Swedish Certification Body for IT Security

Certification Report - F5 BIG-IP v15.1.2.1 including AFM

Issue: 1.0, 2021-Dec-15

Authorisation: Jerry Johansson, Lead Certifier , CSEC

Table of Contents

1 Executive Summary

The Target of Evaluation (TOE) is a firewall networking device, comprised of hardware and software. The TOE provides network traffic management functionality, e.g. local traffic management and access policy management. The TOE consists of the software version 15.1.2.1 including AFM with engineering hotfix 15.1.2.1.0.375.10, 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
- B2250
- C2400
- B4450
- C4480
- 10350V-F

or installed on an F5 Virtual Clustered Multiprocessing (vCMP) environment running on one 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
- B2250
- C2400
- B4450
- C4480
- 10350V-F

TOE is also available for the following hypervisors

- VMWare ESXi 6.5.0
- Hyper-V 10.0
- KVM on CentOS 7

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 Stateful Traffic Filter Firewalls, v1.4e [CFG], which combines the collaborative Protection Profile for Network Devices, v2.2e [NDcPP], and the PP-Module for Stateful Traffic Filter Firewalls, v1.4e [FWMOD].

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 thirteen threats and comply with the one 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 2021-12-09. 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. The evaluation meets the requirements of evaluation assurance level EAL 1, augmented by ASE_SPD.1 Security Problem Definition, and the Evaluation Activities for the Collaborative Protection Profile for Network Devices [EAPP], and the PP-Module for Stateful Traffic Filter Firewalls [EAMOD].

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], and have been reached in agreement with the requirements of the Common Criteria and the Common Methodology for evaluation assurance level:

EAL 1 + ASE_SPD.1 and in accordance with the Evaluation Activities for the Collaborative Protection Profile for Network Devices [EAPP], and the PP-Module for Stateful Traffic Filter Firewalls [EAMOD].

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

2 Identification

Certification Identification	
Certification ID	CSEC2020017
Name and version of the certified IT product	F5 BIG-IP v15.1.2.1 including AFM with engineering hotfix 15.1.2.1.0.375.10
Security Target Identification	F5 BIG-IP® 15.1.2.1 including AFM Security Target, F5 Inc., 2021-12-08, document version 5.8
EAL	EAL 1 + ASE_SPD.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	2.0
Scheme Notes Release	18.0
Recognition Scope	CCRA
Certification date	2021-12-15

3 Security Policy

The TOE provides the following security services:

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

3.1 Security Audit

BIG-IP implements syslog capabilities to generate audit records for security-relevant 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 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. These cryptographic implementations utilize the cryptographic module which provides random number generation, key generation, key establishment, key storage, key destruction, hash operations, encryption/decryption operations, and digital signature operations.

3.3 User Data Protection

BIG-IP implements residual information protection on network packets traversing through it. In other words, network packets traversing through the BIG-IP do not contain any residual data.

3.4 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.

3.5 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.

3.6 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.

3.7 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.

3.8 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.

3.9 Firewall

The TOE offers basic firewall functionality, including stateful packet inspection and network address translation, and logic to mitigate denial-of-service attacks.

4 Assumptions and Clarification of Scope

4.1 Assumptions on the Usage and the Environment

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.

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 PP-Modules for particular types of Network Devices (e.g., firewall).

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).

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.

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 thirteen 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 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.NETWORK_DISCLOSURE

An attacker may attempt to "map" a subnet to determine the machines that reside on the network, and obtaining the IP addresses of machines, as well as the services (ports) those machines are offering. This information could be used to mount attacks to those machines via the services that are exported.

T.NETWORK_ACCESS

With knowledge of the services that are exported by machines on a subnet, an attacker may attempt to exploit those services by mounting attacks against those services.

T.NETWORK_MISUSE

An attacker may attempt to use services that are exported by machines in a way that is unintended by a site's security policies. For example, an attacker might be able to use a service to "anonymize" the attacker's machine as they mount attacks against others.

T. MALICIOUS_TRAFFIC

An attacker may attempt to send malformed packets to a machine in hopes of causing the network stack or services listening on UDP/TCP ports of the target machine to crash.

The Security Target contains one Organisational Security Policy (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.

5 Architectural Information

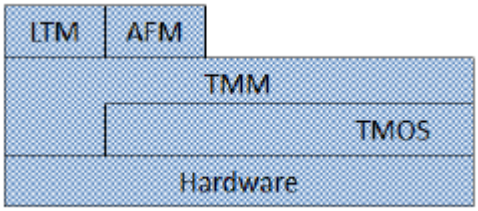
The TOE is separated into two distinct planes, the control plane and the data plane. The control plane validates, stores, and passes configuration data to all necessary systems. It also provides all administrative access to the TOE. The data plane passes user traffic through the TOE.

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.

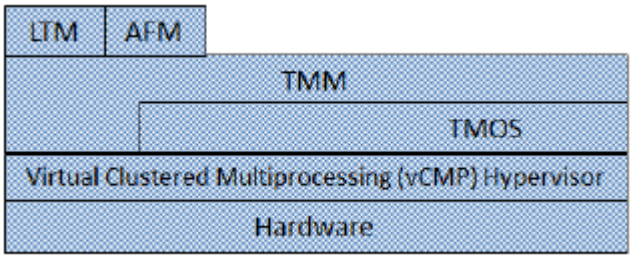
The TOE is divided into the following subsystems:

- F5 Device (hardware or virtual) for F5 devices or vCMP deployments,
- Hardware for hypervisor deployments,
- Hypervisor for hypervisor deployments,
- Traffic Management Operating System (TMOS),
- Traffic Management Micro-kernel (TMM),
- Advanced Firewall Manager (AFM), and
- Local Traffic Manager (LTM).

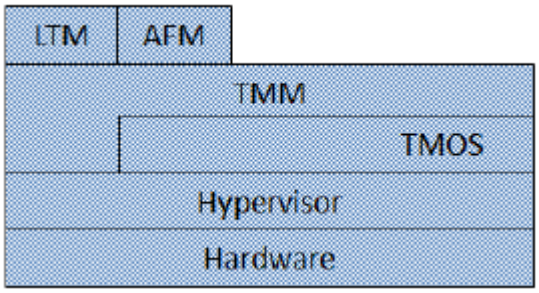
BIG-IP running on a hardware appliance:



BIG-IP running on vCMP:



BIG-IP running on third party hypervisor:



F5'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 AFM implements stateful traffic filtering on Level 3 and Level 4 network traffic packets using administrator-defined packet-filtering rules that are based on network packet attributes.

TMOS is a Linux operating system that runs directly on device hardware, in a vCMP environment, or directly on the supported hypervisor. TMOS is a modified version of the RedHat Linux kernel. In addition to providing the standard operating system features (such as process management, file management, etc), the TMOS provides the following security features for the TOE:

- Auditing functionality, using the host system's syslog capabilities. (In addition, a concept called "high-speed logging" (HSL) allows TMM instances to send certain log traffic directly to external audit servers.)
- Time stamping
- Management functionality, presented to consumers via a dedicated shell providing a command line interface (traffic management shell, "tmsh") that can be reached by administrators via SSH (OpenSSH); and via a web GUI ("Configuration Utility"), a SOAP protocol interface ("iControl API"), or REST interface ("iControl REST API") that can be reached through a network interface via HTTPS. Those management interfaces are implemented in the background by a central management control program daemon (mcpd) that provides configuration information to individual TOE parts and coordinates its persistent storage.
- Authentication functionality is enforced on all administrative interfaces. Administrative interfaces implement an internal password-based repository for authentication of administrative users.
- Cryptographic algorithms provided by OpenSSL.
- Individual daemons introduced by BIG-IP packages, such as the modules implementing the LTM and AFM logic.

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 multi-threaded (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 pack-ages. 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 the Application Delivery Controller Deployments include:

- Local Traffic Manager (LTM) only for Application Delivery Firewall deployments: authentication of HTTP (based on Apache) traffic and advanced traffic forwarding directives
- Advanced Firewall Manager (AFM): network filtering as described in [FWMOD].

6 Documentation

The main guide to installing the TOE into the evaluated configuration is:

[ECG] BIG-IP® Common Criteria Evaluation Configuration Guide BIG-IP® Release 15.1.2.1

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 cryptographic testing was performed within the Cryptographic Algorithm Validation Program (CAVP). The CAVP certificates covers all TOE hardware appliances, with and without vCMP, and the following third party hypervisor configurations:

• VMWare ESXi 6.5.0 on Intel Xeon E5-2690v4 processor

• Hyper-V 10.0 on Windows Server 2019 and Intel Xeon E5-2660v3 processor

• KVM on CentOS 7 and Intel Xeon E5-2690v4 processor

All other tests were performed on the i4800 model, the i5800 model with vCMP, and on VMWare ESXi 6.5.0, with the software version 15.1.2.1. The testing was performed with the APM license instead of the AFM license.

After a software patch, a test sample covering all functionality types was performed on the same TOE models, and with the software build 15.1.2.1.0.375.10.

Additionally, the test cases specific to the PP-Module for Stateful Traffic Filter Firewalls [FWMOD] were performed on an i5800 model with vCMP.

The testing of the version with the hotfix was successful and did not reveal any errors.

7.2 Penetration Testing

Port scanning was performed to find open ports that should not be open. The i4800 model, the i5800 model with vCMP, and on VMWare ESXi 6.5.0, with the software build 15.1.2.1.0.375.10 were tested. The testing was performed with the APM license instead of the AFM license.

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 disabling root access to the TOE operating system, and in disabling the bash shell.
- Certificate validation is performed using CRLs.
- 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. (applicable to F5 devices and vCMP only)
  - 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

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 respective 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 FWMOD		PASS

10 Evaluator Comments and Recommendations

The evaluators do not have any comments or recommendations concerning the product nor regarding its usage.

11 Glossary

ADC	Application Delivery Controller
AFM	Advanced Firewall Manager
APM	Access Policy Manager
CA	Certificate Authority
CC	Common Criteria
CLI	Command Line Interface
CRL	Certificate Revocation List
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
IP	Internet Protocol
IPv4	Internet Protocol version 4
LTM	Local Traffic Manager
NDcPP	Network Device Collaborative Protection Profile
OS	Operating System
PP	Protection Profile
SHA	Secure HashAlgorithm
SSH	Secure Shell
ST	Security Target
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TMM	Traffic Management Microkernel
TMOS	Traffic Management Operating System
tmsh	Traffic management shell
TSF	TOE Security Functions
TSFI	TSF Interface
UDP	User Datagram Protocol
vCMP	Virtual Clustered Multi-Processing

12 Bibliography

ST	F5 BIG-IP® 15.1.2.1 including AFM Security Target, F5 Inc., 2021-12-08, document version 5.8
ECG	BIG-IP® Common Criteria Evaluation Configuration Guide BIG-IP® Release 15.1.2.1, F5 Inc., 2021-09-16, document version 5.18
CFG	PP-Configuration for Network Device and Stateful Traffic Filter Firewalls, 2020-Jun-25, document version 1.4E
FWMOD	PP-Module for Stateful Traffic Filter Firewalls, 2020-Jun-25, document version 1.4E
EAMOD	Evaluation Activities for Stateful Traffic Filter Firewalls PP-Module, ND iTC, Jun 2020, document version 1.4E
NDcPP	Collaborative Protection Profile for Network Devices, ND iTC, 2020-Mar-23, document version 2.2E
EAPP	Evaluation Activities for Network Device cPP, ND iTC, Dec 2019, 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

Appendix A Scheme Documentation and Versions

A.1 Quality Management System

During the certification project, the following versions of the quality management system (QMS) have been applicable since the certification application was registered 2020-06-23:

QMS 1.23.2	valid from 2020-05-11
QMS 1.24	valid from 2020-11-19
QMS 1.24.1	valid from 2020-12-03
QMS 1.25	valid from 2021-06-17
QMS 2.0	valid from 2021-11-24

In order to ensure consistency in the outcome of the certification, the certifier has examined the changes introduced in each update of the quality management sys-tem.

The changes between consecutive versions are outlined in “Ändringslista CSEC QMS 2.0”.

The certifier concluded that, from QMS 1.23.2 to the current QMS 2.0, there are no changes with impact on the result of the certification.

A.2 Applicable Scheme Notes

SN-15 Testing

SN-18 Highlighted requirements on the ST

SN-22 Vulnerability assessment

SN-23 Evaluation reports for NIAP PPs and cPPs

SN-25 CAVP-tests in evaluations