Swedish Certification Body for IT Security

Certification Report F5 BIG-IP 17.5.0 including SSLO

Issue: 1.0, 2026-feb-26

Authorisation: Theodora Arvanitidis, Junior Certifier , CSEC

Table of Contents

1 Executive Summary

The Target of Evaluation (TOE) is a Networking Device. When running on iSeries and VIPRION devices, the TOE is a physical Network Device. When running on F5OS on rSeries or VELOS devices, the TOE is a virtual Network Device. The TOE claiming conformance to this ST is identified as BIG-IP Version 17.5.0 including SSLO (Build Hotfix-BIGIP-17.5.0.0.190.15-ENG, also referred to as 17.5). The TOE consists of following:

Supported Physical Network Devices:

• I15000 model series, including I15600, I15800 and I15820-DF

• C2400 model series, including C2400-AC

• C2400 with B2250

• C4480 model series, including C4480-AC

• C4480 with B4450

Supported Virtual Network Devices:

• R4000 model series, including R4600 and R4800

• R5000 model series, including R5600, R5800, R5900 and R5920-DF

• R10000 model series, including R10600, R10800, R10900 and R10900-DF

• R12000 model series, including R12600DS, R12800DS and R12900DS

• CX410 model series, including CX410-AC

• BX110 with CX410

• CX1610 model series, including CX1610-AC

• BX520 with CX1610

• BX520 with CX410

The Security Target [ST] claims exact conformance to PP-Configuration for Network Device and SSL/TLS Inspection Proxy (STIP) (CFG_NDcPP-STIP_V2.0), version 2.0 (2024-04-25). CFG_NDcPP-STIP_V2.0 consists of the following components:

• Collaborative Protection Profile for Network Devices (NDcPP), Version 3.0e (2023-12-06)

• PP-Module for SSL/TLS Inspection Proxy (STIPM), Version 1.1 (2022-11-17)

The [ST] claims exact conformance to the Functional Package for Secure Shell (SSH) (PKG_SSH), version 1.0 (2021-05-13).

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

There are seven 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 sixteen 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 and was completed in 2026-02-09 The evaluation was conducted in accordance with the requirements of Common Criteria, version 3.1, revision 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 SWEDAC according to ISO/IEC 17025 for Common Criteria evaluation.

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].

The technical information in this report is based on the Security Target 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	CSEC2024029
Name and version of the certified IT product	F5 BIG-IP® 17.5.0 including SSLO
Security Target Identification	F5 BIG-IP® 17.5 including APM Security Target, F5, Inc., 2026-01-21, version 17.58
EAL	CFG_NDcPP-STIP_V2.0
Sponsor	F5, Inc.
Developer	F5, Inc.
ITSEF	atsec information security AB
Common Criteria version	3.1 revision 5
CEM version	3.1 revision 5
QMS version	2.6.1
Scheme Notes Release	22.0
Recognition Scope	CCRA, EA-MLA
Certification date	2026-02-26

3 Security Policy

The TOE provides the following security services:

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

3.1 Security Audit

BIG-IP implements auditing functionality based on standard syslog functionality. This includes the support of remote audit servers for capturing of audit records. Audit records are generated for all security relevant events, such as the use of configuration interfaces by administrators, the authentication of traffic, and the application of network traffic rules.

While the TOE can store audit records locally for cases when an external log server becomes unavailable, in the evaluated configuration an external log server is used as the primary means of archiving audit records.

In the evaluated configuration, BIG-IP logs a warning to notify the administrator when the local audit storage exceeds a configurable maximum size. Once the configurable maximum size is reached, BIG-IP overwrites the older audit records.

3.2 Cryptographic Support

All cryptographic operations, including algorithms and key generation used by the TOE are provided by the F5 cryptographic module (OpenSSL) within the TMOS.

Various security functions in BIG-IP rely on cryptographic mechanisms for their effective implementation. Trusted paths for the TOE administrator are provided by SSH for the tmsh administrative interface and by TLS for the Configuration utility, iControl API and iControl REST API. For administrative sessions, the TOE always acts as a server. For traffic sessions, the TOE may act as a TLS client or server. Trusted channels between the TOE and external entities, such as a syslog server, are provided by TLS connections.

For TLS sessions, the TOE implements certificate validation using the OpenSSL crypto library. Time synchronization with an NTP server uses SHA-1 message digests to verify the integrity of the NTP packets.

The TOE utilizes cryptographic algorithms that have been validated using the NIST ACVP tests.

For F5 devices, the underlying hardware platforms of the TOE include a third party proprietary cryptographic acceleration card that is used to provide both sufficient entropy to support random number generation (RNG) and acceleration.

Key Generation

The TOE can generate asymmetric keys using RSA schemes and ECC schemes. For F5 devices, the underlying hardware platforms of the TOE include a third party proprietary cryptographic acceleration card that is used to provide sufficient entropy to support RNG. For F5 devices, the TOE provides a total of four entropy sources. The TOE can generate keys (and certificates) for a number of uses, including:

• Keypairs for the SSH server functionality

• TLS server and client certificates

• Session keys for SSH and TLS sessions

SSL/TLS Inspection Proxy

The TOE implements an administrator-configurable SSL/TLS Inspection proxy. The administrator configures SSL forward proxy profiles to define which TLS connections are subject to inspection, to define the TLS session parameters of the connections, and to define any inspection services that will be performed on the connection.

The SSLO module accomplishes the inspection operation by terminating TLS sessions between a monitored client and the requested server that meet the SSLO policy conditions, then replacing the end-to-end connection with two TLS sessions that terminate at the TOE. The TOE establishes a TLS session between the TOE (acting as the monitored client) and the requested server and a second TLS session between the TOE (acting as the requested server) and the monitored client. By intercepting the TLS session, the TOE can send the decrypted traffic to an external inspection service for processing.

As configured by the SSL forward proxy profiles, SSLO also determines which TLS sessions should bypass inspection processing and be routed without decryption, inspection, and modification. When SSLO determines that a session is not authorized, the session is blocked and the traffic is not routed to the other endpoint.

3.3 Identification and Authentication

The TOE identifies individual administrative users by user name and authenticates them by passwords stored in a local configuration database; the TOE can enforce a password policy based on overall minimum length and number of characters of different types required. BIG-IP obscures passwords entered by users.

Authentication of administrators is enforced at all configuration interfaces, i.e. at the shell (tmsh, via SSH), the Configuration utility (web-based GUI), iControl API, and iControl REST API.

3.4 Security Management

The TOE allows administrators to configure all relevant aspects of security functionality implemented by the TSF. For this purpose, BIG-IP offers multiple interfaces to administrators:

• Configuration utility

The Configuration utility presents a web-based GUI available to administrators via HTTPS that allows administration of most aspects of the TSF.

• traffic management shell (tmsh)

tmsh is a shell providing a command line interface that is available via SSH. It allows administration of all aspects of the TSF.

• iControl API

The iControl API is a SOAP based protocol interface that allows programmatic access to the TSF configuration via HTTPS.

• iControl REST API

The iControl REST API is effectively a front-end to tmsh and is built on the Representational State Transfer (REST), which allows programmatic access to the TSF via HTTPS.

The TOE provides the ability to administer the TOE both locally and remotely using any of the four administrative interfaces. Local administration is performed via the serial port console. By default and in the evaluated configuration, remote access to the management interfaces is only made available on the dedicated management network port of a BIG-IP system.

BIG-IP implements a hierarchy of roles that are pre-defined to grant administrators varying degrees of control over the basic configuration of the TOE, and additional roles are introduced for module-specific tasks. These roles can be assigned to users by authorized administrators.

In addition to roles, the TOE allows the definition of partitions. Configuration objects, such as server pools or service profiles, can be assigned to individual partitions, as can administrative users. This allows administrative access of individual administrators to be restricted to configuration objects that belong to the partition that has been assigned to the user.

3.5 Protection of the TSF

The TOE is designed to protect critical security data, including keys and passwords. In addition, the TOE includes self-tests that monitor continue operation of the TOE to ensure that it is operating correctly. The TOE also provides a mechanism to provide trusted updates to the TOE firmware or software and reliable timestamps in order to support TOE functions, including accurate audit recording. Time is provided by a local real-time clock managed by either the Security Administrator setting the time or synchronizing with an NTP server

3.6 TOE Access

The TOE implements session inactivity time-outs for Configuration utility and tmsh sessions and displays a warning banner before establishing an interactive session between a human user and the TOE.

3.7 Trusted Path / Channels

This chapter in the [ST] summarizes the security functionality provided by the TOE in order to protect the confidentiality and integrity of network connections described below.

Generic network traffic

The BIG-IP allows the termination of data plane TLS connections on behalf of internal servers or server pools. External clients can thus connect via TLS to the TOE, which acts as a TLS server and decrypts the traffic and then forwards it to internal servers for processing of the content. It is also possible to (re-) encrypt traffic from the TOE to servers in the organization with TLS, with the TOE acting as a TLS client.

Administrative traffic

The TOE secures administrative traffic (i.e., administrators connecting to the TOE in order to configure and maintain it) as follows:

• Remote access to the traffic management shell (tmsh) is secured via SSH.

• Remote access to the web-based Configuration utility, iControl REST API, and iControl API is secured via TLS.

OpenSSH

The TOE SSH implementation is based on OpenSSH; however, the TOE OpenSSH configuration sets the implementation via the sshd_config as follows:

• Supports two types of authentication, RSA public-key and password-based

• Packets greater than (256*1024) bytes are dropped

• The transport encryption algorithms are limited to AES-CBC-128, AES-CBC-256, AES-CTR-128, AES-CTR-256

• The SSH public-key authentication algorithms are limited to ecdsa-sha2-nistp256 and ecdsa-sha2- nistp384

• The transport data integrity algorithm is limited to HMAC-SHA2-256

• The SSH protocol key exchange mechanism is limited to ecdh-sha2-nistp256 and ecdh-sha2- nistp384.

Remote logging

The TOE offers the establishment of TLS sessions with external log hosts in the operational environment for protection of audit records in transfer.

3.8 User Data Protection

The TOE implements certificate profiles for TLS server certificates issued by the CA embedded in the TOE and issues certificates as specified by these profiles. The TOE is also capable of providing a method to link the TLS server certificates validated by the TOE to the forged certificate issued by the TOE to represent that server. The TOE performs TLS plaintext processing policies when the policy authorizes inspection processing. Residual information contained in TLS buffers is not available upon allocation of the resource. Trusted public keys and certificates used in SSLO are protected.

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

The Security Target [ST] makes seven assumptions on the usage and 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 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).

If a virtual TOE evaluated as a pND, following Case 2 vNDs as specified in Section 1.2, the VS is considered part of the TOE with only one vND instance for each physical hardware platform. The exception being where components of a distributed TOE run inside more than one virtual machine (VM) on a single VS. In Case 2 vND, no non-TOE guest VMs are allowed on the platform.

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

A.NO_THRU_TRAFFIC_PROTECTION

A 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 PP-Modules 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).

4.2 Clarification of Scope

The Security Target contains sixteen 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 tunnelling 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 includes replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the Administrator or device credentials for use by the attacker. Threat agents may also be able to take advantage of weak administrative passwords to gain privileged access to the device.

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 Policy (OSP), 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 Administrators 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

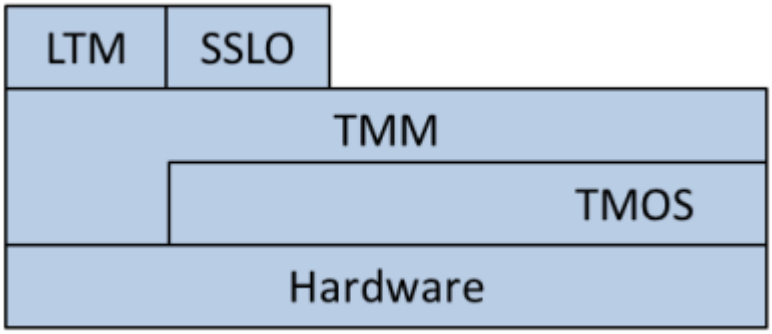
5 Architectural Information

The 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.

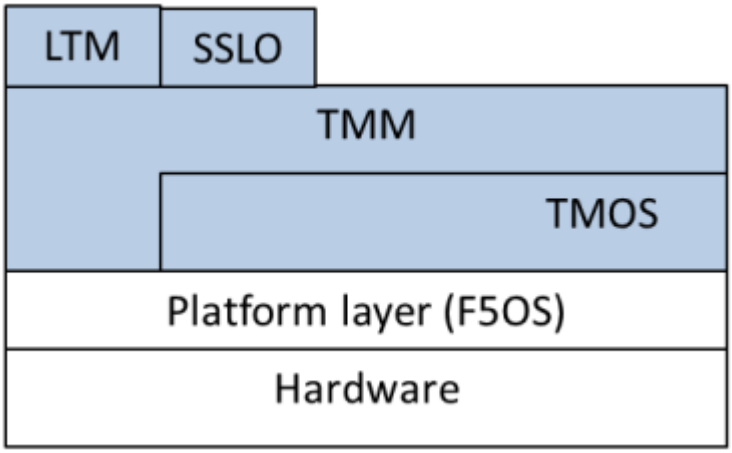
The data plane passes user traffic through the TOE. The TOE implements and supports the following network protocols: TLS (client and server), SSH, HTTPS, FTP. The TOE protects remote connections to its management interfaces with TLS and SSH. The TOE also protects communication channels with audit servers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

The TOE is divided into the following subsystems:

- F5 Device Hardware,
- F5 platform layer for rSeries or VELOS devices,
- Traffic Management Operating System (TMOS),
- Traffic Management Micro-kernel (TMM),
- SSL Orchestrator (SSLO), and
- Local Traffic Manager (LTM).



BIG-IP Subsystems for F5 iSeries and VIPRION Devices in Application Delivery Controller Deployments



BIG-IP Subsystems for F5 rSeries and VELOS Devices in Application Delivery Controller Deployments

6 Documentation

[ECG] BIG-IP Common Criteria Evaluation Configuration Guide BIG-IP Release 17.5.0 Including SSLO

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

The TOE documentation is collected in an ISO file that can be downloaded via https from the F5 website.

7 IT Product Testing

7.1 Evaluator Testing

The evaluator has conducted testing on the BIG-IP running version 17.5.0 on the TOE running on hardware appliance (i15820), on the TOE's running on hardware appliance with platform layer (r10920, r12900, VELOS). For [CPP_ND_V3.0E], the TOE running on VMWare ESXi Hypervisor (VMWare) was also tested. All models were fully tested. The evaluator testing of the TOE was performed between January 2026 and February 2026. The cryptographic algorithm testing is covered by Cryptographic Algorithm Validation System (CAVS), and the Cryptographic Algorithm Validation Program (CAVP) certificates.

Algorithm test vectors were generated by ACVT tool to test all cryptographic algorithms of the TOE. The testing is valid for all hardware appliance and hypervisors supported by the TOE, which is evident from the certificates: KVM, VMWare and Hyper-V.

7.2 Penetration Testing

In addition to the testing as mandated by the Protection Profile(s), i.e. the Fuzz testing and ROBOT tests, the evaluator performed a port scan. The scan was performed to mitigate the risk of undocumented or unexpected open ports in the default coniguration.

The evaluator found the following TCP ports open. All of these ports are expected to be open.

- 22/tcp: ssh: OpenSSH 7.4 (protocol 2.0)
- 161/tcp: snmp
- 443/tcp: ssl/http: Apache httpd
- 4433/tcp: ssl/ssl: Apache httpd (SSL-only mode)
- 4353/tcp: ssl/f5-iquery

The port scanning results do not indicate any certainly-open UDP ports. Therefore the port scanning did not reveal any potential flaws in the TOE. The evaluator determined the TOE in its operational environment is resistant to an attacker who possesses a Basic attack potential.

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 Management2 capabilities of the system is disabled.
  - TLS v1.1 (for non-SSLO functions)
- 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 evaluators also applied all assurance activities implied by the collaborative PP [NDcPP], [STIP-PPM] and [SSH_PKG].

The certifier reviewed the work of the evaluators and determined that the evaluation was conducted in accordance with the Common Criteria [CC] and the evaluation activities implied by the collaborative PP [NDcPP] and [STIP-PPM].

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
Security Target Evaluation		ASE	PASS
	ST Introducation	ASE_INT.1	PASS
	Conformance Claims	ASE_CCL.1	PASS
	Security Objectives	ASE_OBJ.1	PASS
	Extended Components Definition	ASE_ECD.1	PASS
	Security Requirements	ASE_REQ.1	PASS
	Security Problem Definition	ASE_SPD.1	PASS
	TOE Summary Specification	ASE_TSS.1	PASS
		ASE_NDCPP.1	PASS
		ASE_STIPPPM.1	PASS
		ASE_SSHPKG.1	PASS
Development		ADV	PASS
	Functional Specification	ADV_FSP.1	PASS
		ADV_NDCPP.1	PASS
Guidance documents		AGD	PASS
	Operational user guidance	AGD_OPE.1	PASS
	Preparative procedures	AGD_PRE.1	PASS
		AGD_NDCPP.1	PASS
		AGD_STIPPPM.1	PASS
		AGD_SSHPKG.1	PASS
Life-Cycle Support		ALC	PASS
	CM Capabilities	ALC_CMC.1	PASS
	CM Scope	ALC_CMS.1	PASS
Tests		ATE	PASS
	Independent Testing	ATE_IND.1	PASS

	ATE_NDCPP.1	PASS
	ATE_STIPPPM.1	PASS
	ATE_SSHPKG.1	PASS
Vulnerability Assessment	AVA	PASS
Vulnerability Analasis	AVA_VAN.1	PASS
	AVA_NDCPP.1	PASS

10 Evaluator Comments and Recommendations

None.

11 Glossary

CC	Common Criteria
CEM	Common Evaluation Methodology
LTM	Local Traffic Manager
PP	Protection Profile
SSH	Secure Shell
ST	Security Target
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TSF Interface

12 Bibliography

ST	F5 BIG-IP® including SSLO Security Target, F5 Inc., 2026-xx-xx, Document version 17.xx
CPP_ND_V3.0e	collaborative Protection Profile for Network Devices Version 3.0e 2023-12-06
MOD_STIP_V1.1	PP-Module for SSL/TLS Inspection Proxy Version 1.1 2022-11-17
PKG_SSH_V1.0	Functional Package for SSH Version 1.0, NIAP, 2021-05-13
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
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
2.6.1	2025-10-16	None
2.6	2025-03-27	None
2.5.2	Application	Original version

A.2 Scheme Notes

The following Scheme Notes have been considered during the evaluation:

- Scheme Note 15 – Testing
- Scheme Note 18 – Highlighted Requirements on the Security Target
- 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
- Scheme Note 27 – ST Requirements at the Time of Application for Certification
- Scheme Note 28 – Updated procedures for application, evaluation and Certification
- Scheme Note 31 – New procedures for site visit oversight and testing oversight