Australian Government
Department of Defence

Australasian Information Security Evaluation Program

FortiGate SOC2 appliances running FortiOS version 5.4

Certification Report
2018/114

14-11-2018
Version 1.1

Amendment Record

Version	Date	Description
0.1	05 - 03 - 2018	Internal
1.0	04 – 04 - 2018	Public Release
1.1	14 – 11 – 2018	Amended for Cross-posting

Executive Summary

This report describes the findings of the IT security evaluation of FortiGate SOC2 appliances running FortiOS version 5.4 against Common Criteria and a Protection Profile.

The Target of Evaluation (TOE) is FortiGate SOC2 appliances running FortiOS version 5.4.

The TOE is designed to provide next-generation firewall services ensuring network protection for Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) networks. The TOE is capable of robust filtering based on information contained in IPv4, IPv6, ICMPv4, ICMPv6, TCP and UDP headers as specified by their respective RFC's. Additionally the TOE is capable of content inspection of FTP and H.323 protocols to work with the dynamic nature of these protocols.

The functionality defined in the Security Target (Ref 1) that was subsequently evaluated is summarised as follows:

- **Security audit** – The TOE generates logs for auditable events. These logs can be stored locally in protected storage and/or exported to an external audit server via a secure channel
- **Cryptographic support** – The TOE implements a key generation and cryptographic methods to provide protection of data both in transit and at rest within the TOE
- **User data protection** – The TOE ensures that data cannot be recovered once deallocated
- **Identification and authentication –** The TOE implements mechanisms to ensure that users are both identified and authenticated before any access to TOE functionality or TSF data is granted
- **Security management** – The TOE provides a suite of management functionality, allowing for full configuration of the TOE by an authorised administrator
- **Protection of the TSF** – The TOE implements a number of protection mechanisms (including authentication requirements, self-tests and trusted update) to ensure the protection of the TOE and all TSF data
- **TOE access –** The TOE provides session management functions for local and remote administrative sections
- **Trusted path/channels –** The TOE provides secure channels between itself and local/remote administrators and other devices to ensure data security during transit
- **Stateful traffic and packet filtering –** The TOE allows for the configuration and enforcement of stateful packet filtering/firewall rules on all traffic traversing the TOE and

The report concludes that the product has complied with the:

- collaborative Protection Profile for Stateful Traffic Filter Firewalls (FWcPP), Version 1.0, 27 February 2015.

and that the evaluation was conducted in accordance with the Common Criteria and the requirements of the Australasian Information Security Evaluation Program (AISEP). The evaluation was performed by BAE Applied Intelligence and was completed on 19 December 2017.

With regard to the secure operation of the TOE, the Australasian Certification Authority (ACA) recommends that administrators:

a) Ensure that the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment are fulfilled
b) Configure and operate the TOE according to the vendor's product administrator guidance
c) Potential purchasers of the TOE should review the intended operational environment and ensure that they are comfortable that the stated security objectives for the operational environment can be suitably addressed and
d) Verify the hash of the downloaded software, as present on the Fortinet website.

This report includes information about the underlying security policies and architecture of the TOE, and information regarding the conduct of the evaluation.

It is the responsibility of the user to ensure that the TOE meets their requirements. For this reason, it is recommended that a prospective user of the TOE refer to the Security Target and read this Certification Report prior to deciding whether to purchase the product.

Contents

Chapter 1 – Introduction

1.1 Overview

This chapter contains information about the purpose of this document and how to identify the Target of Evaluation (TOE).

1.2 Purpose

The purpose of this Certification Report is to:

a) Report the certification of results of the IT security evaluation of the FortiGate SOC2 appliances running FortiOS version 5.4 against the requirements of the Common Criteria (CC), and

- collaborative Protection Profile for Stateful Traffic Filter Firewalls (FWcPP), Version 1.0, 27 February 2015 (Ref 5)

b) Provide a source of detailed security information about the TOE for any interested parties.

This report should be read in conjunction with the TOE's Security Target (Ref 1), which provides a full description of the security requirements and specifications that were used as the basis of the evaluation.

1.3 Identification

The TOE is of FortiGate SOC2 appliances running FortiOS version 5.4.

Table 1 Identification Information

Description	Version
Evaluation Scheme	Australasian Information Security Evaluation Program
TOE	FortiGate SOC2 appliances running FortiOS version 5.4
Software Version	5.4
Hardware Platforms	• FortiGate-30D; • FortiGate-30D-PoE; • FortiWiFi-30D; • FortiGate-60D; • FortiGate-Rugged-60D; • FortiWiFi-60D; • FortiGate-90D; • FortiGate-90D-PoE; • FortiWiFi-90D; and

	• FortiWiFi-90D-PoE.
Security Target	SECURITY TARGET - FORTIGATE SOC2 APPLIANCES RUNNING FORTIOS 5.4 v1.1, 18 October 2018 Document reference FOS-54-ST v1.1
Evaluation Technical Report	Evaluation Technical Report FORTIGATE SOC2 APPLIANCES RUNNING FORTIOS v1.0 28 March 2018 Document reference EFS-T052-ETR-1.0
Criteria	Common Criteria for Information Technology Security Evaluation Part 2 Extended and Part 3 Conformant, April 2017 Version 3.1.Rev 5
Methodology	Common Methodology for Information Technology Security, April 2017 Version 3.1 Rev 5
Conformance	collaborative Protection Profile for Stateful Traffic Filter Firewalls (FWcPP), Version 1.0, 27 February 2015
Developer	Fortinet Inc. 899 Kifer Road Sunnyvale California 94086 U.S.A.
Evaluation Facility	BAE Applied intelligence Level 1 14 Childers Street 2600

Chapter 2 – Target of Evaluation

2.1 Overview

This chapter contains information about the Target of Evaluation (TOE), including a description of functionality provided, its architectural components, the scope of evaluation, security policies, and its secure usage.

2.2 Description of the TOE

The TOE is FortiGate Soc2 appliances running FortiOS version 5.4.

The TOE is a product designed to provide next-generation firewall services ensuring network protection for Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) networks. The TOE is capable of robust filtering based on information contained in IPv4, IPv6, ICMPv4, ICMPv6, TCP and UDP headers as specified by their respective RFC's. Additionally the TOE is capable of content inspection of FTP and H.323 protocols to work with the dynamic nature of these protocols.

2.3 TOE Functionality

The functionality defined in the Security Target that was subsequently evaluated is summarised as follows:

- **Security audit** – The TOE generates logs for auditable events. These logs can be stored locally in protected storage and/or exported to an external audit server via a secure channel
- **Cryptographic support** – The TOE implements a key generation and cryptographic methods to provide protection of data both in transit and at rest within the TOE
- **User data protection** – The TOE ensures that data cannot be recovered once deallocated
- **Identification and authentication –** The TOE implements mechanisms to ensure that users are both identified and authenticated before any access to TOE functionality or TSF data is granted
- **Security management** – The TOE provides a suite of management functionality, allowing for full configuration of the TOE by an authorised administrator
- **Protection of the TSF** – The TOE implements a number of protection mechanisms (including authentication requirements, self-tests and trusted update) to ensure the protection of the TOE and all TSF data
- **TOE access –** The TOE provides session management functions for local and remote administrative sections and
- **Trusted path/channels –** The TOE provides secure channels between itself and local/remote administrators and other devices to ensure data security during transit.

- **Stateful traffic and packet filtering** The TOE allows for the configuration and enforcement of stateful packet filtering/firewall rules on all traffic traversing the TOE.

2.4 TOE Architecture

The TOE consists of the following major architectural components:

- The TOE maintains its own time source, which is free from outside interference. This timestamp is used for the purposes of generating audit logs and other time-sensitive operations on the TOE including cryptographic key regeneration intervals. The TOE may also connect to an NTP server for synchronisation.
- The TOE utilises X509 certificates in accordance with RFC 5280.
- CPU
- Bootloader
- Kernel
- Firmware
- Entropy gathering and DRBG initialization and
- Cryptographic module.

2.5 Clarification of Scope

The evaluation was conducted in accordance with the Common Criteria and associated methodologies.

The evaluated configuration is based on the default installation of the TOE with additional configuration implemented as per the Guidance (Ref 8).

The scope of the evaluation was limited to those claims made in the Security Target (Ref 1).

2.5.1 Evaluated Functionality

All tests performed during the evaluation were taken from FWcPP (Ref 5) and sufficiently demonstrate the security functionality of the TOE. Some of the tests were combined for ease of execution.

2.5.2 Non-evaluated Functionality and Services

Potential users of the TOE are advised that some functions and services have not been evaluated as part of the evaluation. Potential users of the TOE should carefully consider their requirements for using functions and services outside o**f** the evaluated configuration; Australian Government users should refer to Australian Government Information Security Manual (ISM) (Ref 6) for policy relating to using an evaluated product in an un-evaluated configuration. New

Zealand Government users should consult the NZ Information Security Manual (NZISM) (Ref 7).

The following components are considered outside of the scope of the TOE:

- High-Availability;
- FortiExplorer client;
- Anti-spam;
- Anti-virus;
- Content filtering;
- Web filtering;
- Use of syslog;
- FortiToken and FortiSSO Authentication;
- Stream Control Transmission Protocol (SCTP), BGP, RIP and DHCP protocols; and
- Usage of the boot-time configuration menu to upgrade the TOE.

2.6 Security

2.6.1 Security Policy

The TOE Security Policy (TSP) is a set of rules that defines how the information within the TOE is managed and protected. Access to IPS functionality is provided to all users assigned to an Administrator profile. The administrator profile has full privileges for configuring and activating IPS policies.

Active security policies are enforced in a sequential order (based on the sequence number assigned to each policy). The administrator may change this sequence to suit their needs. If an IPS policy is attached to a security policy, it will be enforced at the same time as the security policy.

The default Implicit Deny policy will be enforced if the received traffic does not match any of the other active policies.

2.7 Usage

2.7.1 Evaluated Configuration

The TOE consists of the software and hardware version as outlined in table 1. The evaluation was conducted on the default installation and configuration of the TOE

with additional guidance and configuration information drawn from the Guidance Documentation (Ref 8).

2.7.2 Secure Delivery

To ensure that the software received is the evaluated product the customer must check the version details received against the list specified in the TOE.
Before installing the FortiGate unit, users should take steps to ensure the unit has not been tampered with during transit. Users should perform the following checks to verify the integrity of the unit prior to installation.

- Courier - Fortinet only uses bonded couriers such as UPS, FedEx or DHL. Verify the shipment was received using a bonded courier.
- Shipping information - verify the shipment information against the original purchase order or evaluation request.
- Verify the shipment has been received directly from Fortinet.
- External packaging - verify the Fortinet branded packing tape sealing the packaging is intact and the packaging has not been cut or damaged to allow access to the unit.
- Internal packaging - verify the unit is sealed in an undamaged, clear plastic bag for non-blade units. For blade units, verify the internal box packaging is intact.
- Warranty seal - For non-blade units, verify the unit's warranty seal is intact. The warranty seal is a small, grey sticker with the Fortinet logo and is normally placed over a chassis access screw. The chassis cannot be opened without destroying the warranty seal.

If users identify any concerns while verifying the integrity of the unit, they should contact the supplier immediately.

2.7.3 Installation of the TOE

The Guidance Documentation (Ref 8) contains all relevant information for the secure configuration of the TOE.

2.8 Version Verification

Install the FIPS-CC firmware build on the FortiGate unit. There are several methods to do this. Refer to the FortiGate Cookbook, FortiGate Handbook or FortiGate CLI Guide for more information.
To verify the firmware version of the unit execute the following command from the command line: *get system status*
The version line of the status display shows the FortiGate model number, firmware version, build number and date. For example:*Version: FortiGate-300D v5.4.4,buildwxyz,YYMMDD*
Verify in the relevant security target document that the firmware version, build number and date are correct.

Updates to the TOE are applied in accordance with the following process:

- The administrator downloads the upgrade image/package from the Fortinet website.
- Once downloaded, the administrator must transfer the image to the TOE via a trusted path (e.g. the web interface).
- Upon initiating the update process, the TOE will attempt to verify the integrity and authenticity of the update package. This is achieved via the verification of a 2048-bit RSA signature that is applied to the package by the Fortinet development team.
- If the signature cannot be verified, or the integrity of the package cannot be confirmed, the upgrade will fail and an audit log generated accordingly.
- If the signature is verified correctly and the integrity of the package is confirmed, the upgrade will be applied and the TOE restarted.

Additionally, MD5 hashes of each update file are published along with the image on the Fortinet website. Administrators may compare these published hashes against the hashes of the file they have downloaded to ensure that the file is valid.

2.9 Documentation and Guidance

It is important that the TOE is used in accordance with Guidance Documentation (Ref 8) in order to ensure secure usage. The following documentation is available to the consumer when the TOE is purchased. All guidance material is available for download at https://support.fortinet.com/

- FortiGate Handbook, Version 5.4.3, 10 January 2017
- Common Criteria Compliant Operation for FortiOS 5.4, October 06 2017
- FortiOS - CLI Reference, Version 5.4.1, 3 June 2016
- FortiGate Cookbook, Version 5.4, 18 February 2016
- FortiOS 5.4.3 Log Reference, 21 December 2016

All Common Criteria guidance material is available at **www.commoncriteriaportal.org**. The Information Security Manual (ISM) is available at **www.asd.gov.au**. The New Zealand Information Security Manual (NZISM) is available from: **https://www.gcsb.govt.nz/publications/the-nz-information-security-manual/**

2.10 Secure Usage

The evaluation of the TOE took into account certain assumptions about its operational environment. These assumptions must hold in order to ensure the security objectives of the TOE are met.

Assumptions	***Description***
A.PHYSICAL_PROTECTION	The firewall is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the firewall's physical interconnections and correct operation. This protection is assumed to be

	sufficient to protect the firewall and the data it contains. As a result, the cPP will not include any requirements on physical tamper protection or other physical attack mitigations. The cPP will not expect the product to defend against physical access to the firewall that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the firewall.
A.LIMITED_FUNCTIONALITY	The firewall is assumed to provide networking and filtering functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example the firewall should not provide computing platform for general purpose applications (unrelated to networking/filtering functionality).
A.TRUSTED_ADMINSTRATOR	The authorised administrator(s) for the firewall are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the firewall. The firewall is not expected to be capable of defending against a malicious administrator that actively works to bypass or compromise the security of the firewall.
A.REGULAR_UPDATES	The firewall firmware and software is assumed to be updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_CREDENTIALS_SECURE	The administrator's credentials (private key) used to access the firewall are protected by the host platform on which they reside.
A.CONNECTIONS	It is assumed that the TOE is connected to distinct networks in a manner that ensures that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks.

Chapter 3 – Evaluation

3.1 Overview

This chapter contains information about the procedures used in conducting the evaluation, the testing conducted as part of the evaluation and the certification result.

3.2 Evaluation Procedures

The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the FWcPP (Ref 5), Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 5, Parts 2 and 3 (Ref 2 and 3).

The methodology used is described in the Common Methodology for Information Technology Security Evaluation Version 3.1 Revision 5 (Ref 4).

The evaluation was carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program (AISEP).

In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (Ref 10) were also upheld.

The evaluation was based on the default installation and configuration of the TOE with additional configuration taken from Guidance Documentation (Ref 8).

3.3 Testing

3.3.1 Testing Coverage

All tests performed by the Evaluators were taken from the FWcPP. These tests are designed in such a way as to provide a full coverage of testing for all security functions claimed by the TOE. All SFRs listed in the Security Target and the Protection Profile packages were exercised during testing.
The evaluation testing was conducted between June and October 2017.

3.4 Entropy Testing

The entropy design description, justification, operation and health tests are assessed and documented in a separate report (Ref 11).

3.5 Penetration Testing

A vulnerability analysis of the TOE was performed in order to identify any obvious vulnerability in the product and to show that the vulnerabilities were not exploitable in the intended environment of the TOE. This analysis included a search for possible vulnerability sources in publicly-available information.

The following factors have been taken into consideration during the penetration tests:

a) Time taken to identify and exploit (elapsed time)

b) Specialist technical expertise required (specialist expertise)

c) Knowledge of the TOE design and operation (knowledge of the TOE)

d) Window of opportunity

e) IT hardware/software or other equipment required for the exploitation.

Chapter 4 – Certification

4.1 Overview

This chapter contains information about the result of the certification, an overview of the assurance provided and recommendations made by the certifiers.

4.2 Assurance

This certification is focused on the evaluation of product compliance with a collaborative Protection Profile and extended packages that cover the technology area of network devices. Agencies can have confidence that the scope of an evaluation against an ASD approved Protection Profile covers the necessary security functionality expected of the evaluated product and known security threats will have been addressed.

The effectiveness and integrity of cryptographic functions are also within the scope of product evaluations performed in line with collaborative Protection Profiles (cPPs). cPPs provide assurance by a full security target and an analysis of the SFR in that ST, guidance documentation and a basic description of the architecture of the TOE, to understand the security behaviour.

4.3 Certification Result

After due consideration of the conduct of the evaluation as reported to the Certifiers and of the Evaluation Technical Report (Ref 9) the Australasian Certification Authority **certifies** the evaluation of the product performed by the Australasian Information Security Evaluation Facility, BAE Applied Intelligence.

BAE Applied Intelligence **has determined** that FortiGate SOC2 appliances running FortiOS version 5.4 uphold the claims made in the Security Target (Ref 1) and **has met** the requirements of FWcPP.

The effectiveness and integrity of cryptographic functions are also within the scope of product evaluations performed in line with collaborative Protection Profiles.

The analysis is supported by testing as outlined in the cPP assurance activities, and a vulnerability survey demonstrating resistance to penetration attackers with a basic attack potential. Compliance also provides assurance through evidence of secure delivery procedures. Certification is not a guarantee of freedom from security vulnerabilities.

4.4 Recommendations

Not all of the evaluated functionality present in the TOE may be suitable for Australian and New Zealand Government users. For further guidance, Australian Government users should refer to ISM (Ref 6) and New Zealand Government users should consult the NZ Information Security Manual (Ref 7).

In addition to ensuring that the assumptions concerning the operational environment are fulfilled and the guidance document is followed, the ACA also recommends that users and administrators:

a) Ensure that the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment are fulfilled
b) Configure and operate the TOE according to the vendor's product administrator guidance
c) Potential purchasers of the TOE should review the intended operational environment and ensure that they are comfortable that the stated security objectives for the operational environment can be suitably addressed and
a) Verify the hash of the downloaded software, as present on the Fortinet website.

Annex A – References and Abbreviations

A.1 References

1. Security Target - FortiGate SOC2 Appliances running FORTIOS 5.4 v1.1, 18 October 2018: Document reference FOS-54-SOC2-ST v1.1

2. Common Criteria for Information Technology Security Evaluation Part 2: Security functional components April- 2017, Version 3.1 Revision 5

3. Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components April- 2017, Version 3.1 Revision 5

4. Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, April 2107, Version 3.1, Revision 5

5. collaborative Protection Profile for Stateful Traffic Filter Firewalls (FWcPP), Version 1.0, 27 February 2015

6. 2017 Australian Government Information Security Manual (ISM), Australian Signals Directorate

7. NZ Information Security Manual (NZISM): https://www.gcsb.govt.nz/publications/the-nz-information-security-manual/

8. Guidance Documentation:

    - FortiGate Handbook, Version 5.4.3, 10 January 2017
    - Common Criteria Compliant Operation for FortiOS 5.4, October 06 2017
    - FortiOS - CLI Reference, Version 5.4.1, 3 June 2016
    - FortiGate Cookbook, Version 5.4, 18 February 2016
    - FortiOS 5.4.3 Log Reference, 21 December 2016

9. Evaluation Technical Report FORTIGATE NGFW APPLIANCES RUNNING FORTIOS, 30 November 2017, Document reference EFS-047-ETR-0.1.0

10. Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, July 2, 2014.

11. Fortinet FortiASIC CP9 and SoC3 Entropy Justification v1.7 September 16, 2016

A.2 Abbreviations

AISEF	Australasian Information Security Evaluation Facility

AISEP	Australasian Information Security Evaluation Program
ASD	Australian Signals Directorate
CA	Certification Authority
CC	Common Criteria
CEM	Common Evaluation Methodology
ETR	Evaluation Technical Report
FTP	File Transfer Protocol
ISM	Information Security Manual
NTP	Network Time Protocol
NDPP	US Government approved Protection Profile for Network Devices
NZISM	New Zealand Information Security Manual
cPP	collaborative Protection Profile
SFP	Security Function Policy
SFR	Security Functional Requirements
SNMP	Secure Network Management Protocol
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy