



**Swedish Certification Body for IT Security**

# Certification Report F5 BIG-IP 17.5.0 including AFM

**Issue: 2.0, 2026-feb-23**

*Authorisation: Theodora Arvanitidis, Junoir Certifier , CSEC*

Swedish Certification Body for IT Security  
Certification Report F5 BIG-IP 17.5.0 including AFM

Table of Contents

<b>1</b>	<b>Executive Summary</b>	<b>3</b>
<b>2</b>	<b>Identification</b>	<b>5</b>
<b>3</b>	<b>Security Policy</b>	<b>6</b>
3.1	Security Audit	6
3.2	Cryptographic Support	6
3.3	User Data Protection	7
3.4	Identification and Authentication	7
3.5	Security Management	7
3.6	Protection of the TSF	8
3.7	TOE Access	8
3.8	Trusted Path / Channels	8
3.9	Firewall	9
<b>4</b>	<b>Assumptions and Clarification of Scope</b>	<b>10</b>
4.1	Usage Assumptions	10
4.2	Clarification of Scope	12
<b>5</b>	<b>Architectural Information</b>	<b>14</b>
<b>6</b>	<b>Documentation</b>	<b>16</b>
<b>7</b>	<b>IT Product Testing</b>	<b>17</b>
7.1	Evaluator Testing	17
7.2	Penetration Testing	17
<b>8</b>	<b>Evaluated Configuration</b>	<b>18</b>
<b>9</b>	<b>Results of the Evaluation</b>	<b>19</b>
<b>10</b>	<b>Evaluator Comments and Recommendations</b>	<b>21</b>
<b>11</b>	<b>Glossary</b>	<b>22</b>
<b>12</b>	<b>Bibliography</b>	<b>23</b>
<b>Appendix A</b>	<b>Scheme Versions</b>	<b>24</b>
A.1	Scheme/Quality Management System	24
A.2	Scheme Notes	24

# 1 Executive Summary

The Target of Evaluation (TOE) is a Stateful Traffic Filter Firewall networking device. When running on iSeries and VIPRION devices, the TOE is a physical Network Device. When running on hypervisors or on F5OS on rSeries or VELOS devices, the TOE is a virtual Network Device. The TOE claiming conformance to ST\_1758 is identified as BIG-IP Version 17.5.0 including AFM (Build Hotfix-BIGIP-17.5.0.0.189.15-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 and C2400B
- C2400 with B2250
- C4480 model series, including C4480-AC and C4400B
- 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 R10920-DF
- R12000 model series, including R12600-DS, R12800-DS and R12900-DS
- CX410 model series, including CX410-AC
- BX110 with CX410
- BX520 with CX410 and CX1610

The TOE is also available for the following hypervisors:

- VMWare ESXi 8.0.3 (build 24414501)
- Hyper-V version 10.0.20348.1 on Windows Server 2022 Standard
- KVM: qemu-system-x86 version 1:6.2+dfsg-2ubuntu6.6 on Ubuntu 22.04.2 LTS

The Security Target [ST] claims exact conformance to the following Protection Profile PP-Configuration for Network Device and Stateful Traffic Filder Firewalls, version 2.0 (2024-04-25) (CFG\_NDcPP-FW\_V2.0). 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 twelve 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 twelve 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 2026-02-02, with additional testing 2026-03-02. The evaluation was conducted in accordance with the requirements of Common Criteria, version 3.1, revision 5.

Swedish Certification Body for IT Security  
Certification Report F5 BIG-IP 17.5.0 including AFM

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	CSEC2024027
Name and version of the certified IT product	F5 BIG-IP 17.5.0 including AFM (build Hotfix-BIGIP-17.5.0.0.189.15-ENG)
Security Target Identification	F5 BIG-IP® 17.5 including AFM Security Target, F5, Inc., 2026-March-05, version 17.60
EAL	CFG_NDcPP-FW_V2.0, including NDcPP v3.0e and FWPPM v1.4
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	2026-02-23

---

## 3 Security Policy

The TOE provides the following security services:

- Security Audit
- Cryptographic Support
- User Data Protection
- 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 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.

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. For hypervisors, the TOE provides a total of two 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

### 3.3 User Data Protection

BIG-IP is designed to ensure that it does not reuse old packet information when transmitting new packets through the device.

### 3.4 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.

### 3.5 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.

### 3.6 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.

### 3.7 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.

### 3.8 Trusted Path / Channels

This chapter in [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, aes-128-gcm@openssh.com, and aes-256-gcm@openssh.com
- 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.

### **3.9 Firewall**

The TOE implements a full-featured stateful firewall for filtering Level 3 / Level 4 network traffic, exceeding the requirements of the FWPPM.

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 twelve assumptions on the usage 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.

#### 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).

#### A.NO\_THRU\_TRAFFIC\_PROTECTION

is still operative for FWPPM , but only for the interfaces in the TOE that are defined by the NDcPP and not the FWPPM.

Swedish Certification Body for IT Security  
Certification Report F5 BIG-IP 17.5.0 including AFM

#### 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\_ISOLATION (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 twelve 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.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 Policies (OSPs), which have been considered during the evaluation.

#### P.ACCESS\_BANNER

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

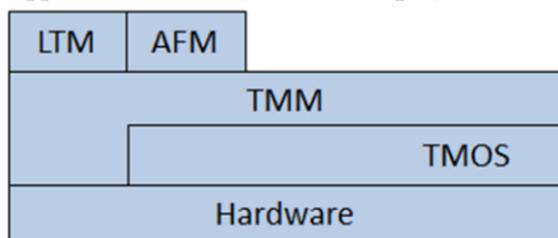
## 5 Architectural Information

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.

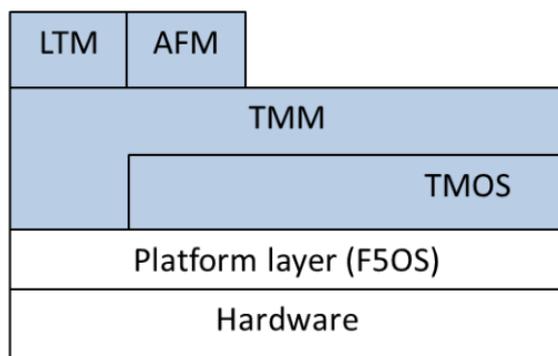
The data plane passes user traffic through the TOE. The TOE implements and supports the following network protocols: TLS (client and server), SSH, HTTPS, FTP. The TOE protects remote connections to its management interfaces with TLS and SSH. The TOE also protects communication channels with audit servers 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 and VELOS devices,
- 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) for Application Delivery Firewall deployments.

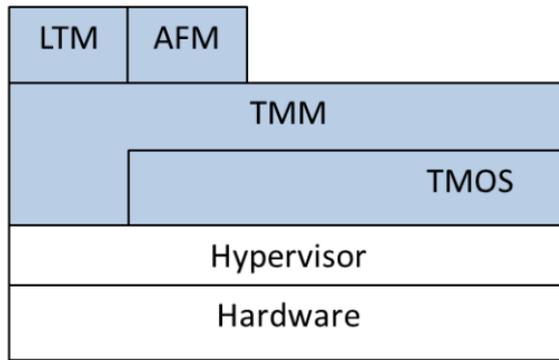


BIG-IP Subsystems for F5 iSeries and VIPRON Devices in Application Delivery Firewall Deployments



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

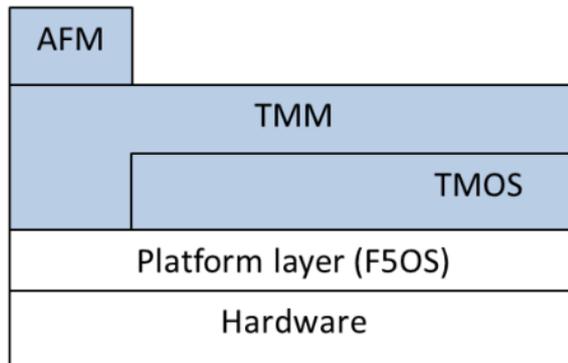
Swedish Certification Body for IT Security  
 Certification Report F5 BIG-IP 17.5.0 including AFM



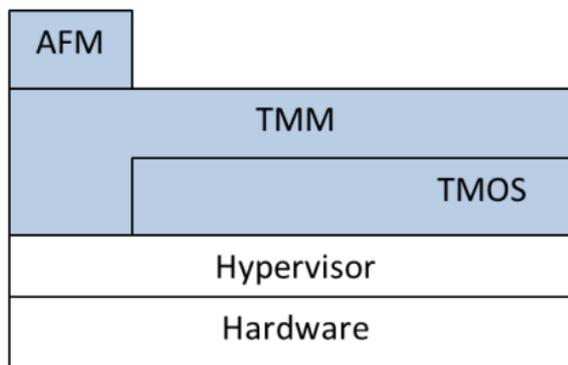
BIG-IP Subsystems for Hypervisors in Application Delivery Firewall Deployments



BIG-IP Subsystems for F5 iSeries and VIPRON Devices in Standalone Advanced Firewall Manager Deployments



BIG-IP Subsystems for F5 rSeries and VELOS Devices in Standalone Advanced Firewall Manager Deployments



BIG-IP Subsystems for Hypervisors in Standalone Advanced Firewall Manager Deployments

## 6 Documentation

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

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 algorithm testing is covered by Cryptographic Algorithm Validation System (CAVS), and the Cryptographic Algorithm Validation Program (CAVP). The CAVS and CAVP certificates covers all TOE hardware appliances, and the following third party hypervisor configurations:

- VMWare ESXi 8.0.3 on Intel® Xeon® Gold 6330N CPU @ 2.20GHz processor
- Hyper-V version 10.0 on Windows Server 2022 and Intel ® Xeon® Silver 4309Y CPU @ 2.80GHz processor
- KVM on Ubuntu 22.04.2 LTS and on Intel ® Xeon® Silver 4309Y CPU @ 2.80GHz processor

All other tests were performed on the i15820, r10920, and the r12900 models, on the VELOS Controller: Intel Atom CPU C3758 and Blade: Intel Xeon D-2177NT, and a virtual deployment on VMWare ESXi 8.0.3, all with the software version 17.5.0 build 0.189.15.

The evaluator testing was successful and did not reveal any errors.

There was additional testing added due to technical decision TD0967, performed 2026-03-02.

All test verdicts were successful and did not reveal any errors.

### 7.2 Penetration Testing

Port scanning was performed to find open ports that should not be open on the i15820, r10920, and the r12900 models, on the VELOS Controller: Intel Atom CPU C3758 and Blade: Intel Xeon D-2177NT, and a virtual deployment on VMWare ESXi 8.0.3, all with the software version 17.5.0 build 0.189.15.

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. Appliance mode disables root access to the TOE operating system and disables 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)
  - Remote (i.e., SSH) access to the Lights Out / Always On Management2 capabilities of the system is disabled. (applicable to F5 devices)
  - TLS v1.1

## 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].

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 PP-configuration for Network Device and Stateful Traffic Filter Firewalls [CFG\_NDcPP-FW\_V2.0].

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 Introduction	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_SSHPKG.1	PASS
	ASE_FWPPM.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_SSHPKG.1	PASS
	AGD_FWPPM.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

Swedish Certification Body for IT Security  
Certification Report F5 BIG-IP 17.5.0 including AFM

	ATE_NDCPP.1	PASS
	ATE_SSHPKG.1	PASS
	ATE_FWPPM.1	PASS
Vulnerability Assessment	AVA	PASS
Vulnerability Analysis	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® 17.5.0 including AFM Security Target, F5 Inc., 2026-03-05, document version 17.60
NDCPP	collaborative Protection Profile for Network Devices, 2023-12-06, document version 3.0e
CFG_NDcPP-FW_v2.0	PP-Configuration for Network Device and Stateful Traffic Filter Firewalls, Version 2.0, 2024-04-25
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