CSEC

Swedish Certification Body for IT Security

Certification Report- PP-Configuration for Network Device and SSL/TLS Inspection Proxy (STIP)

Issue: 1.0, 2024-apr-16

Authorisation: Helén Svensson, Lead certifier , CSEC

Table of Contents

1   Executive Summary

The PP-Configuration for Network Device and SSL/TLS Inspection Proxy (STIP), combines the requirements of the collaborative Protection Profile for Network Devices, Version 2.2e, and the PP-Module for SSL/TLS Inspection Proxy (STIP), Version 1.1.

Thus, the PP-Configuration combines the security requirements for a generic network device with the security requirements for a network device that provides functionality for SSL/TLS Inspection Proxy (STIP).

The PP-Configuration is used in the same way as a PP and is recognised as a PP within the CCRA.

The PP-Configuration for Network Device and SSL/TLS Inspection Proxy (STIP), requires exact conformance.

The PP-Configuration evaluation has been performed by atsec information security AB and was completed on 2024-01-04, and was performed concurrently with, and as a separate part of the product evaluation of the BIG-IP Version 16.1.3.1 including SSLO, which claims conformance to the PP-Configuration.

The evaluation was conducted in accordance with the requirements of Common Criteria, version 3.1, release 5, and the Common Methodology for IT Security Evaluation, version 3.1, release 5, and CC and CEM Addenda - Exact Conformance, Selection-Based SFRs, Optional SFRs, CCDB, May 2017.

The evaluation was performed according to the requirements in assurance class ACE and the assurance components APE_INT.1, APE_SPD.1, APE_OBJ.2, APE_ECD.1, and APE_REQ.2.

atsec information security AB is a licensed evaluation facility for Common Criteria under the Swedish Common Criteria Evaluation and Certification Scheme. atsec information security AB is also accredited by the Swedish accreditation body according to ISO/IEC 17025 for Common Criteria.

The certifier monitored the activities of the evaluator by reviewing all work units in the evaluation report. The certifier determined that the evaluation results have been reached in agreement with the requirements of the Common Criteria and the Common Methodology.

The certification results only apply to the version of the PP-Configuration indicated in the certificate, and on the condition that all the stipulations in the Security Target are met.
This certificate is not an endorsement of the PP-Configuration by CSEC or any other organisation that recognises or gives effect to this certificate, and no warranty of the PP-Configuration by CSEC or any other organisation that recognises or gives effect to this certificate is either expressed or implied.

---

2 Identification

Certification Identification	
Certification ID	CSEC2024004
Name and version of the certified PP-Configuration	PP-Configuration for Network Device and SSL/TLS Inspection Proxy (STIP)
PP-Module Identification	PP-Module for SSL/TLS Inspection Proxy (STIP)
Base PP Identification	Collaborative Protection Profile for Network Devices, Version 2.2e
Sponsor	F5 Inc
Developer	NIAP
ITSEF	atsec information security AB
Common Criteria version	3.1 release 5
CEM version	3.1 release 5
QMS version	2.5.1
Scheme Notes Release	21.0
Recognition Scope	CCRA
Certification date	2024-04-16

3   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].

The evaluators' overall verdict is PASS.

The verdicts for the assurance classes and components are summarised in the following table:

Assurance Class/Family	Short name	Verdict
Protection Profile Configuration Evaluation	ACE	PASS
PP-Module Introduction	ACE_INT.1	PASS
PP-Module Conformance Claims	ACE_CCL.1	PASS
PP-Module Security Problem Definition	ACE_SPD.1	PASS
PP-Module Security Objectives	ACE_OBJ.1	PASS
PP-Module Extended Components Definition	ACE_ECD.1	PASS
PP-Module Security Requirements	ACE_REQ.1	PASS
PP-Module Consistency	ACE_MCO.1	PASS
PP-Configuration Consistency	ACE_CCO.1	PASS
Protection Profile Evaluation (selected parts)	APE	PASS
PP Introduction	APE_INT.1	PASS
Security Problem Definition	APE_SPD.1	PASS
Security Objectives	APE_OBJ.2	PASS
Extended Components Definition	APE_ECD.1	PASS
Security Requirements	APE_REQ.2	PASS

4   Evaluator Comments and Recommendations

None.

5   Certifier Comments and Recommendations

During the evaluation of PP-Configuration for Network Device and SSL/TLS Inspection Proxy (STIP), the following interpretations were considered

TD0738   NIT Technical Decision for Link to Allowed-With List, 2023-05-19

Please note that when using the PP-Configuration in a product evaluation, these and other interpretations may apply.

6 Glossary

CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria - CC Part 1-3 refers to the Common Criteria Documentation
CEM	Common Methodology for Information Technology Security Evaluation
PP	Protection Profile
cPP	Collaborative Protection Profile
PP-Configuration	Protection Profile composed of Base Protection Profiles and Protection Profile Module
PP-Module	Implementation-independent statement of security needs for a TOE type complementary to one or more Base Protection Profiles
Base PP	Protection Profile used as a basis to build a Protection Profile Configuration
TOE	Target of Evaluation

7 Bibliography

PP-CFG	PP-Configuration for Network Device and SSL/TLS Inspection Proxy (STIP), October 6, 2023, document version 1.1
STIPM	PP-Module for SSL/TLS Inspection Proxy Version 1.1, 2022-11-17 document version 1.1
STIPM-SD	Supporting Document Mandatory Technical Document PP-Module for SSL/TLS Inspection Proxy, 2022-11-17, document version 1.1
NDcPP	collaborative Protection Profile for Network Devices Version 2.2e, 2020-03-23, document version 2.2e
NDcPP-SD	Supporting Document - Evaluation Activities for Network Device cPP, 2019-12-20, document version 2.2
CCpart1	Common Criteria for Information Technology Security Evaluation, Part 1, version 3.1 revision 5, CCMB-2017-04-001
CCpart2	Common Criteria for Information Technology Security Evaluation, Part 2, version 3.1 revision 5, CCMB-2017-04-002
CCpart3	Common Criteria for Information Technology Security Evaluation, Part 3, version 3.1 revision 5, CCMB-2017-04-003
CC	CCpart1 + CCpart2 + CCpart3
CEM	Common Methodology for Information Technology Security Evaluation, version 3.1 revision 5, CCMB-2017-04-004
CCADD	CC and CEM Addenda - Exact Conformance, Selection-Based SFRs, Optional SFRs, CCDB, May 2017
SP-002	SP-002 Evaluation and Certification, CSEC, 2023-06-02, document version 35.0

Appendix A   Scheme Versions

During the certification the following versions of the Swedish Common Criteria Evaluation and Certification scheme have been used.

A.1   Scheme/Quality Management System

Version	Introduced	Impact of changes
2.5.1	2024-02-29	*None*
2.5	2024-01-25	*None*
2.4.2	Application	Original version

A.2   Scheme Notes

No applicable Scheme Notes were identified