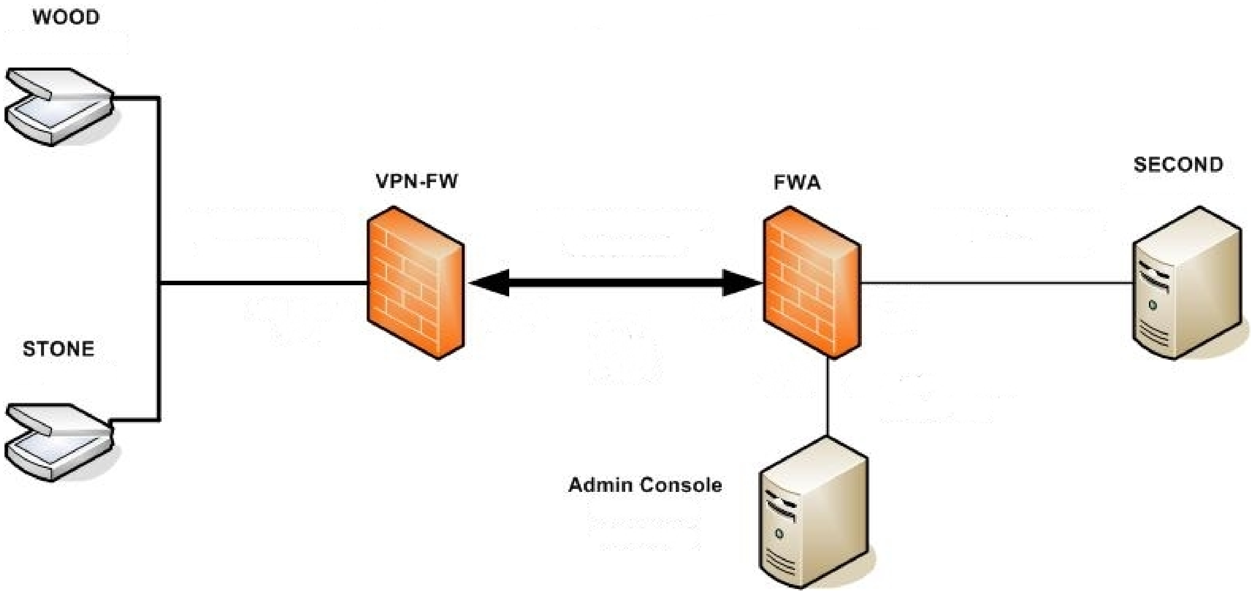
d) A SafeWord Premier Access server was used as the external Authentication Server.

e) DNS requests for the internal network are forwarded to the name server on the internal network for resolution. DNS requests for the external network are forwarded to the name server on the external network.

f) Not shown on the diagram, but reachable from the external network via the Default Gateway, are the license server, patch server and root name server.



35. The Developer also used the following test configuration, specifically for testing the firewall's VPN functionality.



36. FWA is the McAfee Firewall under test, protecting a FreeBSD server named SECOND. VPN-FW is a McAfee Firewall protecting the two VPN clients within a remote network. One of the VPN clients is a Windows XP workstation (named STONE) and the other is a Windows 7 workstation (named WOOD). There is also an Admin Console shared by both Firewalls, hosted on a Windows XP workstation and connected to FWA at the Admin interface, which is not part of the VPN.

37. The Evaluators used the same configurations for their testing.

IV. PRODUCT ARCHITECTURE

Introduction

38. This Chapter gives an overview of the TOE's main architectural features. Other details of the scope of evaluation are given in Chapter III 'Evaluated Configuration' of this report.

Product Description and Architecture

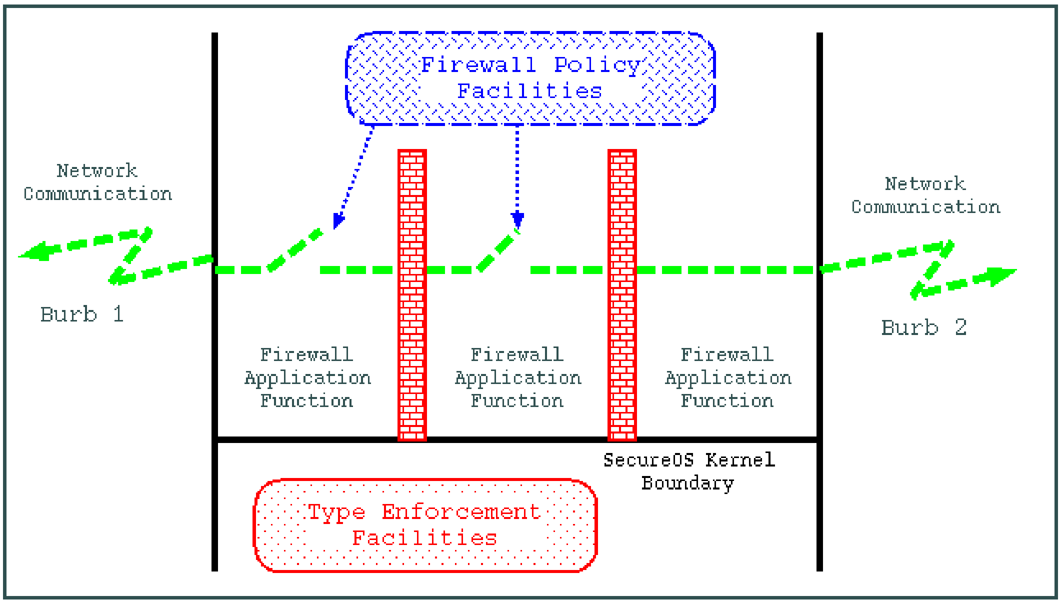
39. A description of the product is provided in the Security Target [ST] Section 2.

40. The McAfee Firewall Enterprise (MFE) appliance provides a high level of security by using SecureOS®, an enhanced UNIX operating system that employs McAfee's patented Type Enforcement® security technology. The Type Enforcement facilities provide mandatory access controls for all processes and data objects, separating all operational elements from those of other modules. The MFE Type Enforcement security policy data is static; it is defined as part of the product release, loaded into the kernel during system initialisation, and cannot be modified by any operational element. It is used to protect the TSF and its data (such as configuration files, executables, scripts and audit logs) from tampering.

41. The enforcement of the firewall policy is done within the firewall application functions which control the inter-network communication that passes through the firewall. This network communication control may be done within the application layer processing (in the case of proxies and servers) or within the network stack processing (for communications controlled by IP-filter functions).

42. The TOE additionally supports encryption for remote administration, remote proxy users and authorized IT entities (e.g. certificate server, NTP server), and generates audit data of security relevant events. The TOE also provides VPN capability to encrypt out-going traffic flowing to a geographically separated enclave and decrypt in-coming traffic from such an enclave.

43. The following diagram provides a high-level view of the security architecture of the TOE.


Firewall Policy Facilities
Network Communication
Network Communication
Burb 1
Burb 2
Firewall Application Function
Firewall Application Function
Firewall Application Function
SecureOS Kernel Boundary
Type Enforcement Facilities

TOE Design Subsystems

44. The TOE subsystems, and their security features/functionality, are as follows:

a) SecureOS Kernel: this comprises the FreeBSD Unix kernel with MFE extensions. In addition to the normal Unix memory management and hardware management functionality, it also implements (as part of the MFE extensions) the Type Enforcement policy and provides low-level support to the IP-Filter, IPsec and Audit Policy enforcement.

b) SecureOS Utilities: this comprises the Core OS daemons and services with MFE extensions. This includes implementation of the MFE Audit Facilities, the Key Management Server, system startup and shutdown functionality, and session establishment.

c) Firewall Management: this comprises the daemons and commands that implement the firewall security management functions. In particular it implements the Admin Console GUI (client and backend) together with the security policy database and configuration files.

d) Firewall Policy: this provides the firewall application layer policies and support software. It implements the four firewall policy elements: Access Control List (ACL), IP-Filter, User Authentication and IPsec. As such it plays a key role in the enforcement of the UNAUTHENTICATED, AUTHENTICATED and VPN SFPs as defined in the Security Target [ST] Section 5.

e) Firewall Communication Control: this provides control and monitoring of network connections through the firewall. It implements the protocol aware proxies (such as HTTP, HTTPS, Telnet and FTP), generic proxies (TCP and UDP) and server proxies (including the ISAKMP server).

f) System Utilities: this comprises a collection of utility commands and libraries used by the above subsystems.

TOE Dependencies

45. The TOE dependencies are as follows:

a) Hardware and software requirements for running the Admin Console client software are specified in the Security Target [ST] Section 2.3.4.1.

b) Hardware security requirements are specified in the Security Target [ST] Section 2.3.4.2.

c) The TOE may be configured to use external authentication servers to authenticate users for specific services.

d) The TOE may also be configured to use external certification or NTP servers.

e) When establishing VPNs, McAfee Firewall will exchange identities and perform device-level authentication of the remote device (peer McAfee Firewall or remote VPN gateway). Device-level authentication is performed using authentication techniques specified in RFC 2409 and RFC 4306. Peers will mutually authenticate themselves to each other before establishing the secure channel.

TOE Interfaces

46. The external TOE Security Functions Interface (TSFI) is described as follows:

a) Network Interfaces, comprising: Link Layer, Network Layer (IPv4, ICMP, IGMP, IPv6, ICMPv6), Transport Protocol Layer (TCP, UDP), Application Layer Proxy Protocol (including protocol aware and generic proxies), and Application Layer Server Protocol.

b) Administrative Interface, which comprises the Admin Console GUI interface. (Note: the product also incorporates a CLI administrative interface, but this is disabled in the evaluated configuration).

c) Serial UPS Interface (which is categorised as SFR non-interfering).

V. TOE TESTING

TOE Testing

47. The Developer’s tests covered:

a) all SFRs;

b) all TOE high-level subsystems, as identified in Chapter IV (in ‘TOE Design Subsystems’) of this report;

c) the TSFI, as identified in Chapter IV (in ‘TOE Interfaces’) of this report.

48. The Developer’s tests also included those TOE interfaces which are internal to the product and thus had to be exercised indirectly.

49. The Developers ran all their tests on high and low-end appliances (FW-4150F and S1104 models, respectively), together with a sample of tests on the FW-2150F-VX04 Virtual Appliance. This testing was supported by a multi-platform rationale (see paragraph 55 below) that justified why the results applied to all platforms claimed in the [ST].

50. The Evaluators devised and ran a total of 17 independent functional tests, different from those performed by the Developer. No anomalies were found.

51. The Evaluators also devised and ran a total of 14 penetration tests to address potential vulnerabilities considered during the evaluation. Penetration testing incorporated a combination of automated and manual techniques, the former including use of `nmap` 5.30BETA and the JBroFuzz protocol fuzzer to generate arbitrary and/or malicious network traffic. No exploitable vulnerabilities or errors were detected, as the test findings resulted in recommendations that were subsequently incorporated into [ECG].

52. The evaluators further validated the Developer’s test platform rationale by carrying out their tests on selected ‘mid-range’ platforms, namely the FW-1100F appliance (for repetition of Developer tests) and the FW-2100F appliance (for additional functional and penetration testing). A selection of tests was also run on the FW-2150F-VX04 Virtual Appliance.

53. The Evaluators completed their penetration tests on 8 December 2010.

Vulnerability Analysis

54. The Evaluators’ vulnerability analysis, which preceded penetration testing and was reported in [ETR], was based on public domain sources and the visibility of the TOE provided by the evaluation deliverables.

Platform Considerations

55. Potential consumers should note the following platform considerations:

a) The Developer provided a rationale for the platform coverage achieved by the Developer's test approach, which listed the platforms claimed in [ST], and enumerated their characteristics. All have the same platform architecture, with the exception of the Virtual Appliance, which uses VMware vSphere Hypervisor (ESXi), version 4.0 and onwards, to virtualise the hardware presented to the TOE. The code paths executed are not dependent on the hardware platform, and differences in characteristics (such as processor speed, RAM or network cards) only have an impact on performance and/or scale.

b) Developer testing on the selected platforms (high and low end, together with the Virtual Appliance) showed no differences in test results between the different platforms.

c) Evaluator testing on the selected mid-range platforms showed no differences in test results between the different platforms.

d) There are nonetheless specific configuration recommendations in [ECG] that should be followed, including applying the latest security patches to the VMware vSphere Hypervisor (ESXi), version 4.0 and onwards, and hardening the VMware implementation.

VI. REFERENCES

[AG] McAfee Firewall Enterprise (Sidewinder) v7.0.1.02 Administration Guide,
McAfee Inc.,
March 2009.

[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.

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

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

[ECG] Common Criteria Evaluated Configuration Guide,
McAfee Firewall Enterprise (Sidewinder) version 7.0.1.02HW02,
McAfee Inc.,
December 2010.

[ETR] Evaluation Technical Report,
Logica CLEF,
LFL/T268/ETR, Issue 1.0, December 2010.

[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).

[PP] U.S. Government Protection Profile for Application-level Firewall in Basic Robustness Environments,
Version 1.1, July 25, 2007.

[ST] McAfee Firewall Enterprise v7.0.1.02 Security Target,
McAfee Inc.,
Issue 1.3, 8 November 2010.

[SUG] McAfee Firewall Enterprise (Sidewinder) v7.0.1 Setup Guide,
McAfee Inc.,
March 2009.

[SUPP] Supplement to LFL/T268 [ETR],
CESG Certification Body,
CB/101210(2)/LFL/T265, (final update) 19 January 2011.

[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.

[VPAG] McAfee Firewall Enterprise (Sidewinder) v7.0.1.02 Virtual Appliance Product Guide,
McAfee Inc.,
April 2009.

VII. ABBREVIATIONS

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

ACL	Access Control List
BSD	Berkeley Software Distribution
DNS	Domain Name System
ISAKMP	Internet Security Association and Key Management Protocol
MFE	McAfee Firewall Enterprise
NTP	Network Time Protocol
RFC	Request for Comments
VM	Virtual Machine
VPN	Virtual Private Network