Certification Report

EAL 4+ Evaluation of

Fortinet FortiGate™-50A, 60, 100A, 200A, 300A, 800, 3000, 3600, 5001 Antivirus Firewalls and FortiOS™ 2.80 Firmware

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Evaluation number: 383-4-29-CR
Version: 1.0
Date: 28 February 2005
Pagination: i to iii, 1 to 13

DISCLAIMER

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved evaluation facility – established under the Canadian Common Criteria Evaluation and Certification Scheme (CCS) – using the *Common Methodology for Information Technology Security Evaluation, Version 1.0*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 2.1*. This certification report, and its associated certificate, apply only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the CCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report, and its associated certificate, are not an endorsement of the IT product by the Communications Security Establishment (CSE), or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the CSE, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

FOREWORD

The Canadian Common Criteria Evaluation and Certification Scheme (CCS) provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the CCS Certification Body, which is managed by the Communications Security Establishment (CSE).

A CCEF is a commercial facility that has been approved by the CCS Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of *ISO Standard 17025, General requirements for the accreditation of calibration and testing laboratories*. Accreditation is performed under the Program for the Accreditation of Laboratories Canada (PALCAN), administered by the Standards Council of Canada.

The CCEF that carried out this evaluation is Electronic Warfare Associates-Canada, Ltd. located in Ottawa, Ontario.

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

This certification report is associated with the certificate of product evaluation dated 28 February 2005, and the security target identified in Section 4 of this report.

The certification report, certificate of product evaluation and security target are posted on the CCS Certified Products list at:
http://www.cse-cst.gc.ca/en/services/common_criteria/trusted_products.html

This certification report makes reference to FortiGate, FortiOS and FortiASIC which are trademarks or registered trademarks of Fortinet, Incorporated.

TABLE OF CONTENTS

Executive Summary

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 4 augmented evaluation is the Fortinet FortiGate™-50A, 60, 100A, 200A, 300A, 800, 3000, 3600, 5001 Antivirus Firewalls and FortiOS™ 2.80 Firmware, from Fortinet Incorporated.

The FortiGate™ series is a set of firewalls that are used to control network access. They provide a NAT/route mode that enforces an information flow control policy between two or more different networks (for example, between a private network and the Internet) and a transparent mode that applies security at any point in a network. The FortiGate™ units are designed to be installed and used in an environment that is configured and controlled in accordance with administrator guidance that is supplied with the product.

Electronic Warfare Associates-Canada, Ltd. is the CCEF that conducted the evaluation. This evaluation was completed on 14 February 2005, and was carried out in accordance with the rules of the Canadian Common Criteria Evaluation and Certification Scheme (CCS).

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for the Fortinet FortiGate™-50A, 60, 100A, 200A, 300A, 800, 3000, 3600, 5001 Antivirus Firewalls and FortiOS™ 2.80 Firmware, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the Fortinet FortiGate™-50A, 60, 100A, 200A, 300A, 800, 3000, 3600, 5001 Antivirus Firewalls and FortiOS™ 2.80 Firmware are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report[1] for this product provide sufficient evidence that it meets the EAL 4+ assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 1.0* (with applicable final interpretations), for conformance to the *Common Criteria for Information Technology Security Evaluation, version 2.1*. The following augmentation is claimed:

- ALC_FLR.3 – Systematic Flaw Remediation

The Communications Security Establishment, as the CCS Certification Body, declares that the Fortinet FortiGate™-50A, 60, 100A, 200A, 300A, 800, 3000, 3600, 5001 Antivirus Firewalls and FortiOS™ 2.80 Firmware evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will be listed on the CCS Certified Products list.

[1] The evaluation technical report is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 4 augmented evaluation is the Fortinet FortiGate™-50A, 60, 100A, 200A, 300A, 800, 3000, 3600, 5001 Antivirus Firewalls and FortiOS™ 2.80 Firmware, from Fortinet Incorporated.

2 TOE Description

The FortiGate™ series is a set of firewalls that are used to control network access. They provide a NAT/route mode that enforces an information flow control policy between two or more different networks (for example, between a private network and the Internet) and a transparent mode that applies security at any point in a network. Figure 1 of the Security Target (ST) shows an example of a FortiGate™ Antivirus Firewall protecting an internal network and providing a second network, termed the Demilitarized Zone (DMZ) that is isolated from both the internal network and the external network. The FortiGate™ units are designed to be installed and used in an environment that is configured and controlled in accordance with administrator guidance that is supplied with the product.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for the Fortinet FortiGate™-50A, 60, 100A, 200A, 300A, 800, 3000, 3600, 5001 Antivirus Firewalls and FortiOS™ 2.80 Firmware is identified in Section 5 of the Security Target.

4 Security Target

The ST associated with this Certification Report (CR) is identified by the following nomenclature:

Title:	Security Target for the Fortinet FortiGate™-50A, 60, 100A, 200A, 300A, 800, 3000, 3600 and 5001 Antivirus Firewalls and FortiOS™ 2.80 CC Compliant Firmware: EAL 4+
Version:	0.90
Date:	2 February 2005

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 1.0*, for conformance to the *Common Criteria for Information Technology Security Evaluation, version 2.1*, incorporating all final interpretations issued prior to 31 December 2003.

The Fortinet FortiGate™-50A, 60, 100A, 200A, 300A, 800, 3000, 3600, 5001 Antivirus Firewalls and FortiOS™ 2.80 Firmware are:

a. Common Criteria Part 2 conformant, with security functional requirements based only upon functional components in Part 2;

b. Common Criteria Part 3 conformant, with security assurance requirements based only upon assurance components in Part 3; and

c. Common Criteria EAL 4 augmented, with all the security assurance requirements in the EAL 4, as well as the following: ALC_FLR.3 - Systematic Flaw Remediation.

The Fortinet FortiGate™-50A, 60, 100A, 200A, 300A, 800, 3000, 3600, 5001 Antivirus Firewalls and FortiOS™ 2.80 Firmware conforms with the *U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments, Version 1.1, April 1999 (TFFWLR PP).*

6 Security Policy

The complete Fortinet FortiGate™-50A, 60, 100A, 200A, 300A, 800, 3000, 3600, 5001 Antivirus Firewalls and FortiOS™ 2.80 Firmware Security Policy is identified in the ST. The following statements are representative of the Security Policy.

6.1 Information Flow Control

Users on the internal network may pass information through the firewall to another connected network if:

a. all of the information security attribute values are unambiguously permitted by the information flow control security policy rules created by the authorized administrator; and

b. the presumed address of the user in the information translates to an internal network address; and

c. the presumed address of the destination in the information translates to an address on the other connected network.

Users on the external network can cause information to flow through the firewall to another connected network if:

a. all of the information security attribute values are unambiguously permitted by the information flow control security policy rules created by the authorized administrator; and

b. the presumed address of the user subject in the information translates to an external network address; and

c. the presumed address of the destination in the information translates to an address on the other connected network.

7 Assumptions and Clarification of Scope

Consumers of the Fortinet FortiGate™-50A, 60, 100A, 200A, 300A, 800, 3000, 3600, 5001 Antivirus Firewalls and FortiOS™ 2.80 Firmware product should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will help to ensure the proper and secure operation of the product.

7.1 Secure Usage Assumptions

The FortiGate™ series of firewalls is designed for use by network administrators and it is assumed that these administrators are appropriately trained and experienced and have no malicious intentions. It assumed that the product will be installed and configured using the guidance documents provided by Fortinet Incorporated. These documents are listed in Section 10.

7.2 Environmental Assumptions

The FortiGate™ series of firewalls is designed to control the flow of information between networks. For these units to be effective it is assumed that information may not flow between the networks without passing through the Firewall.

It is assumed that a securely configured management console is directly connected to the Firewall, and resides in the same physically secure location as the Firewall. The console is assumed to correctly transmit information to the firewall and to correctly display information sent to it by the Firewall. It is further assumed that access to the console is restricted to authorized administrators.

7.3 Clarification of Scope

The FortiGate™ series of firewalls can not prevent authorized administrators from carelessly configuring a Firewall such that the information flow control policy is compromised.

8 Architectural Information

The FortiGate™ series of firewalls consist of a hardware platform and FortiOS™ 2.80 firmware.

The hardware platform includes a CPU, network interfaces, memory (RAM, Flash), a hard drive[2], a serial port, a control panel[3], and the FortiASIC chip that provides encryption and antivirus hardware acceleration.

The FortiOS™ 2.80 firmware is a customized operating system developed by Fortinet Incorporated. FortiOS™ 2.80 provides basic firewall services, a hybrid packet and deep packet inspection firewall engine, secure firewall administration, IPSec based VPN services, as well as support for PPTP and L2TP, an Intrusion Prevention System, antivirus services, and content filtering and URL/file blocking.

9 Evaluated Configuration

The evaluated configurations of the TOE are:

- FortiGate-50A with firmware Fortigate-50A 2.80 build275,050127 and hardware C-5FA27-01
- FortiGate-60 with firmware Fortigate-60 2.80 build275,050127 and hardware C-4AN27-03
- FortiGate-100A with firmware Fortigate-100A 2.80 build275,050127 and hardware C-4DZ47-01
- FortiGate-200A with firmware Fortigate-200A 2.80 build275,050127 and hardware C-4AY89-01
- FortiGate-300A with firmware Fortigate-300A 2.80 build275,050127 and hardware C-4FK88-01
- FortiGate-800 with firmware Fortigate-800 2.80 build275,050127 and hardware C-4UT39-01
- FortiGate-3000 with firmware Fortigate-3000 2.80 build275,050127 and hardware C-4JE25-02
- FortiGate-3600 with firmware Fortigate-3600 2.80 build275,050127 and hardware C-4KW75-02
- FortiGate-5001 with firmware Fortigate-5000 2.80 build275,050127 and hardware P-4CF76-01

[2] Not all models are equipped with a hard drive.

[3] Not all models are equipped with a control panel.

The publication entitled *Operating FortiGate Units in Common Criteria Mode* describes the procedures necessary to install and operate a FortiGate™ Antivirus Firewall in its evaluated configuration.

10 Documentation

Fortinet Incorporated provides a Quick Start Guide, an Installation Guide, and an Administration Guide for each individual model, and provides a Command Line Interface Reference Guide, a Log Message Reference Guide and Operating FortiGate Units in Common Criteria Mode applicable to all models.

The documents listed below are all available to consumers:

a. Operating FortiGate Units in Common Criteria Mode, Document No. 01-28005-0107-20050117, Version 2.2, Dated 11 Feb 2005.
b. FortiGate CLI Reference Guide, Document No. 01-28005-0015-20041015, Version 2.80, 15 Oct 2004.
c. FortiGate Log Message Reference Guide, Document No. 01-28005-0105-20040930, Version 2.80, 30 Sep 2004.
d. FortiGate-50A Quick Start Guide, Document No. 01-28005-0031-20040922, dated 22 Sep 2004.
e. FortiGate-60 Quick Start Guide, Document No. 01-28005-0032-20040922, dated 22 Sep 2004.
f. FortiGate-100A Quick Start Guide, Document No. 01-28005-0066-20041101, dated 1 Nov 2004.
g. FortiGate-200A Quick Start Guide, Document No. 01-28005-0070-20041101, dated 1 Nov 2004.
h. FortiGate-300A Quick Start Guide, Document No. 01-28005-0095-20041008, dated 8 Oct 2004.
i. FortiGate-800 Quick Start Guide, Document No. 01-28005-0038-20041026, dated 26 Oct 2004.
j. FortiGate-3000 Quick Start Guide, Document No. 01-28005-0040-20040922, dated 22 Sep 2004.
k. FortiGate-3600 Quick Start Guide, Document No. 01-28005-0041-20040922, dated 22 Sep 2004.
l. FortiGate-5001 Quick Start Guide, Document No. 01-28005-0124-20041119, dated 19 Nov 2004.
m. FortiGate-5020 Quick Start Guide, Document No. 01-28005-0043-20041119, dated 19 Nov 2004.
n. FortiGate-5050 Quick Start Guide, Document No. 01-28005-0060-20041126, dated 26 Nov 2004.
o. FortiGate-5140 Quick Start Guide, Document No. 01-28005-0123-20041126, dated 26 Nov 2004.

p. FortiGate-50A Installation Guide, Document No. 01-28005-0017-20041101, dated 1 November 2004.
q. FortiGate-60 Installation Guide, Document No. 01-28005-0018-20041101, dated 1 November 2004.
r. FortiGate-100A Installation Guide, Document No. 01-28005-0067-20041015, dated 15 October 2004.
s. FortiGate-200A Installation Guide, Document No. 01-28005-0071-20041015, dated 15 October 2004.
t. FortiGate-300A Installation Guide, Document No. 01-28005-0092-20041015, dated 15 October 2004.
u. FortiGate-800 Installation Guide, Document No. 01-28005-0008-20040924, dated 24 September 2004.
v. FortiGate-3000 Installation Guide, Document No. 01-28005-0026-20041101, dated 1 November 2004.
w. FortiGate-3600 Installation Guide, Document No. 01-28005-0027-20041101, dated 1 November 2004.
x. FortiGate-5000 Installation Guide, Document No. 01-28005-0117-20041028, dated 28 October 2004.
y. FortiGate-50A Administration Guide, Document No. 01-28005-0001-20040924, dated 24 September 2004.
z. FortiGate-60 Administration Guide, Document No. 01-28005-0002-20040924, dated 24 September 2004.
aa. FortiGate-100A Administration Guide, Document No. 01-28005-0068-20041015, dated 15 October 2004.
bb. FortiGate-200A Administration Guide, Document No. 01-28005-0072-20041015, dated 15 October 2004.
cc. FortiGate-300A Administration Guide, Document No. 01-28005-0092-20040924, dated 24 September 2004.
dd. FortiGate-800 Administration Guide, Document No. 01-28005-0008-20040924, dated 24 September 2004.
ee. FortiGate-3000 Administration Guide, Document No. 01-28005-0010-20040924, dated 24 September 2004.
ff. FortiGate-3600 Administration Guide, Document No. 01-28005-0011-20040924, dated 24 September 2004.
gg. FortiGate-5000 Administration Guide, Document No. 01-28005-0113-20040924, dated 24 September 2004.

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of the Fortinet FortiGate™-50A, 60, 100A, 200A, 300A, 800, 3000, 3600, 5001 Antivirus Firewalls and FortiOS™ 2.80 Firmware, including the following areas:

Configuration management: An analysis of the Fortinet FortiGate™-50A, 60, 100A, 200A, 300A, 800, 3000, 3600, 5001 Antivirus Firewalls and FortiOS™ 2.80 Firmware development environment and associated documentation was performed. The evaluators found that the Fortinet FortiGate™-50A, 60, 100A, 200A, 300A, 800, 3000, 3600, 5001 Antivirus Firewalls and FortiOS™ 2.80 Firmware configuration items were clearly marked and that control was exercised over all modifications to the configuration items. The developer's configuration management system was observed during a site visit, and it was found to be mature and well developed.

Secure delivery and operation: The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of the Fortinet FortiGate™-50A, 60, 100A, 200A, 300A, 800, 3000, 3600, 5001 Antivirus Firewalls and FortiOS™ 2.80 Firmware during distribution to the consumer. The evaluators examined and tested the installation, generation and start-up procedures, and determined that they were complete and sufficiently detailed to result in a secure configuration.

Design documentation: The evaluators analysed the Fortinet FortiGate™-50A, 60, 100A, 200A, 300A, 800, 3000, 3600, 5001 Antivirus Firewalls and FortiOS™ 2.80 Firmware functional specification, high-level design, low level design, security policy model and source code. The evaluators determined that the design documents were internally consistent, and completely and accurately described all interfaces and security functions. The evaluators also independently verified that the correspondence mappings between the design documents were correct.

Guidance documents: The evaluators examined the Fortinet FortiGate™-50A, 60, 100A, 200A, 300A, 800, 3000, 3600, 5001 Antivirus Firewalls and FortiOS™ 2.80 Firmware user and administrator guidance documentation and determined that it sufficiently and unambiguously described how to securely use and administer the product, and that it was consistent with the other documents supplied for evaluation.

Life-cycle support: The evaluators assessed the development security procedures during a site visit and determined that they detailed sufficient security measures for the development environment to protect the confidentiality and integrity of the Fortinet FortiGate™-50A, 60, 100A, 200A, 300A, 800, 3000, 3600, 5001 Antivirus Firewalls and FortiOS™ 2.80 Firmware design and implementation. The evaluators determined that the developer has used a documented model of the product life cycle. The evaluators determined that the developer has used well-defined development tools that yield consistent and predictable results. The evaluators determined that the developer has established flaw remediation procedures that describe the tracking of security flaws, the identification of corrective actions, and the distribution of corrective action information to product users. Additionally, the evaluators determined that the developer's procedures provide for the corrections of security flaws, for the receipt of flaw reports from product users, and for assurance that the corrections introduce no new security flaws.

Vulnerability assessment: The strength of function claims made in the Security Target for the Fortinet FortiGate™-50A, 60, 100A, 200A, 300A, 800, 3000, 3600, 5001 Antivirus Firewalls and FortiOS™ 2.80 Firmware were validated through independent evaluator analysis. The evaluators also validated the developer's vulnerability analysis. In addition, the evaluators performed an independent vulnerability and SOF analysis and developed tests that focused on potential vulnerabilities in the Fortinet FortiGate™-50A, 60, 100A, 200A, 300A, 800, 3000, 3600, 5001 Antivirus Firewalls and FortiOS™ 2.80 Firmware.

All these evaluation activities resulted in **PASS** verdicts.

12 ITS Product Testing

Testing at EAL 4 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing independent vulnerability tests. During this evaluation, the evaluators developed their independent tests by examining the design and guidance documentation, examining developer analysis, and repeating a sub-set of developer tests.

12.1 Assessing Developer Tests

The evaluators verified that the developer met their testing responsibilities by examining their test evidence, reviewing their test results and repeating a subset of the developer tests.

The evaluators reviewed the developer's analysis of test coverage and depth and found them to be complete and accurate. The correspondence between the tests identified in the developer's test documentation, and the functional specification and high-level design was complete.

Since the developer's testing covered all of the security functions of the TOE, the evaluators elected to repeat a subset of developer tests by focusing upon specific areas of interest. The following functional areas were selected:

a. Access Control (authorized administrators and internal users passing information through the TOE);
b. Administration (LCD, GUI, CLI device configuration);
c. Information Flow Control (restricting data flow via rules); and
d. Logging (recording events and anomalies to memory or to disk).

Tests were selected which demonstrate that the TOE satisfies the security functional requirements specified in the Security Target. A total of 103 individual tests were selected for the evaluation, representing approximately 20% of the developer's test cases that are applicable to the evaluated configuration.

12.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation, examining the developer's test documentation, executing a sample of the developer's test cases, and creating test cases that augmented the developer tests.

12.3 Independent Vulnerability Testing

After reviewing the technical specifications and product documentation, a flaw hypothesis methodology was used to develop a list of potential vulnerabilities of the TOE. Those vulnerabilities assessed as potentially exploitable by an attacker possessing a low attack potential were used to develop penetration test cases.

The following potential attack areas were assessed during the development of potential attack scenarios:

a. Generic vulnerabilities;
b. Bypassing;
c. Tampering;
d. Direct attacks; and
e. Misuse.

At least one penetration attack and in most cases multiple attacks were developed for each of these areas. A total of 15 penetration attacks were developed and exercised against the TOE.

Penetration testing did not uncover any exploitable vulnerabilities for the Fortinet FortiGate™-50A, 60, 100A, 200A, 300A, 800, 3000, 3600, 5001 Antivirus Firewalls and FortiOS™ 2.80 Firmware in the anticipated operating environment.

12.4 Conduct of Testing

The Fortinet FortiGate™-50A, 60, 100A, 200A, 300A, 800, 3000, 3600, 5001 Antivirus Firewalls and FortiOS™ 2.80 Firmware were subjected to a comprehensive suite of formally-documented, independent, functional and vulnerability tests. The testing took place at the IT Security Evaluation and Testing (ITSET) facility at Electronic Warfare Associates-Canada, Ltd. located in Ottawa, Ontario. The CCS Certification Body witnessed a portion of the independent testing.

The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in the ETR[4].

12.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that the Fortinet FortiGate™-50A, 60, 100A, 200A, 300A, 800, 3000, 3600, 5001 Antivirus Firewalls and FortiOS™ 2.80 Firmware behave as specified in the ST and functional specification.

13 Results of the Evaluation

This evaluation has provided the basis for an **EAL 4+** level of assurance, including the augmentation ALC_FLR.3 – Systematic Flaw Remediation. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

14 Evaluator Comments, Observations and Recommendations

The FortiGate™ units include comprehensive guides for the installation, configuration and operation of the antivirus firewall devices.

15 Glossary

This section expands any acronyms, abbreviations and initializations used in this report.

15.1 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/Initialization	Description
CC	Common Criteria for Information Technology Security Evaluation
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CEM	Common Methodology for Information Technology Security Evaluation
CLI	Command Line Interface
CPU	Central Processing Unit

[4] The evaluation technical report is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

CR	Certification Report
CSE	Communications Security Establishment
DMZ	Demilitarized Zone
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IPS	Intrusion Prevention System
ISO	International Organisation for Standardisation
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
L2TP	Layer 2 Tunneling Protocol
PALCAN	Program for the Accreditation of Laboratories Canada
PP	Protection Profile
PPTP	Point-to-Point Tunneling Protocol
RAM	Random Access Memory
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TFFWLR	U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments, Version 1.1, April 1999
VPN	Virtual Private Network

16 References

This section lists all documentation used as source material for this report:

a) Common Criteria for Information Technology Security Evaluation, CCIMB-99-031/032/033, Version 2.1, August 1999, annotated with final interpretations issued as of 31 December 2003.

b) Common Methodology for Information Technology Security Evaluation, CEM-99/045, Part 2: Evaluation and Methodology, Version 1.0, August 1999, annotated with final interpretations issued as of 31 December 2003..

c) CCS #4: Technical Oversight for TOE Evaluation, Canadian Common Criteria Evaluation and Certification Scheme (CCS), Version 1.0, 3 October 2002.

d) U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments, Version 1.1, April 1999 (TFFWLR PP).

e) Security Target for the Fortinet FortiGate™-50A, 60, 100A, 200A, 300A, 800, 3000, 3600 and 5001 Anti-Virus Firewalls and FortiOS 2.80 CC Compliant Firmware: EAL 4+, Document No. 1476-011-D001, Version 0.90, 2 February 2005.

f) Evaluation Technical Report (ETR), Fortinet FortiGate™ 50A, 60, 100A, 200A, 300A, 800, 3000, 3600 and 5001 Anti-Virus Firewalls and FortiOS 2.80 CC Compliant Firmware, EAL 4+ Evaluation, Common Criteria Evaluation Number, 383-4-29, Document No. 1476-000-D002, Version 0.6, 14 February 2005.