Communications Security Establishment

Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

COMMON CRITERIA CERTIFICATION REPORT

PP-Configuration for Network Device, Intrusion Prevention Systems (IPS), Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways (CFG_NDcPP-IPS-FW-VPNGW_V1.0)

19 December 2021

CCCS-010

Canada

FOREWORD

This certification report is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE).

The PP Configuration identified in this certification report has been evaluated at an approved testing laboratory established under the Canadian Centre for Cyber Security (CCCS). This certification report applies only to the identified version and release of the PP Configuration. The evaluation has been conducted in accordance with the provisions of the Canadian CC Scheme, and the conclusions of the testing laboratory in the evaluation report are consistent with the evidence adduced.

If your organization has identified a requirement for this certification report and would like more detailed information, please contact:

Canadian Centre for Cyber Security
Contact Centre and Information Services
contact@cyber.gc.ca | 1-833-CYBER-88 (1-833-292-3788)

OVERVIEW

The Canadian Common Criteria Scheme provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Testing Laboratory (CCTL) under the oversight of the Certification Body, which is managed by the Canadian Centre for Cyber Security.

A CCTL is a commercial facility that has been approved by the Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of ISO/IEC 17025, the General Requirements for the Competence of Testing and Calibration Laboratories.

This certification report is posted to the Common Criteria portal (the official website of the International Common Criteria Program).

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This report documents the results of the evaluation of the **PP-Configuration for Network Device, Intrusion Prevention Systems (IPS), Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways (CFG_NDcPP-IPS-FW-VPNGW_V1.0)**. It presents a summary of the PP-Config. for CFG_NDcPP-IPS-FW-VPNGW_V1.0 together with the evaluation results.

This PP-Configuration defines (by reference to the Supporting Documents for the included PP-Modules) how to evaluate a TOE that claims conformance to the following:

- Base-PP: collaborative Protection Profile for Network Devices, Version 2.2e (CPP_ND_V2.2E)
- PP-Module: PP-Module for Intrusion Protection Systems (IPS), Version 1.0 (MOD_IPS_V1.0)
- PP-Module: PP-Module for Stateful Traffic Filter Firewalls, Version 1.4 + Errata 20200625 (MOD_FW_1.4E)
- PP-Module: PP-Module for Virtual Private Network (VPN) Gateways, Version 1.1 (MOD_VPNGW_1.1)

To promote thoroughness and efficiency, the evaluation of the PP-Config. for CFG_NDcPP-IPS-FW-VPNGW_V1.0 was performed concurrent with the first product evaluation against the PP-Configuration's requirements. In this case the Target of Evaluation (TOE) for this first product was the **FortiGate/FortiOS Version 6.2.7 (hereafter referred to as "FortiGate")**. The evaluation was performed by the Lightship Security Common Criteria Testing Laboratory and was completed in **December 2021.**

An additional evaluation of the PP-Configuration was performed by the Lightship Security Common Criteria Testing Laboratory to confirm that it meets the claimed ACE/APE assurance requirements.

The evaluations determined that the PP-Config. for CFG_NDcPP-IPS-FW-VPNGW_V1.0 is both Common Criteria Part 2 Extended and Part 3 Conformant. The PP-Config. for CFG_NDcPP-IPS-FW-VPNGW_V1.0 was evaluated at an approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (version 3.1, revision 5) for conformance to the Common Criteria for IT Security Evaluation (version 3.1, revision 5).

The Canadian Centre for Cyber Security, as the Certification Body, found that the evaluations demonstrated that the PP-Config. for CFG_NDcPP-IPS-FW-VPNGW_V1.0 meets the requirements of the ACE/APE components.

1 IDENTIFICATION

The evaluation of the **PP-Configuration for Network Device, Intrusion Prevention Systems (IPS), Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways (CFG_NDcPP-IPS-FW-VPNGW_V1.0)** was performed concurrently with the first product evaluation against the PP-Configuration. The Target of Evaluation (TOE) was the **FortiGate/FortiOS Version 6.2.7 (hereafter referred to as "FortiGate")**. The evaluation was performed by the Lightship Security Common Criteria Testing Laboratory and was completed in December 2021.

The PP-Config. for CFG_NDcPP-IPS-FW-VPNGW_V1.0 contains a set of "base" requirements, comprised of "base" requirements that all conformant STs must include, and additionally contains "Optional" and "Selection-based" requirements. The PP-Configuration contains Implementation-Dependent Optional Requirements that are dependent on the TOE implementing a particular function. The Selection-based requirements are additional requirements based on selections made within the PP-Configuration; if certain selections are made, then additional requirements will need to be included.

The following identifies the PP-Configuration that was the subject of the evaluation and certification, together with supporting information from the base evaluation performed against this PP-Configuration.

PP-Configuration	PP-Configuration for Network Device, Intrusion Prevention Systems (IPS), Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways v1.0
Base-PP	collaborative Protection Profile for Network Devices, Version 2.2e (CPP_ND_V2.2E)
PP-Modules in PP-Configuration	PP-Module: PP-Module for Intrusion Protection Systems (IPS), Version 1.0 (MOD_IPS_V1.0) PP-Module: PP-Module for Stateful Traffic Filter Firewalls, Version 1.4 + Errata 20200625 (MOD_FW_1.4E) PP-Module: PP-Module for Virtual Private Network (VPN) Gateways, Version 1.1 (MOD_VPNGW_1.1)
Security Target	Security Target FortiGate/FortiOS Version 6.2.7, 14 September 2021, v1.5
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended, CC Part 3 Conformant
CC Testing Lab	Lightship Security

1.1 PP-CONFIGURATION DESCRIPTION

The PP-Config. for CFG_NDcPP-IPS-FW-VPNGW_V1.0 describes a network device that provides functionality for Intrusion Protection Systems (IPS), Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways.

2 RESULTS OF THE EVALUATION

The evaluators applied each work unit of the Common Methodology [CEM] within the scope of the evaluation and concluded that the evaluated PP-Configuration meets the requirements in the assurance class ACE and the assurance components APE_INT.1, APE_SPD.1, APE_OBJ.2, APE_ECD.1, and APE_REQ.2. The certifier reviewed the work of the evaluators and determined that the evaluation was conducted in accordance with the Common Criteria [CC].

Table 1 - ACE Evaluation Results

ACE Requirement	Verdict	Verified By
ACE_INT.1: PP-Module Introduction	Pass	• Security Target FortiGate/FortiOS Version 6.2.7, 14 September 2021, v1.5 • Evaluation Technical Report NIAP PP-Configuration for Network Device, Intrusion Prevention Systems (IPS), Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways, 19 December 2021, v1.1
ACE_CCL.1: PP-Module Conformance Claims	Pass	• Security Target FortiGate/FortiOS Version 6.2.7, 14 September 2021, v1.5 • Evaluation Technical Report NIAP PP-Configuration for Network Device, Intrusion Prevention Systems (IPS), Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways, 19 December 2021, v1.1
ACE_SPD.1: PP-Module Security Problem Definition	Pass	• Security Target FortiGate/FortiOS Version 6.2.7, 14 September 2021, v1.5 • Evaluation Technical Report NIAP PP-Configuration for Network Device, Intrusion Prevention Systems (IPS), Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways, 19 December 2021, v1.1
ACE_OBJ.1: PP-Module Security Objectives	Pass	• Security Target FortiGate/FortiOS Version 6.2.7, 14 September 2021, v1.5 • Evaluation Technical Report NIAP PP-Configuration for Network Device, Intrusion Prevention Systems (IPS), Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways, 19 December 2021, v1.1

ACE Requirement	Verdict	Verified By
ACE_ECD.1: PP-Module Extended Components Definition	Pass	Security Target FortiGate/FortiOS Version 6.2.7, 14 September 2021, v1.5 Evaluation Technical Report NIAP PP-Configuration for Network Device, Intrusion Prevention Systems (IPS), Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways, 19 December 2021, v1.1
ACE_REQ.1: PP-Module Security Requirements	Pass	Security Target FortiGate/FortiOS Version 6.2.7, 14 September 2021, v1.5 Evaluation Technical Report NIAP PP-Configuration for Network Device, Intrusion Prevention Systems (IPS), Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways, 19 December 2021, v1.1
ACE_MCO.1: PP-Module Consistency	Pass	Security Target FortiGate/FortiOS Version 6.2.7, 14 September 2021, v1.5 Evaluation Technical Report NIAP PP-Configuration for Network Device, Intrusion Prevention Systems (IPS), Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways, 19 December 2021, v1.1
ACE_CCO.1 : PP-Configuration Consistency	Pass	Security Target FortiGate/FortiOS Version 6.2.7, 14 September 2021, v1.5 Evaluation Technical Report NIAP PP-Configuration for Network Device, Intrusion Prevention Systems (IPS), Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways, 19 December 2021, v1.1

Table 2 - APE Evaluation Results

APE Requirement	Verdict	Verified By
APE_INT.1: PP Introduction	Pass	- Security Target FortiGate/FortiOS Version 6.2.7, 14 September 2021, v1.5 - Evaluation Technical Report NIAP PP-Configuration for Network Device, Intrusion Prevention Systems (IPS), Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways, 19 December 2021, v1.1
APE_SPD.1: Security Problem Definition	Pass	- Security Target FortiGate/FortiOS Version 6.2.7, 14 September 2021, v1.5 - Evaluation Technical Report NIAP PP-Configuration for Network Device, Intrusion Prevention Systems (IPS), Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways, 19 December 2021, v1.1
APE_OBJ.2: Security Objectives	Pass	- Security Target FortiGate/FortiOS Version 6.2.7, 14 September 2021, v1.5 - Evaluation Technical Report NIAP PP-Configuration for Network Device, Intrusion Prevention Systems (IPS), Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways, 19 December 2021, v1.1
APE_ECD.1: Extended Components Definition	Pass	- Security Target FortiGate/FortiOS Version 6.2.7, 14 September 2021, v1.5 - Evaluation Technical Report NIAP PP-Configuration for Network Device, Intrusion Prevention Systems (IPS), Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways, 19 December 2021, v1.1
APE_REQ.2: Security Requirements	Pass	- Security Target FortiGate/FortiOS Version 6.2.7, 14 September 2021, v1.5 - Evaluation Technical Report NIAP PP-Configuration for Network Device, Intrusion Prevention Systems (IPS), Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways, 19 December 2021, v1.1

3 REFERENCES

Reference
Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017.
Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 5, April 2017.
collaborative Protection Profile for Network Devices, v2.2e, 23-March-2020
PP-Module for Stateful Traffic Filter Firewalls, v1.4 + Errata 20200625
PP-Module for Virtual Private Network (VPN) Gateways (MOD_VPNGW), v1.1, 2020-06-18
PP-Module for Intrusion Prevention Systems, v1.0, 2021-05-11
PP-Configuration for Network Device, Intrusion Prevention Systems (IPS), Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways, v1.0, 18 May 2021
Supporting Document Mandatory Technical Document Evaluation Activities for Network Device cPP, v2.2, December 2019
Supporting Document Mandatory Technical Document Evaluation Activities for Stateful Traffic Filter Firewalls PP-Module, June-2020, Version 1.4 +Errata 20200625
Supporting Document Mandatory Technical Document PP-Module for Virtual Private Network (VPN) Gateways, Version: 1.1, 2020-06-18
Supporting Document Mandatory Technical Document PP-Module for Intrusion Prevention Systems (IPS), Version: 1.0, 2021-05-11
Security Target FortiGate/FortiOS Version 6.2.7, 14 September 2021, v1.5
Assurance Activity Report FortiGate/FortiOS Version 6.2.7, 19 November 2021, v1.4
Evaluation Technical Report NIAP PP-Configuration for Network Device, Intrusion Prevention Systems (IPS), Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways, 19 December 2021, v1.1