**Swedish Certification Body for IT Security**

# Certification Report - F5 BIG-IP 12.1.3.4 FWcPP

**Issue: 2.0, 2019-feb-03**

*Authorisation: Imre Juhász, Lead Certifier , CSEC*

SWEDAC ACKREDITERING
Accred. no. 1917
Certification of
Products
ISO/IEC 17065

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 and firewall functionality, e.g. local traffic management, access policy management and access firewall management. The TOE consists of the software version 12.1.3.4 LT+AFM installed on any of the following hardware appliances;

- i5000 model series, including i5600 and i5800,
- i7000 model series including i7600 and i7800,
- B2250 model series, including B2250,
- B4450N model series including B4450N,
- 10000 model series, including 10350v-F,

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

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

The Security Target claims exact conformance to Collaborative Protection Profile for Stateful Traffic Filter Firewalls (FWcPP) v1.0.

There are five assumptions being made in the ST regarding the secure usage and environment of the TOE. The TOE relies on these to counter the thirteen threats and comply with the single organisational security policy (OSP) in the ST. The assumptions, threats and the OSP are described in chapter 4 Assumptions and Clarification of Scope.

The evaluation has been performed by atsec information security AB in their premises in Danderyd, Sweden, and in their foreign location in Austin, USA.

The evaluation was completed 2018-11-07. The evaluation was conducted in accordance with the requirements of Common Criteria (CC), 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 according to ISO/IEC 17025 for Common Criteria.

The certifier monitored the activities of the evaluator by reviewing all successive versions of the evaluation reports. The certifier determined that the evaluation results confirm the security claims in Evaluation Activities for Network Device cPP v1.0, and the Security Target (ST). The certifier has also determined that the requirements of EAL 1 augmented by ASE_SPD have been met.

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

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

# 2 Identification

| Certification Identification | |
|---|---|
| Certification ID | CSEC2017004 |
| Name and version of the certified IT product | F5 BIG-IP 12.1.3.4 LT+AFM installed on the following hardware models:<br>- i5000<br>- i7000<br>- B2250<br>- B4450N,<br>- 10000<br>- vCMP (running on the above stated hardware) |
| Security Target Identification | F5 BIG-IP 12.1.3.4 for LTM+AFM Security Target, F5 Networks, Inc., 2019-01-15, version 1.3 |
| EAL | Evaluation Activities for Network Device cPP v1.0 |
| 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 |
| QMS version | 1.21.4 |
| Recognition Scope | CCRA |
| Certification date | 2018-12-07 |

# 3 Security Policy

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

## 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 oldest 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 Traffic Management Operating System (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.

The TOE utilizes NIST recommended algorithms cryptographic algorithms that have been validated through the NIST Cryptographic Algorithm Validation Program. The CAVP certificate numbers can be found in the ST.

## 3.3 Identification and Authentication

*Administrators*

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.

*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
- traffic management shell (tmsh)
- iControl API
- iControl REST API

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.

## 3.4 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.

## 3.5 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.

## 3.6 Trusted Path/Channels

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

*1.6.4.7.1 Generic network traffic*

BIG-IP Version 12.1.3.4 LTM+AFM's LTM 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 Version OpenSSH_5.3p1; 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 and AES-CBC-256
- The transport mechanism is limited to SSH_RSA public key authentication
- The transport data integrity algorithm is limited to HMAC-SHA1, HMAC-SHA2-256, and HMAC-SHA2-512
- The SSH protocol key exchange mechanism is limited to diffie-hellman-group14-sha1, ecdhsha2-nistp256, ecdh-sha2-nistp384, and ecdh-sha2-nistp521

*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.

## 3.7 Firewall

BIG-IP Version 12.1.3.4 LTM+AFM implements a full-featured stateful firewall for Level 3 / Level 4 network traffic, exceeding the requirements of the FWcPP.

Administrators can define packet filtering rules based on network packet attributes, such as the origin and destination IP addresses, ports, sequence number, code, etc. BIG-IP will only permit traffic to reach its intended destination if it matches such a rule, and does not violate certain other protocol characteristics that generally are considered to represent malicious traffic (such as IP packets specifying the Loose Source Routing option).

BIG-IP takes the state of stateful protocols into account when enforcing firewall rules. For example, TCP traffic will only be permitted if the TCP session was properly established and the initial packets match a firewall rule permitting such traffic.

In addition, the TOE implements SYN cookies in order to identify invalid TCP connection attempts and deal with SYN flooding attempts.

BIG-IP is also capable of generating dynamic rule sets for the FTP protocol which requires more than one connection.

# 4 Assumptions and Clarification of Scope

## 4.1 Usage Assumptions

The Security Target [ST] makes three assumptions on the usage 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.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.

## 4.2 Environmental Assumptions

The Security Target [ST] makes two assumptions 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.

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.

## 4.3 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 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. a 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 faiure in the security functionality of the network device, leaving the device susceptible to attackers.

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.

## 4.4 Organisational Security Policy (OSP)

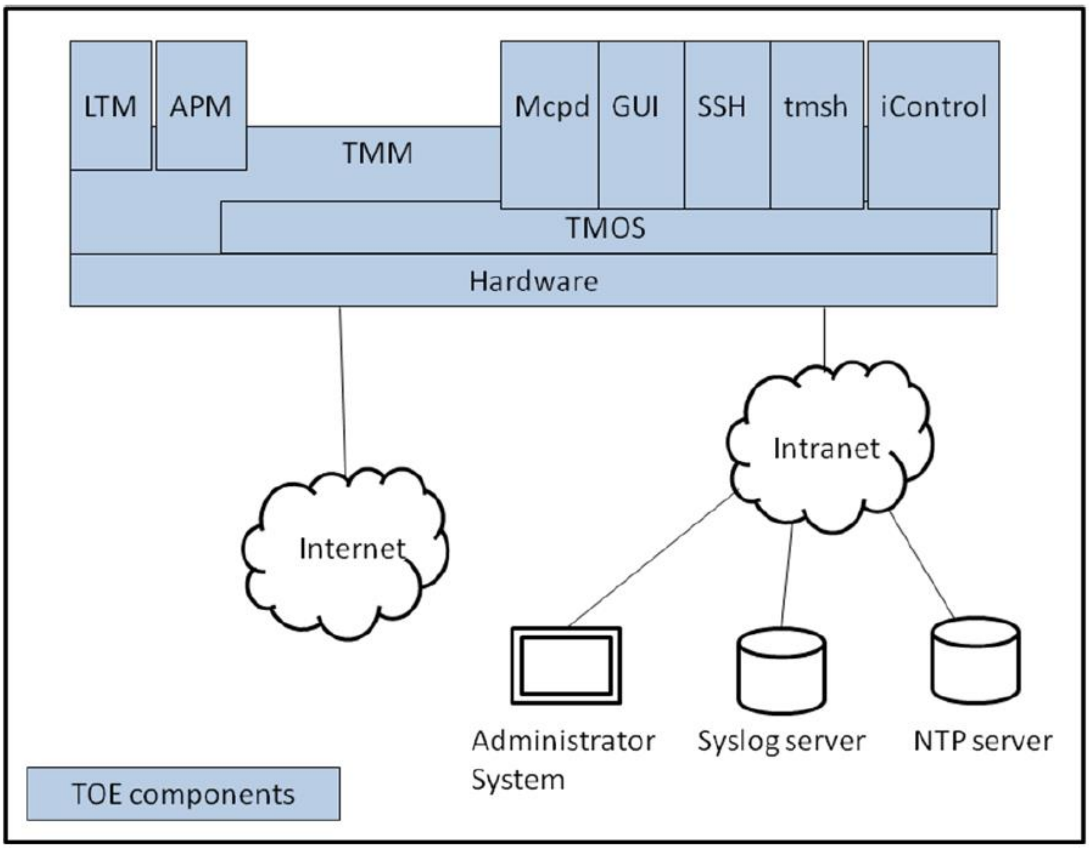
The Security Target contains one Organisational Security Policy, which has been considered during the evaluation.

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 picture below shows the basic components that comprise the TEO.



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 is divided into five (5) subsystems:

- Appliance (hardware or virtual),
- Traffic Management Operating System (TMOS),
- Traffic Management Micro-kernel (TMM),
- Local Traffic Manager (LTM),
- 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, 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.

# 6 Documentation

Relevant guidance documents for the secure set-up and operation of BIG-IP that are part of the TOE are:

- BIG-IP Common Criteria Evaluation Configuration Guide BIG-IP LTM+AFM and BIG-IP LTM+APM Release 12.1.3.4
- K80595439: Common Criteria Certification for BIG-IP 12.1.3.4
- BIG-IP Digital Certificates: Administration
- BIG-IP Local Traffic Manager: Implementations
- BIG-IP Local Traffic Manager: Monitors Reference
- BIG-IP Local Traffic Manager: Profiles Reference
- BIG-IP System: Essentials
- BIG-IP System: SSL Administration
- BIG-IP System: User Account Administration
- BIG-IP Systems: Getting Started Guide
- BIG-IP TMOS: Implementations
- BIG-IP TMOS: Routing Administration
- External Monitoring of BIG-IP Systems: Implementations
- iControl SDK
- iControl REST SDK
- K12042624: Restricting access to the configuration utility using client certificates (12.x – 13.x)
- K13092: Overview of securing access the the BIG-IP system
- K13302: Configuring the BIG-IP system to use an SSL chain certificate (11.x – 13.x)
- K13454: Configuring SSH host-based authentication on BIP-IP systems (11.x – 12.x)
- K14620: Managing SSL Certificates for BIG-IP systems using the Configuration utility
- K14783: Overview of the Client SSL profile (11.x – 13.x)
- K14806: Overview of the Server SSL profile (11.x – 13.x)
- K15497: Configuring a secure password policy for the BIG-IP system (11.x – 12.x)
- K15664: Overview of BIG-IP device certificates (11.x – 13.x)
- 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
- K7752: Licensing the BIG-IP system
- Platform Guide: 10000 Series
- Platform Guide: i5000/i7000/i10000 Series
- Platform Guide: VIPRION® 2200
- Platform Guide: VIPRION® 4400 Series

- Traffic Management Shell (tmsh) Reference

# 7 IT Product Testing

The TOE and the test environment was configured and set-up using the guidance documentation (specified in the ST) and the ST.

## 7.1 Developer Testing

Not applicable, in accordace with FWcPP

## 7.2 Evaluator Testing

The evaluator verified the installation and the configuration of the "BIG-IP 10200F" machine according to the guidance documentations. In addition, an additional unconfigured appliance "BIG-IP i5800" was shipped by the developer to atsec office in Austin, Texas. The evaluator configured the "BIG-IP i5800" machine and installed the BIG-IP 12.1.3.4 Build 0.0.2 remotely according to the guidance documentation. The evaluator verified that both "BIG-IP i5800" and "BIG-IP 10200F" machines were consistent with the ST and that BIG-IP Version 12.1.3.4 LTM+AFM Version 12.1.3.4. was correctly installed.

The algorithm testing is covered by CAVS, and the CAVS certificates are specified in ST.

Depth :

The evaluator has performed tests to ensure that the TOE behaves as specified in the ST and the guidance documentation as well as to perform tests described in FWcPP. All tests have been executed on version 12.1.3.4 HF2. Two types of testing was performed: independent testing and algorithm testing. HW models tested during these two types of testing are:

- Independent testing: one HW model from BIG-IP i5000 and 10000 series
- Algorithm testing: one HW model from each series BIG-IP i5000, i7000, B2250, B4450N, 10000 and vCMP running on 10350v-F.

The evaluator also performed firewall functionality testing as described in FWcPP.

The evaluator confirmed that all test cases passed successfully.

Algorithm testing:

Multiple algorithm testing is required to be performed by FWcPP Supporting Document. Twelve different sets of algorithm test vectors for AES and DRBG were generated by Cryptographic Algorithm Validation System (CAVS) tool version 21.3 to test all hardware family series. Each hardware platforms was tested twice on each platform for AES-NI implementation and AES assembler implementation.

Twelve different sets of algorithm test vectors for SHA, HMAC were generated. Each hardware platform was tested twice for SSSE3 implementation (testing SHA-1 and HMAC-SHA-1) and assembler implementation testing (SHA-1, SHA-256, SHA-384 and HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384).

Six different sets of algorithm test vectors for RSA, ECDSA and KAS ECC were generated for all hardware family series (models tested: i5600, i7800, B2250, B4450N and 10000).

The additional set of algorithms is for vCMP that run on the 10350v-F.

All applicable tests passed successfully.

## 7.3 Penetration Testing

The penetration test was performed on the TOE in the evaluated configuration. The approach for the penetration test was to scan all TCP ports on the TOE platform to identify all open ports. All TCP/IP ports were scanned. The results of the port scan found three open ports as expected.

The evaluator also performed fuzzy testing to generate flaw hypotheses. The following types of fuzzy testing was performed:

- the evaluator created mutated ICMPv4 and ICMPv6
- the evaluator performed fuzzy testing on UDP Header fields
- the evaluator performed fuzzy testing on TCP Header fields

The evaluator did not detect any unexpected TOE behavior.

# 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.
- 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.
  - Serial port console (disabled by policy after the initial power on and communications setup of the hardware)
  - SSH client

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

In the evaluated configuration, the cryptographic acceleration cards are not used for acceleration or key storage. These capabilities that are present on the accelerator cards are disabled in the evaluated configuration.

# 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 performed all evaluation activities for Stateful Traffic Filter Firewalls (FWcPP) v1.0.

The certifier reviewed the work of the evaluator and determined that the evaluation was conducted in accordance with the Common Criteria [CC].

The evaluators overall verdict is PASS.

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

| *Assurance Class/Family* | *Component* | *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 FWcPP | | PASS |

# 10 Evaluator Comments and Recommendations

None

# 11 Glossary

| | |
|---|---|
| ADC | Application Delivery Controller |
| APM | Access Policy Manager |
| CC | Common Criteria |
| CEM | Common Methodology for Information Technology Security, document describing the methodology used in Common Criteria evaluations |
| CPU | Central Processing Unit |
| CRL | Certificate Revocation List |
| CRLDP | Certificate Revocation List Distribution Point |
| cPP | Collaborative Protection Profile |
| FPGA | Field-Programmable Gate Array |
| GUI | Graphical User Interface |
| ITSEF | IT Security Evaluation Facility, test laboratory licensed to operate within a evaluation and certification scheme |
| LTM | Local Traffic Manager |
| NIST | National Institute of Standards and Technology |
| RNG | Random Number Generation |
| SNMP | Simple Network Management Protocol |
| SSH | Secure Shell |
| ST | Security Target, document containing security requirements and specifications , used as the basis of a TOE evaluation |
| TCP | Transmission Control Protocol |
| TOE | Target of Evaluation |
| TLS | Transport Layer Security |
| tmsh | Traffic management shell |
| TMM | Traffic Management Microkernel |
| TMOS | Traffic Management Operating System |
| TSF | TOE Security Functions |
| vCMP | Virtual Clustered Multi-Processing |

# 12 Bibliography

CC Common Criteria for Information Technology Security Evaluation, CCMB-2017-04-001 through 003, document versions 3.1 revision 5

CEM Common Methodology for Information Technology Security Evaluation, CCMB-2017-04-004, document version 3.1 revision 5

ECG BIG-IP® Common Criteria Evaluation Configuration Guide BIG-IP® LTM+AFM and BIG-IP® LTM+APM Release 12.1.3.4, Networks, Inc., version 2.18, 2018-08-19

FWcPP Collaborative Protection Profile for Stateful Traffic Filter Firewalls, NIAP, v1.0, 2015-02-27

FWcPP Supporting Supporting Document Mandatory Technical Document - Evaluation Activities for Stateful Traffic Filter Firewalls cPP, NIAP, v1.0 2015-02-27

ST F5 BIG-IP 12.1.3.4 for LTM+AFM Security Target, F5 Networks, Inc., version 1.3, 2019-01-15

# Appendix A Scheme Versions

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

## A.1 Scheme/Quality Management System

During the certification the following versions of the Swedish Common Criteria Evaluation and Certification scheme has been used:

| Version | Introduced | Impact of changes |
|---|---|---|
| 1.21.5 | 2018-11-15 | *None* |
| 1.21.4 | 2018-09-06 | *None* |
| 1.21.3 | 2018-05-24 | *None* |
| 1.21.2 | 2018-03-09 | *None* |
| 1.21.1 | 2018-03-09 | *None* |
| 1.21 | 2017-11-15 | *None* |
| 1.20.5 | 2017-06-28 | *None* |
| 1.20.4 | 2017-05-11 | *None* |
| 1.20.3 | Application | *Initial version* |

## A.2 Scheme Notes

Scheme Note 15 - Demonstration of test coverage

Scheme Note 18 - Highlighted Requirements on the Security Target

Scheme Note 21 - NIAP PP Certifications