UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME

122-B

COMMON CRITERIA CERTIFICATION REPORT No. P186

3Com Embedded Firewall

Version 1.5.1

Issue 1.0

June 2003

UK IT Security Evaluation and Certification Scheme
Certification Body, PO Box 152
Cheltenham, Glos GL52 5UF
United Kingdom

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 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 contained in the certificate and Certification Report are those of the Qualified Certification Body which issued it and of the Evaluation Facility which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party. [*]

[*] Whilst the Arrangement has not yet been extended to address ALC_FLR.1 (basic flaw remediation), a working agreement exists amongst Parties to the Arrangement to recognise the Common Evaluation Methodology ALC_FLR supplement (Reference [h] in this report) and the resultant inclusion of ALC_FLR.1 elements in certificates issued by a Qualified Certification Body.

Trademarks:

The following trademarks are acknowledged:

Secure Computing is a trademark of Secure Computing Corporation; 3Com is a trademark of 3Com Corporation; Intel and Pentium are trademarks of Intel Corporation; Microsoft, Windows, Windows 2000, Windows NT and Windows XP are trademarks of Microsoft Corporation, Airborne and Airborne Express are trademarks of Airborne Express Incorporated.

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

CERTIFICATION STATEMENT

The 3Com Embedded Firewall is a distributed firewall and access control security platform for the enterprise.

The 3Com Embedded Firewall Version 1.5.1 has been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme and has met the specified Common Criteria Part 3 augmented requirements incorporating Evaluation Assurance Level EAL2 with ALC_FLR.1 for the specified Common Criteria Part 2 functionality in the specified environment when running on the platforms specified in Annex A.

Originator	**CESG** Certifier
Approval and Authorisation	**CESG** Head of the Certification Body UK IT Security Evaluation and Certification Scheme
Date authorised	30 June 2003

(This page is intentionally left blank)

TABLE OF CONTENTS

(This page is intentionally left blank)

ABBREVIATIONS

ACL	Access Control List
CC	Common Criteria
CEM	Common Evaluation Methodology
CLEF	Commercial Evaluation Facility
DBMS	Database Management System
DES	Data Encryption Standard
EAL	Evaluation Assurance Level
EFW	The 3Com Embedded Firewall
EFW Device	An NIC running EFW firmware
ETR	Evaluation Technical Report
IP	Internet Protocol
IPSEC	IP Security
ITSEC	Information Technology Security Evaluation Criteria
LAN	Local Area Network
NIC	Network Interface Card
SFR	Security Functional Requirement
SoF	Strength of Functions
TOE	Target of Evaluation
TSF	TOE Security Functions
UDP	User Data Protocol
UKSP	United Kingdom Scheme Publication
VPN	Virtual Private Network

(This page is intentionally left blank)

REFERENCES

a. 3Com Embedded Firewall Version 1.5.1 Security Target,
Secure Computing Corporation,
00-0937467-B, 5 March 2003.

b. Common Criteria Part 1,
Common Criteria Interpretations Management Board,
CCIMB-99-031, Version 2.1, August 1999.

c. Common Criteria Part 2,
Common Criteria Interpretations Management Board,
CCIMB-99-032, Version 2.1, August 1999.

d. Common Criteria Part 3,
Common Criteria Interpretations Management Board,
CCIMB-99-033, Version 2.1, August 1999.

e. Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 5.0, July 2002.

f. The Appointment of Commercial Evaluation Facilities,
UK IT Security Evaluation and Certification Scheme,
UKSP 02, Issue 3.0, 3 February 1997.

g. Common Methodology for Information Technology Security Evaluation,
Part 2: Evaluation Methodology,
Common Criteria Evaluation Methodology Editorial Board,
Version 1.0, CEM-099/045, August 1999.

h. Common Methodology for Information Technology Security Evaluation,
Part 2: Evaluation Methodology, Supplement: ALC_FLR - Flaw Remediation,
Common Criteria Evaluation Methodology Editorial Board,
CEM-2001/0015R, Version 1.1, February 2002.

i. Final Evaluation Technical Report for LFL/T155, Embedded Firewall 1.5.1,
Logica London CLEF,
CLEF.28463/7.2/1, Issue 1.0, 11 April 2003.

j. Administration Guide for 3Com Corporation Firewall (EFW) Version 1.5.1,
3Com Corporation,
86-0937734-A, 22 November 2002.

k. Quick Start Guide,
Secure Computing Corporation,
09-2110-002, November 2002.

l. Embedded Firewall 1.5.1 Evaluated Configuration Guide,
Secure Computing Corporation,
00-0937471-D, 7 April 2003.

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria security evaluation of 3Com Embedded Firewall Version 1.5.1 to the Sponsor, Secure Computing Corporation, 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 [Reference a] which specifies the functional, environmental and assurance evaluation requirements.

Evaluated Product

3. The version of the product evaluated was:

3Com Embedded Firewall Version 1.5.1.

This product is also described in this report as the Target of Evaluation (TOE). Developers were Secure Computing Corporation and 3Com Corporation.

4. The 3Com Embedded Firewall (EFW) is a distributed firewall and access control security platform designed for the enterprise. EFW is software that applies security policy enforcement capabilities (including packet filtering) to all traffic transmitted from and received by individual server and workstation machines.

5. Network Interface Cards (NIC) running EFW firmware (called EFW Devices) enforce policies in the EFW system. In particular the TOE uses a NIC from the family of 3Com NICs that support triple DES encryption. The EFW Policy Server automatically adjusts its level of encryption to match that of the devices it is managing.

6. EFW software provides transparent packet filtering in accordance with rules that are set up by an administrator. The rules are defined through a centralized Management Console and are communicated to EFW Devices via the Policy Server. EFW support management of EFW Devices that have a User Data Protocol (UDP) connection available to the Policy Server, including remote devices for which UDP traffic is encrypted under a Virtual Private Network (VPN) between the EFW Device and some computer (typically a VPN gateway) on the network on which the Policy Server resides.

7. EFW allows an administrator to specify policies for EFW Devices using the Management Console. A policy is a set of security criteria enforced by an EFW Device. A policy comprises various settings and an ordered list of rules, called an Access Control List (ACL), that determines what actions will take place and what events will be audited for any EFW Device associated with that policy. A rule consists of various parameters that determine the characteristics for which incoming and outgoing packets will be screened, and specifies what action will be taken if a match occurs.

8. EFW Devices in a computer that roams between two locations can detect their location and load a different policy for each of these locations. The typical example for this is a laptop computer that may connect directly to the enterprise Local Area Network (LAN), or may connect to the LAN via the enterprise VPN gateway when remote.

9. Version 1.5.1 of EFW contains a number of fixes and three minor enhancements to Version 1.5.

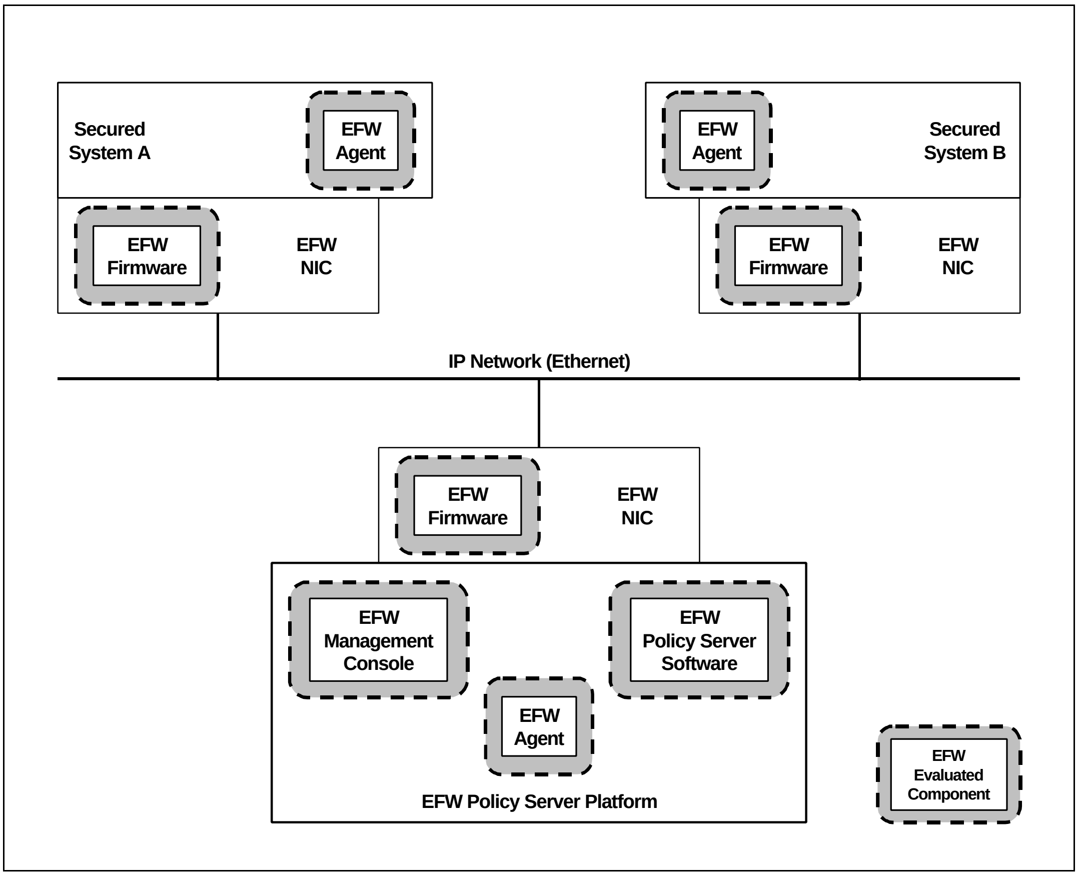
10. Details of the evaluated configuration, including the TOE's supporting guidance documentation, are given in Annex A.

11. An overview of the TOE's security architecture can be found in Annex B.

TOE Scope

12. The TOE is configured as in Figure 1 below.

Figure 1: TOE Configuration



13. The configured system consists of the following:

a. a combined Management Console and Policy Server running Windows 2000 Server, with a server or desktop triple DES NIC in the 3CRFW or 3CR990 family;

b. a laptop Secured Computer running Windows 2000 Professional, with a mobile model NIC in the 3CRFW family; and

c. a laptop Secured Computer running Windows XP Professional, with a mobile model NIC in the 3CRFW family.

14. All of these are protected by a triple DES EFW Device.

15. In addition to LAN connections, one of the laptop Secured Computers is equipped with an IPSEC VPN client to support VPN connection. It is configured to detect its location either by its IP address or by the presence or absence of a VPN connection.

16. The Policy Server is assumed to be in an area of controlled physical access and it supports administrative operations only through its directly connected console.

17. The following EFW functionality is excluded from the TOE and may be disabled and/or unsupported by the TOE configuration:

a. remote access for the EFW Management Console;

b. replicated EFW Policy Servers;

c. additional EFW locator options;

d. multiple NICs on Secured Computers;

e. management of NICs behind a router configured for Network Address Translation;

f. NICs installed on systems running Windows 98 or Windows NT; and

g. NICs running DES rather than triple DES.

18. The TOE consists of:

a. EFW Policy Server software;

b. EFW Management Console software (co-located with Policy Server software);

c. EFW Agent software; and

d. EFW firmware on NICs.

19. Other components which form part of the TOE environment include:

a. Operating Systems of the Policy Server and Secured Computers and

b. hardware of the Policy Server and Secured Computers and their NICs.

Protection Profile Conformance

20. The Security Target [a] did not claim conformance to any protection profile.

Assurance

21. The Security Target [a] specified the assurance requirements for the evaluation. The assurance incorporated predefined evaluation assurance level EAL2, augmented by ALC_FLR.1. Common Criteria Part 3 [d] describes the scale of assurance given by predefined assurance levels EAL1 to EAL7 (where EAL0 represents no assurance). An overview of CC is given in CC Part 1 [b].

Strength of Function Claims

22. The minimum Strength of Function (SoF) was SoF-Basic. This was claimed for the correct implementation of the triple DES encryption of security critical parameters transmitted over the network.

23. The cryptographic mechanism contained in the TOE, triple DES, is publicly known and as such it is the policy of the national authority for cryptographic mechanisms, CESG, not to comment on its appropriateness or strength.

Security Policy

24. The TOE security policies are detailed in the Security Target [a].

Security Claims

25. The Security Target [a] fully specifies the TOE's security objectives, the threats which these objectives counter and security functional requirements and security functions to elaborate the objectives. All of the Security Functional Requirements (SFRs) are taken from CC Part 2 [c]. Use of this standard facilitates comparison with other evaluated products.

Evaluation Conduct

26. The evaluation was carried out in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme as described in United Kingdom Scheme Publication (UKSP) 01 and UKSP 02 [e, f]. The Scheme has established a Certification Body which is managed by CESG on behalf of Her Majesty's Government. As stated on page ii of this Certification Report, the Certification Body is a member of the Common Criteria Mutual Recognition Arrangement, and the evaluation was conducted in accordance with the terms of this Arrangement.

27. The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [a], 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 3 [d], the Common Evaluation Methodology (CEM) [g], and all Common Criteria Interpretations effective up to April 2003.

28. The Certification Body monitored the evaluation which was carried out by the LogicaCMG Commercial Evaluation Facility (CLEF) at Leatherhead. The evaluation was completed when the CLEF submitted the final Evaluation Technical Report (ETR) [i] to the Certification Body in April 2003. The Certification Body then produced this Certification Report.

General Points

29. The evaluation addressed the security functionality claimed in the Security Target [a] with reference to the assumed operating environment specified by the Security Target. The evaluated configuration was that specified in Annex A. Prospective consumers are advised to check that this matches their identified requirements and to give due consideration to the recommendations and caveats of this report.

30. Certification is not a guarantee of freedom from security vulnerabilities; there remains a small probability (smaller with greater assurance) that exploitable vulnerabilities may be discovered after a certificate has been awarded. This Certification Report reflects the Certification Body’s view at the time of certification. Consumers (both prospective and existing) 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 products and whether such patches have been evaluated and certified.

31. The issue of a Certification Report is not an endorsement of a product.

(This page is intentionally left blank)

II. EVALUATION FINDINGS

Introduction

32. The evaluation addressed the requirements specified in the Security Target [a]. The results of this work were reported in the ETR [i] under the CC Part 3 [d] headings. The following sections note considerations that are of particular relevance to either consumers or those involved with the subsequent assurance maintenance and re-evaluation of the TOE.

Delivery

33. 3Com Corporation produce, market and sell the Embedded Firewall which is jointly developed by Secure Computing Corporation and 3Com.

34. 3Com retrieve the product software from Secure Computing's password-protected web site. They use a standard carrier, Airborne Express, for delivery to retailers. Retailers then deliver the product, shrink-wrapped and labeled with the ordered part number, to end-users.

35. 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 in delivery.

Installation and Guidance Documentation

36. For guidance on installation and configuration, users should refer to the Administration Guide [j] and the Quick Start Guide [k].

37. For secure configuration as evaluated, users should refer to the Evaluated Configuration Guide [l].

Strength of Function

38. The SoF claim for the TOE was as given above under “Strength of Function Claims”. Based on their examination of all the evaluation deliverables, the Evaluators confirmed that the SoF claim of SoF-Basic was upheld.

39. The Security Target [a] identifies two security mechanisms:

a. a cryptographic communication mechanism which was deemed to be out of scope for the evaluation; and

b. a password mechanism which met the claim of SoF-Basic.

Vulnerability Analysis

40. The Evaluators’ vulnerability analysis was based on both public domain sources and the visibility of the TOE given by the evaluation process.

41. Penetration Testing was carried at the Secure Computing Corporation site in Roseville, Minnesota on 26-27 March 2003.

42. As a result of the Penetration Testing, the Evaluators recommend that the Administration Guide [j] should be amended at its next update to state explicitly that a reboot of the EFW secured host should be performed on changing location.

43. Following their Vulnerability Analysis and Penetration Testing, the Evaluators concluded that the TOE has no exploitable vulnerabilities.

Assurance Maintenance and Re-evaluation Issues

44. The Evaluators reported that flaw remediation procedures are in place to report, track and resolve security flaws in the TOE.

III. EVALUATION OUTCOME

Certification Result

45. After due consideration of the ETR [i], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, the Certification Body has determined that 3Com Embedded Firewall Version 1.5.1 meets the specified Common Criteria Part 3 augmented requirements of Evaluation Assurance Level EAL2 with ALC.FLR.1 (Flaw Remediation), in the specified environment, when running on the platforms specified in Annex A.

46. The minimum Strength of Function for the implementation of triple DES was SoF-Basic. The Certification Body has determined that the TOE meets this minimum SoF claim.

Recommendations

47. Prospective consumers of 3Com Embedded Firewall Version 1.5.1 should understand the specific scope of the certification by reading this report in conjunction with the Security Target [a]. The TOE should be used in accordance with a number of environmental considerations as specified in the Security Target.

48. Only the evaluated TOE configuration should be installed. This is specified in Annex A with further relevant information given above under ‘TOE Scope’ and ‘Evaluation Findings’.

49. The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration.

50. The above ‘Evaluation Findings’ include a number of recommendations relating to the secure receipt, installation, configuration and operation of the TOE.

(This page is intentionally left blank)

ANNEX A: EVALUATED CONFIGURATION

TOE Identification

1. The TOE consists of the following systems, connected together in a simple network structure.

   a. a combined Management Console and Policy Server running Windows 2000 Server, with a server or desktop triple DES NIC in the 3CRFW or 3CR990 family;

   b. a laptop Secured Computer running Windows 2000 Professional, with a mobile model NIC in the 3CRFW family; and

   c. a laptop Secured Computer running Windows XP Professional, with a mobile model NIC in the 3CRFW family.

2. These systems use 3Com triple DES 3CR990 NICs with EFW firmware.

3. The Policy Server, installed on the same server as the Management Console, must be configured with static IP addresses. It should not be configured as a Windows 2000 Domain Controller, should not allow remote administrator access, and should not have any nonessential software applications.

4. The laptop configured as a roaming device should be configured with an IPSEC VPN client.

TOE Documentation

5. The supporting guidance documents evaluated were the Administration Guide [j] and the Quick Start Guide [k], as described in Section II under the heading ‘Installation and Guidance Documentation’.

TOE Configuration

6. The configuration used for testing was as described above under 'TOE Identification'. For further details, see [l].

Environmental Configuration

7. For details of the environmental configuration see [l].

(This page is intentionally left blank)

ANNEX B: PRODUCT SECURITY ARCHITECTURE

1. This annex gives an overview of the main product architectural features that are relevant to the security of the TOE. Other details of the scope of evaluation are given in the main body of the report and in Annex A. Note that the exact evaluated configuration (as described in Annex A) is more specifically defined than the general description given here.

Architectural Features

2. The EFW configuration consists of the following:

a. an EFW Management Console;

b. one to three EFW Policy Servers;

c. a number of EFW Devices, each of which includes EFW firmware, running on EFW NICs; and

d. EFW Agent software running on the host Operating System.

Design Subsystems

3. The EFW Management Console is the administrative interface to the Policy Server. It can be installed on the same machine as a Policy Server or remotely on a different machine. The Management Console platform (and the EFW Policy Server platform, if not co-located) can be protected with an EFW Device.

4. EFW Policy Servers control EFW Devices by implementing administrative actions received from the Management Console as follows:

a. accepting high-level commands from the Management Console and converting them to low-level packet filtering rules for the EFW Devices;

b. receiving and processing heartbeat messages from EFW Devices that contain updates on the IP addresses and resident policy version for the devices;

c. receiving and processing audit messages from the EFW Devices; and

d. storing EFW system data in a Database Management System (DBMS).

5. Each EFW Device must be assigned to a primary EFW Policy Server. The Policy Server can also specify a second Policy Server to act as a backup Policy Server and, if desired, a third Policy Server in case neither the primary nor secondary servers are available or reachable.

6. EFW Devices filter incoming and outgoing packets based on the rules and policy settings for the policy they are enforcing.

7. A secured computer, which may be a server or workstation, can have any number of EFW devices (each using different policies if desired) as long as each EFW Device has a different IP address.

Hardware and Firmware Dependencies

8. EFW Devices consist of EFW firmware loaded on to NICs.

9. Both the Management Console and the Policy Server are supported through EFW firmware in their EFW Devices.

TSF Interfaces

10. The external interfaces of the Policy Server are:

    a. the Policy Server Management Request Interface;

    b. the Policy Server Audit Collection Interface; and

    c. the Policy Server Device Management Interface.

11. The external interfaces of the EFW Devices are:

    a. Ethernet packets from the host or from the network connection; and

    b. driver commands from the host.

ANNEX C: PRODUCT TESTING

IT Product Testing

1. The TSF interfaces are listed in Annex B.

2. Developer tests, Evaluator Functional tests and Penetration testing all covered the 4 major architectural components:

   a. the EFW Management Console,

   b. the EFW Policy Server,

   c. EFW Devices, and

   d. EFW Agent.

3. The tests to repeat Developer's tests, separate independent tests, and penetration tests were carried out over the period from 24 to 27 March 2003.

4. Testing of the TOE was performed using the following tools:

   e. Ethereal;

   f. IPConfig;

   g. NMap;

   h. Sendip;

   i. TCP-Relay;

   j. UDP Flooder; and

   k. the Developer's own test tool.

Platform Issues

5. For a general description of platforms considered for this evaluation, see the section 'TOE Scope'. The Evaluators considered that the use of different platforms (within the generic definition of the TOE Scope) would not affect the results of the evaluation.

(This page is intentionally left blank)