A Certification Body of atsec information security AB
under the atsec Common Criteria scheme

Certification Report – F5 BIG-IP® 17.1.0.1 including AFM

Issue: 1.0, 2024-08-16

Authorization: Helmut Kurth, Lead Certifier, atsec information security CB

atsec information security AB
Svärdvägen 23
SE-182 33 Danderyd
Phone: +46 8 55 110 400
Fax: +46 8 55 110 401
www.atsec.com

Table of Contents

1 Executive Summary

The Target of Evaluation (TOE) is BIG-IP Version 17.1.0.1 including AFM (Build Hotfix-BIGIP-17.1.0.1.0.61.4-ENG, also referred to as 17.1.0.1 + EHF) with the following elements:

- Application Delivery Firewall Deployment, which includes the Local Traffic Manager (LTM)
- Standalone Advanced Firewall Manager deployment

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 firewall functionality. TOE consists of the software version (Build Hotfix-BIGIP-17.1.0.1.0.61.4-ENG, also referred to as 17.1.0.1 + EHF), running on any of the devices identified below and any of the hypervisors identified in Section below. The TOE is deployed with the following license modes/modules:

The TOE can be deployed with two different sets of license modes/modules:

- Application Delivery Firewall deployment
  - ApplianceMode
  - Traffic Management Operating System (TMOS) modules
  - Traffic Management Microkernel (TMM) module
  - Advanced Firewall Manager (AFM) module
  - Local Traffic Manager (LTM) module
- Standalone Advanced Firewall Manager deployment
  - Appliance Mode
  - Traffic Management Operating System (TMOS) modules
  - Traffic Management Microkernel (TMM) module
  - Advanced Firewall Manager(AFM) module

Hardware Devices:

- iSeries:
  - i4000 model series,
  - i5000 model series,
  - i7000 model series,
  - i10000 model series,
  - i11000 DS model series,
  - i15000 model series,
  - i15000-DF model series,
- VIPRION:
  - B2250,
  - C2400,
  - B4450,
  - C4480,
- rSeries:
  - R4000,
  - R5000,
  - R10000,
  - R12000,
- VELOS:
  - BX110,
  - CX410

Hypervisors:

- VMWare ESXi 8.0.0.10100 (Build: 20920323) (tested on Dell PowerEdge R650)
- Hyper-V version 10.0.20348.1 on Windows Server 2022 Standard (tested on Dell PowerEdge R450)
- KVM: qemu-system-x86 Version: 1:6.2+dfsg-2ubuntu6.6 on Ubuntu 22.04.1 LTS (tested on Dell PowerEdge R450)

The TOE hardware appliances above are delivered via trusted couriers. The TOE software is downloaded from the F5 website.

The Security Target [ST] claims exact conformance to

- PP-Configuration for Network Device and Stateful Traffic Filter Firewalls (CFG_NDcPP-FW_v1.4e), Version 1.4 +Errata20200625, 25 June 2020

CFG_NDcPP-FW_v1.4e consists of the following components:

- collaborative Protection Profile for Network Devices (NDcPP), Version 2.2e, 23-March 2020
- PP-Module for Stateful Traffic Filter Firewalls (FWPPM), Version 1.4 + Errata 20200625, 25- June-2020 [FWPPMv1.4e].

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

There are eleven assumptions being made in the ST regarding the secure usage and the operational environment of the TOE. The TOE relies on these to counter the nine 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 2024-07-07. 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 and NDcPP-FW Evaluation Activities as defined in [NDcPPv2.2-SD] and [FWPPMv1.4e-SD].

atsec information security AB is a licensed evaluation facility for Common Criteria under the Swedish Common Criteria Evaluation and Certification Scheme and also licensed by the atsec information security certification body. atsec information security AB is also accredited by the Swedish accreditation body SWEDAC according to ISO/IEC 17025 for Common Criteria evaluation.

The certifier monitored the activities of the evaluator by reviewing all successive versions of the evaluation reports. The certifier determined that the evaluation results confirm the security claims in the Security Target [ST], and have been reached in agreement with the requirements of the Common Criteria and the Common Methodology for evaluation assurance level:

- EAL 1 + ASE_SPD.1 and in accordance with the Evaluation Activities for Collaborative Protection Profile for Network Devices as defined in [CFG_NDcPP- FW_v1.4e].

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 IT product identified in this certificate has been evaluated at an accredited and licensed evaluation facility established under the atsec Common Criteria Evaluation and Certification Scheme using the Common Methodology for IT' Security Evaluation, version 3.1 revision 5, for conformance to the Common Criteria for IT Security Evaluation, version 3.1 revision 5.

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. The evaluation has been conducted in accordance with the provisions of the atsec Common Criteria Evaluation and Certification Scheme and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

This certificate is not an endorsement of the IT product by the atsec CB or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by the atsec CB or any other organisation that recognises or gives effect to this certificate is either expressed or implied.

The validity of the certificate may change over time. For information regarding the current status of the certificate, please contact the atsec certification body or look at the atsec website.

2 Identification

Certification ID:	ATSEC-CC-002
Name and version of the certified IT product :	BIG-IP Version 17.1.0.1 including APM (Build Hotfix-BIGIP-17.1.0.1.0.61.4-ENG, also referred to as 17.1.0.1 + EHF)
Security Target Identification:	F5 BIG-IP® 17.1.0.1 including AFM Security Target, Document Number: CC2023-ASE_ST-001, Document Version: 7.4, Date: July 28, 2023
EAL:	EAL 1 + ASE_SPD.1 (CFG_NDcPP- FW_v1.4e) PP-Configuration for Network Device and Stateful Traffic Filter Firewalls (CFG_NDcPP- FW_v1.4e), Version 1.4 +Errata20200625, 25 June 2020 CFG_NDcPP-FW_v1.4e consists of the following components: • collaborative Protection Profile for Network Devices (NDcPP), Version 2.2e, 23-March 2020 • PP-Module for Stateful Traffic Filter Firewalls (FWPPM), Version 1.4 + Errata 20200625, 25- June-2020.
Sponsor:	F5, Inc
Developer:	F5, Inc
ITSEF:	atsec information security AB
Common Criteria version CEM version	V3.1R5 CCMB-2017-04-001

3 Security Policies

The TOE provides the following security services:

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

Security Audit

The TOE implements 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.

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.

Cryptographic Support

The TOE implements cryptographic functionality which 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.

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.

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

Identification and Authentication

The TOE provides an internal password-based repository that 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.

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 Function Management

The TOE offers 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”) 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.

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.

Protection of the TSF

The TOE is designed to protect critical security data, including keys and passwords.

In addition, the TOE 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.

TOE Access

Prior to interactive user authentication, the TOE can display an administrative defined banner. The TOE terminates interactive sessions after an administrator-defined period of inactivity and allows users to terminate their own authenticated session.

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.

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-SHA1 and 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.

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 Threat Environment

This section describes the threat model for the TOE and identifies the individual threats that are assumed to exist in the operational environment of the TOE.

The **assets** to be protected by the TOE are:

- Critical network traffic (administration traffic, authentication traffic, audit traffic, etc.) to/from the TOE
- Organizational data hosted on remote systems (server pools) in physical and virtual network segments connected directly or indirectly to the TOE. (The TOE can be used to protect the assets on those systems from unauthorized exploitation by mediating network traffic from remote users before it reaches the systems or networks hosting those assets.)
- The TSF and TSF data

The **threat agents** having an interest in manipulating the TOE and TSF behavior to gain access to these assets can be categorized as:

- Unauthorized third parties (“attackers”, such as malicious remote users, parties, or external IT entities) which are unknown to the TOE and its runtime environment. Attackers are traditionally located outside the organizational environment that the TOE is employed to protect, but may include organizational insiders, too.
- Authorized users of the TOE (i.e., administrators) who try to manipulate configuration data that they are not authorized to access. TOE administrators, as well as administrators of the operational environment, are assumed to be trustworthy, trained and to follow the instructions provided to them with respect to the secure configuration and operation of the systems under their responsibility. Hence, only inadvertent attempts to manipulate the safe operation of the TOE are expected from this community.

The motivation of threat agents is assumed to be commensurate with the assurance level pursued by this evaluation, i.e., the TOE intends to resist penetration by attackers with a Basic attack potential.

4.2 Threats

The threats identified in this section may be addressed by the TOE, TOE environment, or a combination of both. The threat agents are authorized persons/processes, unauthorized persons/processes, or external IT entities not authorized to use the TOE itself. The threats identified assume that the threat agent is a person with a low attack potential who possesses an average expertise, few resources, and low to moderate motivation.

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., shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the Administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the Network Device itself could be compromised.

T.UPDATE_COMPROMISE

Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.

T.UNDETECTED_ACTIVITY

Threat agents may attempt to access, change, and/or modify the security functionality of the Network Device without Administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the Administrator would have no knowledge that the device has been compromised.

T.SECURITY_FUNCTIONALITY_COMPROMISE

Threat agents may compromise credentials and device data enabling continued access to the Network Device and its critical data. The compromise of credentials include replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the Administrator or device credentials for use by the attacker.

T.PASSWORD_CRACKING

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

T.SECURITY_FUNCTIONALITY_FAILURE

An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.

T.NETWORK_DISCLOSURE

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

T.NETWORK_ACCESS

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

T.NETWORK_MISUSE

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

T. MALICIOUS_TRAFFIC

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

4.3 Organisational Security Policies

The TOE environment must include and comply with the following organizational security policies.

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.

4.4 Assumptions

The assumptions defined below are made on the operational environment to ensure that the security functionality defined in chapter 3 can be provided by the TOE. Note that some assuptions are related to virtual network devices (vNDs) only. They are marked accordingly. For a definiton of a virtual network device, see [NDcPPv2.2e].

A.PHYSICAL_PROTECTION

The Network Device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP will not include any requirements on physical tamper protection or other physical attack mitigations. The cPP will not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device. For vNDs, this assumption applies to the physical platform on which the VM runs.

A.LIMITED_FUNCTIONALITY

The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example the device should not provide a computing platform for general purpose applications (unrelated to networking functionality).

In the case of vNDs, the VS is considered part of the TOE with only one vND instance for each physical hardware platform. The exception being where components of the distributed TOE run inside more than one virtual machine (VM) on a single VS. There are no other guest VMs on the physical platform providing non-Network Device functionality.

A.NO_THRU_TRAFFIC_PROTECTION

The standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the Network Device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the Network Device, destined for another network entity, is not covered by the NDcPP. It is assumed that this protection will be

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

A.TRUSTED_ADMINISTRATOR

The Security Administrator(s) for the Network Device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The Network Device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device.

For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).

A.REGULAR_UPDATES

The Network Device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.

A.ADMIN_CREDENTIALS_SECURE

The Administrator's credentials (private key) used to access the network device are protected by the platform on which they reside.

A.RESIDUAL_INFORMATION

The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g., cryptographic keys, keying material, PINs, passwords, etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

A.VS_TRUSTED_ADMINISTRATOR (applies to vNDs only)

The Security Administrators for the VS are assumed to be trusted and to act in the best interest of security for the organization. This includes not interfering with the correct operation of the device. The Network Device is not expected to be capable of defending against a malicious VS Administrator that actively works to bypass or compromise the security of the device.

A.VS_REGULAR_UPDATES (applies to vNDs only)

The VS software is assumed to be updated by the VS Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.

A.VS_ISOLATON (applies to vNDs only)

For vNDs, it is assumed that the VS provides, and is configured to provide sufficient isolation between software running in VMs on the same physical platform. Furthermore, it is assumed that the VS adequately protects itself from software running inside VMs on the same physical platform.

A.VS_CORRECT_CONFIGURATION (applies to vNDs only)

For vNDs, it is assumed that the VS and VMs are correctly configured to support ND functionality implemented in VMs.

5 Architectural Information

The BIG-IP products subject to this evaluation represent Application Delivery Controllers based on F5's Traffic Management Operating System (TMOS). In particular,

- Application Delivery Firewall, which includes the Local Traffic Manager (LTM) and Advanced Firewall Manager (AFM) modules, provides network traffic management and firewall capabilities.
- Standalone Advanced Firewall Manager, which includes the Advanced Firewall Manager (AFM) module, provides firewall capabilities.

BIG-IP products run on appliance or blade hardware, or hardware and platform layer, provided by F5 listed in Section 1 or on one of the hypervisors listed in Section 1. When running on a third-party hypervisor, there may be only one guest virtual machine running on the hypervisor and only one instance of BIG-IP for each hardware platform.

The TOE's Traffic Management Microkernel (TMM), along with additional software, provides basic networking functionality, with the TOE operating as a network switch and reverse proxy.

Typical BIG-IP network environments include an internal network, administrator network, external network, server pools, and redundant BIG-IP systems. In this typical example,

- Internet connections are mediated by BIG-IP to provide access to certain resources located in an organization's internal server pool, for example to a web-based e-commerce system presenting a storefront to consumers
- Users in the organization's Intranet also access resources in the server pools to interact with the internal server pool. Although not included in the TOE, BIG-IP provides server termination of traffic flowing to a backend server by implementing a TLS client protocol.
- Network administrators connect to BIG-IP via a dedicated network interface to administer the TOE
- The TOE is optionally set up in a redundant failover configuration, with heartbeat monitoring and reporting via a data link between the two instances

When deployed as two redundant systems configured in an active/standby failover configuration, the two systems can synchronize their configuration data and provide state and persistence monitoring. The TOE will fail over to the redundant system while maintaining a secure configuration if failures the active device sends a request to the standby device or if the standby device detects missing heartbeats from the active device. The new active device will continue to enforce security policies for new (and possibly active) connections mediated by the TOE. BIG-IP uses CMI (Central Management Infrastructure), a proprietary protocol, for the incremental exchange of configuration data and failover status between TOE instances; CMI is encapsulated in TLS to provide integrity and confidentiality protections. In this configuration a physical network port will be dedicated on each device for the exchange of synchronization data and failover monitoring with the standby device. Failover / redundancy is not in the scope of the evaluated configuration.

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 (TLSv1.1 and TLSv1.2). The cryptographic functionality implemented in the TOE is provided by OpenSSL.

The TOE is divided into the following subsystems:

- F5 Device Hardware,

- 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.

F5's TMOS is a Linux-based operating system customized for performance and to execute on the TOE hardware. The TMM is the data plane of the product and all data plane traffic passes through the TMM. The LTM controls network traffic coming into or exiting the local area network (LAN) and provides the ability to intercept and redirect incoming network traffic. The APM module terminates TLS-based VPN connections from remote clients although these features are not included in the evaluated configuration.

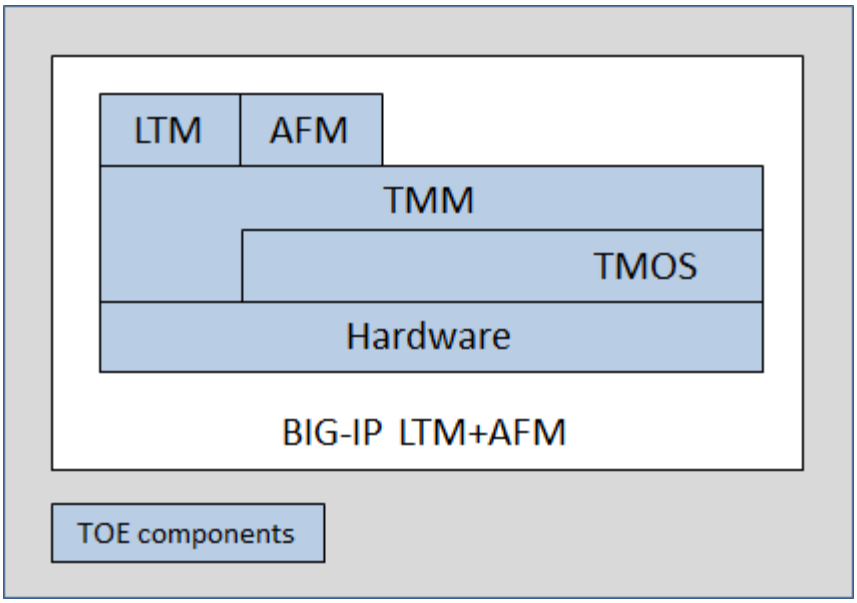

Figure 1: BIG-IP Subsystems for F5 Devices (except rSeries and VELOS) in Application Delivery Firewall Deployments

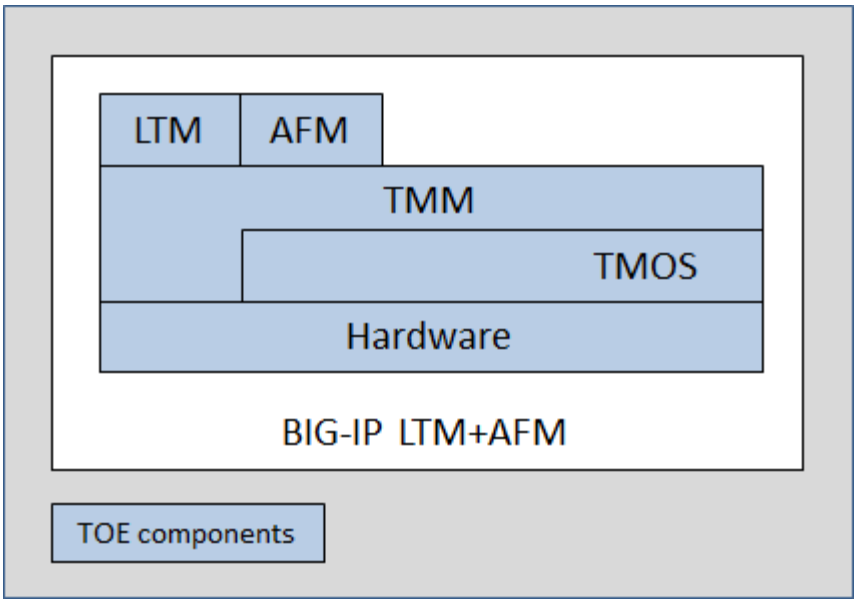

Figure 2: BIG-IP Subsystems for F5 rSeries and VELOS Devices in Application Delivery Firewall Deployments

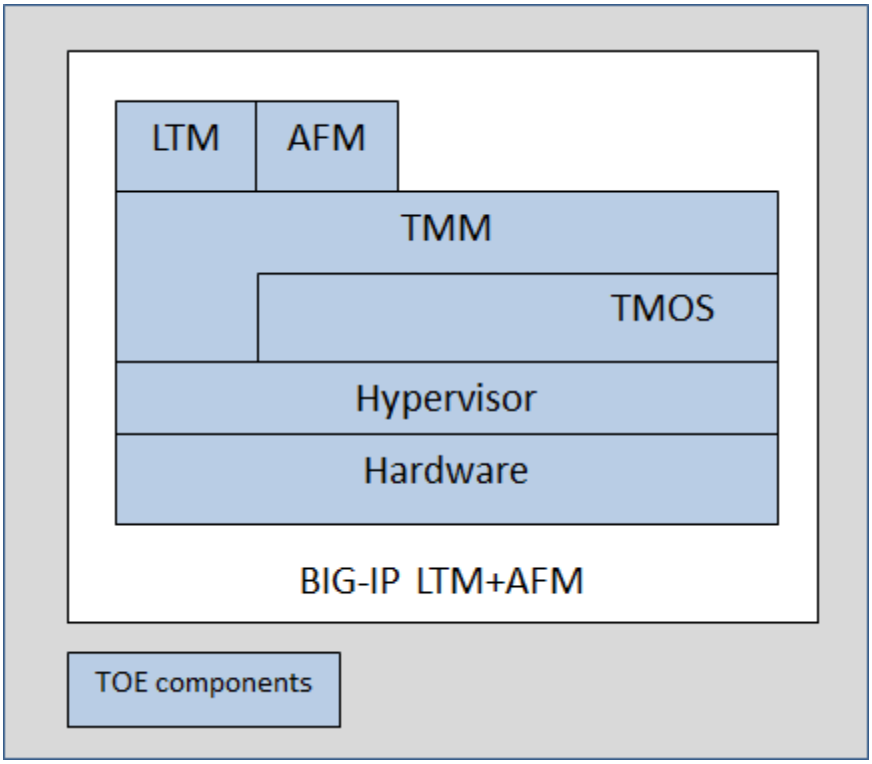

Figure 3: BIG-IP Subsystems for Hypervisors in Application Delivery Firewall Deployments

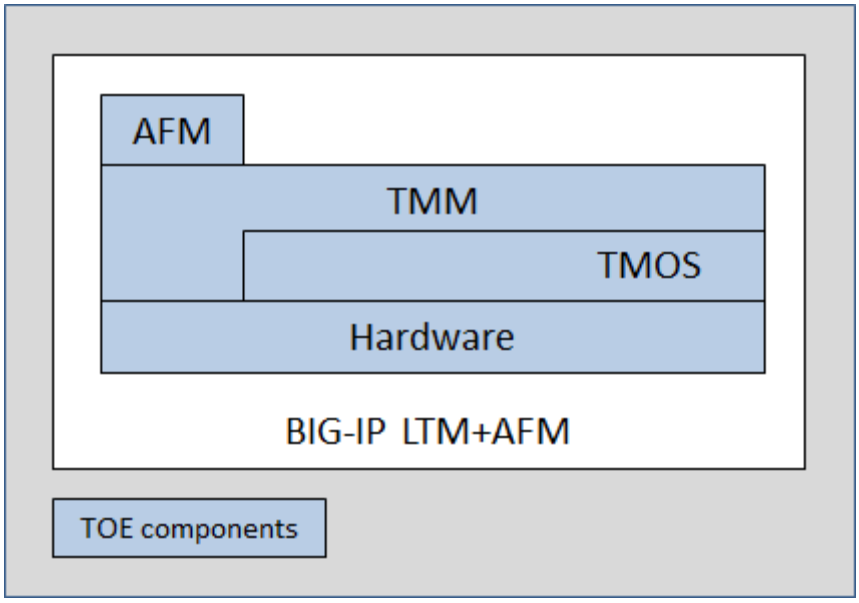

Figure 4: BIG-IP Subsystems for F5 Devices (except rSeries and VELOS) in Standalone Advanced Firewall Manager Deployments

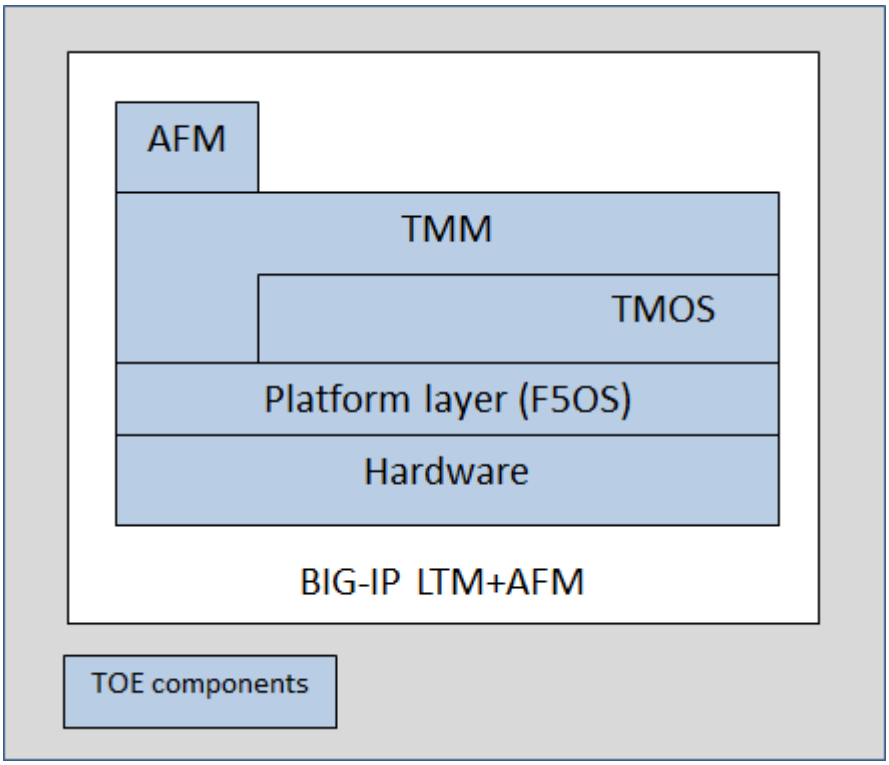

Figure 5: BIG-IP Subsystems for F5 rSeries and VELOS Devices in Standalone Advanced Firewall Manager Deployments

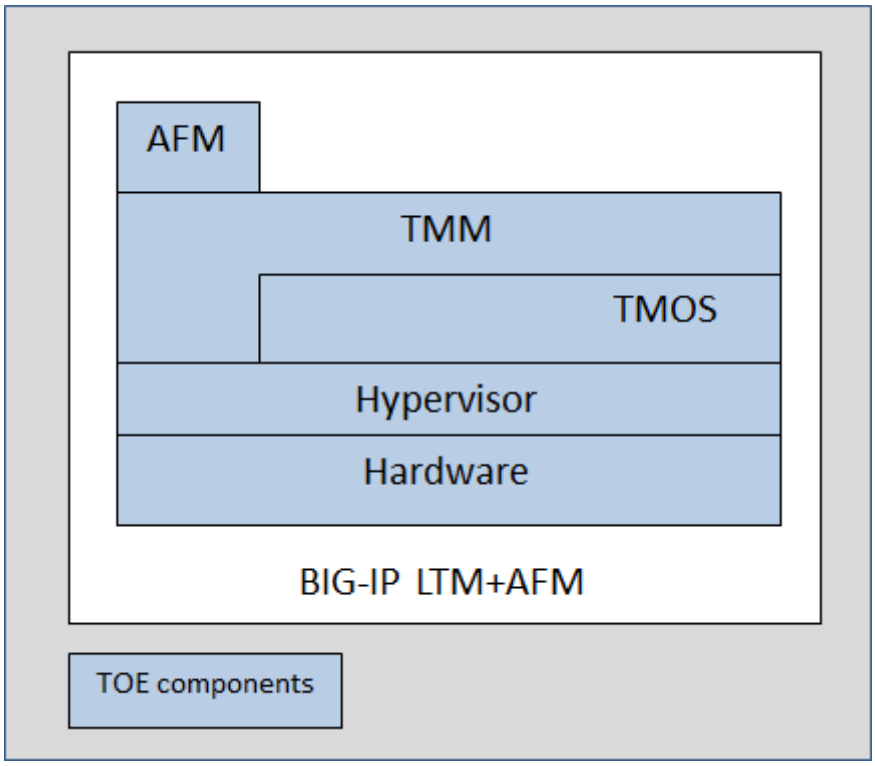

Figure 6: BIG-IP Subsystems for Hypervisors in Standalone Advanced Firewall Manager Deployments

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

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

At the core of BIG-IP is a concept referred to as Traffic Management Microkernel (TMM), representing the data plane of the product when compared to traditional network device architectures. It is implemented by a daemon running with root privileges, performing its own memory management, and having direct access to the network hardware or hypervisor. TMM implements a number of sequential filters both for the “client-side” and “server-side” network

interfaces served by BIG-IP. The filters implemented in TMM include a TCP, TLS, compression, and HTTP filter, amongst others. If the hardware or hypervisor provides more than one CPU, TMM runs multi-threaded (one thread per CPU). In this case, disaggregators in the kernel are responsible for de-multiplexing and multiplexing network traffic for handling by an individual TMM thread. In addition to the actual switch hardware, F5 appliance hardware also contains a High-Speed Bridge (HSB, implemented by means of an FPGA) that performs basic traffic filtering functionality as instructed by TMM.

Additional plug-in filters can be added to this queue by individual product 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 the Application Delivery Controller Deployments are shown in Figures 10, 11, and 12.. These plug-in modules include:

- Local Traffic Manager (LTM): authentication of HTTP (based on Apache) traffic and advanced traffic forwarding directives
- Advanced Firewall Manager (AFM): network filtering as described in FWPPM.

A diagram depicting aspects of the TOE's architecture and the boundaries of the TOE are provided in Figures 7 - 12.

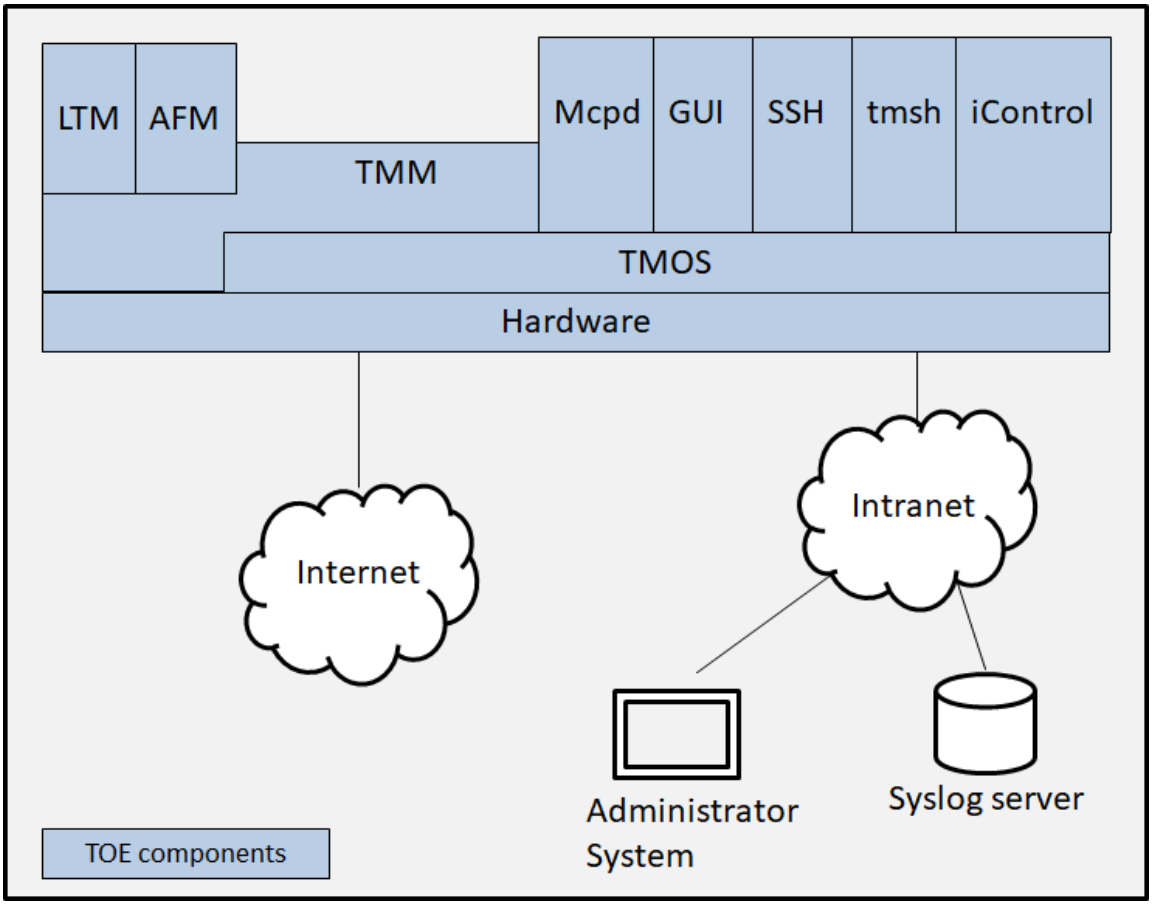

Figure 7: Architectural aspects of BIG-IP – F5 Device (except rSeries and VELOS) in Application Delivery Controller Deployments

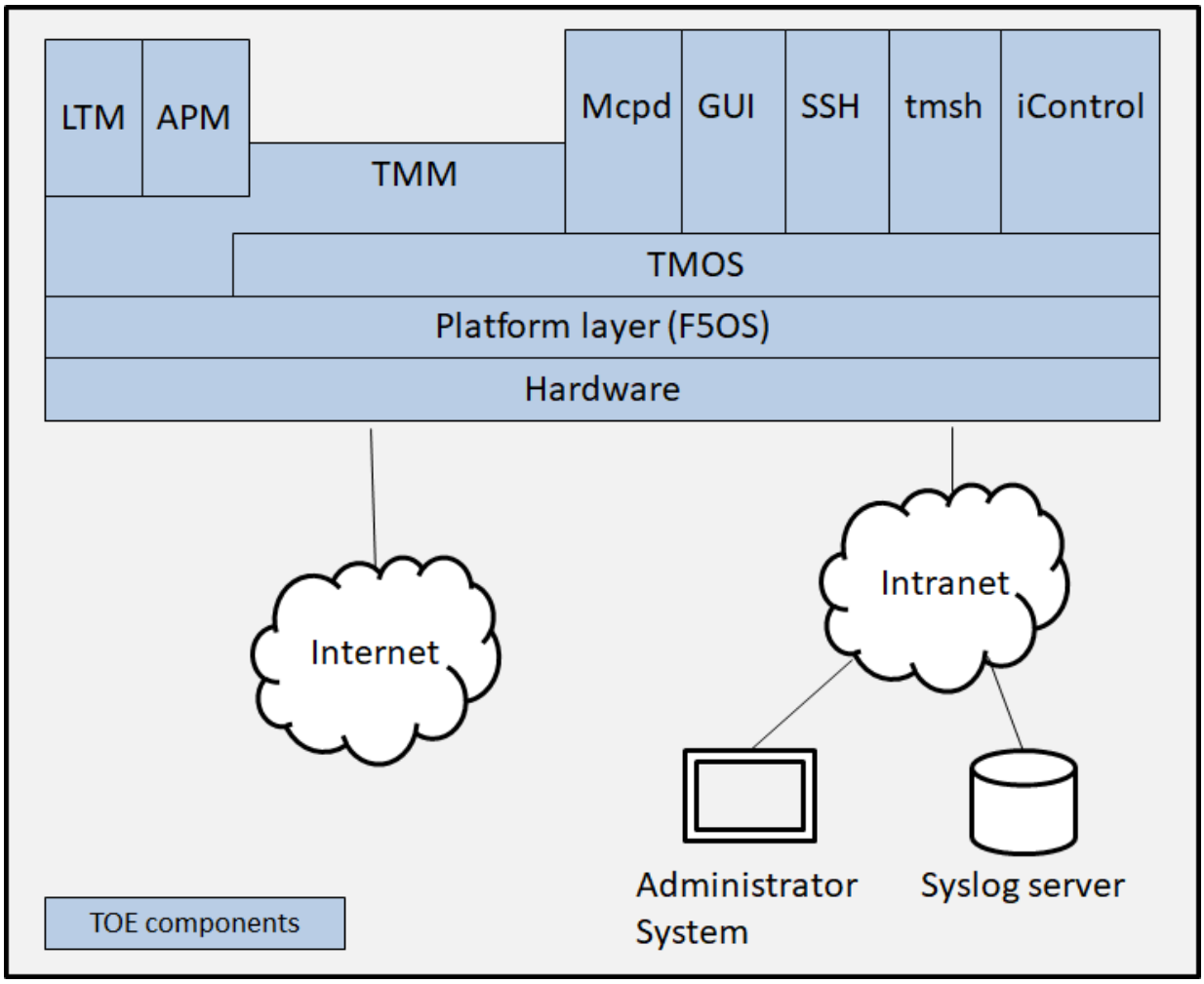

Figure 8: Architectural aspects of BIG-IP – F5 Device (except rSeries and VELOS) in Application Delivery Firewall Deployments

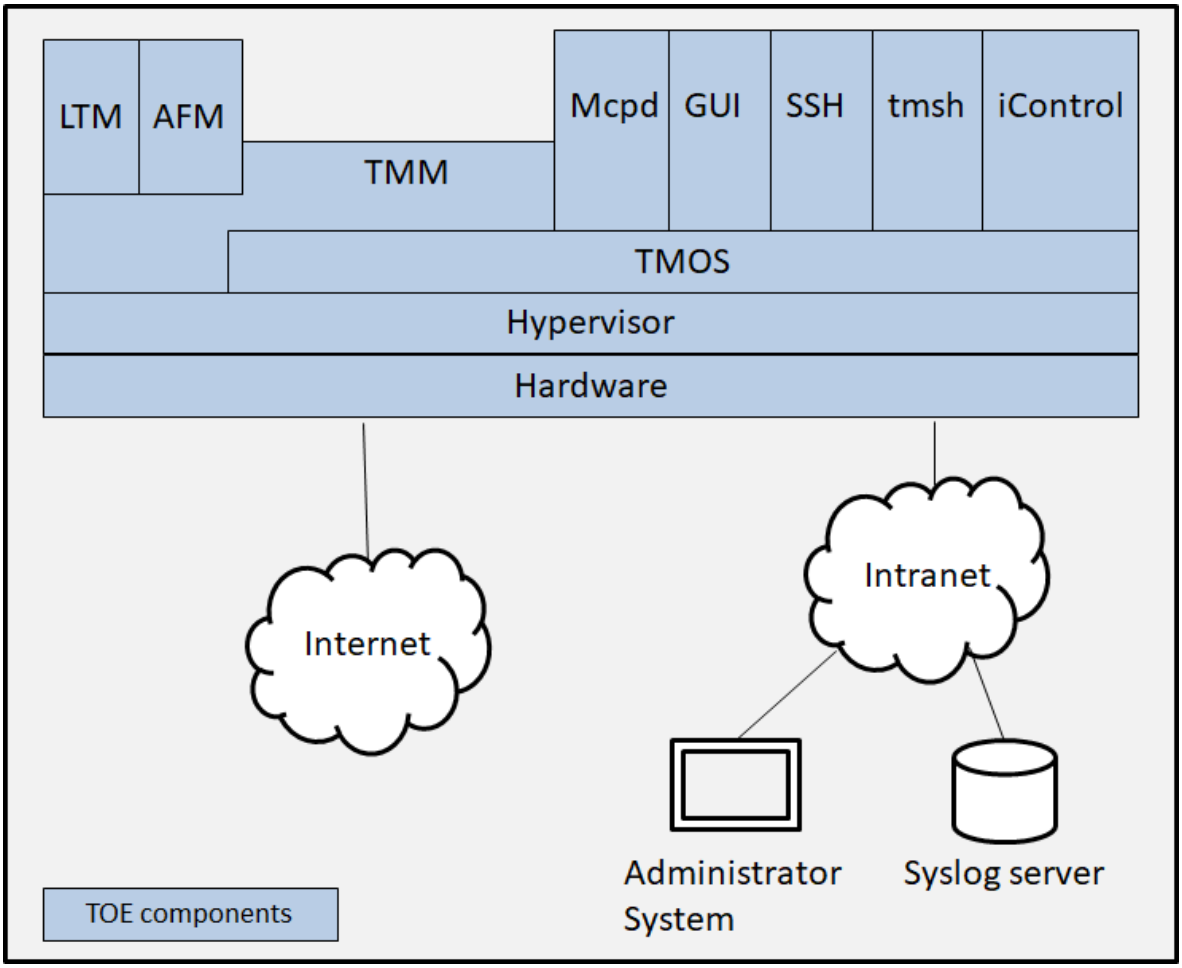

Figure 9: Architectural aspects of BIG-IP - Hypervisor in Application Delivery Firewall Deployments

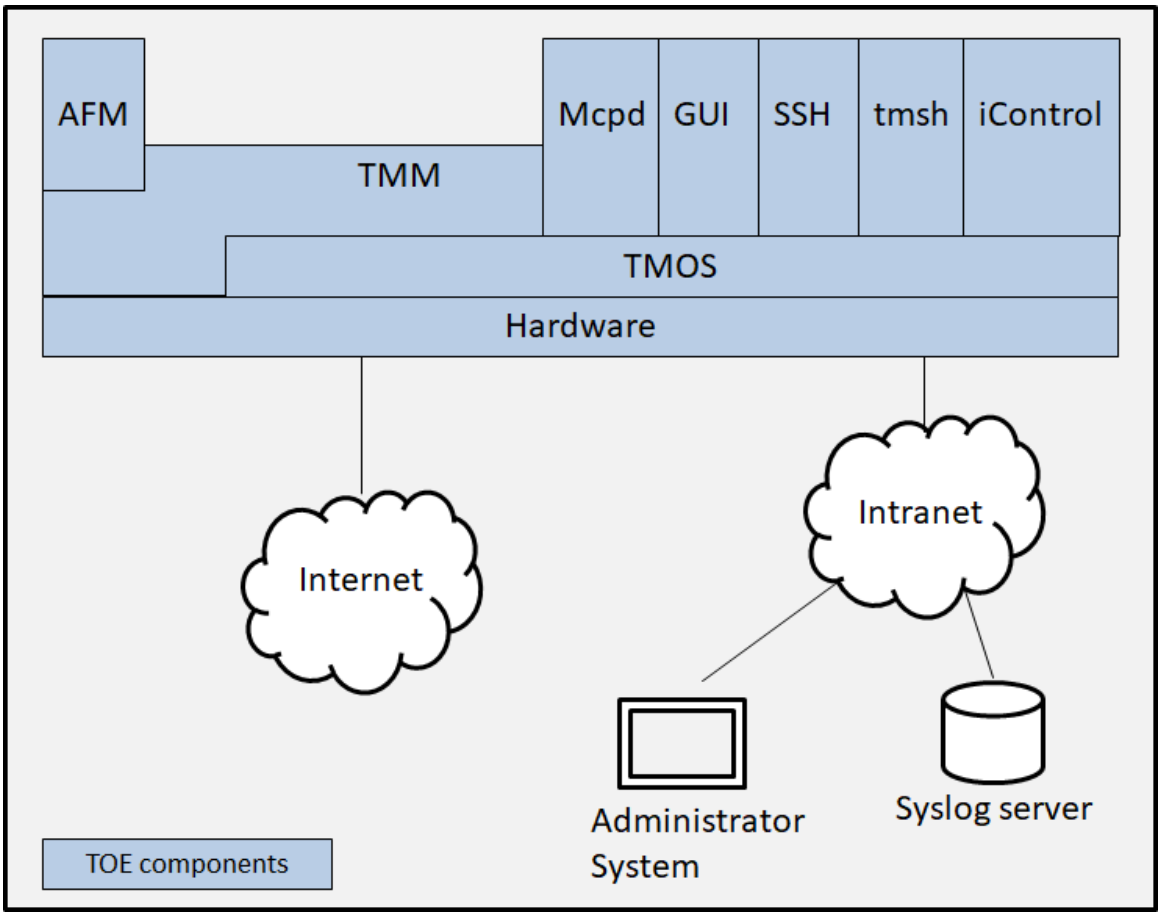

Figure 10: Architectural aspects of BIG-IP – F5 Device (except rSeries and VELOS) in Standalone Advanced Firewall Manager Deployments

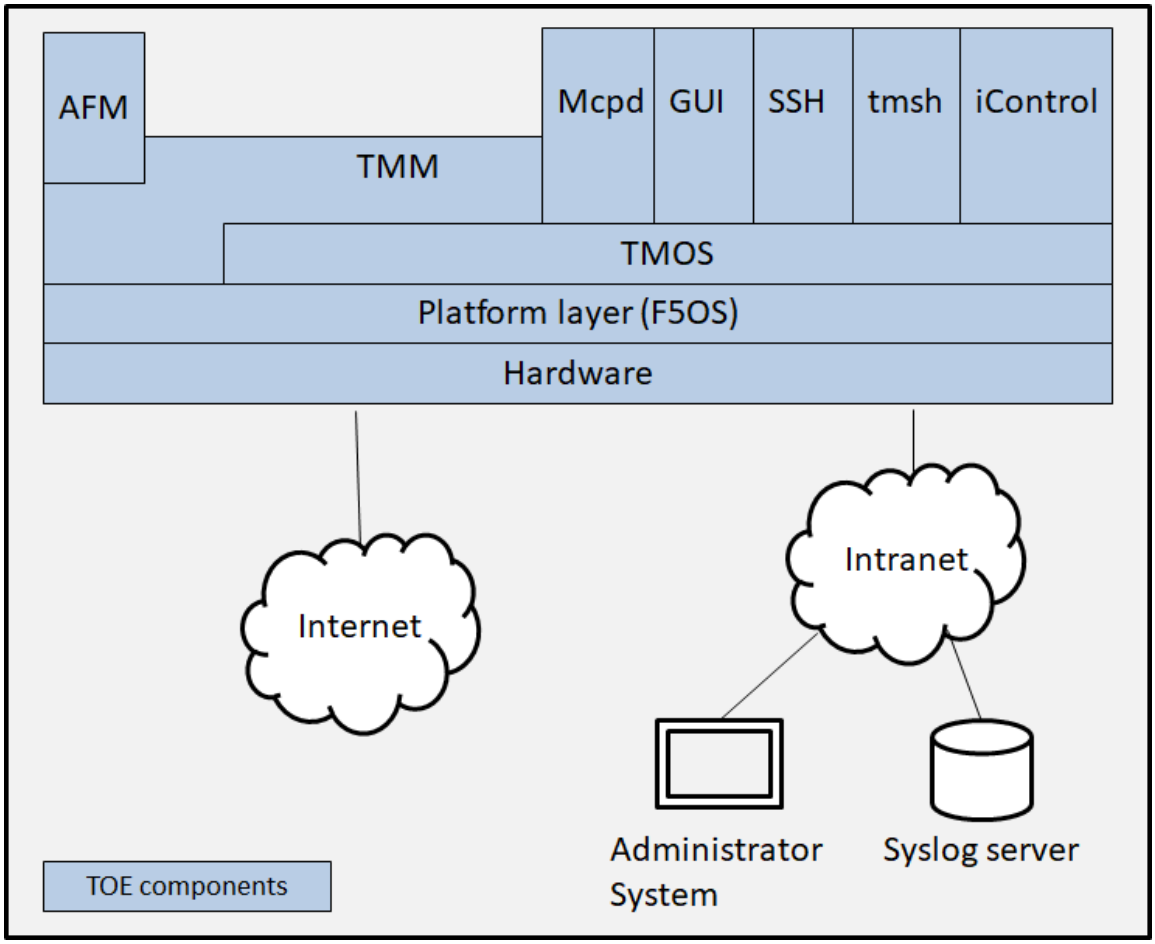

Figure 11: Architectural aspects of BIG-IP – F5 rSeries and VELOS Devices in Standalone Advanced Firewall Manager Deployments

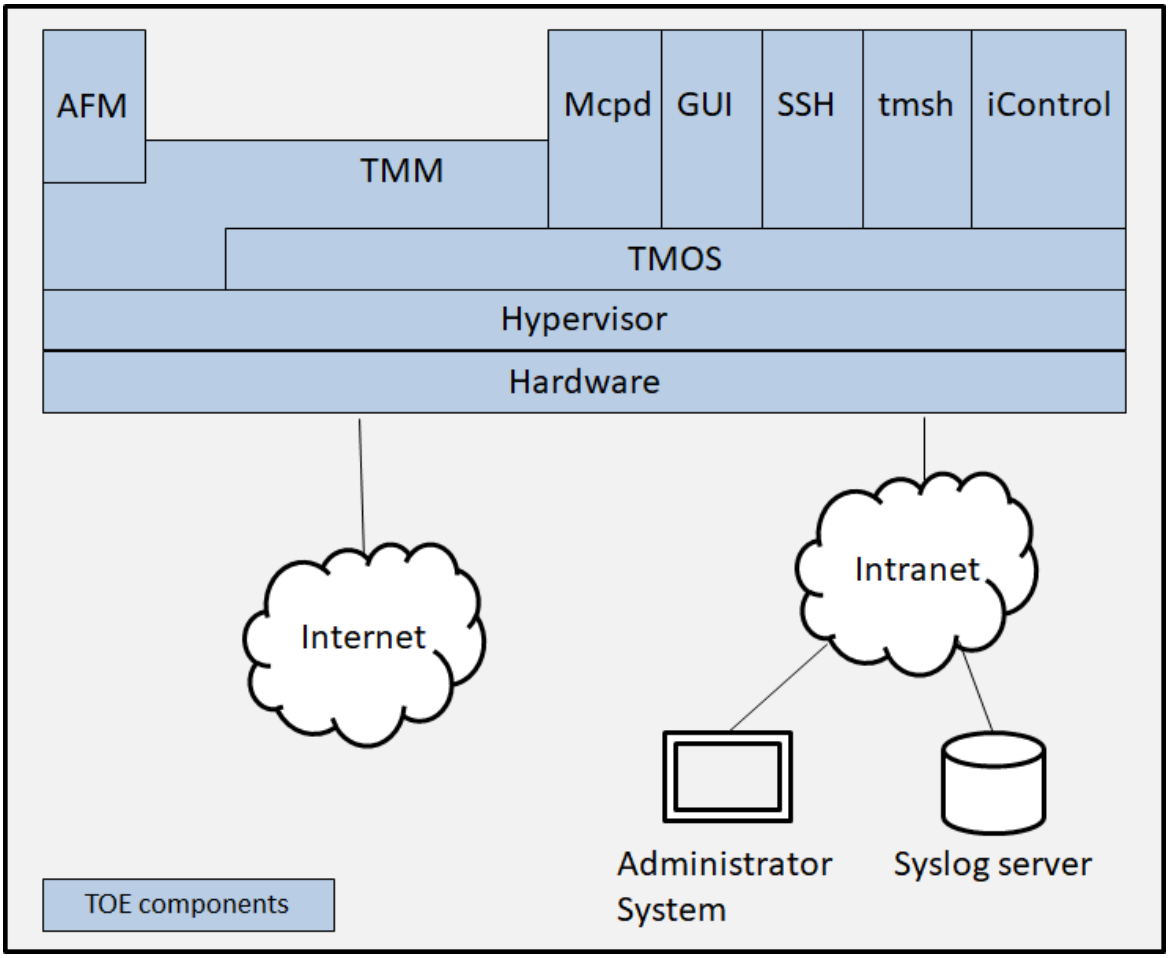

Figure 12: Architectural aspects of BIG-IP - Hypervisor in Standalone Advanced Firewall Manager Deployments

Physical Boundaries

This section lists the physical components of the product and denotes which are in the TOE and which are in the environment.

When BIG-IP version 17.1.0.1 is running on one of the F5 devices identified in Section 1, the TOE includes hardware and software physical components as identified in Section 1. When BIG-IP version 17.1.0.1 is running on one of the hypervisors identified in Section 1, the TOE includes hypervisor, hardware, and software physical components as identified in Section 1.

The evaluated configuration of *BIG-IP Version 17.1.0.1 including AFM* represents a licensing option with the following F5 modules present and operational:

- Application Delivery Controller deployment
  - Appliance Mode
  - Traffic Management Operating System (TMOS) modules
  - Traffic Management Microkernel (TMM) module
  - Advanced Firewall Manager(AFM) module
  - Local Traffic Manager(LTM) module
- Standalone Advanced Firewall Manager deployment
  - Appliance Mode
  - Traffic Management Operating System (TMOS) modules
  - Traffic Management Microkernel (TMM) module
  - Advanced Firewall Manager (AFM) module

The following required components can be found in the operating environment of the TOE on systems other than those hosting the TOE:

- audit servers

Client software (e.g., the BIG-IP Client for TLS VPN connections, endpoint inspection software executed on clients) are optional components that are not part of the TOE.

6 ICT Product Testing

The configuration of the test environment, including the TOE, is documented in [NDETP] and [FWETP]. The evaluator used the guidance documentation listed in [ST] for the management of the TOE, namely the evaluated configuration guide [ECG].

6.1 Testing approach

The evaluator has conducted testing on the BIG-IP running version 17.1.0.1 on the TOE running on hardware appliance (i7800), on the TOE's running on hardware appliance with platform layer (r5900, r12900, VELOS), and on the TOE running on VMWare ESXi Hypervisor (VMWare). All five models were fully tested. The evaluator followed and documented all test procedures and test results in [NDETP]. Detailed test outputs, test logs and traffic captures have been provided to the certification body where applicable in a separate compressed archive.

The evaluator testing of the TOE was performed by Markus Engqvist, Paolo Molinaro, and Robin Klint between August 2023 and February 2024.

The cryptographic algorithm testing is covered by Cryptographic Algorithm Validation System (CAVS), and the Cryptographic Algorithm Validation Program (CAVP) certificates.

6.2 Configuration

The evaluator configured the TOE and set up the test environment as described in [NDETP]. The evaluator verified that the configured TOE and environment is consistent with the requirements of the [ST]. The evaluator used the relevant developer documentation during the installation and configuration of the TOE:

The evaluation has performed tests as described in [NDcPPv2.2-SD] and [MOD_FW_v1.4e-SD] for each SFR in the [ST] to ensure that the TOE behaves as specified in the ST and guidance documentation. All tests have been executed on version 17.1.0.1 of the TOE.

6.3 Independent Testing

The independent testing was performed on the TOE in the form that it is delivered to customers. The evaluation has performed more than 50 test cases, including extensive testing to test cryptographic protocols (SSH, TLS, HTTPS) as well as underlying cryptographic operations (FCS_COP, FCS_CKM) that were also separately tested in algorithm testing, as described below.

Independent testing was performed on the hardware appliance BIG-IP i7800, the hardware appliance with platform layer (F5OS) BIG-IP r5900, BIG-IP r12900, and VELOS, as well as on the TOE running on VMWare ESXi. All tests were performed remotely from the atsec office in Sweden. The evaluation confirmed that all test cases passed successfully.

6.4 Algorithm testing

Algorithm testing is required to be performed by the [NDcPPv2.2-SD]. Algorithm test vectors were generated by the ACVT tool to test all cryptographic algorithms of the TOE. The testing is valid for all hardware appliance and hypervisors supported by the TOE, which is evident from the CAVP certificates: KVM, VMWare and Hyper-V.

The TOE contains a single implementation of the OpenSSL module. Separate instances of this OpenSSL module run on both the control plane and the data plane.

6.5 Evaluator Penetration Testing

Testing approach

The approach for the penetration test was to scan all TCP and UDP ports on the TOE platform to identify all open ports.

Test configuration

The penetration test was performed on the TOE in the evaluated configuration. During the execution of the port scans, all devices were configured with LTM+APM+AFM licenses.

Test depth

All TCP and UDP ports were scanned.

Test results

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

- 22/tcp: ssh
- 80/tcp: http
- 161/tcp: snmp
- 443/tcp: ssl/http
- 4433/tcp: tcpwrapped
- 4353/tcp: ssl/f5-iquery
- 7001/tcp - 7008/tcp: OpenSSH 7.4 (protocol 2.0)
- 8888/tcp open ssl/http

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

7 Results of the Evaluation and Information Regarding the Certificate

7.1 Evaluation Report and Evaluation Results

The following are the Single Evaluation Reports received by the Certification Body:

- ASE - ETR-Part ASE - 2024-05-06 (ATSEC-CC-002_ASE_240226_v1.0.pdf)
- ADV - ETR-Part ADV - 2024-07-12 (ATSEC-CC-002_ADV_240702_v2.0.pdf)
- ALC - ETR-Part ALC - 2024-05-06 (ATSEC-CC-002_ALC_240301_v1.0.pdf)
- AGD - ETR-Part AGD - 2024-07-12 (ATSEC-CC-002_AGD_240702_v2.0.pdf)
- ATE - ETR-Part ATE - 2024-07-12 (ATSEC-CC-002_ATE_240703_v2.0.pdf)
- AVA - ETR-Part AVA - 2024-07-12 (ATSEC-CC-002_240704_v2.0.pdf)

The following table lists the assurance components of CC V3.1R5 that have been used in the evaluation with the evaluation result. Note that assurance components ending with NDCPP.1 are refinements of assurance components in CC V3.1R5 defined in [NDCPPv2.2e] and [NDcPPv2.2-SD].

Component	Evaluator Action	Verdict
ASE: Security Target evaluation		
ASE_INT.1		PASS
	ASE_INT.1.1E	PASS
	ASE_INT.1.2E	PASS
ASE_CCL.1		PASS
	ASE_CCL.1.1E	PASS
ASE_OBJ.1		PASS
	ASE_OBJ.1.1E	PASS
ASE_ECD.1		PASS
	ASE_ECD.1.1E	PASS
	ASE_ECD.1.2E	PASS
ASE_REQ.1		PASS
	ASE_REQ.1.1E	PASS
ASE_SPD.1		PASS
	ASE_SPD.1.1E	PASS

Component	Evaluator Action	Verdict
ASE_TSS.1		PASS
	ASE_TSS.1.1E	PASS
	ASE_TSS.1.2E	PASS
ASE_NDCPP.1		PASS
	ASE_NDCPP.1.1E	PASS
	ASE_NDCPP.1.2E	PASS
ASE_FWPPM.1		PASS
	ASE_FWPPM.1.1E	PASS
ADV: Development		
ADV_FSP.1		PASS
	ADV_FSP.1.1E	PASS
	ADV_FSP.1.2E	PASS
ADV_NDCPP.1		PASS
	ADV_NDCPP.1.1E	PASS
AGD: Guidance documents		
AGD_OPE.1		PASS
	AGD_OPE.1.1E	PASS
AGD_PRE.1		PASS
	AGD_PRE.1.1E	PASS
	AGD_PRE.1.2E	PASS
AGD_NDCPP.1		PASS
	AGD_NDCPP.1.1E	PASS
	AGD_NDCPP.1.2E	PASS
AGD_FWPPM.1		PASS
	AGD_FWPPM.1.1E	PASS

Component	Evaluator Action	Verdict
ATE: Tests		
ATE_IND.1		PASS
	ATE_IND.1.1E	PASS
	ATE_IND.1.2E	PASS
ATE_NDCPP.1		PASS
	ATE_NDCPP.1.1E	PASS
	ATE_NDCPP.1.2E	PASS
ATE_FWPPM.1		PASS
	ATE_FWPPM.1.1E	PASS
AVA: Vulnerability assessment		
AVA_VAN.1		PASS
	AVA_VAN.1.1E	PASS
	AVA_VAN.1.2E	PASS
	AVA_VAN.1.3E	PASS
AVA_NDCPP.1		PASS
	AVA_NDCPP.1.1E	PASS
ALC: Life-cycle support		
ALC_CMC.1		PASS
	ALC_CMC.1.1E	PASS
ALC_CMS.1		PASS
	ALC_CMS.1.1E	PASS

The overall verdict for this evaluation is: PASS.

The TOE

1) has exact conformance to the PP-Configuration for Network Device and Stateful Traffic Filter Firewalls (CFG_NDcPP- FW_v1.4e), Version 1.4 +Errata20200625, 25 June 2020

   CFG_NDcPP-FW_v1.4e consists of the following components:

i. collaborative Protection Profile for Network Devices (NDcPP), Version 2.2e, 23-March 2020

ii. PP-Module for Stateful Traffic Filter Firewalls (FWPPM), Version 1.4 + Errata 20200625, 25- June-2020 [FWPPMv1.4e].

2) is CC part 2 extended;

3) is CC part 3 conformant;

4) meets all security objectives for the TOE stated in the Security Target;

5) meets all security functional requirements for the TOE stated in the Security Target;

6) meets the applicable Technical Decisions for [NDcPPv2.2e] and [FWPPMv1.4e].

7.2 Evaluated Configuration of the TOE

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. (applicable to F5 devices only)
  - Remote (i.e., SSH) access to the Lights Out / Always On Management capabilities of the system is disabled. (applicable to F5 devices only)
  - SSH client

7.3 Extensions of Results to other Configurations

None.

7.4 Special Restrictions and Exceptions

None.

7.5 Additional Evaluation Results

None.

7.6 Failures and Inconsistencies

None.

7.7 Obligations and Notes for the Usage of the TOE

None.

7.8 Obligations and Notes for the Developer

None.

8 Bibliography

CC	**Common Criteria for Information Technology Security Evaluation,** Version 3.1R5, April 2017 Location http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R5.pdf http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf
CFG_NDcPP-FW_v1.4e	PP-Configuration forNetwork Device and Stateful Traffic Filter Firewalls, Version 1.4 +Errata20200625, 25 June 2020
ECG	BIG-IP Common Criteria Evaluation Configuration Guide BIG-IP Release 17.1.0.1, Version 7.7, Date 2024-03-08
FER	Final Evaluation Technical Report F5 BIG-IP® 17.1.0.1 including AFM, Version 1.0, Date 2024-07-19
NDcPPv2.2e	collaborative Protection Profile for Network Devices Version 2.2e Version 2.2e, Date 2020-03-23 Location https://www.niap-ccevs.org/MMO/PP/CPP_ND_V2.2E.pdf
FWPPMv1.4e	collaborative Protection Profile Module for Stateful Traffic Filter Firewalls v1.4 + Errata 20200625 Version 1.4e, Date 2020-06-25
NDcPPv2.2-SD	Supporting Document - Evaluation Activities for Network Device cPP Version 2.2, Date 2019-12-20 Location https://www.niap-ccevs.org/MMO/PP/CPP_ND_V2.2-SD.pdf
MOD_FW_v1.4e-SD	Supporting Document - Evaluation Activities for Stateful Traffic Filter Firewalls PP-Module, June-2020, Version 1.4 +Errata 20200625
NDETP	F5 BIG IP 17.1.0.1 NDcPP Evaluator Test Plan, atsec information security AB, Version 1.0, Date 2024-02-27
FWETP	F5 BIG IP 17.1.0.1 FWPPM Evaluator Test Plan, atsec information security AB, Version 1.0, Date 2024-03-02
ST	F5 BIG-IP® 17.1.0.1 including AFM Security Target, Document Number: CC2023-ASE_ST-001, Document Version 7.9, Date February 15, 2024