Swedish Certification Body for IT Security

Certification Report - F5 BIG-IP v13.1.1 NDcPP

Issue: 2.0, 2019-aug-12

Report Distribution: Arkiv

Table of Contents

1 Executive Summary

The Target of Evaluation (TOE) is a 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 13.1.1 LTM+APM (build 13.1.1-0.0.4) with engineering hotfix 13.1.1.0.100.4-ENG installed on any of the following hardware appliances;

- i5000 model series, including i5600, i5800 and i5820-DF
- i7000 model series including i7600, i7800 and i7820-DF
- i10000 model series, including i10600, i10800
- 10000 model series, including 10350v-F
- i11000-DS model series, including i11800-DS
- i15000 model series, including i15800
- B2250 model series, including B2250
- B4450N model series including B4450N
- C2400 model series including C2400-AC
- C4480 model series including C4480-AC

or installed on F5 Virtual Clustered Multiprocessing (vCMP) environment running on any of the appliances listed above.

The TOE hardware is delivered via trusted couriers, while the software is delivered as a downloadable ISO image from the F5 website.

The ST claims exact conformance to the Collaborative Protection Profile for Network Devices (NDcPP), version 2.0 + Errata 20180314.

The NIT technical decisions that have been applied to the Network Device Collaborative Protection Profile can be found in the ST.

There are seven assumptions being made in the ST regarding the secure usage and environment of the TOE. The TOE relies on these to counter the nine threats and comply with the one organisational security policy (OSP) in the ST. The assumptions, the threat 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 2019-Jun-04. 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 NDcPP Evaluation Activities..

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 NDcPP Evaluation Activities.

The certification results only apply to the versions of the products indicated in the certificate, and on the condition that all the stipulations in the Security Target [ST] are met.

This certificate is not an endorsement of the IT product by CSEC or any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by CSEC or any other organization that recognizes or gives effect

2 Identification

Certification Identification

Certification ID	CSEC2017021
Name and version of the certified IT product	F5 BIG-IP v13 LTM + APM with software version 13.1.1 LTM+APM (build 13.1.1-0.0.4) and the engineering hotfix 13.1.1.0.100.4-ENG, running on any of the following appliances or on the hypervisor vCMP, installed on any of the following appliances: i5600, i5800, i5820-DF, i7600, i7800, i7820-DF, i10600, i10800, 10350v-F, i11800-DS, i15800, B2250, B4450N, C2400-AC, and C4480-AC
Security Target	BIG-IP Version 13.1.1 LTM+APM Security Target
Assurance level	EAL 1 + ASE_SPD.1 and NDcPP v2.0+Errata 20180314
Sponsor	F5 Networks Inc.
Developer	F5 Networks Inc.
ITSEF	atsec information security AB
Common Criteria version	3.1 release 5
CEM version	3.1 release 5
Certification date	2019-06-19

3 Security Policy

The TOE provides the following security services:

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

3.1 Security Audit

The TOE 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

The TOE provides cryptographic functionality is provided by the OpenSSL cryptographic module. The TOE provides a secure shell (SSH) to allow administrators to connect over a dedicated network interface. The TOE also implements the TLS protocol to allow administrators to remotely manage the TOE. The TOE 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 Identification and Authentication

An internal password-based repository is implemented for authentication of management users. The TOE 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.

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.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 computing platform for general purpose applications (unrelated to networking functionality).

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 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.

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.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.

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.

4.2 Organizational Security Policies

The Security Target [ST] places one Organizational Security Policy on the TOE.

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.

4.3 Clarification of Scope

The Security Target [ST] contains nine threats, which have been considered during the evaluation.

T.UNATHORIZED_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

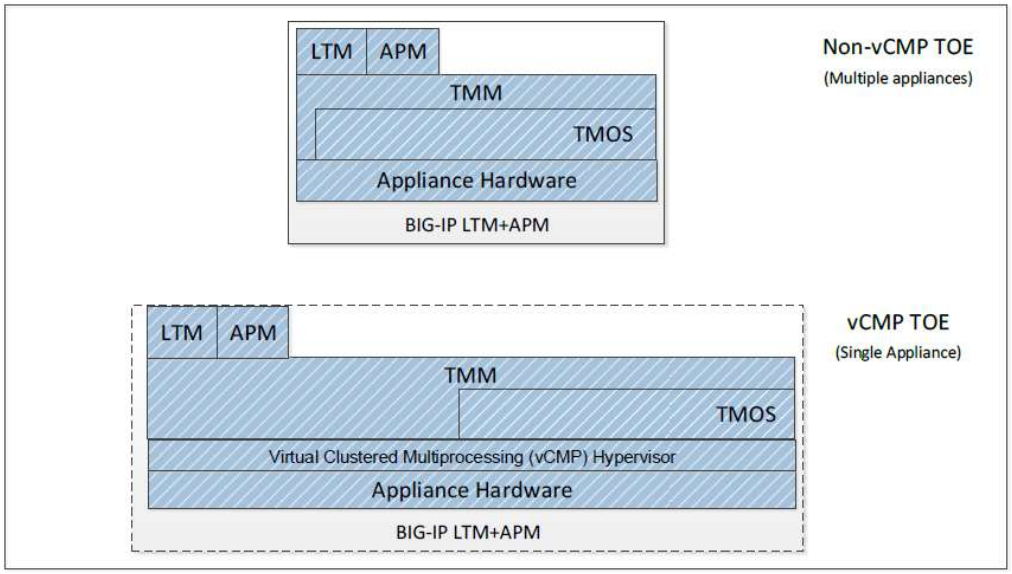
Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic, and may allow them to take advantage of any trust relationships with other network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

T.SECURITY_FUNCTIONALITY_FAILURE

A component of the network device may fail during start-up or during operations causing a compromise or failure in the security functionality of the network device, leaving the device susceptible to attackers.

5 Architectural Information

The following diagram shows the basic components that comprise the TOE:



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 five (5) subsystems: Appliance (hardware or virtual), Traffic Management Operating System (TMOS), Traffic Management Micro-kernel (TMM), Local Traffic Manager (LTM), and Access Policy Manager (APM). F5's TMOS is a Linux-based operating system customized for performance and to execute on the TOE appliance hardware or in the TOE Virtual Clustered Multiprocessing (vCMP) environment. The vCMP is a 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.

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. 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 provides more than one CPU, TMM runs multi-threaded (one thread per CPU). In this case, disaggregators implemented in hardware or, depending on the underlying appliance, firmware, 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 shown in figure above include:

- Local Traffic Manager (LTM): authentication of HTTP (based on Apache 2.2.15) traffic and advanced traffic forwarding directives
- Access Policy Manager (APM): TLS-based client connectivity.

6 Documentation

For proper configuration of the TOE into the evaluated configuration, the following guidance documents are available:

- BIG-IP® Common Criteria Evaluation Configuration Guide BIG-IP® LTM+AFM and BIG-IP® LTM+APM Release 13.1.1 [ECG]
- BIG-IP System: Digital Certificates: Administration
- BIG-IP System: Essentials
- BIG-IP System: SSL Administration
- BIG-IP System: User Account Administration
- BIG-IP Systems: Getting Started Guide
- BIG-IP Local Traffic Management: Monitors Reference
- BIG-IP Local Traffic Management: Profiles Reference
- BIG-IP Local Traffic Manager: Implementations
- BIG-IP Network Firewall: Policies and Implementations
- BIG-IP TMOS: Implementations
- BIG-IP TMOS: Routing Administration
- External Monitoring of BIG-IP Systems: Implementations
- iControl Guidance Documentation (available on-line)
- iControl REST API User Guide
- Traffic Management Shell (tmsh) Reference Guide
- Platform Guide: i5000/i7000/i10000 Series
- Platform Guide: 10000 Series
- Platform Guide: i15000 Series
- Platform Guide: VIPRION® 2200 Series
- Platform Guide: VIPRION® 4400 Series
- vCMP for Appliance Models: Administration
- vCMP for VIPRION Systems: Administration
- K80425458: Modifying the list of ciphers and MAC algorithms used by the SSH service on the BIG-IP system or BIG-IQ system
- K52343814: Common Criteria Certification for BIG-IP 13.1.1
- K12042624: Restricting access to the Configuration utility using client certificates
- K13092: Overview of securing access the BIG-IP system
- K13302: Configuring the BIG-IP system to use an SSL chain certificate
- K13454: Configuring SSH host-based authentication on BIP-IP systems
- K14620: Managing SSL Certificates for BIG-IP systems using the Configuration utility
- K14783: Overview of the Client SSL profile

- K14806: Overview of the Server SSL profile
- K15497: Configuring a secure password policy for the BIG-IP system
- K15664: Overview of BIG-IP device certificates
- K42531434: Replacing the Configuration utility's self-signed SSL certificate with A CA-signed SSL certificate
- K5532: Configuring the level of information logged for TMM-specific events
- K6068: Configuring a pre-login or post-login message banner for the BIG-IP or Enterprise Manager system
- K7683: Connecting a serial terminal to a BIG-IP system
- K7752: Licensing the BIG-IP system
- K9908: Configuring an automatic logout for idle sessions

7 IT Product Testing

7.1 Independent Evaluator Testing

The cryptographic algorithm testing was performed on ten TOE models running on hardware appliances and two TOE models running on top of vCMP, covering the different CPUs. For each of these models, two crypto modules were tested. The algorithm tests were performed using the CAVS framework - in all 24 sets of CAVS certificates were issued.

Most of the remaining independent tests were performed on the i11800 appliance, complemented by tests on the i5800 appliance. A subset of these tests, selected to cover different functionality, was tested using vCMP on the B2250 appliance. The testing was performed between August and November 2018.

The results of all test cases were consistent with the expected test results, and all tests were judged to pass.

7.2 Evaluator Penetration Testing

A port scan was performed on a TOE running on an i5800 appliance. No unexpected open ports were discovered.

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 to 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.
- Remote (i.e. SSH) access to the Lights Out/Always On Management capabilities of the system is disabled.
- SSH client

Cryptographic acceleration is always used in the evaluated configuration, in particular, during testing of the cryptographic mechanisms.

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

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
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	BIG-IP Version 13.1.1 LTM+APM Security Target, F5 Networks Inc. 2019-07-16, document version 0.20
ECG	BIG-IP® Common Criteria Evaluation Configuration Guide BIG-IP® LTM+AFM and BIG-IP® LTM+APM Release 13.1.1, F5 Networks Inc., 2019-02-07, document version 3.26
NDcPP	Collaborative Protection Profile for Network Devices, 2018-03-14, document version 2.0E (v2.0 + Errata 20180314)
EA	Evaluation Activities for Network Device cPP, 2018-03-14, document version 2.0E (v2.0 + Errata 20180314)
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
SP-002	SP-002 Evaluation and Certification, CSEC, 2019-01-21, document version 30.0
SP-188	SP-188 Scheme Crypto Policy, CSEC, 2018-01-16, document version 8.0

Appendix A QMS Consistency

During the certification project, the following versions of the quality management system (QMS) have been applicable since the certification application was registered 2017-11-17:

QMS 1.21	valid from 2017-11-15
QMS 1.21.1	valid from 2018-03-09
QMS 1.21.2	valid from 2018-03-09 SIC!
QMS 1.21.3	valid from 2018-05-24
QMS 1.21.4	valid from 2018-09-13
QMS 1.21.5	valid from 2018-11-19
QMS 1.22	valid from 2019-02-01
QMS 1.22.1	valid from 2019-03-08
QMS 1.22.2	valid from 2019-05-02
QMS 1.22.3	valid from 2019-05-20

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 system.

The changes between consecutive versions are outlined in “Ändringslista CSEC QMS 1.22.3”.

The certifier concluded that, from QMS 1.21 to the current QMS 1.22.3, there are no changes with impact on the result of the certification.