Diarienummer: 23FMV4091-28

Dokument ID CSEC2023009

CSEC

Swedish Certification Body for IT Security

Certification Report - F5 BIG-IP 16.1.3.1 including SSLO

Issue: 1.0, 2024-apr-16

Authorisation: Helén Svensson, Lead certifier , CSEC

Table of Contents

1 Executive Summary

The Target of Evaluation (TOE) is a networking device comprised of hardware and software. TOE is the BIG-IP Version 16.1.3.1 including SSLO (build Hotfix-BIGIP-16.1.3.1.0.128.11-ENG), installed on one of the following hardware appliances:

- i4000 model series, including i4600, and i4800,
- i5000 model series, including i5600, i5800, and i5820-DF
- i7000 model series, including i7600, i7800, and i7820-DF
- i10000 model series, including i10600, and i10800
- i11000 DS model series, including i11600-DS, and i11800-DS
- i15000 model series, including i15600, and i15800
- i15000-DF model series, including i15820-DF
- B2250
- C2400
- B4450
- C4480

or installed on an F5 Virtual Clustered Multiprocessing (vCMP) environment running on any of the following hardware appliances:

- i5000 model series, including i5800, and i5820-DF
- i7000 model series, including i7800, and i7820-DF
- i10000 model series, including i10800
- i11000 DS model series, including i11600-DS, and i11800-DS
- i15000 model series, including i15800
- i15000-DF model series, including i15820-DF
- B2250
- C2400
- B4450
- C448

The TOE hardware appliances above are delivered via trusted couriers. The TOE software is downloaded from the F5 website.

The Security Target [ST] claims exact conformance to the PP-Configuration for Network Device and SSL/TLS Inspection Proxy [CFG_ND-STIP_V1.1], which combines the collaborative Protection Profile for Network Devices [NDcPP], and PP-Module for SSL/TLS Inspection Proxy [STIPM]

A list of the NIT technical decisions considered during the evaluation is available in the ST.

There are eleven assumptions being made in the ST regarding the secure usage and the operational environment of the TOE. The TOE relies on these to counter the seventeen threats and comply with the two organisational security policy (OSP) in the ST.

The assumptions, threats, and the OSP are described in chapter 4 Assumptions and Clarification of Scope.

The evaluation has been performed by atsec information security AB in Danderyd, Sweden.

The evaluation was completed on 2024-03-13. The evaluation was conducted in accordance with the requirements of Common Criteria (CC), version. 3.1 release 5.

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 successive versions of the evaluation reports. The certifier determined that the evaluation results confirm the security claims in the Security Target (ST) and the Common Methodology for evaluation assurance level EAL 1 + ASE_SPD.1 and in accordance with the Evaluation Activities for Collaborative Protection Profile for Network Devices [NDcPP-SD] and Supporting Document Mandatory Technical Document PP-Module for SSL/TLS Inspection Proxy [STIPM-SD].

The technical information in this report is based on the Security Target (ST) and the Final Evaluation Report (FER) produced by atsec information security AB.

The certification results only apply to the version of the product 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 IT product by CSEC or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product 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	CSEC2023009
Name and version of the certified IT product	BIG-IP Version 16.1.3.1 including SSLO build Hotfix-BIGIP-16.1.3.1.0.128.11-ENG
Security Target Identification	F5 BIG-IP 16.1.3.1 including SSLO Security Target, F5 Inc., 2023-12-14, document version 6.12
EAL	EAL 1 + ASE_SPD.1 (CFG_ND-STIP_V1.1)
Sponsor	F5 Inc.
Developer	F5 Inc.
ITSEF	atsec information security AB
Common Criteria version	3.1 release 5
CEM version	3.1 release 5
QMS version	2.5
Scheme Notes Release	21.0
Recognition Scope	CCRA, EA/MLA
Certification date	2024-04-16

3 Security Policy

The following security functions provided by the TOE are described in more detail in the subsections

below:

- Security Audit
- Cryptographic Support
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channels
- User Data Protection

3.1 Security Audit

BIG-IP implements syslog capabilities to generate audit records for securityrelevant events. In addition, the BIG-IP protects the audit trail from unauthorized modifications and loss of audit data due to insufficient space.

3.2 Cryptographic Support

In BIG-IP, cryptographic functionality in the control plane is provided by the OpenSSL cryptographic module. The BIG-IP provides a secure shell (SSH) to allow administrators to connect over a dedicated network interface. BIG-IP also implements the TLS protocol to allow administrators to remotely manage the TOE. BIG-IP implements a TLS client for interactions with other TLS servers. The BIG-IP SSLO cryptography is provided by the cryptographic module within TMM, also based on OpenSSL. SSLO implements the TLS protocol with forward proxy capabilities including inspection processing, bypassing inspection processing, and blocking unauthorized sessions.

Both of these cryptographic implementations utilize a cryptographic module which provides random number generation, key generation, key establishment, key storage, key destruction, hash operations, encryption/decryption operations, and digital signature operations.

A limited Certification Authority (CA) is also embedded in the BIG-IP SSLO to issue certificates in order to establish TLS sessions with the monitored client and the requested server endpoint.

3.3 Identification and Authentication

An internal password-based repository is implemented for authentication of management users. BIG-IP enforces a strong password policy and disabling user accounts after a configured number of failed authentication attempts.

3.4 Security Function Management

A command line interface (available via the traffic management shell "tmsh"), web-based GUI ("Configuration utility"), a SOAP-based API ("iControl API"), and a REST-based API (“iControl REST API”) are offered to administrators for all relevant configuration of security functionality. The TOE manages configuration objects in a partition which includes users, server pools, etc. This includes the authentication of administrators by user name and password, as well as access control based on pre-defined roles and, optionally, groups of objects ("Profiles"). "Profiles" can be defined for individual servers and classes of servers that the TOE forwards traffic from clients to, and for traffic that matches certain characteristics, determining the kind of treatment applicable to that traffic. Management capabilities offered by the TOE include the definition of templates for certain configuration options. The management functionality also implements roles for separation of duties.

3.5 Protection of the TSF

BIG-IP implements many capabilities to protect the integrity and management of its own security functionality. These capabilities include the protection of sensitive data, such as passwords and keys, self-tests, product update verification, and reliable time stamping.

3.6 TOE Access

Prior to interactive user authentication, the BIG-IP can display an administrative-defined banner. BIG-IP terminates interactive sessions after an administrator-defined period of inactivity and allows users to terminate their own authenticated session.

3.7 Trusted Path / Channels

The TOE protects remote connections to its management interfaces with TLS and SSH. The TOE also protects communication channels with audit servers using TLS.

3.8 User Data Protection

The BIG-IP SSLO implements certificate profiles for TLS server certificates issued by the CA embedded in the TOE, enforces TLS plaintext processing policies, ensures residual information contained in TLS buffers is not available, protects trusted public keys and certificates used in SSLO, and performs inspection operations and proxy functions of SSLO sessions.

4 Assumptions and Clarification of Scope

4.1 Usage and Environmental Assumptions

The Security Target [ST] makes eleven assumptions on the usage and on the operational environment of the TOE.

A.PHYSICAL_PROTECTION

The Network Device 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 device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device 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 device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device. For vNDs, this assumption applies to the physical platform on which the VM runs.

A.LIMITED_FUNCTIONALITY

The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example the device should not provide a computing platform for general purpose applications (unrelated to networking functionality).

In the case of vNDs, the VS is considered part of the TOE with only one vND instance for each physical hardware platform. The exception being where components of the distributed TOE run inside more than one virtual machine (VM) on a single VS. There are no other guest VMs on the physical platform providing non-Network Device functionality.

The assumed functionality of the TOE includes the behavior needed to satisfy the functional claims of STIPM.

A.NO_THRU_TRAFFIC_PROTECTION

The standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the Network Device to protect data that originates on or is destined to the device itself, to include administrative data and audit data.

Traffic that is traversing the Network Device, destined for another network entity, is not covered by the NDcPP. It is assumed that this protection will be covered by cPPs and PPModules for particular types of Network Devices (e.g., firewall).

This assumption only applies to the interfaces of the TOE that are defined by the NDcPP and not STIPM.

A.TRUSTED_ADMINISTRATOR

The Security Administrator(s) for the Network Device 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 device. The Network Device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device.

For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).

The functional claims of STIPM offer a limited ability to protect against malicious administrators, which is not within the scope of the original assumption.

A.REGULAR_UPDATES

The Network Device 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 network device are protected by the platform on which they reside.

A.RESIDUAL_INFORMATION

The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g., cryptographic keys, keying material, PINs, passwords, etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

Residual information is expanded to include information relevant to STIP operation (e.g. decrypted SSL/TLS payload, ephemeral keys).

A.VS_TRUSTED_ADMINISTRATOR (applies to vNDs only)

The Security Administrators for the VS are assumed to be trusted and to act in the best interest of security for the organization. This includes not interfering with the correct operation of the device. The Network Device is not expected to be capable of defending against a malicious VS Administrator that actively works to bypass or compromise the security of the device.

A.VS_REGULAR_UPDATES (applies to vNDs only)

The VS software is assumed to be updated by the VS Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.

A.VS_ISOLATON (applies to vNDs only)

For vNDs, it is assumed that the VS provides, and is configured to provide sufficient isolation between software running in VMs on the same physical platform. Furthermore, it is assumed that the VS adequately protects itself from software running inside VMs on the same physical platform.

A.VS_CORRECT_CONFIGURATION (applies to vNDs only)

For vNDs, it is assumed that the VS and VMs are correctly configured to support ND functionality implemented in VMs.

4.2 Clarification of Scope

The Security Target contains seventeen threats, which have been considered during the evaluation.

T.UNAUTHORIZED_ADMINISTRATOR_ACCESS

Threat agents may attempt to gain Administrator access to the Network Device by nefarious means such as masquerading as an Administrator to the device, masquerading as the device to an Administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between Network Devices. Successfully gaining Administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.

T.WEAK_CRYPTOGRAPHY

Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.

T.UNTRUSTED_COMMUNICATION_CHANNELS

Threat agents may attempt to target Network Devices that do not use standardized secure tunneling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the Network Device itself.

T.WEAK_AUTHENTICATION_ENDPOINTS

Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g., shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the Administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the Network Device itself could be compromised.

T.UPDATE_COMPROMISE

Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.

T.UNDETECTED_ACTIVITY

Threat agents may attempt to access, change, and/or modify the security functionality of the Network Device without Administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the Administrator would have no knowledge that the device has been compromised.

T.SECURITY_FUNCTIONALITY_COMPROMISE

Threat agents may compromise credentials and device data enabling continued access to the Network Device and its critical data. The compromise of credentials include replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the Administrator or device credentials for use by the attacker.

T.PASSWORD_CRACKING

Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic and may allow them to take advantage of any trust relationships with other Network Devices.

T.SECURITY_FUNCTIONALITY_FAILURE

An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.

T.UNTRUSTED_COMMUNICATION

Untrusted intermediate systems have access to provide unauthorized communications to the TOE, or to manipulate authorized TLS messages in an attempt to compromise the TOE, the monitored clients, or the requested servers. Within this PP-Module, the focus is on an adversary that controls or exploits a requested server that may attempt to cause the device to inappropriately bypass inspection.

Use of weak cryptography can allow adversary access to plaintext intended by the monitored clients to be encrypted. Such access could disclose user passwords that facilitate additional activities against users of monitored clients. Within this PP-Module, the focus is on the use of weak cryptography and adversary attempts to degrade the cryptographic operations within the TLS protocol.

External network security devices may communicate with the TOE to apply security services to the exposed plaintext. An adversary may attempt to gain access the plaintext via misrouting of traffic or manipulate the traffic in such a way as to cause unauthorized exposure, denial of service, or corruption of the underlying plaintext.

T.AUDIT

Certificates issued by the device are trusted by monitored clients, and are required for analysis if traffic processed by the device causes the client to fail or become compromised. Unknown activity related to the issuance and use of certificates can allow an adversary to mask client exploits through or via the TOE, especially if the device fails before the incident can be understood. Unknown activity associated to routing configurations, communications with the TOE, as well as the decision to bypass inspection of traffic can allow an adversary to mask attempts to access monitored clients.

T.UNAUTHORIZED_USERS

In addition to managing administrative credentials, authorized users may have role restrictions to limit their access to the device's certification authority functionality. In addition to the threat of disclosure or modification of authorized user credentials to users without authorized access to the device, a user with limited access might attempt to extend their access by gaining access to other user's credentials.

T.CREDENTIALS

In addition to device credentials used in protected communications, the device maintains a trusted certification authority signing key. A malicious user or flawed TOE implementation may cause the disclosure or unauthorized manipulation of the signing key which can result in unintended certificates, signed executables, or signed data that would be trusted by monitored clients. Any modification of the signing key can result in denial of service to inspection capabilities, or to the monitored clients.

T.SERVICES

Manipulation of the device can result in issued certificates being used for unauthorized purposes or abuse of inspection services. An authorized user (AU) (or adversary able to gain access to AU credentials) can access or misuse device services, or disclose sensitive or security critical data.

T.DEVICE_FAILURE

Failure of the certification authority component can result in unauthorized or improperly constrained certificates, or the inability to properly manage the validity of issued certificates. Failure of routing traffic to inspection processing (internal or external) can result in unauthorized disclosure or modification of traffic, or denial of service to monitored clients.

T.UNAUTHORIZED_DISCLOSURE

In addition to general threats to network devices, the TOE controls access to sensitive data that is intended by the monitored client to be encrypted. A malicious user or flawed TOE implementation could cause data to be transmitted in cleartext for which a user has a reasonable expectation of confidentiality.

T.INAPPROPRIATE_ACCESS

Decryption services applied to traffic between monitored clients and unintended servers can violate privacy laws, or disclose unauthorized traffic to inspection processes. Certification authority signature applied to unauthorized data could facilitate adversary exploits of monitored clients.

The Security Target contains two Organisational Security Policies (OSPs), which have been considered during the evaluation.

P.ACCESS_BANNER

The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

P.AUTHORIZATION_TO_INSPECT

The authority to inspect client traffic may be limited by law, regulation, or policies based on the monitored client, requested server, or nature of the traffic. The TOE may be required to additionally provide a consent to monitor notice for users whose traffic is inspected by the device, if the monitored client might not provide such a banner.

5 Architectural Information

The following diagram shows the basic components that comprise the TOE illustrating the deployment supported in the evaluated configuration.

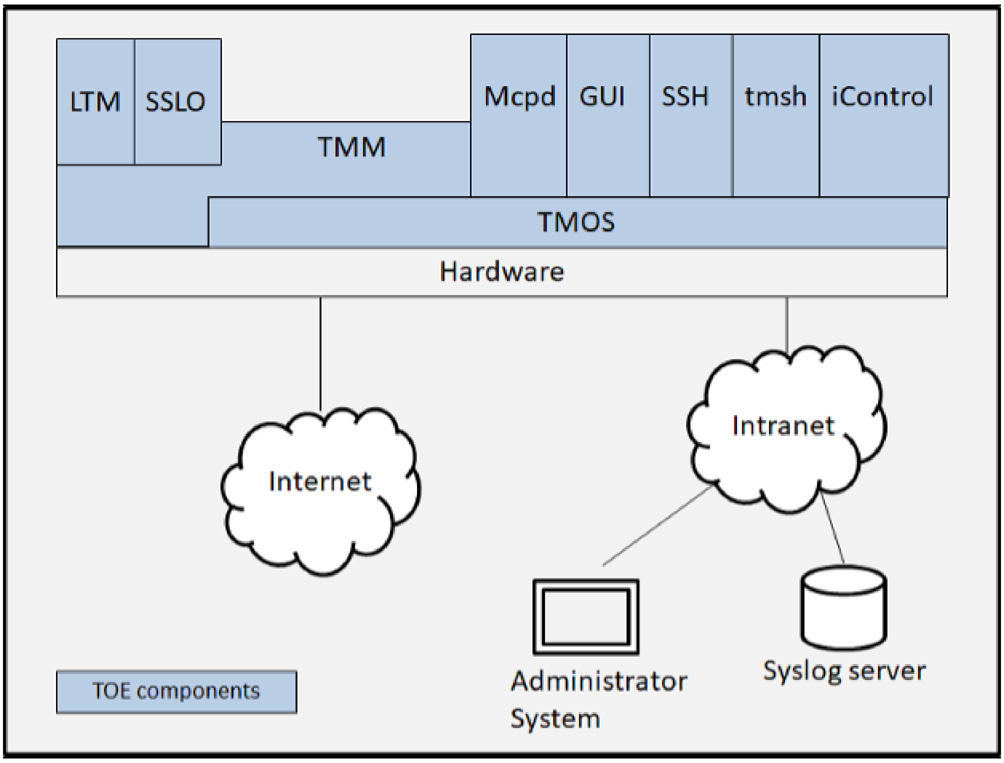

Figure 1: Architectural aspects of BIG-IP – F5 Device and vCMP in Application Delivery Controller Deployments

The TOE is separated into two (2) distinct planes, the control plane and the data plane. The control plane validates, stores, and passes configuration data to all necessary systems. It also provides all administrative access to the TOE. The data plane passes user traffic through the TOE.

The TOE implements and supports the following network protocols: TLS (client and server), SSH, HTTPS, FTP. The TOE protects remote connections to its management interfaces with TLS and SSH. The TOE also protects communication channels with audit servers using TLS (TLSv1.1 and TLSv1.2). The cryptographic functionality implemented in the TOE is provided by OpenSSL.

The TOE is divided into the following subsystems: F5 Device (hardware or virtual) for F5 devices or vCMP deployments, Traffic Management Operating System (TMOS), Traffic Management Micro-kernel (TMM), SSLO Inspection Proxy (SSLO), and Local Traffic Manager (LTM). The TOE's TMOS is a Linux-based operating system customized for performance and to execute on the TOE hardware or in the TOE Virtual Clustered Multiprocessing (vCMP) environment. The vCMP is an embedded hypervisor that allows multiple instances of the TOE to execute on the same underlying hardware. The TMM is the data plane of the product and all data plane traffic passes through the TMM. The LTM controls network traffic coming into or exiting the local area network (LAN) and provides the ability to intercept and redirect incoming network traffic. The APM module terminates TLS-based VPN connections from remote clients although these features are not included in the evaluated configuration.

At the core of BIG-IP is a concept referred to as Traffic Management Microkernel (TMM), representing the data plane of the product when compared to traditional network device architectures. It is implemented by a daemon running with root privileges, performing its own memory management, and having direct access to the network hardware or hypervisor. TMM implements a number of sequential filters both for the “client-side” and “server-side” network interfaces served by BIG-IP. The filters implemented in TMM include a TCP, TLS, compression, and HTTP filter, amongst others. If the hardware or hypervisor provides more than one CPU, TMM runs multithreaded (one thread per CPU). In this case, disaggregators in the kernel are responsible for de-multiplexing and multiplexing network traffic for handling by an individual TMM thread. In addition to the actual switch hardware, F5 appliance hardware also contains a High-Speed Bridge (HSB, implemented by means of an FPGA) that performs basic traffic filtering functionality as instructed by TMM.

Additional plug-in filters can be added to this queue by individual product packages. These plug-ins typically have a filter component in TMM, with additional and more complex logic in a counter-part implemented in a Linux-based daemon (module). The plug-in modules relevant to this evaluation include:

- Local Traffic Manager (LTM): authentication of HTTP (based on Apache) traffic and advanced traffic forwarding directives
- SSLO Inspection Proxy (SSLO): TLS-based STIP functionality.

6 Documentation

The guides to installing the TOE into the evaluated configuration are:

- BIG-IP Common Criteria Evaluation Configuration Guide BIG-IP Release 16.1.3.1 Including SSLO [ECG]
- K76615426: Common Criteria Certification for BIG-IP 16.1.3.1 [K76615426]

The [ST], section 1.6.3.2 provides a full list of the guidance documents that are part of the TOE.

7 IT Product Testing

7.1 Evaluator Testing

Independent testing was performed on all the hardware appliance BIG-IP i4800 and the hardware appliance that support Virtual Clustered Multiprocessing (vCMP) BIG-IP i7800. The evaluators confirmed that all test cases passed successfully

The cryptographic testing was performed within the Cryptographic Algorithm Validation Program (CAVP). All applicable tests passed successfully

7.2 Penetration Testing

The approach for the penetration test was to scan all TCP ports on the TOE platform to identify all open ports.

The penetration test was performed on the TOE in the evaluated configuration. During the execution of the port scans, all devices were configured with LTM+SSLO licenses.

No discrepancies were found during the penetration testing

8 Evaluated Configuration

The following configuration specifics apply to the evaluated configuration of the TOE:

- Appliance mode is licensed. This results in root access to the TOE operating system and bash shell being disabled.
- Certificate validation is performed using CRLs (for non-SSLO functions)
- Disabled interfaces:
  - All command shells other than tmsh are disabled. For example, bash and other user-serviceable shells are excluded.
  - Management of the TOE via SNMP is disabled.
  - Management of the TOE via the appliance's LCD display is disabled.
  - Remote (i.e., SSH) access to the Lights Out / Always On Management capabilities of the system is disabled. (applicable to F5 devices and vCMP only)
  - SSH client
- SSL Orchestrator is licensed, enabling the SSL/TLS inspection proxy functionality, with the associated cryptographic options.

9 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 TOE meets the security objectives stated in the Security Target [ST] for an attack potential of Basic.

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*
Development	ADV	PASS
Functional Specification	ADV_FSP.1	PASS
Guidance Documents	AGD	PASS
Operational User Guidance	AGD_OPE.1	PASS
Preparative Procedures	AGD_PRE.1	PASS
Life-cycle Support	ALC	PASS
CM Capabilities	ALC_CMC.1	PASS
CM Scope	ALC_CMS.1	PASS
Security Target Evaluation	ASE	PASS
ST Introduction	ASE_INT.1	PASS
Conformance Claims	ASE_CCL.1	PASS
Security Problem Definition	ASE_SPD.1	PASS
Security Objectives	ASE_OBJ.1	PASS
Extended Components Definition	ASE_ECD.1	PASS
Security Requirements	ASE_REQ.1	PASS
TOE Summary Specification	ASE_TSS.1	PASS
Tests	ATE	PASS
Independent Testing	ATE_IND.1	PASS
Vulnerability Assessment	AVA	PASS
Vulnerability Analysis	AVA_VAN.1	PASS
Evaluation Activities for NDcPP		PASS
Evaluation Activities for STIPM		PASS

10 Evaluator Comments and Recommendations

None.

11 Glossary

CC	Common Criteria
CMI	Central Management Infrastructure
CRL	Certificate Revocation List
CRLDP	Certificate Revocation List Distribution Point
GUI	Graphical User Interface
HSL	High-Speed Logging
LTM	Local Traffic Manager
OSP	Organisational Security Policy
PP	Protection Profile
SFP	Security Function Policy
SFR	Security Functional Requirement
SOAP	Simple Object Access Protocol
TLS	Transport Layer Security
TMM	Traffic Management Microkernel
TMOS	Traffic Management Operating System
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
vCMP	Virtual Clustered Multi-Processing
VE	Virtual Edition

12 Bibliography

ST	F5 BIG-IP® 16.1.3.1 including SSLO Security Target F5 Inc., 2023-12-14, document version 6.12
ECG	BIG-IP Common Criteria Evaluation Configuration Guide BIG-IP Release 16.1.3.1 Including SSLO, F5 Inc., 2023-12-13
K76615426	K76615426: Common Criteria Certification for BIG-IP 16.1.3.1, document version 2023-04-26
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
CFG_ND-STIP_V1.1	PP-Configuration for Network Device and SSL/TLS Inspection Proxy (STIP), 2023-10-06, 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
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

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

Scheme Note 21 - NIAP PP Certifications

Scheme Note 22 - Vulnerability assessment

Scheme Note 23 - Evaluation reports for NIAP PPs and cPPs

Scheme Note 25 - Use of CAVP-tests in CC evaluations

Scheme Note 27 - ST requirements at the time of application for certification

Scheme Note 28 - Updated procedures for application, evaluation ad certification