F5 Networks
BIG-IP® Local Traffic Manager 6400
High Availability pair (qty 2)
Security Target

Release Date:	April 9, 2007
Document ID:	05-948-R-0105
Version:	V1.4

Prepared By: InfoGard Laboratories, Inc.

Prepared For: F5 Networks
401 Elliott Avenue West
Seattle, WA 98119

Table of Contents

List of Tables

List of Figures

Document History

Document Version	Date	Author	Comments
V1.4	4/9/07	M. McAlister	Updated based on final VOR verdicts 4th round

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), conformance claims, ST organization, document conventions, and terminology. It also includes an overview of the evaluated product.

1.1 Identification

TOE Identification:	F5 BIG-IP Local Traffic Manager 6400 High Availability pair (qty 2) F5 BIG LTM 6400 Hardware PN: 200-0153-05 Rev. C Software Ver. 9.2.3 + Hotfix CR69440*
ST Identification:	F5 Networks BIG-IP® Local Traffic Manager 6400 High Availability pair (qty 2) Security Target
ST Version:	1.4
ST Publish Date:	April 9, 2007
ST Authors:	Mike McAlister (InfoGard)
PP Identification:	N/A

Documentation: The Big-IP 6400 TOE must be configured in accordance with the following Guidance Documents:

BIG-IP® Network and System Management Guide version 9.2.3

MAN-0185-02

Configuration Guide for Local Traffic Management version 9.2.0

MAN-0182-00

Platform Guide: 1500, 3400, 6400, and 6800 MAN-0183-00 August 16, 2006.

Configuration Worksheet PUB-0090-02 0905

Installation, Licensing, and Upgrades for BIG-IP® Systems Version 9.2

MAN-0184-00

BIG-IP® Quick Start Instructions PUB-0089-03 1205

Common Criteria Supplement EAL2 F5 Networks BIG-IP® Local Traffic Manager 6400 High Availability pair (qty 2), 05-948-R-0134 V1.2.

The guidance is part of the TOE components and is downloaded via the F5 website at https://tech.f5.com/home/solutions/sol7252.html

*note: Revision 9.2.3 + Hotfix CR69440 are also referred to as build 142.0

1.2 CC Conformance Claim

The TOE is Common Criteria (CC) Version 2.2[1] Part 2 extended.

The TOE is Common Criteria (CC) Version 2.2 Part 3 conformant at EAL2 Augmented with ALC_FLR.1.

The TOE is also compliant with all International interpretations with effective dates on or before 10/13/05.

This TOE is not conformant to any Protection Profiles (PPs).

1.3 Overview

The BIG-IP device is a port-based, multilayer switch with multiple ports and a powerful host system for advanced processing. The system reduces the need for routers and IP routing by managing traffic at the data-link layer (Layer 2). The multilayer capability of the BIG-IP system provides the ability for the system to process traffic at all OSI layers. The BIG-IP system performs basic Layer 4 load balancing and is fully capable of managing traffic at Layer 7. The system performs IP routing at Layer 3 when needed, and manages TCP and application traffic at Layers 4 and 7.

The BIG-IP system provides the ability to monitor the devices for which it manages traffic and provide audit trails relating to the use of network resources. BIG-IP information flow control rules ensure that critical connections using protocols such as HTTP, HTTPS, LDAP, SNMP, SMTP, and FTP reach a destination server that responds properly.

The BIG-IP system also enhances network security through features such as Denial of Service (DoS) protection and application filters. In addition to these features, the Network Administrator can configure the BIG-IP appliance to offload processor intensive SSL processing from backend servers and secure traffic destined to the server pools based on a variety of encryption algorithms.

The TOE employs a proprietary BIG-IP operating system that further protects the system through intelligent application resource restrictions.

The BIG-IP® system is provides a wealth of features which provide performance enhancements, which are non-security related and therefore are not evaluated as part of the Common Criteria Evaluation. These include: the ability to load balance and optimize network and application traffic by using compression, caching data, using session persistence, and other traffic optimization techniques. In addition, monitors provide the ability to route connections around

[1] Common Criteria (CC) for Information Technology Security Evaluation – January 2004, Version 2.2.

slower or degraded resources, and as a result, critical connections are made using the optimal route. The output of the monitors provides the ability for the Network Administrator to view network efficiency.

The BIG-IP appliance may be configured with an Application Security module which integrates Web application security with F5's application traffic manager, however, this option (Application Security Module) is excluded from the Common Criteria Evaluated configuration.

1.4 Organization

Section	Title	Description
1	Introduction	Provides an overview of the security target.
2	TOE Description	Defines the hardware and software that make up the TOE, and the physical and logical boundaries of the TOE.
3	TOE Security Environment	Contains the threats, assumptions and organizational security policies that affect the TOE.
4	Security Objectives	Contains the security objectives the TOE is attempting to meet and the corresponding rationale.
5	IT Security Requirements	Contains the functional and assurance requirements for this TOE and the corresponding rationale.
6	TOE Summary Specification	A description of the security functions and assurances that this TOE provides and the corresponding rationale.
7	PP Claims	Protection Profile Conformance Claims
8	Rationale	Contains pointers to the rationales contained throughout the document.

Table 1: ST Organization and Description

1.5 Document Conventions

The CC defines four operations on security functional and assurance requirements. The conventions below define the conventions used in this ST to identify these operations. When NIAP interpretations are included in requirements, the changes from the interpretations are displayed as refinements.

Assignment: **indicated with bold text**

Selection: indicated with underlined text

Refinement: ***additions indicated with bold text and italics***

deletions indicated with strike-through ~~bold text and italics~~

Iteration: indicated with typical CC requirement naming followed by a lower case letter for each iteration (e.g., FMT_MSA.1a)

The explicitly stated requirements claimed in this ST are denoted by the ".EXP" extension in the unique short name for the explicit security requirement.

1.6 Document Terminology

Please refer to CC Part 1 Section 2.3 for definitions of commonly used CC terms.

1.6.1 ST Specific Terminology

Address Resolution Protocol	A network protocol, which maps a network layer protocol address to a data link layer hardware address.
Administrator	Role applied to user with full access to all aspects of the BIG-IP appliance. Member of Administrative Users definition.
Administrative Users	This term connotes within this ST an Administrative User of the BIG-IP appliance. Members of this grouping term include: Administrator, Operator and Guest.
Application Security Module	The BIG-IP Application Security Module (ASM) runs on the BIG-IP application traffic management platform, providing robust application security with BIG-IP traffic management capabilities in a single system without the need to buy or install more hardware. EXCLUDED from the Common Criteria Evaluated configuration.
Authenticated Traffic User	This term connotes a User of the traffic which traverses the BIG-IP appliance, not a direct User of the appliance itself, which is required to authenticate through the TSF prior to accessing backend server resources. This is a role within the BIG-IP appliance and is a member of the traffic users grouping term.
Back-end Servers	Within this ST, this term refers to the group of application servers, organized in Pools, which are served by the BIG-IP

	appliance. The effective use of the BIG-IP appliance would result in increased availability for traffic users to these resources.
Content Server	Within this ST, a content server refers to the BIG-IP application client servers which are grouped in Pools as illustrated in Figure 2 and 3.
iRules™	An iRule is a user-written script that controls the behavior of a connection passing through the LTM system. iRules™ are an F5 Networks feature and are frequently used to direct certain connections to a non-default load balancing pool. However, iRules can perform other tasks, such as implementing secure network address translation and enabling session persistence. iRules can define criteria for pool-member selection, as well as perform content transformations, logging, and custom protocol support.
Local traffic management	The process of managing network traffic that comes into or goes out of a local area network (LAN), including an intranet.
Node	An application client server within the BIG-IP® managed environment
Operator	Role applied to the User with limited access to the appliance. This role has read only access to TSF and beyond that may only enable/disable Nodes. The Operator is a member of the Administrative Users definition.
OCSP	A scheme for maintaining the security of a server and other network resources
OneConnect™	A traffic management feature, OneConnect™ uses session keep-alive to reduce overhead on the network, server, and client by maintaining a single TCP connection for HTTP traffic.
Pool	A grouping of Nodes or application server clients
Pool Nodes	This term refers to Nodes which are assigned to one or more Pools.
Protocol Aware	This term refers to the fact that the TMM subsystem can readily identify protocols that flow on top of TCP, such as HTTP, FTP, and routing protocols. Since TMM's functionality includes

	decoding these protocols, extra information about the traffic stream can be extracted.
SSL Traffic Offloading	Within this security target, this term refers to the BIG-IP appliance providing SSL session termination at the appliance rather than at the backend servers. This allows all SSL processing to occur at a single point on the TOE appliance rather than multiple backend servers. This may also include SSL re-encryption of the traffic to the backend server when so configured.
Traffic Authentication	This term refers to authentication functions based on HTTP user name/password and SSL certificate credentials
Traffic User	This term connotes a user of the traffic which traverses the BIG-IP appliance but not a direct user of the appliance itself. Members of this termed group include: authenticated traffic users and unauthenticated traffic users.
Unauthenticated traffic user	Role within the BIG-IP appliance to indicate a User of traffic flowing through the TOE to backend servers which does not require authentication support from the BIG-IP appliance.

1.6.2 Acronyms

ARP	Address Resolution Protocol
HMAC	Keyed-hash message authentication code
LTM	Local Traffic Management
GTM	Global Traffic Management
VLANs	Virtual Local Area Networks
VNIC	Virtual Network Interface Card (driver)
TCP	Transmission Control Protocol
GUI	Graphical User Interface
OCSP	Online Certificate Status Protocol

OS	Operating System
SNAT	Secure Network Address Translation
SSL	Secure Socket Layer
TLS	Transport Layer Security
HTTP	Hypertext Transport Protocol
HTTPS	Hypertext Transport Protocol (Secure)
LDAP	Lightweight Directory Access Protocol
SSH	Secure Shell
OpenSSH	Open Secure Shell
SMTP	Simple Mail Transfer Protocol
SFP	Security Function Policy
FTP	File Transfer Protocol
CC	Common Criteria
TOE	Target of Evaluation
RADIUS	Remote Authentication Dial In User Service
DoS	Denial of Service
OSI	Open Systems Interconnection
URI	Uniform Resource Indicator

1.7 Common Criteria Product type

The TOE is a Traffic Management appliance classified as a **Switch/Router** for Common Criteria. The TOE includes both hardware and software components.

2 TOE Description

2.1 Overview

The TOE is a hardware and software based traffic management appliance that provides a highly configurable method of selective rule based routing,, traffic analysis and response, and bulk SSL processing capabilities. Through effective implementation of the BIG-IP Appliance, users can avoid additional infrastructure expense through effective use and traffic management of existing resources. The F5 BIG-IP appliance provides efficiency gains through local traffic management techniques (LTM)) and offloading processes, such as SSL processing, from back-end servers to result in increased resource availability, thereby allowing increased traffic utilization from existing back-end server resources.

2.2 Architecture Description

The BIG-IP system architecture is divided into the following sections in this ST:

- BIG-IP Hardware
- Traffic Management MicroKernel
- VLANs
- Pluggable Authentication Module (PAM)
- Virtual Network Interface Card (VNIC)
- Traffic Management Operating System (TM/OS)

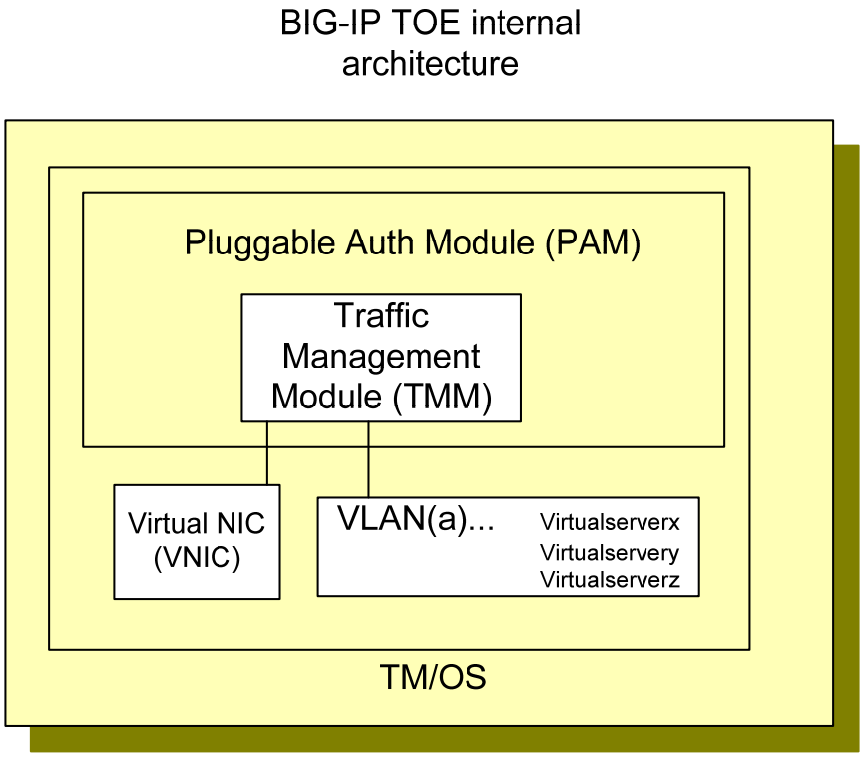

Figure 1: TOE Internal Architecture – software components

2.2.1 TOE Hardware

2.2.1.1 BIG-IP Hardware Device

The BIG-IP hardware device is a port-based, multilayer switch. It features dual AMD® Opteron™ processors contained within a forced fan-cooled chassis. The 6400 platform (applicable to this ST) contains 16 copper, Gigabit level ports and 4 fiber optic Gigabit level ports. Additionally, a single Ethernet management network interface is included. One DB9 serial port is for console access and another DB9 serial port used for redundant pair communication. Layer 4 processing is accelerated using the F5 Packet Velocity™ ASIC. A hardware based Cavium® Nitrox™ cryptographic module is included for SSL handshaking and bulk encryption. Through bulk encryption techniques, SSL encryption processes are offloaded to the BIG-IP device which can manage encryption for many sessions at once, leading to greater availability on the host servers.

2.2.2 TOE Software

All of the TOE software is maintained within the TOE appliance and is made up of a single BIG-IP software release. The following software subsystems are all consolidated within the BIG-IP release:

2.2.2.1 Traffic Management MicroKernel (TMM)

The Traffic Management MicroKernel is the core of the BIG-IP's Local Traffic Management (LTM) system. It routes traffic between nodes and pools. TMM is protocol aware, meaning it can readily identify protocols that flow on top of TCP, such as HTTP, FTP, and routing protocols. Through this, level 7 communication protocols are identified and BIG-IP can use this information to enhance HTTP traffic with compression, SSL termination, OneConnect™, iRules, or traffic authentication. Traffic can be authenticated via LDAP and RADIUS or SSL client certificate authentication via LDAP over SSL.

Key features of the Traffic Management MicroKernel (TMM) include:

- Balancing traffic to tune and distribute the server load on a network for scalability.
- Delegation of standard server tasks to the TMM, such as HTTP data compression, SSL session authentication, and SSL encryption to improve server performance.
- Establishing and managing session and connection persistence.
- Handling application-traffic authentication and authorization functions based on User name/password and SSL certificate credentials.
- Managing packet throughput to optimize performance for specific types of connections.
- Improving performance by aggregating multiple client requests into a server-side connection pool. This aggregation of client requests is part of the BIG-IP OneConnect™ feature.
- Applying configuration settings to customize the flow of application-specific traffic (such as HTTP and SSL traffic).
- Customizing the management of specific connections according to user-written scripts based on the industry-standard Tool Command Language (TCL).

Through the use of proprietary functions, iRules™, traffic can be routed based on a rules driven configuration to optimize traffic flows based on pre-configured conditions. iRules are a user-written script that controls the behavior of a connection passing through the LTM system. There are no restrictions on the use of iRules for Common Criteria.

These features use the BIG-IP Virtual LAN and Virtual Server infrastructure (see 2.2.3) to increase network efficiency.

2.2.2.2 Virtual Local Area Networks (VLANs)

Central to the functionality of the TOE is the creation of VLANs for developing the architecture needed for traffic management and load balancing. A VLAN is composed of multiple network ports and contains a series of virtual servers configured based on the load balancing scheme. Within the system are virtual servers and load balancing pools.

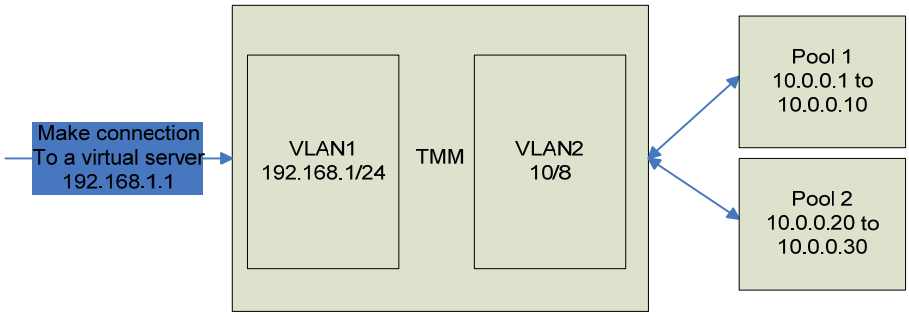

Figure 2: VLAN architecture demonstrating how the BIG-IP uses Virtual LANs to optimize traffic routing

Virtual servers receive incoming traffic; perform basic source IP and destination IP address translation, and direct traffic to nodes, which are grouped together in load balancing pools.

A virtual server receives a client request, and instead of sending the request directly to the destination IP address specified in the packet header, it sends it to any of several content servers that make up a load balancing pool. Virtual servers increase the availability of resources for processing client requests.

A virtual server can enable compression on HTTP request data as it passes through the LTM system, or decrypt and re-encrypt SSL connections and verify SSL certificates. For each type of traffic, such as TCP, UDP, HTTP, SSL, and FTP, a virtual server can apply an entire group of settings, to affect the way that the LTM system manages that traffic type.

The BIG-IP system uses Virtual Servers to:

• Distribute client requests across multiple servers to balance server load
• Apply various behavioral settings to multiple traffic types
• Enable persistence for multiple traffic types
• Direct traffic according to User-written iRules™

There are 2 types of virtual servers configured for TOE operation: Host and Network.

A *network virtual server* is a virtual server whose IP address has no bits set in the host portion of the IP address (that is, the host portion of its IP address is **0**).

> There are two kinds of network virtual servers: those that direct client traffic based on a range of destination IP addresses, and those that direct client traffic based on specific destination IP addresses that the LTM system does not recognize.

A *host virtual server* represents a specific site, such as an Internet web site or an FTP site, and it load balances traffic targeted to content servers that are members of a pool.

2.2.2.3 Pluggable Authentication Module (PAM)

The pluggable authentication module running under the BIG-IP operating system is a suite of shared libraries that enable the TOE Administrator to choose how applicable content server clients authenticate traffic. PAM allows separation of the authentication function from the core LTM system. The Administrator selects the appropriate authentication scheme to use to authenticate application traffic coming into the BIG-IP system. PAM is also used for authentication of administration sessions via the administration management port to the TOE operating system.

Local Traffic Management (LTM) modules, within the TMM subsystem, control access to authenticate traffic users and their client requests and to control User and application access to server resources.

These authentication modules provide the ability to use a remote system to authenticate or authorize application requests that pass through the LTM system.

The authentication modules provided in the TOE are as follows:

• **An LDAP module**
Uses a remote LDAP server to perform User name/password User authentication.

• **A RADIUS module**
Uses a Remote Authentication Dial In User Service (RADIUS) server to perform User name/password User authentication.

• **An SSL Client Certificate LDAP module**
Uses a remote LDAP server to perform SSL certificate-based authorization of client SSL traffic.

The following authentication module is not evaluated as part of the CC Evaluated Configuration:

OCSP module
Uses a remote Online Certificate Status Protocol (OCSP) server to provide up-to-date SSL certificate revocation status for the purpose of authenticating client and server SSL traffic.

2.2.2.4 Virtual Network Interface Card (VNIC)

The VNIC is a BIG-IP operating system driver that transfers network packets to the TMM where load balancing decisions are made. If the TMM subsystems determine that the packets are destined for other portions of the TM/OS, the VNIC forwards the packet to the OS Kernel for TCP stack deconstruction and processing by the appropriate daemon.

2.2.2.5 Traffic Management Operating System (TM/OS)

The TM/OS represents the Traffic Management Operating System functionality. The TM/OS is a customized implementation of a Linux OS. The security enhanced proprietary BIG-IP operating system, based on configuration settings made during the build, restricts access of

services, modules and applications to those authorized for execution within the TOE Operating System (OS). This allows basic OS enforcement mechanisms to protect the OS, from outsider or insider threats related to unused operating system components. The end result is an extra layer of security; even if an application has vulnerability, an attacker who exploited that vulnerability would have no permissions in addition to that of the application. This is a fixed aspect of the software build implemented by F5 at the time of software development and build process.

The TM/OS interfaces the Node Web Applications with the traffic manager functions of the BIG-IP system through the pluggable authentication module (PAM).

The BIG-IP Appliance functionality provides a translation function between the server and the client applications to optimize data transfer based on conditions that are continuously verified through a system of monitors.

A monitor can be either a health monitor or a performance monitor, designed to check the status of a pool, pool member, or node on an ongoing basis, at a set interval. If a pool member or node being checked does not respond within a specified timeout period, or the status of a pool member or node indicates that performance is degraded, the LTM system can redirect the traffic to another pool member or node.

2.2.3 Statement of Non-Bypassibility of the TSF

TOE security functions cannot be bypassed. Through proper configuration of the appliance within the network all traffic destined to back ends server resources must first travel through the TOE. Traffic enters the TOE through Ethernet or Fiber ports on the front of the appliance and is routed based on information flow control rules to backend server resources. Traffic flowing through the appliance is thoroughly isolated from the TOE security management functions, security attributes and associated TSF data as it travels only through the TMM subsystem. Administrator sessions flow through a separate path to access the configuration data within the Master Control Process daemon within the Traffic Management Operating System.

All access to TOE security functions requires Administrator level access to the TOE. The BIG-IP authentication process ensures that a secure User name and password combination must be entered prior to allowing any changes to TSF settings. This applies to GUI sessions which are secured via SSL. The authentication process for the Administrator role is maintained within the TOE operating system using the Pluggable Authentication Module (PAM) for added security. A dedicated Administrative domain is maintained for Administrator role access, further restricting possible bypass of TSF functions. Administrator console access, which is used only during installation process, is secured via the SSH protocol using the AES algorithm to ensure data is not corrupted or bypassed in transit.

2.3 Physical Boundaries

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

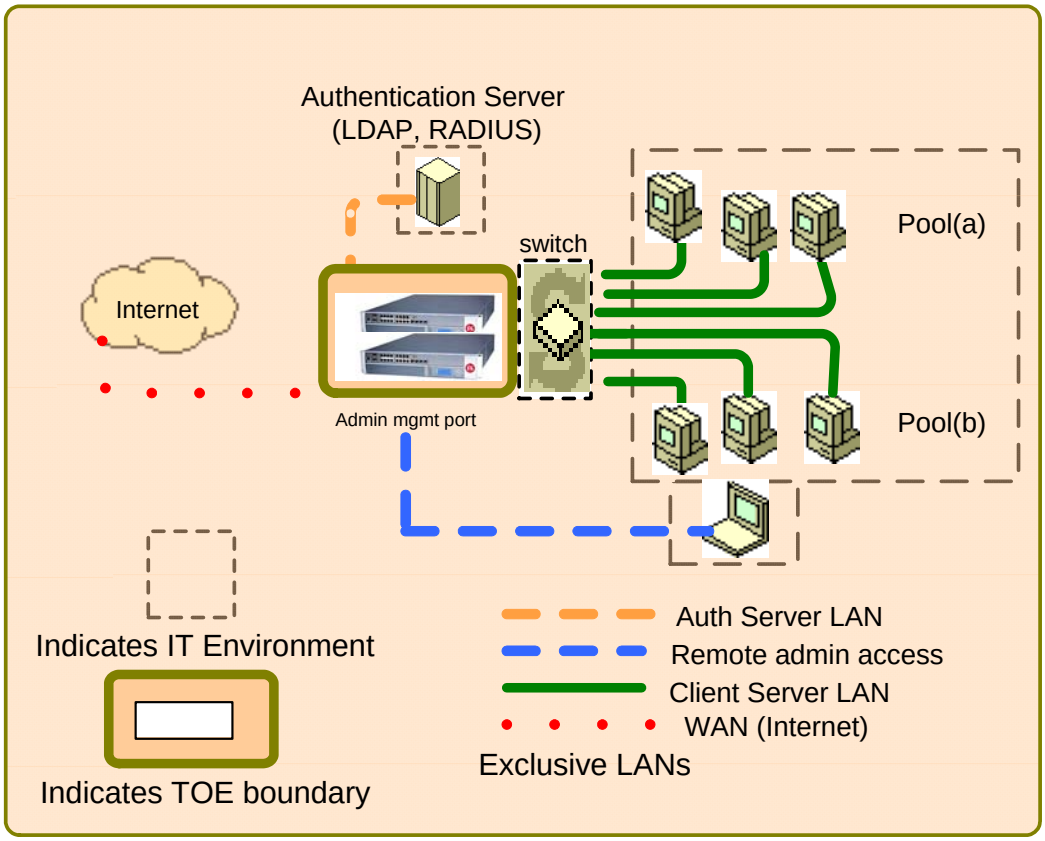

Figure 3: TOE Physical Boundaries

In terms of logical boundaries, the following table enumerates the division between services

provided *by* the TOE and services provided *to* the TOE from the Operating Environment:

Functional Area	Services Provided *By* The TOE	Services Provided *To* The TOE By The Operating Environment
Identification and Authentication	Identification and authentication to the BIG-IP appliance (local) using the Linux based OS. Also includes authentication of back end servers when load balancing is necessary.	Remote authentication servers that store and protect user account parameters.
Audit	A collection of security relevant traffic and security related events such as System Events, Packet Filter Events, Local Traffic Events and Audit Events.	Optional storage and protection of audited records (not included in the evaluated configuration).
Information Flow Control	Information Flow Control policies that are configured in the TOE to assure that traffic flows only to and from properly authenticated and authorized sources/destinations.	Back-end servers located in the resource pool.
Security Management	Graphical user interfaces accessible by the Administrator that support configuration and modification of the options of the TOE. These modules provide services to configure TOE resources based on individual nodes, connection pools and protocol based traffic profile settings which support the Information Flow Control according to the appropriate authorized user/authorized role	Administrator Workstation Operating System Supported Browser
Secure Communications	Communication techniques in the TOE for administrator remote access via SSL or SSH. This is implemented using commercially available encryption algorithms and certificates.	Storage and management of SSL or SSH client application and certificate used for authentication purposes. Operating system and browser component in Admin workstation (SSL session).
Secure Traffic	The TOE secures traffic using a hardware based security processor for SSL traffic, a software based TMM MicroKernel within the BIG-IP operating system. This security feature is used when load balancing the system and may be configured to terminate SSL at the appliance, thereby offloading this process from the back-end servers.	Pool resources contain SSL or SSH client and certificates.
Protection of the TOE	Encryption for transmission between separated parts of the TOE	Storage of the certificates used for SSL communication.

Table 2: TOE Services vs. Environment provided services

2.3.1 Hardware Components

This table identifies hardware components and indicates whether or not each component is in the TOE.

TOE or Environment	Component	Description
TOE	BIG-IP Hardware	2 processor 6400 series appliance
Environment	Authentication Server	Applicable Auth. Server (LDAP, RADIUS)
Environment	Application Servers	Node application servers – Web Servers
Environment	Remote CPU	Remote PC or Laptop for remote admin access
Environment	Network Switch(s)	Switch between TOE and Application Servers

Table 3: Hardware Components

2.3.2 Software Components

This table identifies software components and indicates whether or not each component is in the TOE.

TOE or Environment	Component	Description
TOE	BIG-IP software version 9.2.3 + Hotfix CR69440 (aka build 142.0)	Software package installed on appliance, includes all TOE items listed below: TM/O.S. (Linux 2.4.21) Operating System with F5 Kernel changes, Apache Web server 2.0.53 Traffic Manager MicroKernel (v1.0) F5 Traffic Manager Kernel in Linux VNIC (v1.0)Virtual Network Card software Pluggable Authentication module (v.75)Linux authentication enhancement

Environment	Authentication Server OS	Authentication Server Operating System
Environment	Server Applications	Host Server Applications
Environment	Microsoft Windows XP, Server 2003 (or) Unix/Linux any versions that support browsers listed below	Remote Computer Operating System
Environment	Microsoft® Internet Explorer™, version 6.x and later (or) Netscape® Navigator™, version 7.1, Mozilla™, Firefox™, and Camino™.	Remote Computer Browser

Table 4: Software Components

2.3.3 Guidance Documents

The following guidance documents are provided with the TOE upon delivery in accordance with EAL 2 requirements:

- AGD_ADM - Administrator Guidance –
  - BIG-IP® Network and System Management Guide version 9.2.3 MAN-0185-02
  - Configuration Guide for Local Traffic Management version 9.2.0 MAN-0182-00
  - Platform Guide: 1500, 3400, 6400, and 6800 MAN-0183-00 August 16, 2006.
  - Configuration Worksheet PUB-0090-02 0905
  - Common Criteria Supplement EAL2 F5 Networks BIG-IP® Local Traffic Manager 6400 High Availability pair (qty 2) Document ID: 05-948-R-0134
- ADO_IGS – Installation Guidance –
  - Installation, Licensing, and Upgrades for BIG-IP® Systems Version 9.2 MAN-0184-00
  - BIG-IP® Quick Start Instructions PUB-0089-03 1205
  - Common Criteria Supplement EAL2 F5 Networks BIG-IP® Local Traffic Manager 6400 High Availability pair (qty 2) Document ID: 05-948-R-0134

***Note: Product usage is transparent to network users therefore this requirement (AGD_USR.1) requirement is vacuously satisfied (ref: PD-0106: Situations Where AGD_USR May Be Vacuously Satisfied)**

All documentation delivered with the product is germane to and within the scope of the TOE.

2.4 Logical Boundaries

This section contains the product features and denotes which are in the TOE.

2.4.1 Identification and Authentication

The BIG-IP TOE allows access to TSF functions only to those Users with the role of Administrator or Operator who are identified and authenticated through the BIG-IP operating system. Operators may only enable or disable Nodes, all other control of TSF functions is limited to the Administrator. Account type and associated roles determine access level.

Both local (within the appliance) and remote identification and authentication mechanisms are available; however, Administrator role access is managed locally within the BIG-IP for security purposes.

The BIG-IP manages identification and authentication through the Linux based operating system for the web-based UI and SSH/console access.

The types of remote authentication servers that can be used to store user accounts for BIG-IP TOE Administrators are:

- Active Directory™ servers (not included in the Evaluated Configuration)
- Lightweight Directory Access Protocol (LDAP) servers
- Remote Authentication Dial-in User Service (RADIUS)

The Common Criteria Evaluated Configuration specifies the use of an external authentication server in the IT Environment (either LDAP or RADIUS) for authenticating all users except the Administrator role.

Authenticated traffic flow is discussed below in Section 2.4.3 Information Flow Control. This usage of “authentication” relates to data protection and not the Identification and Authentication security function.

2.4.2 Audit

The TOE generates 4 types of audit logs: System Events, Packet Filter Events, Local Traffic Events and Audit (type) Events. Within this ST, these categories of audit logs may be collectively referred to as Audit logs or Audit records, unless otherwise stated. Additional information relating to Local Traffic and Packet Filter events are contained in Section 6.1.2: Audit.

System Events relate to underlying (Linux) Operating System events, Packet Filter Events pertain to events generated through Packet Filter rules in effect during operation; Local Traffic Events relate to events generated through Local Traffic Management functions of the TOE; Audit (type) Events pertain to logging of configuration changes within the appliance.

TSF related changes can only be executed by Administrator or Operator roles and are logged by the BIG-IP operating system (audit (type) events log). Operators may enable/disable nodes but may not make any other TSF changes. Audit records are stored local to the appliance and may be exported to external storage devices in the IT Environment. This option is not included in the CC Evaluated Configuration.

Local Traffic and Audit (type) logs may be configured to various logging levels based on the type of events will trigger the generation of a log record. Audit (type) logs may be disabled; however, all other log types do not include this capability. The Common Criteria Evaluated configuration requires that all logs are enabled and specifies minimum logging level in Common Criteria Administrator Guidance.

Audit records are generated for underlying Operating System events, Packet Filter events, traffic management events and Administrator related transactions. Audit records within the TOE may be selectively filtered and searched based on various characteristics. Audit records are accessed through the Administrator Console GUI. Administrative Users (Administrator, Operator, and Guest) are allowed access to query audit records. Audit records cannot be modified or deleted by any user. Protection of the audit system is provided by the underlying BIG-IP operating system and access controls.

2.4.3 Information Flow Control

Information Flow Control policies are configured in the TOE to assure that traffic flows only to and from properly authenticated and authorized sources/destinations. This is implemented primarily through the configuration of the VLANs and associated virtual servers.
Based on the type of traffic, the BIG-IP will implement the appropriate flow control policy based on Administrator configuration. Options include: SSL secure traffic, Content based compression of HTTP traffic, and Rules based Pool selection to assure highest availability and processing speed. Back-end Servers are managed in resource Pools as depicted in Figure 3 and flow control policies are enforced according to Pool memberships.

Standard load balancing schemes are included in addition to configurable selections.

In all cases, the TOE authenticates Back-end Servers through either SSL session keys and/or by TM/OS authentication. The TOE will enforce the same security policy within all Pool members.

2.4.4 Security Management

Security Management is managed by authorized Administrators utilizing the BIG-IP operating system through the Administrator Console GUI. Access to the Security Management user interface is secured by the core Operating System authentication scheme and role based permissions. Access to Security Management functions is addressed through the PAM module functionality within the BIG-IP operating system. Access is coordinated utilizing Role based access control mechanisms. Access to the Administrator Console is supported through a web GUI within the APACHE operating environment (integrated with the TM/OS) or through an SSH connection.

A series of traffic management configuration options allow the Administrator to configure

resources based on individual nodes, connection pools and protocol based traffic profile settings which support the Information Flow Control requirements listed in section 2.4.3 and enforced through the unauthenticated/authenticated traffic management SFP.

Within the PAM module, rules are established for the creation of passwords assuring a minimum length, type and lifetime for system passwords. Password policy enforced is realized through technical means for user except for the Administrator role, where procedural compliance to this policy is required through administrator guidance.

2.4.5 Secure Communications

Secure Communication techniques are made available in the TOE for administrator access via SSL or SSH. An Administrator management port is provided for dedicated local access.

By default, the TOE uses uniquely generated 1024 bit RSA keys with self-signed certificates for securing communications with the web-based UI. An Administrator may generate new keys of 512, 1024 or 2048 bits. These keys may also be signed by any signing authority.

2.4.6 Secure Traffic

The TOE secures traffic using a hardware based security processor for SSL traffic, a software based TMM MicroKernel within the BIG-IP operating system for SSL handshaking, and an OpenSSL library for support local X509 certificate verification.

To increase availability and capacity within the supported back-end servers, the TOE may be configured to terminate SSL at the appliance thereby offloading this process from the back-end servers. Through this function, the TOE establishes and terminates SSL traffic on behalf of the back-end server pools. When SSL termination is selected within the TOE, certificate verification and revocation checks are executed within the TOE.

SSL session persistence can be enabled based on configurable Client or Server SSL persistence profiles.

2.4.7 Protection of TOE Functions

Physical and logical protection of the TOE is required to assure that TOE related security functions are not bypassed or altered. This is provided by the TOE through the secure communication methods described in 2.4.6.

2.5 Items Excluded from the TOE (security relevant)

This section identifies any **security relevant** items that are specifically excluded from the TOE:

1. Application Security Module
2. Use of the CLI (via console or SSH) for any purpose other than initial IP configuration during installation
3. Authentication of traffic users on the appliance (these users use external authentication

servers).

4. Offloading of audit logs to an external server or storage resource.
5. Support Account type for F5 use in supporting the appliance (disabled by default)
6. Use of Active Directory Authentication servers
7. The use of an OCSP server in the IT Environment.
8. The following aspects of BIG-IP functionality/protocols are not included in the Evaluated Configuration:
    - SNMP (Remote Management of BIG-IP): administrative use of SNMP
    - Trunk (link aggregation)
    - Packet Filter configuration & Administrator usage (audit events are allowed)
    - Archives (relating to Backup Configurations)

2.6 Items not Evaluated (not security relevant)

This section identifies aspects of the TOE that were not evaluated as part of the Common Criteria Evaluation. Items in this category include those features which may provide significant functional capability within the TOE but are not security relevant and are therefore not included/evaluated in the Common Criteria Evaluation:

- Optimization of network and application traffic
- HTTP compression
- Caching
- Aggregation of client requests
- Routing around slower or degraded routes
- Selective data compression

3 TOE Security Environment

The TOE is intended to be used either in environments in which, at most, sensitive but unclassified information is processed, or the sensitivity level of information in both the internal and external networks is equivalent.

This section contains assumptions regarding the security environment and the intended usage of the TOE and threats on the TOE and the IT environment.

3.1 Assumptions

The assumptions are ordered into three categories: personnel assumptions, physical environment assumptions, and operational assumptions.

3.1.1 Personnel Assumptions

A.ADMIN	The Administrators are appropriately trained, not careless, not willfully negligent, non hostile and follow and abide by the instructions provided in the guidance documentation.

3.1.2 Physical Environment Assumptions

A.LOCATE	Appropriate physical security is provided commensurate with value of the IT assets protected by the TOE and the value of the information stored or processed through the BIG-IP Appliance.

3.1.3 Operational Assumptions

A.USE	The BIG-IP Appliance is dedicated to its primary function and does not provide any general purpose computing or storage capabilities.

3.2 Threats

The TOE or IT environment addresses the threats identified in this section. 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.SEC_FUNC	Administrators may make changes to TOE security functionality without accountability.
T.MASK	An unauthorized user may masquerade as an authorized user or an authorized IT entity to gain access to data or TOE resources.

T.CONFIG	Unintentional errors in implementation of the TOE deployment may occur, leading to flaws which may be exploited by a malicious User or program.
T. PRIORITY	Traffic may be routed to backend servers without prioritization resulting in poor quality of service and loss of backend server availability for concurrent sessions.
T.RESOURCE_X	A malicious process or user may block others from TOE system resources (e.g., connection state tables) via a resource exhaustion denial of service attack.
T.TOE_FAIL	The failure of a TOE appliance may result in loss of traffic and/or failure to meet the TSF.
T.TSF_COMP	An attacking User or process may cause, through an unsophisticated attack, TSF data, or executable code to be inappropriately accessed (viewed, modified, or deleted).
T.UNID_ACTION	An Administrator may not have the ability to notice potential security violations, thus limiting the administrator's ability to identify and take action against a possible security breach.
T.UNSEC_DATA	Data Transfer between the BIG-IP Appliance and Administrator workstation may be modified or disclosed in transit.

3.3 Organizational Security Policies

There are no Organizational Security Policies for this TOE.

4 Security Objectives

This chapter describes the security objectives for the TOE and the TOE's operating environment. The security objectives are divided between TOE Security Objectives (for example, security objectives addressed directly by the TOE) and Security Objectives for the Operating Environment (for example, security objectives addressed by the IT domain or by non-technical or procedural means).

4.1 Security Objectives For The TOE

This section defines the IT security objectives that are to be addressed by the TOE.

Security Objective	Description
O.AUDIT_GEN	The TOE will provide the capability to detect and create records of security relevant events associated with Users.
O. AUDIT_PROT	The TOE will provide the capability to protect audit information.
O. AUDIT_REVIEW	The TOE will provide the capability to selectively view audit information and alert the Administrator of identified potential security violations.
O.CRYPTO	The TOE will provide encryption/decryption of Administrator sessions and SSL network traffic (on behalf of backend servers) when configured for SSL offloading.
O.MANAGE	The TOE will provide all the functions and facilities necessary to support the Administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
O.SELF_PROT	The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure.
O.TIME_STAMPS	The TOE shall provide reliable time stamps and the capability for the Administrator to set the time used for these time stamps.
O.PRIORITY	The TOE shall provide mechanisms to assign a priority to each (traffic) subject traveling through the TOE and mediate access to server client's support by the TOE, by the assigned priority.
O.ROBUST_TOE	The TOE provides mechanisms that control a User's logical access to the TOE and to explicitly deny access to specific Users when appropriate.

O.RESOURCE_X	The TOE provides mechanisms to identify and thwart DoS attempts on the appliance.
O.SECURE_DATA	The TOE will establish Flow Control SFPs and secure communication methods to ensure secure and unmodified data transfer within the TOE and between the TOE and trusted IT products.
O.SAFE_FAIL	The TOE will protect the TSF in the event of all failure conditions and preserve correct operations during specified failure events.

Table 5: TOE Security Objectives

4.2 Security Objectives for the Environment

The following IT security objectives for the environment are to be addressed by the IT environment by technical means.

OE.DATA_PROT	The environment provides authentication and access control mechanisms protecting TSF data.
OE.DOMAIN_SEP	A Security Domain is established and enforced within the environment for the TSF that protects against tampering.
OE.NO _BYPASS	Information cannot flow between external and internal networks located in different enclaves without passing through the TOE.

The following non-IT security objectives for the environment listed below are to be satisfied without imposing technical requirements on the TOE. Thus, they will be satisfied through application of procedural or Administrative measures.

OE.ADMIN	Sites using the TOE will ensure that the authorized Administrators are appropriately trained, not careless, not willfully negligent, non-hostile and follow all instructions within administrative guidance.
OE.DEDICATED	Administrators will assure that the BIG-IP Appliance is dedicated to its primary function and does not provide any general purpose computing or storage capabilities.

OE.PHYSICAL	The TOE is physically secure and physical access is controlled to assure only authorized Administrators have access.

4.3 Mapping of Security Environment to Security Objectives

The following table represents a mapping of the threats, assumptions, and OSPs to the security objectives defined in this ST.

	A.USE	A.ADMIN	A.LOCATE	T.SEC_FUNC	T.MASK	T.UNID_ACTION	T.CONFIG	T.PRIOIRTY	T.TSF_COMP	T.TOE_FAIL	T.RESOURCE_X	T.UNSEC_DATA
O.AUDIT_GEN				☑		☑						
O. AUDIT_PROT				☑		☑						
O. AUDIT_REVIEW				☑		☑						
O.CRYPTO												☑
O.MANAGE							☑					
O.PRIORITY								☑				
O.SELF_PROT									☑			
O.TIME_STAMPS				☑		☑						
O.ROBUST_TOE					☑							
O.RESOURCE_X											☑	
O.SECURE_DATA												☑
O.SAFE_FAIL										☑		
OE.DATA_PROT					☑							
OE.DOMAIN_SEP									☑			
OE.NO_BYPASS									☑			☑
OE.ADMIN		☑										
OE.PHYSICAL			☑									
OE.USE	☑											

Table 6: Threats & IT Security Objectives Mappings

4.4 Rationale For Threat Coverage

This section provides a justification that for each threat, the security objectives counter the threat.

T.SEC_FUNC	O.AUDIT_GEN, O.AUDIT_PROT, O.AUDIT_REVIEW mitigates this threat by creating audit record data, protecting it from loss or modification, providing the ability to review to identify any changes to TSF related functions and/or security related events. O.TIME_STAMPS supports the audit function by assuring that accurate time stamps are provided for audit records generated.
T.PRIORITY	O.PRIORITY mitigate this threat by assigning a priority to each traffic subject managed by the TOE and assuring traffic managed by the TOE to application server clients is mediated on the basis of the traffic subject's assigned priority
T. MASK	O.ROBUST_TOE helps mitigate this threat by providing mechanisms that control access to the TOE and to explicitly deny access when appropriate. OE.DATA_PROT provides access control mechanisms protecting TSF data in the TOE environment.
T.CONFIG	O.MANAGE provides that the functions and facilities needed for secure configuration are provided by the TOE and TSF is protected from unauthorized use.
T.RESOURCE_X	O.RESOURCE_X mitigates this threat by providing mechanisms within the TOE to identify and thwart DoS attacks.
T.TSF_COMP	O.SELF_PROT mitigates this threat by maintaining a domain for the BIG-IP Appliance execution that protects and its resources from external interference, tampering or unauthorized disclosures through its own interfaces. OE.NO_BYPASS further mitigates this threat by assuring that TOE security mechanisms cannot be bypassed through the IT Environment. OE.DOMAIN_SEP further mitigates this threat by assuring that a Security Domain is established and enforced within the IT Environment for the TSF that protects against tampering.

T.TOE_FAIL	O.SAFE_FAIL mitigates this threat by preserving correct TSF operations and/or protecting the TSF in the event of a failure of a single appliance in a redundant pair configuration.
T.UNID_ACTION	O.AUDIT_GEN, O.AUDIT_PROT, O.AUDIT_REVIEW mitigates this threat by creating audit record data, protecting it from loss or modification, providing the ability to review to identify any changes to TSF related functions and/or security related events. O.TIME_STAMPS supports the audit function by assuring that accurate time stamps are provided for audit records generated.
T.UNSEC_DATA	O.SECURE_DATA mitigates this threat by the implementation of secure communication methods (SSL/SSH) for all communications between the TOE and Administration Workstation. O.CRYPTO further mitigates this threat by specifying that the TOE will provide encryption/decryption of Administrator sessions and SSL network traffic (on behalf of backend servers) when configured for SSL offloading. OE.NO_BYPASS assures that that all traffic cannot flow between internal and external networks without passing through the TOE thereby protecting TOE SFP execution.

4.5 Rationale For Organizational Policy Coverage

There are no Organizational Policies for this TOE.

4.6 Rationale For Assumption Coverage

This section provides a justification that for each assumption, the security objectives for the environment cover that assumption.

A.ADMIN:	This assumption is restated in the form of OE.ADMIN which specifies that the TOE Environment Administrator is not willfully negligent, non-hostile and follows applicable instructions.
A.LOCATE	This assumption is restated in the form of OE.PHYSICAL which states that the TOE is physically secure and physical access is controlled to assure only authorized Administrators have access.
A.USE	This assumption is restated in the form of OE.USE assuring that the BIG-IP Appliance is dedicated to its primary function.

5 IT Security Requirements

The security requirements that are levied on the TOE and the IT environment are specified in this section of the ST. These security requirements are defined in Sections 5.1 - 5.4.

TOE Security Functional Requirements (from CC Part 2)	
FAU_ARP.1	Security alarms
FAU_SAA.1	Potential Violation Analysis
FAU_SAR.1	Audit Review
FAU_SAR.3a	Selectable audit review –Packet Filter Events Log, Local Traffic Events Log
FAU_SAR.3b	Selectable audit review – System Log
FAU_SAR.3c	Selectable audit review – Audit Log
FAU_STG.1	Protected audit trail storage
FAU_STG.4	Prevention of audit data loss
FCS_CKM.1a	Cryptographic Key Generation-Secure Traffic
FCS_CKM.1b	Cryptographic Key Generation-Administrator Sessions
FCS_CKM.1c	Cryptographic Key Generation-Asymmetric Keys
FCS_CKM.1d	Cryptographic Key Generation-Symmetric Keys
FCS_COP.1a	Cryptographic Operation-Secure Traffic
FCS_COP.1b	Cryptographic Operation-Administrator Sessions
FCS_COP.1c	Cryptographic Operation-Random Number Generator
FCS_COP.1d	Cryptographic Operation – Diffie-Hellman
FDP_IFC.1a	Subset information flow control-unauthenticated
FDP_IFC.1b	Subset information flow control-authenticated
FDP_IFF.1a	Simple security attributes-unauthenticated
FDP_IFF.1b	Simple security attributes-authenticated
FDP_UCT.1	Basic data exchange confidentiality
FDP_UIT.1	Data exchange integrity
FIA_ATD.1	User Attribute Definition
FIA_UAU.1	Timing of authentication-authenticated traffic users

FIA_UAU.2	User authentication before any action
FIA_UID.2	User identification before any action
FMT_MOF.1a	Management of security functions behaviour
FMT_MOF.1b	Management of security functions behaviour
FMT_MSA.1a	Management of Security Attributes
FMT_MSA.1b	Management of Security Attributes -Pools & VLAN
FMT_MSA.2	Secure Security Attributes
FMT_MSA.3	Static Attribute Initialisation
FMT_MTD.1a	Mgmt of TSF data - Delete
FMT_MTD.1b	Mgmt of TSF data-Modify
FMT_MTD.1c	Mgmt of TSF data-Query Audit
FMT_MTD.1d	Mgmt of TSF data-Query
FMT_SMF.1	Specification of mgmt functions
FMT_SMR.1	Security Roles
FPT_FLS.1	Failure with preservation of secure state
FPT_ITA.1	Inter-TSF availability within a defined avail metric
FPT_ITC.1	Inter-TSF confidentiality during transmission
FPT_ITI.1	Inter-TSF detection of modification
FPT_RVM.1	Non-bypassability of the TSP
FPT_SEP.1	TSF Domain Separation
FPT_STM.1	Reliable Time Stamps
FRU_FLT.1	Degraded fault tolerance
FRU_PRS.1	Limited priority of service
FRU_RSA.1a	Maximum quotas-TCP Connections
FRU_RSA.1b	Maximum quotas-BIG-IP Memory Resources
Explicitly Stated TOE Security Functional Requirements	
FAU_GEN.EXP.1	Audit data generation
FCS_COP.EXP.1	Cryptographic Support - SSL Traffic Offloading
FIA_UAU.EXP.1	Timing of authentication (Remote)

FIA_UID.EXP.1	Timing of Identification (Remote)

Table 7: Functional Requirements

5.1 TOE Security Functional Requirements

The SFRs defined in this section are taken from Part 2 of the CC.

5.1.1 Security Audit

5.1.1.1 FAU_ARP.1 Security alarms

FAU_ARP.1.1 The TSF shall take **the following action: alert the Administrator via email** upon detection of a potential security violation.

5.1.1.2 FAU_SAA.1 Potential Violation Analysis

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:
a) Accumulation or combination of **SYN flood DoS attack Threshold Activation (max = 16384)** known to indicate a potential security violation;

b) **no additional rules**.

5.1.1.3 FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide **Administrator, Operator, Guest** with the capability to read **all audit trail data** from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.1.1.4 FAU_SAR.3a Selectable audit review –Packet Filter Events Log, Local Traffic Events* Log

FAU_SAR.3.1a The TSF shall provide the ability to perform searches and sorting of audit data based on:

a) Log Type

b) Keyword filter

c) Log Level

d) Timestamp

e) Host Name

f) Service

g) Status Code

*Application Note: Specifics relating to Local Traffic and Packet Filter events are contained in Section 6.1.2 Audit

5.1.1.5 FAU_SAR.3b Selectable audit review – System Log

FAU_SAR.3.1b The TSF shall provide the ability to perform searches and sorting of audit data based on:

a) Log Type

b) Keyword filter

c) Log Level

d) Timestamp

e) Host Name

f) Service

5.1.1.6 FAU_SAR.3c Selectable audit review – Audit Log

FAU_SAR.3.1c The TSF shall provide the ability to perform searches and sorting of audit data based on:

a) Log Type

b) Keyword filter

c) Log Level

d) Timestamp

e) User Name

f) Transaction #

g) Event

5.1.1.7 FAU_STG.1 Protected audit trail storage

FAU_STG.1.1 The TSF shall protect the stored audit records from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to prevent unauthorised modifications to the stored

audit records in the audit trail.

5.1.1.8 FAU_STG.4 Prevention of audit data loss

FAU_STG.4.1 The TSF shall overwrite the oldest stored audit records and **no other actions** if the audit trail is full.

5.1.2 Cryptographic Support*

5.1.2.1 FCS_CKM.1a Cryptographic key generation-Secure Traffic

FCS_CKM.1.1a The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **RSA** and specified cryptographic key sizes **RSA with key lengths of 512, 1024, 2048 or 4096** that meet the following: **PKCS #1.**

5.1.2.2 FCS_CKM.1b Cryptographic key generation-Administrator Sessions

FCS_CKM.1.1b The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **RSA** and specified cryptographic key sizes **RSA with key lengths of 1024** that meet the following: **PKCS #1.**

5.1.2.3 FCS_CKM.1c Cryptographic Key Generation – Asymmetric Keys

FCS_CKM.1c The TSF shall generate **Diffie-Hellman asymmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm **a software random number generator (SHA-1, MD5 OpenSSL/OpenSSH based)** and specified cryptographic key sizes **default 1024 bits and maximum 4096 bits** that meets the following **none**.

5.1.2.4 FCS_CKM.1d Cryptographic Key Generation –Symmetric Keys

FCS_CKM.1d The TSF shall generate **symmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm **a software random number generator (OpenSSL based)** and specified cryptographic key sizes **minimum 56 bits, (128 bits, RC4)** that meets the following **none**.

5.1.2.5 FCS_COP.1a Cryptographic operation – Secure Traffic

FCS_COP.1.1a The TSF shall perform **Secure Traffic Encryption/Decryption** in accordance with a specified cryptographic algorithm **per (SSLv2, SSLv3 or TLS) ciphersuites listing in Appendix A** and cryptographic key sizes **as noted in Appendix A** that **meet the following: IKE RFC 2409.**

5.1.2.6 FCS_COP.1b Cryptographic operation – Administrator Sessions

FCS_COP.1.1b The TSF shall perform **Administrator Session Encryption/Decryption** in accordance with a specified cryptographic algorithm **RC4 (or) DES (or) 3DES (or) AES** and cryptographic key sizes **56 bits or greater (128 RC4)** that **meet the following: RFC 4345 (RC4), RFC 2405(DES), FIPS 46.3 (3DES), RFC 3364 (AES).**

5.1.2.7 FCS_COP.1c Cryptographic operation - Random Number Generator

FCS_COP.1.1c The TSF shall perform **OpenSSL based pseudo random number generation functions** in accordance with a specified cryptographic algorithm **SHA, MD5** and cryptographic key size **not applicable** that meet the following **none.**

5.1.2.8 FCS_COP.1d Cryptographic operation – Diffie-Hellman

FCS_COP.1.1d The TSF shall perform **OpenSSL based Asymmetric Key Generation** in accordance with a specified cryptographic algorithm **Diffie-Hellman (Ephemeral-Ephemeral)** and cryptographic key size **default 1024 bits and maximum 4096 bits** that meet the following **none**.

***note: Cryptographic functionality correctness represented by these claims and algorithm usage is based on F5 Networks assertion of product usage.**

5.1.3 User Data Protection

5.1.3.1 FDP_IFC.1a Subset information flow control - Unauthenticated

FDP_IFC.1.1a The TSF shall enforce the **unauthenticated Traffic Management information flow control SFP** on

a. Subject: All IT entities that send/receive information through the TOE to assigned Back-end Server Resources

b. Information: Traffic sent through the TOE from one subject to another

c. Operation: Pass Traffic

5.1.3.2 FDP_IFC.1b Subset information flow control - authenticated

FDP_IFC.1.1b The TSF shall enforce the **authenticated Traffic Management information flow control SFP** on

a. Subject: All IT entities that send/receive information through the TOE to assigned Back-end Server Resources only after the human user initiating the information flow has authenticated through the TOE via the external authentication server per FIA_UAU.1, FIA_ AUTH.EXP.1.

b. Information: Traffic sent through the TOE from one subject to another

c. Operation: Initiate SSL session Pass Traffic

5.1.3.3 FDP_IFF.1a Simple security attributes-unauthenticated

.

FDP_IFF.1.1a The TSF shall enforce the **unauthenticated Traffic Management information flow control SFP** based on the following types of subject and information security attributes**:**

a. Subject Security Attributes: presumed address

b. Information Security Attributes: Presumed IP address of source subject, Presumed IP address of destination subject, transport layer protocol, Identity of the interface on which the TOE received the packet, URI attributes, Header attributes

FDP_IFF.1.2a The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

Information is allowed to pass through the TOE via TOE interfaces if:

- **The presumed IP address of the source/destination subject translates to a configured VLAN resource, information security attribute values are unambiguously permitted by the**

information security policy rules as configured by the Administrator including: iRules based rules permit traffic flow for Pool member, availability rules permit routing to resource in accordance with established configuration, availability/performance metrics and TOE monitor responses indicate destination resources are available, URI and header attributes translate to a backend server resource Pool assignment

FDP_IFF.1.3a The TSF shall enforce the: **no additional information flow control rules**.

FDP_IFF.1.4a The TSF shall provide the following **no additional SFP capabilities.**

FDP_IFF.1.5a The TSF shall explicitly authorize an information flow based on the following rules: **no additional information flow control rules**.

FDP_IFF.1.6a The TSF shall explicitly deny an information flow based on the following rules:

1. **Using the Reaper High Water Mark function, the TOE will stop accepting new connections based on Administrator configured memory usage settings to avoid a Denial of Service type attack.**
2. **Packets that are determined to be malformed or do not meet protocol standards are rejected and discarded to protect TOE resources.**

5.1.3.4 FDP_IFF.1b Simple security attributes-authenticated

.

FDP_IFF.1.1b The TSF shall enforce the **authenticated Traffic Management information flow control SFP** based on the following types of subject and information security attributes**:**

a. Subject Security Attributes: presumed address, username, password, user role

b. Information Security Attributes: Presumed IP address of source subject, Presumed IP address of destination subject, Identity of the interface on which the TOE received the packet, URI attributes, Header attributes

FDP_IFF.1.2b The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

Information is allowed to pass through the TOE via TOE interfaces if:

- **The presumed IP address of the source/destination subject translates to a configured VLAN resource, information security attribute values are unambiguously permitted by the information security policy rules as configured by the Administrator including: iRules based rules permit traffic flow for Pool member, availability rules permit routing to resource in accordance with established configuration, availability/performance metrics and TOE monitor responses indicate destination resources are available, URI and header attributes translate to a backend server resource Pool assignment**

- **Successful negotiation of SSL protocol, username/password combination resolves to a valid authenticated User role, required key exchange has successfully taken place, certificate verification and revocation checks are successful.**

FDP_IFF.1.3b The TSF shall enforce the: **no additional information flow control rules**.

FDP_IFF.1.4b The TSF shall provide the following **no additional SFP capabilities.**

FDP_IFF.1.5b The TSF shall explicitly authorize an information flow based on the following rules:

Traffic: When session persistence is enabled, traffic is explicitly authorized within the same session based on the previous session authentication for the time specified in the configuration.

FDP_IFF.1.6b The TSF shall explicitly deny an information flow based on the following rules:

1. **Using the Reaper High Water Mark function, the TOE will stop accepting new connections based on Administrator configured memory usage settings to avoid a Denial of Service type attack.**
2. **Packets that are determined to be malformed or do not meet protocol standards are rejected and discarded to protect TOE resources.**

5.1.3.5 FDP_UCT.1 Basic data exchange confidentiality

FDP_UCT.1.1b The TSF shall enforce the **Authenticated Traffic Management information flow SFP** to be able to transmit, receive objects in a manner protected from unauthorised disclosure.

5.1.3.6 FDP_UIT.1 Data exchange integrity

FDP_UIT.1.1 The TSF shall enforce the **Authenticated Traffic Management information flow SFP** to be able to transmit, receive user data in a manner protected from modification, deletion, insertion errors.

FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion has occurred.

5.1.4 Identification and Authentication

5.1.4.1 FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

- **User ID,**
- **User Password**
- **User Role**

5.1.4.2 FIA_UAU.1 Timing of authentication-authenticated traffic users

FIA_UAU.1.1 The TSF shall allow **access to backend server logon screens** on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.1.4.3 FIA_UAU.2 User authentication before any action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing **any other TSF-mediated actions** on behalf of that user.

5.1.4.4 FIA_UID.2 User identification before any action

FIA_UID.2.1 The TSF shall require each user to identify itself before allowing **any other TSF mediated actions** on behalf of that user.

5.1.5 Security Management

5.1.5.1 FMT_MOF.1a Management of security functions behaviour

FMT_MOF.1.1a The TSF shall restrict the ability to disable, enable, modify the behaviour of the functions **Audit security function (Audit Logs)** to **Administrator role**.

5.1.5.2 FMT_MOF.1b Management of security functions behaviour

FMT_MOF.1.1b The TSF shall restrict the ability to modify the behaviour of the functions **Audit Security Functions (System, Local Traffic & Packet Filter Logs) Authentication function, Information Flow Control function, Security Management function** to **Administrator role**.

5.1.5.3 FMT_MOF.1c Management of security functions behaviour

FMT_MOF.1.1c The TSF shall restrict the ability to disable, enable the functions **operational status of Nodes** (subset of Information Flow Control) to **Operator role**.

5.1.5.4 FMT_MSA.1a Management of security attributes

FMT_MSA.1.1a The TSF shall enforce the authenticated **Traffic Management information flow SFP:** to restrict the ability to query, modify, delete the security attributes **User Definitions, iRules settings, Password Policy settings and Role Assignments** to the **Administrator Role**.

5.1.5.5 FMT_MSA.1b Management of security attributes- Pools & VLAN

FMT_MSA.1.1b The TSF shall enforce the authenticated **Traffic Management information flow SFP:** to restrict the ability to query, modify the security attributes **Node settings** to the **Administrator, Operator Role**.

5.1.5.6 FMT_MSA.2 Secure security attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

5.1.5.7 FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1 The TSF shall enforce the **Unauthenticated Traffic Management information flow SFP** to provide permissive default values for security attributes that are used to enforce the *SFP*.

FMT_MSA.3.2 The TSF shall allow the **Administrator** to specify alternative initial values to override the default values when an object or information is created.

5.1.5.8 FMT_MTD.1a Management of TSF data-Delete

FMT_MTD.1.1a The TSF shall restrict the ability to delete **User Roles, Passwords, SSL certificates** to **the Administrator Role.**

5.1.5.9 FMT_MTD.1b Management of TSF data-Modify

FMT_MTD.1.1b The TSF shall restrict the ability to modify **User Roles, Passwords, SSL certificate data** to **the Administrator Role.**

5.1.5.10 FMT_MTD.1c Management of TSF data-Query Audit

FMT_MTD.1.1c The TSF shall restrict the ability to query **Audit records** to **the Administrator, Operator, and Guest Roles.**

5.1.5.11 FMT_MTD.1d Management of TSF data-Query

FMT_MTD.1.1d The TSF shall restrict the ability to query **User Roles, Passwords, SSL certificates** to **the Administrator Role.**

5.1.5.12 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions:

- **Enabling/Disabling of Audit functions***
- **Review of Audit logs**
- **User Role Management**
- **Virtual LAN/Server Management**
- **Password Policy Management**
- **Node Configuration (traffic management)**
- **Pool configuration (traffic management)**
- **Protocol Profile configuration (traffic management)**
- **iRules configuration**
- **Enable/Disable Nodes**

*note: disable function applies only the audit (type) logs

5.1.5.13 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles **Administrator, Operator, Guest, unauthenticated traffic user, authenticated traffic user**.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

5.1.6 Protection of the TSF

5.1.6.1 FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur:

- **Operational failure of a Server Node**
- **Loss of sufficient availability in a given Pool or Server Node**
- **Operational failure of the network switch hardware**
- **Operational failure of a single TOE hardware device**

5.1.6.2 FPT_ITA.1 Inter-TSF availability within a defined availability metric

FPT_ITA.1.1 The TSF shall ensure the availability of **BIG-IP TSF** provided to a remote trusted IT product **97% uptime** given the following conditions **Common Criteria Evaluated Configuration (high availability redundant pair).**

5.1.6.3 FPT_ITC.1 Inter-TSF confidentiality during transmission

FPT_ITC.1.1 The TSF shall protect all TSF data transmitted from the TSF to a remote trusted IT product from unauthorized disclosure during transmission.

5.1.6.4 FPT_ITI.1 Inter-TSF detection of modification

FPT_ITI.1.1 The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and a remote trusted IT product within the following metric: **a single Message Authentication Code (MAC) error during transmission.**

FPT_ITI.1.2 The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and a remote trusted IT product and perform **resending of transmitted data** if modifications are detected.

5.1.6.5 FPT_RVM.1 Non-bypassability of the TSP

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.1.6.6 FPT_SEP.1 TSF domain separation

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

5.1.6.7 FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

5.1.7 Resource Allocation

5.1.7.1 FRU_FLT.1 Degraded fault tolerance

FRU_FLT.1.1 The TSF shall ensure the operation of **maintain full TOE functionality** when the following failures occur: **any failure of a single TOE when in a high availability redundant pair configuration**

5.1.7.2 FRU_PRS.1 Limited priority of service

FRU_PRS.1.1 The TSF shall assign a priority to each subject in the TSF.

FRU_PRS.1.2 The TSF shall ensure that each access to **TOE application server clients** shall be mediated on the basis of the subject's assigned priority.

5.1.7.3 FRU_RSA.1a Maximum quotas – *TCP Connections*

FRU_RSA.1.1a The TSF shall enforce maximum quotas of the following resources: **new or untrusted TCP connections** that subjects can use simultaneously**.**

5.1.7.4 FRU_RSA.1b Maximum quotas – *Memory Usage*

FRU_RSA.1.1b The TSF shall enforce maximum quotas of the following resources: **BIG-IP Memory Resources** that subjects can use simultaneously**.**

5.2 Explicitly Stated TOE Security Functional Requirements

The SFRs defined in this section are explicitly stated and are derived from similar requirements in Part 2 of the CC.

5.2.1 Audit Data Generation

5.2.1.1 FAU_GEN.EXP.1 Audit data generation

FAU_GEN.EXP.1.1 The TSF shall be able to generate a log record of the following auditable events:

a) Start-up ~~*and shutdown*~~ of the audit functions for system, local traffic & packet filter logs;

b) Start-up and shutdown of the audit functions for audit logs;

c) All auditable events for the minimal level of audit; and

d) the auditable events listed in Table 8.

FAU_GEN.EXP.1.2 The TSF shall record within each log record at least the following

information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, No additional audit relative information**.**

Functional Component	Auditable Event
FIA_UAU.2	Log-in authentication failure
FIA_UID.2	Log-in identification failure
FMT_MSA.1a	Modification of security attributes
FMT_MSA.1b	Modification of security attributes – Pools & VLAN
FMT_MTD.1a	Modification of TSF values-Delete
FMT_MTD.1b	Modification of TSF values-Modify
FMT_SMR.1	Modification to Admin (security) roles
FMT_SMF.1	Use of security management functions
FDP_IFF.1a, 1b	Local Traffic event log records*
FDP_IFF.1a, 1b	Packet Filter event log records*
FMT_SMF.1	System log records

*Application Note: Specifics relating to Local Traffic and Packet Filter events are contained in Section 6.1.2 Audit

Table 8: FAU_GEN.EXP.1 Auditable Events

5.2.2 Cryptographic Support

5.2.2.1 FCS_COP.EXP.1 Cryptographic Support - SSL Traffic Offloading

FCS_COP.EXP.1.1 The TSF shall perform SSL Traffic Offloading of backend servers in accordance with a specified cryptographic algorithm per FCS_COP.1A and cryptographic key sizes per FCS_COP.1A that meet the following: as listed in FCS_COP.1A.

FCS_COP.EXP.1.2 The TSF shall re-encrypt SSL traffic prior to routing to backend servers when so configured by the authorized Administrator.

5.2.3 Identification and Authentication

5.2.3.1 FIA_UAU.EXP.1 Timing of authentication: Remote Authentication

FIA_UAU.EXP.1.1 The TSF of the TOE shall deny remote User Access to the TSF pending successful authentication with the applicable Authentication Server

5.2.3.2 FIA_UID.EXP.1 Timing of identification: Remote Identification

FIA_UID.EXP.1.1 The TSF of the TOE shall deny remote User Access to the TSF pending successful identification verification with the applicable Authentication Server

5.3 IT Environment Security Requirements

The SFRs on the IT environment defined in this section are taken from Part 2 of the CC.

IT Environment Security Functional Requirements	
FPT_ITC.1	Inter-TSF confidentiality during transmission
FPT_RVM.1	Non-bypassability of the TSP
FPT_SEP.1	TSF domain separation
IT Environment Explicitly Stated Security Functional Requirements	
FIA_ AUTH.EXP.1	Authentication Database: Authentication

5.3.1.1 FPT_ITC.1 Inter-TSF confidentiality during transmission

.

FPT_ITC.1.1 The ***IT Environment*** shall protect all TSF data transmitted from remote trusted IT product to the TSF a from unauthorized disclosure during transmission.

5.3.1.2 FPT_RVM.1 Non-bypassability of the TSP

FPT_RVM.1.1 The ***IT Environment*** shall ensure that TSP enforcement functions ***occurring within the IT Environment (external authentication validation)*** are invoked and succeed before each ***related*** function within the TSC is allowed to proceed.

5.3.1.3 FPT_SEP.1 TSF domain separation

FPT_SEP.1.1 The ***IT Environment*** shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The ***IT Environment*** shall enforce separation between the security domains of subjects in the TSC.

5.4 Explicitly Stated IT Environment Security Functional Requirements

5.4.1.1 FIA_ AUTH.EXP.1 Authentication Database: Authentication

FIA_ AUTH.EXP.1 The applicable Authentication Server within the TOE IT Environment shall validate the User Name and Password when requested by the TOE for remote authentication.

5.5 TOE Strength of Function Claim

The only probabilistic or permutational mechanisms in the product are the password mechanism used to authenticate users and the cryptographic mechanisms. The password policy for the Administrator role is enforced on a procedurally basis only, all others are enforced by TOE technical mechanisms.

Strength of cryptographic algorithms is outside the scope of the Common Criteria.

The claimed minimum strength of function is SOF-basic. FIA_UAU.2 & FIA_UAU.EXP.1 are the only non-cryptographic TOE security functional requirements that contain a permutational function.

5.6 TOE Security Assurance Requirements

The assurance security requirements for this Security Target are taken from Part 3 of the CC. These assurance requirements compose an Evaluation Assurance Level 2 (EAL2 Augmented ALC_FLR.1) as defined by the CC. The assurance components are summarized in the following table.

Assurance Class	Assurance Components	
ACM: Configuration management	ACM_CAP.2	Configuration items
ADO: Delivery and operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation, and start-up procedures
ADV: Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.1	Descriptive high-level design
	ADV_RCR.1	Informal correspondence demonstration
AGD: Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance*
ATE: Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
AVA: Vulnerability assessment	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis
ALC: Life Cycle Support	ALC_FLR.1	Basic Flaw Remediation

Table 9: Assurance Requirements: EAL2 Augmented ALC_FLR.1

***Note: Product usage is transparent to network users therefore this requirement (AGD_USR.1) requirement is vacuously satisfied (ref: PD-0106: Situations Where AGD_USR May Be Vacuously Satisfied)**

5.6.1 ACM_CAP.2 Configuration items

Developer action elements:

ACM_CAP.2.1D The developer shall provide a reference for the TOE.

ACM_CAP.2.2D The developer shall use a CM system.

ACM_CAP.2.3D The developer shall provide CM documentation.

Content and presentation of evidence elements:

ACM_CAP.2.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.2.2C The TOE shall be labelled with its reference.

ACM_CAP.2.3C The CM documentation shall include a configuration list.

ACM_CAP.2.4C The configuration list shall uniquely identify all configuration items that comprise the TOE.

ACM_CAP.2.5C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.2.6C The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.2.7C The CM system shall uniquely identify all configuration items.

Evaluator action elements:

ACM_CAP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.6.2 ADO_DEL.1 Delivery procedures

Developer action elements:

ADO_DEL.1.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.1.2D The developer shall use the delivery procedures.

Content and presentation of evidence elements:

ADO_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

Evaluator action elements:

ADO_DEL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.6.3 ADO_IGS.1 Installation, generation, and start-up procedures

Developer action elements:

ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

Content and presentation of evidence elements:

ADO_IGS.1.1C The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation, and start-up of the TOE.

Evaluator action elements:

ADO_IGS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1.2E The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.6.4 ADV_FSP.1 Informal functional specification

Developer action elements:

ADV_FSP.1.1D The developer shall provide a functional specification.

Content and presentation of evidence elements:

ADV_FSP.1.1C The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.1.2C The functional specification shall be internally consistent.

ADV_FSP.1.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions, and error messages, as appropriate.

ADV_FSP.1.4C The functional specification shall completely represent the TSF.

Evaluator action elements:

ADV_FSP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security requirements.

5.6.5 ADV_HLD.1 Descriptive high-level design

Developer action elements:

ADV_HLD.1.1D The developer shall provide the high-level design of the TSF.

Content and presentation of evidence elements:

ADV_HLD.1.1C The presentation of the high-level design shall be informal.

ADV_HLD.1.2C The high-level design shall be internally consistent.

ADV_HLD.1.3C The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.1.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.1.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.1.6C The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.1.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

Evaluator action elements:

ADV_HLD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_HLD.1.2E The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.6.6 ADV_RCR.1 Informal correspondence demonstration

Developer action elements:

ADV_RCR.1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

Content and presentation of evidence elements:

ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

Evaluator action elements:

ADV_RCR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.6.7 AGD_ADM.1 Administrator guidance

Developer action elements:

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

Content and presentation of evidence elements:

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.

AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

Evaluator action elements:

AGD_ADM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.6.8 AGD_USR.1 User guidance

Developer action elements:

AGD_USR.1.1D The developer shall provide user guidance.

Content and presentation of evidence elements:

AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2C The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.

AGD_USR.1.5C The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

Evaluator action elements:

AGD_USR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.6.9 ATE_COV.1 Evidence of coverage

Developer action elements:

ATE_COV.1.1D The developer shall provide evidence of the test coverage.

Content and presentation of evidence elements:

ATE_COV.1.1C The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

Evaluator action elements:

ATE_COV.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.6.10 ATE_FUN.1 Functional testing

Developer action elements:

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation of evidence elements:

ATE_FUN.1.1C The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

Evaluator action elements:

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.6.11 ATE_IND.2 Independent testing - sample

Developer action elements:

ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation of evidence elements:

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements:

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.6.12 AVA_SOF.1 Strength of TOE security function evaluation

Developer action elements:

AVA_SOF.1.1D The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

Content and presentation of evidence elements:

AVA_SOF.1.1C For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2C For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

Evaluator action elements:

AVA_SOF.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_SOF.1.2E The evaluator shall confirm that the strength claims are correct.

5.6.13 AVA_VLA.1 Developer vulnerability analysis

Developer action elements:

AVA_VLA.1.1D The developer shall perform a vulnerability analysis.

AVA_VLA.1.2D The developer shall provide vulnerability analysis documentation.

Content and presentation of evidence elements:

AVA_VLA.1.1C The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP.

AVA_VLA.1.2C The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.

AVA_VLA.1.3C The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

Evaluator action elements:

AVA_VLA.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VLA.1.2E The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

5.6.14 ALC_FLR.1 Basic flaw remediation

Developer action elements

ALC_FLR.1.1D The developer shall provide flaw remediation procedures addressed to TOE developers.

Content and presentation of evidence elements

ALC_FLR.1.1C The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.1.2C The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

ALC_FLR.1.3C The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

ALC_FLR.1.4C The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

Evaluator action elements

ALC_FLR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.7 Rationale For TOE Security Requirements

5.7.1 TOE Security Functional Requirements

	O.AUDIT_GEN	O. AUDIT_PROT	O. AUDIT_REVIEW	O.CRYPTO	O.RESOURCE_X	O.MANAGE	O.PRIORITY	O.SELF_PROT	O.TIME_STAMPS	O.ROBUST_TOE	O.SECURE_DATA	O.SAFE_FAIL
FAU_ARP.1			☑									
FAU_SAA.1			☑									
FAU_SAR.1			☑									
FAU_SAR.3a			☑									
FAU_SAR.3b			☑									
FAU_SAR.3c			☑									
FAU_STG.1		☑										
FAU_STG.4		☑										
FAU_GEN.EXP.1	☑											
FCS_CKM.1a				☑								
FCS_CKM.1b				☑								
FCS_CKM.1c				☑								
FCS_CKM.1d				☑								
FCS_COP.1a				☑								
FCS_COP.1b				☑								
FCS_COP.1c				☑								
FCS_COP.1d				☑								
FCS_COP.EXP.1				☑								
FDP_IFC.1a											☑	
FDP_IFC.1b											☑	
FDP_IFF.1a											☑	
FDP_IFF.1b											☑	
FDP_UCT.1											☑	
FDP_UIT.1											☑	
FIA_ATD.1										☑		
FIA_UAU.1										☑		
FIA_UAU.2										☑		
FIA_UID.2										☑		

	O.AUDIT_GEN	O. AUDIT_PROT	O. AUDIT_REVIEW	O.CRYPTO	O.RESOURCE_X	O.MANAGE	O.PRIORITY	O.SELF_PROT	O.TIME_STAMPS	O.ROBUST_TOE	O.SECURE_DATA	O.SAFE_FAIL
FIA_UAU.EXP.1										☑		
FIA_UID.EXP.1										☑		
FMT_MOF.1a						☑						
FMT_MOF.1b						☑						
FMT_MOF.1c						☑						
FMT_MSA.1a						☑						
FMT_MSA.1b						☑						
FMT_MSA.2				☑								
FMT_MSA.3						☑						
FMT_MTD.1a						☑						
FMT_MTD.1b						☑						
FMT_MTD.1c						☑						
FMT_MTD.1d						☑						
FMT_SMF.1						☑						
FMT_SMR.1						☑						
FPT_FLS.1												☑
FPT_ITA.1								☑				
FPT_ITC.1								☑			☑	
FPT_ITI.1											☑	
FPT_RVM.1								☑				
FPT_SEP.1								☑				
FPT_STM.1									☑			
FRU_FLT.1												☑
FRU_PRS.1							☑					
FRU_RSA.1a					☑							
FRU_RSA.1b					☑							

Table 10: SFR and Security Objectives Mapping

Security Objective	Mapping Rationale
O.AUDIT_GEN	FAU_GEN.EXP.1 specifies the security related items that the TOE must log in the course of TOE operation to assure accountability for security function alterations and visibility to security related events.
O.AUDIT_PROT	FAU_STG.1, specifies that audit records are protected from unauthorized access, modification or deletion. FAU_STG.4 specifies that audit records stored on the BIG IP appliance are overwritten upon exhausting allocated storage resources and overwrites the oldest audit record first.
O.AUDIT_REVIEW	FAU_SAR.1 specifies that audit records may be reviewed via the GUI by authorized users in a suitable form. FAU_SAR.3a, b, c, specifies that audit records are selectable allowing the authorized user to view records by various attributes based on the type of audit. Packet Filter Events log, Local Traffic Events log, System log, and Audit log review aspects are included. FAU_ARP.1 specifies that the TSF will send an email alert to the TOE Administrator upon identification of a potential security violation. FAU_SAA.1 specifies that the TSF will apply a set of rules in determining a potential security violation and lists the rules applied for this purpose.
O.CRYPTO	FCS_COP.1a,b,c,d specifies the cryptographic algorithms and key sizes to be used for SSL traffic offloading services and Administrator sessions. FCS_CKM.1a,b,c,d specifies the key generation techniques and algorithms used for SSL traffic sessions and Administrator sessions. FCS_COP.EXP.1 specifies that the TSF can be configured to provide SSL offloading in support of backend server resources in the IT Environment, including re-encryption of traffic to backend server when so configured. FMT_MSA.2 specifies that only secure values will be accepted for use by the TOE in support of cryptographic operations.
O.MANAGE	FMT_MSA.1a, b specifies the management of security attributes by authorized Users/User roles. This assures that sufficient control and visibility is present within the TOE to effectively manage security functions. FMT_MSA.3 specifies restrictive default values for security attributes and specifies that only the Administrator can change initial values.

	FMT_MTD.1a,b,c,d places restrictions on which Users/roles may modify TSF data specified attributes thereby affecting security functionality within the TOE. FMT_SMF.1 specifies the management functions that the TOE uses to define parameters under which the TOE manages security related aspects of operation. The TOE provides detailed Administrator guidance to ensure correction configuration and management of security functions. FMT_SMR.1 specifies that the TOE supports specific roles for use by the Administrator in managing TSF access limitations by the type of User. The TOE maintains Administrator, Operator and Guest roles and associates Users with those roles for use and management of the TOE. FMT_MOF.1a, b, c specifies the restrictions placed by the TSF on the enable, disable and modification of security function behavior to the Administrator and Operator roles.
O.PRIORITY	FRU_PRS.1 specifies that the TOE assigns priorities to traffic subjects and mediates access (routes traffic) to backend server based on this priority.
O.SELF_PROT	FPT_ITC.1 provides that the TSF maintains a domain for protection of TSF resources and to avoid disclosure or interference. FPT_SEP.1 specifies that the TOE will provide a secure domain for its execution and will enforce separation between subjects in the TSC. FPT_RVM.1 specifies that the TOE may not be able to be bypassed to avoid this protective domain. FPT_ITA.1 specifies an availability metric for TOE functionality to assure a high probability that TSF functionality will be available, in this case, through a redundant pair configuration.
O.TIME_STAMPS	FPT_STM.1 provides for the capability to annotate audit logs with a time stamp produced during TOE operation for accurate time related rendition of TOE auditable activities.
O.ROBUST_TOE	FIA_ATD.1 specifies security attributes that must be maintained in the TOE by individual users. The inclusion of FIA_UID.2, FIA_UID.EXP.1, FIA_UAU.EXP.1 and FIA_UAU.2 maintains access control security for these attributes. FIA_UAU.1 specifies that authenticated traffic users will be presented a log on screen to provide credentials prior to identification, all other access requires identification prior to access.
O.RESOURCE_X	FRU_RSA.1a, FRU_RSA.1b specifies maximum quotas for connections & memory usage established or used by subjects simultaneously.
O.SECURE_DATA	FPT_ITC.1 assures protection of data during this transfer from unauthorized disclosure or unauthorized modification. FPT_ITI.1 specifies that modification during inter-TSF transfer is detected.

	FDP_IFC.1a specifies the Subject and Objects controlled by the unauthenticated Traffic Management information flow control SFP FDP_IFC.1b specifies the Subject and Objects controlled by the authenticated Traffic Management information flow control SFP FDP_IFF.1a specifies the rules that are invoked by the SFP established in FDP_IFC.1a. FDP_IFF.1b specifies the rules that are invoked by the SFP established in FDP_IFC.1b. FDP_UCT.1 specifies that data transferred between the TOE and Backend Server pools is protected from unauthorized disclosure FDP_UIT.1 specifies that data transferred between the TOE and Backend Server pools is protected from modification or deletion.
O.SAFE_FAIL	FPT_FLS.1 specifies that the TOE will preserve a secure state through specified failure events. FRU_FLT.1 provides for a specific level of functionality given a specified failure mode.

5.7.2 IT Environment Security Functional Requirements

	OE.DATA_PROT	OE.DOMAIN_SEP	OE.NO _BYPASS
FPT_ITC.1	☑		
FPT_RVM.1			☑
FPT_SEP.1		☑	
FIA_ AUTH.EXP.1	☑		

Table 11: SFR and Security Objectives Mapping

Security Objective	Mapping Rationale
OE.DATA_PROT	FPT_ITC.1 specifies that the IT Environment protects all TSF data transmitted from remote trusted IT product to the TSF from unauthorized disclosure during transmission
OE.DOMAIN_SEP	FPT_SEP.1 specifies that the IT Environment maintains a security domain for its own execution and protects it from interference and tampering by untrusted subjects. The IT Environment also enforces separation between the security domains of subjects within the TOE scope of control.
OE.NO _BYPASS	FPT_RVM.1 specifies that the IT Environment ensures that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed; thereby preventing bypass. FIA_AUTH.EXP.1 specifies that an Authentication Server is provided within the TOE IT Environment to validate the User Name and Password when requested by the TOE for remote authentication

5.7.3 TOE Security Assurance Requirements

EAL2 (Augmented ALC_FLR.1) was chosen to provide a low to moderate level of independently assured security. The chosen assurance level is consistent with the threat environment as described in 5.11. Specifically, that the threat of malicious attacks is not greater than moderate and the product will have undergone a search for obvious flaws.

5.8 Rationale for Explicitly Stated Security Requirements

Table 12 presents the rationale for the inclusion of the explicit requirements found in this Security Target.

Explicit Requirement	Identifier	Rationale

Explicit Requirement	Identifier	Rationale
FAU_GEN.EXP.1	Logging of Audit Function activation/inactivation	This requirement is explicitly stated because the TOE does not include logging of audit function de-activation for audit (type) logs within the TOE's auditing capability.
FAU_UAU.EXP.1	Timing of Authentication (remote)	This requirement is explicitly stated because the TOE requires the entry of ID and password but denies access pending successful authentication by the remote server, which is in the TOE Environment.
FCS_COP.EXP.1	Cryptographic Operation – SSL Offloading	This requirement is explicitly stated because it includes the configurable option of providing cryptographic services on behalf of resource in the IT Environment based on Administrator settings.
FIA_UID.EXP.1	Timing of Identification (remote)	This requirement is explicitly stated because the TOE requires the entry of ID and password but denies access pending successful authentication by the remote server, which is in the TOE Environment.
FIA_ AUTH.EXP.1	Authentication Database: Authentication	This requirement is explicitly stated to define the requirement for the Authentication Server in the IT Environment to validate the User Name and Password when requested by the TOE for remote authentication.

Table 12: Explicitly Stated SFR Rationale

5.9 Rationale For IT Security Requirement Dependencies

This section includes a table of all the security functional requirements and their dependencies and a rationale for any dependencies that are not satisfied.

Functional Component	Dependency	Included/Rationale
FAU_ARP.1	FAU_SAA.1	Yes
FAU_SAA.1	FAU_GEN.1	Yes (FAU_GEN.EXP.1)
FAU_SAR.1	FAU_GEN.1	Yes (FAU_GEN.EXP.1)
FAU_SAR.3a, b, c	FAU_GEN.1	Yes (FAU_GEN.EXP.1)

Functional Component	Dependency	Included/Rationale
FAU_STG.1	FAU_GEN.1	Yes
FAU_STG.4	FAU_STG.1	Yes
FCS_COP.1a,b,c,d	FCS_CKM.1, FCS_CKM.4, FMT_MSA.2	No, FCS_CKM.4
FCS_CKM.1a,b,c,d	FCS_COP.1, FCS_CKM.4, FMT_MSA.2	Yes
FCS_COP.EXP.1	FCS_CKM.1, FCS_CKM.4, FMT_MSA.2	No, FCS_CKM.4
FDP_IFC.1a,b	FDP_IFF.1	Yes
FDP_IFF.1a,b	FDP_IFC.1, FMT_MSA.3	Yes
FDP_UCT.1	FDP_IFC.1, FTP_ITC or FTP_TRP	No, FTP_ITC or FTP_TRP
FDP_UIT.1	FDP_IFC.1, FTP_ITC or FTP_TRP	No, FTP_ITC or FTP_TRP
FIA_ATD.1	None	None
FIA_UAU.1	None	None
FIA_UAU.2	FIA_UID.1	Yes (FIA_UID.2)
FIA_UID.2	None	None
FMT_MOF.1a	FMT_SMR.1, FMT_SMF.1	Yes
FMT_MOF.1b	FMT_SMR.1, FMT_SMF.1	Yes
FMT_MSA.1a,b	FMT_SMR.1, FMT_SMF.1, FDP_IFC.1	Yes
FMT_MSA.2	FDP_IFC.1, FMT_MSA.1 FMT_SMR.1	Yes
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	Yes
FMT_MTD.1a,b,c,d	FMT_SMR.1, FMT_SMF.1	Yes
FMT_SMF.1	None	None
FMT_SMR.1	FIA_UID.1	Yes (FIA_UID.2)
FPT_FLS.1	ADV_SPM.1	Yes*
FPT_ITA.1	None	None
FPT_ITC.1	None	None
FPT_ITI.1	None	None
FPT_RVM.1	None	None
FPT_SEP.1	None	None

Functional Component	Dependency	Included/Rationale
FPT_STM.1	None	None
FRU_FLT.1	FPT_FLS.1	Yes
FRU_PRS.1	None	None
FRU_RSA.1a	None	None
FRU_RSA.1b	None	None
FAU_GEN.EXP.1	FPT_STM.1	Yes
FIA_UAU.EXP.1	FIA_UID.EXP.1	Yes
FIA_UID.EXP.1	FIA_UAU.EXP.1	Yes
FIA_AUTH.EXP.1	None	None

Table 13: SFR Dependencies

***ADV_SPM.1 satisfied within Security Target**

5.9.1 Rationale for Unsatisfied Dependencies

The following security requirements are depended upon by the security requirements for the TOE, yet were not included within this ST. These requirements and their justification are provided below.

Requirement	Unsatisfied Dependencies	Dependency Analysis and Rationale
FDP_UCT.1a FDP_UIT.1a	FPT_ITC.1 or FTP_TRP.1	The dependencies for FDP_UCT.1 and FDP_UIT.1 of FTP_ITC.1 or FTP_TRP.1 are not required due to the fact that the communication between the BIG-IP Appliance and Back-End Servers is between the TOE and a trusted IT product within a protected network. Flow Control policies enforced by the BIG-IP appliance assure proper routing of data and assure data integrity.

Requirement	Unsatisfied Dependencies	Dependency Analysis and Rationale
FCS_COP.1a,b,c,d FCS_CKM.1a,b,c,d FCS_COP.EXP.1	FCS_CKM.4	The dependency of FCS_CKM.4 for FCS_COP.1a,b,c,d and FCS_CKM.1a,b,c,d is not required as the use of cryptography by the TOE is limited to negotiating SSL sessions (on behalf of backend servers) or Administrator sessions and creating sessions keys for theses purposes. These session keys generated are only valid for the current session; therefore destruction of these keys to preclude reuse is unnecessary. RSA keys stored on the TOE (used to generate session keys) are protected by A.ADMIN & A.LOCATE assumptions which specify that the TOE is deployed in a physically secure location and accessed only by trusted Administrators; these are also protected through the Protection of the TOE security function (FPT_SEP.1, FPT_RVM.1).

Table 14: Unsatisfied SFR Dependencies

5.10 Rationale For Internal Consistency and Mutually Supportive

The selected requirements are internally consistent. The ST includes all the SFRs provided by the TOE. All operations performed on the security requirements comply with the rules and intent required by the operation in the CC. The requirements defined in the ST are not contradictory.

The selected requirements together form a mutually supportive whole by:

- satisfying all dependencies as demonstrated in **Table 13: SFR Dependencies**
- tracing security functional requirements to security objectives and justifying that tracing as demonstrated in Section 5.8
- including the SFRs FPT_RVM.1 and FPT_SEP.1 to protect the TSF
- including audit requirements to detect security-related actions and potential attacks
- including security management requirements to ensure that the TOE is managed and configured securely.

5.11 Rationale For Strength of Function Claim

The rationale for choosing SOF-basic is based on the low to moderate attack potential of the threats identified in this ST. While the TOE may be deployed in environments where WAN traffic is routed to backend servers at a substantial rate, the TOE appliance is transparent to traffic users (unauthenticated/authenticated). Since the TOE appliance is transparent to these

users and traffic user traffic is managed separately from TSF data (i.e.: Security Management functions) as specified in Section 6.1.7, the attack potential of the TOE itself is considered to be low to moderate, therefore, leading to a basic strength of function claim.

The security objectives provide probabilistic security mechanisms and the strength of function claim is satisfied by the password management features provided by the TOE.

6 TOE Summary Specification

6.1 TOE Security Functions

The TOE consists of the following Security Functions:

- Identification and Authentication
- Audit
- Information Flow Control
- Security Management
- Secure Communications
- Secure Traffic
- Protection of the TOE

6.1.1 Identification and Authentication

The BIG-IP Appliance has an internal authentication capability and can also be configured to use an external authentication server. The Administrative user holding the Administrator role of the appliance must be authenticated within the appliance itself to assure that the Administrator can always access the appliance. All other administrative users may either authenticate internal to the appliance or using an external authentication server based on configuration. The CC Evaluated Configuration utilizes authentication within the appliance for the BIG-IP role: Administrator and users: Operator, Guest and authenticated traffic users are authenticated using an external authentication server (LDAP, RADIUS).

User Security Attributes for Identification and Authentication (FIA_ATD.1)

User attributes are stored within the TOE OS locally and within the TOE Environment remotely when applicable. User attributes are maintained by Username and Password and include User ID, User Password User Role in a MD5 hashed format.

The BIG-IP TOE requires administrative users be positively identified and authenticated within the system prior to acquiring administrative access and/or performing any security functions. The TOE utilizes User accounts and roles to control access and manage privileges. For the purposes of this ST, access to the TOE security function commutates an Administrator user access based on an assigned role.

The password mechanism of the Identification and Authentication security function satisfies the SOF claim of Basic, through technical means for non-Administrator roles and through procedural means for Administrator role users..

The TOE constructs a secure channel with a trusted peer for access to TSF functions. The secure channel is established only after each device authenticates itself.

User accounts can be managed locally in the BIG-IP operating system or through LDAP or RADIUS authentication servers similar to the traffic authentication described in Section 2.2.2.3. In all cases, TOE security attributes are stored securely requiring Administrator level permissions to access, modify or delete.

Local Authentication by BIG-IP (FIA_UAU.2, FIA_UID.2)

For Local Authentication (administrative users), the TOE requires identification and authentication via a username and password combination. Authentication occurs internal to the TOE via the resident OS through the PAM module described in Section 2.2.4. Identification and Authentication is required prior to accessing TSF functions. By design, Administrative users holding the role, Administrator, are always locally authenticated to ensure local access is always available to this full access Administrative role. The Administrator can configure the TOE for which Administrative users are allowed to authenticate locally. Password hashes are securely stored in the OS using an MD5 hash. When a user needs to authenticate, they enter their password, the TOE hashes the password, and if it matches, then the user is authenticated.

Remote Authentication by Authentication Server (FIA_UAU.1, FIA_UAU.EXP.1, FIA_UID.EXP.1)

For Remote Authentication, a remote authentication server is utilized. The authenticated traffic user is presented with a logon screen prior to being authenticated. Upon entering credentials on the provided screen, the User is identified and authenticated for access to backend resources requiring authentication.

The types of remote authentication servers used for storing User accounts for BIG-IP are: Lightweight Directory Access Protocol (LDAP) servers, and Remote Authentication Dial-in User Service (RADIUS). Only Users with the role of Administrator can manage User roles for remote User accounts.

Security of TSF data transfer with External Authentication Server (FPT_ITA.1, FPT_ITC.1, FPT_ITI.1)

Communication with the authentication server (trusted IT product) is secured through an SSL based connection using the methods described in Secure Communications, Section 6.1.5, to assure that TSF data such as username, passwords or other authentication data is not disclosed to unauthorized parties, modified or deleted. The TOE can detect a single Message Authentication Code (MAC) error during transmission and upon detecting this error will execute a resend command. The TOE utilizes a redundant pair configuration and maintains a 97% uptime minimum to assure access to TSF and the authentication process is not interrupted.

Through use of the [Users.LocalOnly] key in the BIGDB database, the Administrator can establish which User accounts must reside locally on the TOE and are not allowed to reside on the remote authentication server.

Security attributes and login information is protected during remote authentication through an SSL session (or SSH for remote administration) as described in Sections 6.1.6 & 6.1.7.

The TOE receives the remote authentication request (username & password) and routes that request to the remote authentication server for validation. Prior to successful validation, no access to TOE TSF is allowed. By design, Administrators given access remotely via SSH have full (root level) privileges within BIG-IP, however, the Common Criteria Evaluated configuration only includes the use of CLI (via console or SSH) for the purpose of initial IP configuration during installation.

User roles are maintained in the local TOE database. Following identification and authentication via a remote server, the role information is accessed locally for the identified user.

The password authentication mechanism is realized by a probabilistic or permutational security mechanism and meets the claim of SOF-BASIC.

Password Policy for Common Criteria Evaluated Configuration

The minimum password policy enforced by BIG-IP through technical means (except for the Administrator role) requires at least 8 characters, and at least one from capital letters, lowercase letters, numbers, and punctuation. The following is the set of available characters for password selection:

- (alpha)A-Z a-z
- (numeric) 0-9
- (special characters) `~!@#$%^&*()-_+=[]{};':",./<>?|\

This set includes:

52 alphabetic characters (26 upper and 26 lower)

10 digits

10 punctuation marks from the shifted digits

22 more punctuation marks from other keys

For a total of 94 characters.

After each failed authentication, there is a delay of 2 seconds to confound intruders.

Users must change their password every 90 days.

This password policy is enforced by TSF technical mechanisms for all users except the Administrator role.

This password policy applies to all Users except for the role: Administrator, however, guidance documentation requires the Administrator role users to adhere to this policy on a procedural basis.

6.1.2 Audit

The TOE provides a full audit capability that generates audit records and provides an audit trail of TOE security function activities and traffic management events through the TOE. Through the GUI interface, the Administrative users (Administrator, Operator, Guest) may view audit logs and filter displayed results based on the information contained in the audit record. The audit function can be configured to log specific parameters of traffic management activity to allow for detailed analysis of performance. The mechanism that the BIG-IP system uses to log events is the Linux utility, syslog-ng. The syslog-ng utility is an enhanced version of the standard UNIX and Linux logging utility, syslog.

Audit generation and management (FAU_GEN.EXP.1)

The BIG-IP appliance generates audit records for the following events at a minimum:

FIA_UAU.2	Log-in authentication failure
FIA_UID.2	Log-in identification failure
FMT_MSA.1a	Modification of security attributes
FMT_MSA.1b	Modification of security attributes – Pools & VLAN
FMT_MTD.1a	Modification of TSF values-Delete
FMT_MTD.1b	Modification of TSF values-Modify
FMT_SMR.1	Modification to Admin (security) roles
FMT_SMF.1	Use of security management functions

Local Traffic Events records – FAU_SAR.1, FAU_SAR.3a

The Local Traffic Events logs produce audit events for Local Traffic Management events such as:

- Address Resolution Protocol (ARP) packet and ARP cache events
- HTTP protocol events
- IP packet discard events due to exceptional circumstances or invalid parameters (such as a bad checksum)
- Layer 4 events (events related to TCP, UDP, and Fast L4 processing)
- MCP/TMM configuration events
- Monitor configuration events
- Network events (layers 1 and 2)
- Packet Velocity® ASIC (PVA) configuration events
- iRules events related to run-time iRules processing
- SSL traffic processing events
- General TMM events such as TMM startup and shutdown

Local Traffic Event logs include Timestamp, Host Name, Description, Service and Status Code information within each audit record. In addition to these parameters, audit records can be searched/sorted by Audit Log type, keyword filter and logging level. Local traffic logs cannot be disabled.

Local Traffic Events logs are accessed through the GUI and are formatted for easy viewing of pertinent information.

Packet Filter Events records – FAU_SAR.1, FAU_SAR.3a

The Packet Filter Events log is configured to identify packet discard events (from unidentified or questionable packets) that may indicate thwarted attacks in the CC evaluated configuration based on the Administrator configured packet filter rules enforced by the TOE appliance. Packet Filter Event records include Timestamp, Host Name, Description, Service and Status Code information in each audit record generated. In addition to these parameters, audit records can be searched/sorted by Audit Log type, keyword filter and logging level. Packet Filter logs cannot be disabled.

Packet Filter Events logs are accessed through the GUI and are formatted for easy viewing of pertinent information.

System Log records – FAU_SAR.1,FAU_SAR.3b

System Log records are generated for Operating System level events within the appliance and include Timestamp, Host Name, Description and Service information within each audit record. In addition to these parameters, audit records can be searched/sorted by Audit Log type, keyword filter and logging level. System logs cannot be disabled.

System Logs are accessed through the GUI and are formatted for easy viewing of pertinent information.

Audit (type) Log records - FAU_SAR.1, FAU_SAR.3c

Audit (type) logging logs messages whenever a BIG-IP system object, such as a virtual server or a load balancing pool, is configured; that is, created, modified, or deleted. There are three ways that objects can be configured:

- By user action
- By system action
- By loading configuration data

Audit (type) Log records are generated for these administrator related transactions and are grouped in the Administrator Management web interface (GUI) by Timestamp, Username, Transaction Type and Event. In addition to these parameters, audit records can be

searched/sorted by Audit Log type, keyword filter and logging level.

The Administrator role can disable audit (type) log auditing which creates an audit record prior to shutting down the particular type of auditing, however, the Common Criteria Evaluated configuration required that audit logging is enabled and set to the minimum level specified in the Common Criteria Administrator Guidance.

Audit (type) Logs are accessed through the GUI and are formatted for easy viewing of pertinent information. Administrator, Operator and Guest roles may access these log records.

Audit Records – Timestamps & Protection (FPT_STM.1, FAU_STG.1, FAU_STG.4)

The BIG-IP appliance maintains an internal time source within the appliance that is used to provide a reliable time reference for audit records. All audit records include time/date information indicating when the event occurred.

The audit trail is protected through O.S. authentication access within the TOE. Only trusted Administrators (roles: Administrator, Operator, Guest) have access to audit files, in addition, audit records stored on the BIG-IP appliance cannot be modified or deleted by any user.

Audit records are stored locally in the TOE appliance in a separate file system from the rest of the appliance; therefore, if this space is filled it does not affect other appliance functionality. The TOE appliance allocates 17 GB for audit storage. Upon reaching the limit allocated for audit records, records are overwritten. Audit records are overwritten in an “oldest record first” manner.

The system also will alert the Administrator (role: administrator) via email to a suspected SYN flood attack (FAU_ARP.1, FAU_SAA.1) if TCP SYN requests exceed the threshold of 16384 TCP SYN packets. This function is enabled by default and is part of the CC evaluated configuration.

Auditing and logging functions are managed entirely by the SYSLOG daemon within the BIG-IP Operating System. The audit function may be configured through the syslog utility on the BIG-IP system to send BIG-IP system log information to a remote logging host, using an encrypted network connection. The use of a remote logging host is not included in the Evaluated Configuration.

Identification and Authentication failures are logged providing a resource to determine if unauthorized personnel may be attempting to access TSF functions.

6.1.3 Information Flow Control

The BIG-IP appliance enforces the unauthenticated/authenticated Traffic Management Information Flow SFP to assure that traffic flowing through the appliance is properly terminated and re-routed within the device, based on configured traffic management techniques. The BIG-IP appliance manages HTTP, HTTPS, SMTP, and FTP based traffic and provides routing based on traffic type, protocol, VLAN configuration settings and backend server availability. The

unauthenticated/authenticated Traffic Management information flow SFP assures the effectiveness of the traffic management techniques employed by the device, accuracy of the traffic routing process through the use of configured VLANs and the appropriate termination and routing of secure data via HTTPS, where applicable. Among the methods used for defining Information Flow Control rules is the iRules™ feature, which allows Administrators to configure rules sets based on traffic management related events. See Section 6.1.4 for information relating to iRules configuration.

Flow Control Policy Enforcement
(FDP_IFC.1a,b, FDP_UCT.1, FDP_UIT.1, FRU_FLT.1, FRU_PRS.1)

Information Flow Control policies are configured per the unauthenticated/authenticated Traffic Management information flow SFP in the TOE to assure that traffic flows only to and from properly authenticated (where required) and authorized sources/destinations. This is implemented primarily through the configuration of the VLANs and associated virtual servers.

A virtual server receives a client request, and instead of sending the request directly to the destination IP address specified in the packet header, sends it to any of several content servers that make up a load balancing pool. Virtual servers increase the availability of resources for processing client requests. IP addressing to the internal network is mapped securely from External Addresses using SNAT internal to the BIG-IP appliance.

Traffic is prioritized to Back-end Servers based on the Traffic Management SFP enforced rule set that provide accommodations for optimizing traffic flow and routing to Pool members based on traffic attributes. Traffic optimization techniques include the BIG-IP OneConnect™ feature which improves performance by aggregating multiple client requests into a server-side connection pool. This gain in efficiency results in greater utilization and increases the availability of the backend server pool. Additional features that support throughput and priority features are described in Section 2.2.2. (FRU_PRS.1)

Traffic Management Flow Control Rules (FDP_IFF.1a,b)

The TOE supports flow control through Administrator configurable functions that can perform the following flow control policies:

The rules that must be met for the routing of HTTP traffic includes that Network IP addresses must be validated within the BIG-IP, configured iRules requirements must be met for the applicable Pool members, authentication must be successful and routing must meet availability and load balancing rules in place within the appliance. SSL based traffic (HTTPS) must have executed a successful SSL connection with required certificate exchange.

SSL Termination (HTTPS protocol):
When appropriately configured, the TOE terminates SSL connections within the TM/OS and routes the traffic to a pool of local servers. This provides off-loading of SSL services from local servers thereby increasing resource availability. When required, the TOE can be

configured to re-encrypt traffic to the local servers to maintain a secure path. The TOE can also be configured to encrypt based on different types of content through established policies.

Header Inspection of Packets:
This feature allows the TOE to alter the flow of packets based upon headers or other criteria. This can be used to select a different pool based upon URI or to authenticate traffic before sending the request to the applicable servers.

HTTP Compression:
Based on content related parameters, HTTP traffic may be compressed using hardware and software compression techniques to provide increased network application speed and efficiency. HTTP compression is not evaluated as part of the Common Criteria evaluation.

Rules based Pool Selection:
Based on Administrator configurable iRules, traffic is routed to local servers based on speed, availability or content. Various monitors are utilized to continuously measure availability and throughput for use in rules based real time routing decisions. These include health and performance based monitors.

Standard load balancing schemes are included in addition to configurable selections.

Flow Control Traffic Authentication:

The Virtual Server infrastructure assures correct traffic routing by enforcing the Traffic Management Information Flow SFP.

Network traffic can be authenticated via modules built around the PAM authentication system. Modules specific to the authentication protocol are implemented to coordinate the traffic authentication process. For the purposes of this TOE, the supported authentication protocols are LDAP and RADIUS.

SSL Traffic Management:

The LTM system can securely manage server side HTTPS (SSL) traffic by re-encrypting a decrypted request before sending it on to a target server. The LTM system performs the same verification functions for local server certificates as for client certificates.

The TOE may also authenticate SSL traffic with client-supplied client certificates. Prior to routing traffic, the TOE verifies client certificate revocation status via Certificate Revocation List (CRL).

6.1.4 Security Management

Security Management within the TOE is managed by the Operating System through User Access controls and role based privileges. (FMT_MSA.1a) The TOE provides the Security

Management security function to allow the Administrator to configure security attributes which support the Traffic Management SFP. Role based user access controls restrict the ability to query, modify, or delete the following security attributes to the Administrator role: User Definitions, iRules settings, Password Policy settings and Role Assignments.

iRules Overview

An iRule is a script that allows the TOE Administrator to allow individual connections to target a pool other than the default pool defined for a virtual server. iRules allow Administrators to more directly specify which Pools in which to direct traffic. Using iRules, the TOE Administrator can send traffic not only to pools, but also to individual pool members, ports, or URIs. There are no restrictions on the use of iRules for the Common Criteria evaluated configuration.

iRule are constructed by creating scripts which specify a given event, a conditional rule set and an action to take given the condition. The syntax used to write iRules is based on the Tool Command Language (Tcl) programming standard. Thus, the Administrator can use many of the standard Tcl commands, plus a robust set of extensions that the TOE provides to create these scripts. iRules (scripts) are made up of Event declarations, Operators and iRule commands which allow the Administrator to customize the traffic management action to take based on the event. For instance, if an HTTP_REQUEST event was received, it could trigger an iRule which contains a rule set based on Operators (If contains “x”, then “y”, else “z” etc) which when matched results in the execution of an iRule command (example), HTTP::header remove <name>, which strips the named header for a request or response.

iRules and TM/OS Security Management

The iRules function allows for the control of connections passing through the Local Traffic Manager. Through this configurable iRules function, security policies are established and assigned to defined profiles to further manage functionality of the TSF. iRules functionality is accessible to authorized administrators (role: Administrator) only.

The Operator role is allowed to enable or disable Nodes in order to make changes based on operational aspects of traffic served by the BIG IP appliance. (FMT_MSA.1b)

The following roles are available to limit access to TOE security functions (FMT_SMR.1), it should be noted that these are administrative users of the appliance:

Administrator

Full access allowed. Administrators may be given console/SSH access where they have full privileges on the machine. CLI access to the TOE for Common Criteria is limited to initial IP address configuration during the installation process. All other uses of CLI are excluded from the Common Criteria Evaluated configuration.

This User role provides the user with full access to all administrative tasks. By default, users with this User role can access the BIG-IP system through the GUI, but not through the command line interface. CLI access can be granted on a by user basis.

Operator

This role allows for the enabling or disabling of nodes. The Operator user role allows the user to view information and to enable or disable nodes. Operators can access the BIG-IP system through the GUI only.

Guest

The Guest user role grants read-only access to the user, through the GUI only. A user with this user role has no access to the command-line interface. A user with the Guest role can view configuration information and audit records, but cannot create new objects or modify existing ones. Users with this access level do not have access to various GUI elements such as Create buttons, Update buttons, and Delete buttons.

User accounts, roles and associated permissions are protected from unauthorized access through the PAM module functionality within the BIG-IP operating system. This allows no access to TOE security functions.

Authenticated and unauthenticated traffic users are users of the traffic which travels through the BIG-IP appliance. They have no administrative access to the BIG-IP TOE itself or to any administrative functions. The BIG-IP TOE appliance is transparent to these users. These users establish sessions with backend servers that are served by the BIG-IP appliance, but are only aware of the backend server resource that is hosting their session. The unauthenticated traffic users are those who may access backend servers without prior authentication and the authenticated traffic users are those who must first be successfully authenticated by the backend server, or external authentication server, prior to gaining access to backend server resources.

Administrators manage TSF Access and associated permissions within the TOE using role based privileges. New Administrative Users are allocated the appropriate permissions by role through selections made by the Administrator during User Configuration. (FMT_MSA.3)

Section 6.1.1 details security functions management relating to Identification and Authentication within the TOE, which require administrator level access.

Remote access is supported through a web-based UI within the APACHE operating environment integrated within the TM/OS or through an SSH connection. Access is addressed through the PAM module functionality within the BIG-IP operating system.

Administrator access is required for managing all security functions to include the following security management functions: (FMT_SMF.1)

- Enabling/Disabling of Audit functions*
- Review of Audit logs
- User Role Management
- Virtual LAN/Server Management
- Password Policy Management

- Node configuration (traffic management)
- Pool configuration (traffic management)
- Protocol Profile configuration (traffic management)
- iRules configuration
- Enable/Disable Nodes

*note: disable function applies only the audit (type) logs

Audit related attributes can be set only by the TOE Administrator through the logging screens in the GUI.

Node Configuration

Backend servers supported by the TOE appliance are configured on the appliance as nodes. The Administrator configures the nodes based on address settings, name, health/performance monitors to place on the node (detect network resource failure), availability decision (# of monitors required for use), ratio weighting for load balancing and the maximum number of concurrent connections to allow on the node.

Connection Pools

Backend server resource nodes can be pooled to allow for greater flexibility in managing traffic. These pools batch node resource and are established by the Administrator through settings which include: health/performance monitor requirements for a Pool to be active, Pool switching guidelines in the event of failure, ramp time to apply a gradually increasing amount of traffic to a newly switched pool, Quality of Service requirements, and which load balancing technique to use (round robin is default).

Profiles

Profiles are provided within the BIG-IP appliance to allow administrators to configure application specific network traffic in specific ways based on protocol type (Fast L4, Fast HTTP, TCP, UDP), Services type (HTTP, FTP), Session Persistence options, Authentication profiles (LDAP, RADIUS), Connection Pooling. These profiles are objects that contain configuration settings based on the type of traffic behavior or protocol in use. For example, the TOE can be configured through profiles to compress HTTP response data.

Management of Security Function behavior (FMT_MOF.1a, FMT_MOF.1b, FMT_MOF.1c)

Through the security management security function, authorized administrative users can access configurations options that allow the tailoring of security function behavior based on each deployment scenario. Access to these settings is controlled via Role based access controls as described above.

The Administrator role may either disable, enable or modify the behavior of the Audit security function. For example, the Administrator could enable or disable certain types of audit records or aspects of the Audit function for troubleshooting or evaluation purposes. In such a case, an

audit record is generated to indicate the activation or inactivation of auditing prior to the change being executed.

Settings available through the GUI, related to the Authentication function, Information Flow Control function and Security Management function allow the Administrator to modify the behavior of these security functions. This security function behavior may be modified through security attribute configuration as detailed in FMT_MSA.1a.

Users authenticated under the Operator role may enable or disable the operational status of Nodes which may be required based on performance issues or failure of particular nodes or servers within the environment. Operators may be assigned to specific Nodes and manage those resources using by enabling and disable operational status as needed as described in FMT_MSA.1b.

Protected TSF data access – (FMT_MTD.1a, FMT_MTD.1b, FMT_MTD.1c, FMT_MTD.d)

Access to modify TSF data is restricted based on the specific type of data and the User's authenticated role. Administrators who are properly authenticated local to the BIG-IP appliance in the Administrator role may query, delete or modify User Roles, Passwords, and SSL certificate data. Audit records may be queried or deleted by the Administrator; however, they may not be modified by any user.

Administrators, Operators or Guests may query audit records

6.1.5 Secure Communications*

Secure Communications:

(FPT_ITC.1, FPT_ITI.1, FCS_COP.1b,c,d FCS_CKM.1b,c,d, FMT_MSA.2)

The TOE provides secure communication channels for Administrator access through an SSL[2] protected web-based UI or SSH. A dedicated Gigabit management port is provided for remote SSH or web-based UI access, although other ports may also be used.

No TSF data is accessible prior to establishment of a valid SSL or SSH connection through validated certificates.

Administrator GUI based access requires physical connectivity to the management port through the dedicated LAN, establishment of the SSL session through username and password and accurate configuration to the applicable IP address. The TOE features centralize control of Client/Server Key and Certificates when configured for local Key Management for SSL.

[2] The evaluation laboratory did not evaluate the cryptography related to SSL sessions.

Certificates may be self signed or issued from a Certificate Authority (CA). All certificates created include expiration dates.

The TOE by default uses uniquely generated 1024 bit RSA keys with self-signed certificates. An Administrator may generate new keys of 512, 1024 or 2048 bits. Theses keys may also be signed by any signing authority. The TOE access requires that secure attributes are utilized to direct cryptographic operations through the minimum session requirements noted below.

Administrative session keys generated by the TOE utilize the following algorithm/key sizes for SSL based GUI access:

RC4 – 128 bit
DES – 56 bits or greater
3DES – 112 bits or greater
AES – 128 bits or greater

Administrative session keys are generated using an OpenSSL based software pseudo-random number generator which produces Diffie-Hellman asymmetric keys and symmetric keys based on the key pair definitions listed within Appendix A.

This represents the minimum values accepted for SSL session negotiation with the management computer in the IT Environment.

CLI access can be made through direct console connection to the TOE or via establishment of the SSH tunnel through authenticated username and password. The Common Criteria excludes all uses of the CLI except for initial IP configuration. Session keys for SSH are generated using OpenSSH utilizing cipher block chaining (CBC) mode with an HMAC of the MD5 hash with an AES key size of 128 bits.

***note: Cryptographic functionality correctness represented by these claims and algorithm usage is based on F5 Networks assertion of product usage.**

6.1.6 Secure Traffic*

Secure Traffic:

(FDP_IFF.1, FDP_UCT.1, FDP_UIT.1, FCS_CKM.1a,c,d FCS_COP.1a,c,d FMT_MSA.2)

The TOE enforces requirements on communications through the Traffic Information Flow Control Security Function Policy (SFP). For non-secure communications, the TOE ensures that the presumed IP address of the source/destination subject translates to a configured VLAN resource, identification and authentication has been validated and that monitors indicate the client servers are enabled by BIG-IP to process traffic.

The transfer of data between the BIG-IP appliance and Back-end Servers (trusted IT products) is protected from disclosure, modification or deletion through the flow control mechanisms

enforced by the Traffic Management Flow Control SFP. When required, the BIG-IP appliance may be configured to encrypt traffic flows to back-end server pools to provide added security during transit (FCS_COP.EXP.1).

For secure traffic, in addition to the requirements above, the Traffic Information Flow SFP requires that a successful SSL session has been established through verified key exchange and certificate validation. Pool members are authenticated by their virtual LAN server address and the status of the pool member being enabled.

The TOE provides SSL offloading functions (when so configured) which allows the BIG-IP Appliance to establish sessions between traffic users attempting to connect using SSL with backend web servers. The BIG-IP performs the negotiation and Internet Key Exchange (IKE) utilizing ciphers included in the SSLv2, SSLv3 or TLS protocol. These ciphersuite algorithms and key sizes are listed in Appendix A. Secure security attributes reflecting the use and type of session keys are required by the TOE for SSL session cryptography settings.

SSL traffic session keys are generated using an OpenSSL based software pseudo-random number generator which produces Diffie-Hellman asymmetric keys and symmetric keys based on the key pair definitions listed within Appendix A.

These session keys are generated by the RSA key generation algorithm based on TOE configuration. RSA key lengths of 512, 1024, 2048 and 4096 are supported by the TOE for SSL traffic in accordance with Public Key Cryptography Specification (PKCS) #1.

Session persistence may be configured in the Evaluated Configuration to enable traffic based on previously established authentication for a specified period of time as configured by the TOE Administrator.

The TOE uses three components to cryptographically secure traffic.

- The Cavium Nitrox™ Security Macro Processor resides on a mezzanine board in the BIG-IP unit and provides hardware-assistance for SSL handshake processing, asymmetric RSA cryptographic operations, symmetric ciphers (3DES, RC4, AES) and cryptographic hashing functions (HMAC, MD5, SHA-1).
- The TMM MicroKernel manages the SSL handshake and SSL record processing.
- The OpenSSL library component provides support to the TMM MicroKernel for X509 certificate verification operations.

The TOE manages SSL connections based on Administrator established profiles. The two types of SSL profiles within the TOE are Client and Server.

- Client profiles allow the TOE to manage SSL connections for connections coming into the TOE from the (WAN) client system.

- Server profiles allow the TOE to process encryption tasks for connections being sent from the TOE to a target server, effectively representing the (WAN) client with certificate credentials on behalf of the client.

Where appropriate, secure connections may be Administrator configured to be re-encrypted within the TOE prior to routing to the client to maintain a secure channel at all times. This configuration is not required in the CC evaluated configuration (FCS_COP.EXP.1).

When SSL termination is selected within the TOE, certificate verification and revocation checks are executed within the TOE.

SSL session persistence may be enabled based on Administrator configurable Client or Server SSL persistence profiles but is not required in the CC Evaluated Configuration.

The ciphers that the LTM system portion of the TOE supports are include SSLv2, SSLv3 and TLS supported ciphersuites as listed in Appendix A.

***note: Cryptographic functionality correctness represented by these claims and algorithm usage is based on F5 Networks assertion of product usage.**

6.1.7 Protection of the TOE

Protection of the TSF: (FPT_ITC.1, FPT_ITI.1, FPT_RVM.1)

Physical and logical protection of the TOE is required to assure that TOE related security functions are not bypassed or altered. This is provided by the TOE and Operating System Environment identification and authentication features and through the secure communication methods described in 6.1.5. All TOE interfaces require identification and authentication at the administrator level to allow access to TSF functions.

Physical protection of the TOE and physical access restrictions are provided by the A.LOCATE and A.USE assumptions, assuring a controlled restricted environment and exclusive use.

TM/OS based TOE Protection

The traffic management operating system restricts the OS from executing operations that have not been pre-approved based on the range of uses within the BIG-IP appliance. The security policy of allowed operations is fixed by F5 during the software build process. Any functionality not explicitly allowed is disabled within the Operating System. Therefore, remote exploits that can cause code execution may be rendered ineffective. As an example, if an attacker were able to exploit previously unknown remote code execution vulnerability in Apache, the attempt to execute remote code would be limited to only those operations that Apache could normally do. Since Apache is limited to read access for only allowed web files, the attacker would not be able to read or write important files on the system. The attacker would also not be able to execute a shell, or any other privileged code.

Protection of the TOE – Domain Separation (FPT_SEP.1)

The TM/OS provides TSF Domain Separation by protecting the TSF from subjects initiating actions through its interfaces through the functionality of the underlying Operating System, which restricts access to the TSF to authorized Administrators. Access controls enforced by the OS support this separation as well as flow control policies implemented through the TMM module which assure that the routing of TSF data or traffic conforms to the Traffic Management information flow SFP.

The TOE has a clear separation between administrative configuration and information flow (traffic). Configuration information lives within (Master Control Process daemon) MCPd* and other daemons. Information flow only travels through the TMM subsystem as depicted below. That traffic information flow may be modified based upon configuration settings (through altered behavior of the TMM), but the actual flow never touches the configuration.

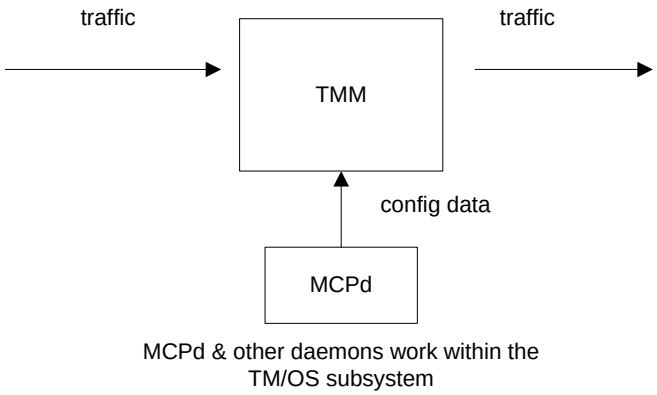

Figure 4: Conceptual drawing showing isolation of traffic & configuration data

* MCPD is a message passing and configuration storage daemon. When other processes receive configuration data from an external source, such as the GUI or user interaction, the data is sent to MCPD, where it is stored and sent to processes that may be interested in the data. MCPD is commonly known as a message pump.

Protection of TOE Flow Control:

The TOE OS also protects itself through the Local Traffic Manager based on configurable settings. If suspicious traffic meets predefined criteria, the LTM system can direct such traffic to specific servers, thereby mitigating potential damage in the event of an attack. The system also can be configured to alert Administrators to a suspected attack or TOE penetration attempt. Local Traffic Manager security features include:

- Packets that are determined to be unauthorized or with questionable content are rejected and discarded to protect TOE resources.
- Authentication failures are logged providing a resource to determine if

unauthorized personnel may be attempting to access TSF functions.

- Fragmented packets may be reassembled to stop fragmentation attacks.

Denial of Service Protection (FRU_RSA.1a, FRU_RSA.1b, FDP_IFF.1)

Availability is protected via the use of SYN cookies. When a predetermined threshold is reached for new or untrusted connections, the SYNCheck™ feature is activated, initiating the use of SYN cookies. This allows for mitigation of attempted SYN ACK DoS type attacks. The number of new or untrusted TCP connections that can be established before the system activates the SYN Cookies authentication method for subsequent TCP connections is set by default at 16834 to protect against DoS (SYN ACK) based attacks.

Also configurable for DoS protection is the Reaper High Water Mark function. Based on Administrator configured memory usage settings, the TOE will stop accepting new connections upon reaching the set threshold. The default setting for memory usage is set at 90%. Once the system meets the "Reaper High-Water Mark", the system does not establish new connections until the memory usage drops below the "reaper low-water mark" to protect against DoS through resource exhaustion.

Protection through audit functions and traceability (FPT_STM.1):

An audit function directed by the OS syslog feature assures that events which could indicate attempted compromise of the TOE are logged by Timestamp, Username, Transaction Type and Event. Administrator changes to the TSF that could relate to security related protection issues within the TOE are also audited.

Failure in Secure State (FPT_FLS.1, FRU_FLT.1, FPT_ITA.1):

The Evaluated Configuration of the TOE is in the High Availability Redundant Pair configuration allowing for maximum availability under various failure conditions.
The BIG-IP appliance assures a minimum of 97% uptime given the Common Criteria Evaluated Configuration (high availability redundant pair).

The TOE preserves a secure state during any of the following failure conditions:

1) Operational failure of a Server Node
    - BIG-IP reroutes traffic per the Traffic Management SFP
2) Loss of sufficient availability in a given Pool or Server Node
    - BIG-IP reroutes traffic per the Traffic Management SFP
3) Operational failure of a single TOE hardware device
    - Fail-Over is executed with no loss of traffic & TSF when configured in the Evaluated Configuration.
4) Operational failure of a single TOE hardware device
    - Fail-Over is executed with no loss of traffic & TSF when configured in the Evaluated Configuration.

The TOE is protected from software or hardware failures via a "Fail-over" system facilitated by a hardwired serial connection between two identical BIG-IP hardware units configured in redundant fail over configuration. The TOE utilizes a process called Connection mirroring to keep a stateful record of each connection on both the active and the standby unit. This ensures a reliable flow of traffic, even if the active unit fails unexpectedly.

The following redundant features are available:

- Failover – defines behavior relating to protection of availability via failover redundancy functionality
- Configuration synchronization – defines behavior related to synchronizing the TOE's redundant pair configuration
- System fail-safe – related to fail safe operation parameters

When properly configured by the Administrator, the BIG-IP system will switch traffic from the failed unit to the Active Standby unit automatically.

When System FailSafe is configured, the BIG-IP system monitors various hardware components, as well as the heartbeat of the adjacent appliance, and takes action if the system detects a failure. A delay in communication of the heartbeat signal of <200mS will result in the non-responding appliance being set to "inactive".

Two fail-safe monitors assist the TOE in providing this function:

- Gateway fail-safe: monitors traffic between the active BIG-IP system and a pool containing a gateway router, thereby protecting the system from a loss of an internet connection by triggering a failover when a gateway router is unreachable for a specified duration.

- VLAN fail-safe: monitors traffic and based on a loss of traffic during the fail-safe timeout period. The system generates ARP (Address Resolution Protocol) requests to nodes accessible through the VLAN to attempt to generate traffic. If the system does not receive traffic before the timeout period expires, then fail-over may be initiated and control switched to the standby unit.

For maximum reliability, the BIG-IP system supports failure detection on all VLANs. Through the fail-safe option on a VLAN, the BIG-IP system monitors network traffic going through a VLAN.

Remote transfer of TSF data (FPT_ITC.1, FPT_ITI.1, FCS_COP.1b,c,d FCS_CKM.1b,c,d)
The TOE allows only remote Administrator access to TSF data via SSL, TLS or SSH secure transmissions as described in the Secure Communications Section: 6.1.5.

Protection of the TOE's TSF related data types is assured through secure transmission techniques (SSL, TLS or SSH) and dedicated Administrator networks as required through the Administrator Guidance document and as depicted in Figure 3: TOE physical boundaries. Administrator sessions between the management computer and the TOE are secured using one of the following supported algorithms/key sizes:

RC4 – 128 bit
DES – 56 bits or greater
3DES – 112 bits or greater
AES – 128 bits or greater

These keys are generated by default using the 1024 bit RSA key generation algorithm conforming to the Public key cryptography standard (PKCS) #1. Key generation for this purpose is enacted through the use of OpenSSL, which includes a software based random number generator producing Diffie-Hellman asymmetric keys (SHA, MD5) and symmetric key pair combinations as listed in Appendix A.

(FPT_SEP.1) A dedicated Administrator management port and secure transmission assure the confidentiality of TSF data to trusted IT products and prevents modification during transfer.

The TOE detects potential modification of data transmitted by identification of a single MAC error during a given transmission and provides for verification of the integrity of all transmissions. Packets that are determined to be unauthorized or containing questionable content are rejected and discarded to protect TOE resources.

Authentication failures are logged providing a resource to determine if unauthorized personnel may be attempting to access TSF functions.

6.2 Security Assurance Measures

The documentation titles in the table below will be updated with new titles and version numbers during the course of the evaluation.

Assurance Requirement	Assurance Components
ACM_CAP.2	The description of the configuration items is provided in F5 Networks BIG-IP® Traffic Manager 6400 High Availability pair (qty 2) EAL 2 Configuration Management Documentation, 05-948-R-0145
ADO_DEL.1	The description of the delivery procedures is provided in Common Criteria Supplement EAL2 Secure Delivery Document F5 Networks BIG-IP® Traffic Manager 6400 High Availability pair (qty 2) ,05-948-R-0144

Assurance Requirement	Assurance Components
ADO_IGS.1	The installation, generation, and start-up procedures are provided in Installation, Licensing, and Upgrades for BIG-IP® Systems Version 9.2 MAN-0184-00 BIG-IP® Quick Start Instructions PUB-0089-03 1205 Common Criteria Supplement EAL2 F5 Networks BIG-IP® Local Traffic Manager 6400 High Availability pair (qty 2) Document ID: 05-948-R-0134
ADV_FSP.1	The informal functional specification is provided in EAL 2 Design Documentation F5 Networks BIG-IP® , 06-948-R-0011
ADV_HLD.1	The descriptive high-level design is provided in EAL 2 Design Documentation F5 Networks BIG-IP® , 06-948-R-0011.
ADV_RCR.1	The informal correspondence demonstration is provided in EAL 2 Design Documentation F5 Networks BIG-IP® , 06-948-R-0011.
AGD_ADM.1	The administrator guidance is provided in the following documents: BIG-IP® Network and System Management Guide version 9.2.3 MAN-0185-02 Configuration Guide for Local Traffic Management version 9.2.0 MAN-0182-00 Platform Guide: 1500, 3400, 6400, and 6800 MAN-0183-00 August 16, 2006. Configuration Worksheet PUB-0090-02 0905 Common Criteria Supplement EAL2 F5 Networks BIG-IP® Local Traffic Manager 6400 High Availability pair (qty 2) Document ID: 05-948-R-0134
AGD_USR.1	This Assurance Measure is N/A *See Below
ATE_COV.1	The evidence of coverage is provided in Tests Activity ATE F5 Networks BIG-IP® Traffic Manager 6400 High Availability pair (qty 2) EAL 2,06-948-R-0041
ATE_FUN.1	The functional testing description is provided in Tests Activity ATE F5 Networks BIG-IP® Traffic Manager 6400 High Availability pair (qty 2) EAL 2,06-948-R-0041.
ATE_IND.2	The TOE and testing documentation were made available to the CC testing laboratory for independent testing.
AVA_SOF.1	The strength of function analysis performed is provided in EAL 2 Strength of Function Analysis F5 Networks BIG-IP® Local Traffic Manager 6400 High Availability pair (qty 2), 06-948-R-0012
AVA_VLA.1	The vulnerability analysis performed is provided in F5 Networks BIG-IP® Local Traffic Manager 6400 High Availability pair (qty 2) Common Criteria Vulnerability Analysis AVA_VLA.1 EAL 2, 05-948-R-0148
ALC_FLR.1	The Flaw Remediation description is provided in EAL 2 Basic Flaw Remediation F5 Networks BIG-IP® Traffic Manager 6400 High Availability pair (qty 2), TBD

Table 15: Assurance Requirements: EAL2 Augmented ALC_FLR.1

***Note: Product usage is transparent to network users therefore this requirement (AGD_USR.1) requirement is vacuously satisfied (ref: PD-0106: Situations Where AGD_USR May Be Vacuously Satisfied)**

6.3 Rationale for TOE Security Functions

This section provides a table demonstrating the tracing of TOE security functions back to aspects of the security functional requirements (SFRs).

A justification that the security functions are suitable to cover the SFRs can be found in Section 6.1.

	ID & Authentication	Audit	Info. Flow Control	Security Management	Secure Communications	Secure Traffic	Protection of the TOE
FAU_ARP.1		X					
FAU_SAA.1		X					
FAU_GEN.EXP.1		X					
FAU_SAR.1		X					
FAU_SAR.3a		X					
FAU_SAR.3b		X					
FAU_SAR.3c		X					
FAU_STG.1		X					
FAU_STG.4		X					
FCS_CKM.1a						X	
FCS_CKM.1b					X		X
FCS_CKM.1c					X	X	X
FCS_CKM.1d					X	X	X
FCS_COP.1a						X	
FCS_COP.1b					X		X

	ID & Authentication	Audit	Info. Flow Control	Security Management	Secure Communications	Secure Traffic	Protection of the TOE
FCS_COP.1c					X	X	X
FCS_COP.1d					X	X	X
FCS_COP.EXP.1						X	
FDP_IFC.1a			X				
FDP_IFC.1b			X				
FDP_IFF.1a			X			X	X
FDP_IFF.1b			X			X	X
FDP_UCT.1			X			X	
FDP_UIT.1			X			X	
FIA_ATD.1	X						
FIA_UAU.1	X						
FIA_UAU.2	X						
FIA_UAU.EXP.1	X						
FIA_UID.2	X						
FIA_UID.EXP.1	X						
FMT_MOF.1a				X			
FMT_MOF.1b				X			
FMT_MSA.1a				X			
FMT_MSA.1b				X			
FMT_MSA.2					X	X	
FMT_MSA.3				X			
FMT_MTD.1a				X			
FMT_MTD.1b				X			

	ID & Authentication	Audit	Info. Flow Control	Security Management	Secure Communications	Secure Traffic	Protection of the TOE
FMT_MTD.1c				X			
FMT_MTD.1d				X			
FMT_SMF.1				X			
FMT_SMR.1				X			
FPT_FLS.1							X
FPT_ITA.1	X						X
FPT_ITC.1	X				X		X
FPT_ITI.1	X				X		X
FPT_RVM.1							X
FPT_SEP.1							X
FPT_STM.1		X					X
FRU_FLT.1			X				X
FRU_PRS.1			X				
FRU_RSA.1a							X
FRU_RSA.1b							X

Table 16: TOE Security Function to SFR Mapping

6.4 Appropriate Strength of Function Claim

The claim of SOF-basic for the Identification and Authentication security function is consistent with the claim of SOF-basic for FIA_UAU.2 and FIA_UAU.EXP.1 SFRs that map to that security function.

6.5 Rationale for Security Assurance Measures

The assurance documents listed below were developed to meet the developer action and content and presentation of evidence elements for each assurance required defined in the CC.

The documentation titles in the table below will be updated with new titles and version numbers

during the course of the evaluation.

Assurance Requirement	Assurance Measures	Assurance Rationale
ACM_CAP.2	F5 Networks BIG-IP® Traffic Manager 6400 High Availability pair (qty 2) EAL 2 Configuration Management Documentation, 05-948-R-0145	The configuration management documents defines the configuration items and contains the necessary information to demonstrate that a CM system is used and that there is a unique reference for the TOE.
ADO_DEL.1	Common Criteria Supplement EAL2 Secure Delivery Document F5 Networks BIG-IP® Traffic Manager 6400 High Availability pair (qty 2) ,05-948-R-0144	The delivery document describes the steps performed to deliver the TOE. It describes the process used to create distribution copies of the TOE software and the steps taken to ensure consistent, dependable delivery of the TOE to the customer.
ADO_IGS.1	Installation, Licensing, and Upgrades for BIG-IP® Systems Version 9.2 MAN-0184-00 BIG-IP® Quick Start Instructions PUB-0089-03 1205 Common Criteria Supplement EAL2 F5 Networks BIG-IP® Local Traffic Manager 6400 High Availability pair (qty 2) Document ID: 05-948-R-0134	The installation, documents describe the steps necessary for secure installation, generation and start-up of the TOE.
ADV_FSP.1	EAL 2 Design Documentation F5 Networks BIG-IP® , 06-948-R-0011	The informal functional specification document identifies the external interfaces that completely represent the TSF and describes the purpose and method of use of all external TSF interfaces. It also describes the effects, exceptions, and error messages for each of the external TSF interfaces.
ADV_HLD.1	EAL 2 Design Documentation F5 Networks BIG-IP® , 06-948-R-0011.	The descriptive high-level design describes the complete TSF in terms of subsystems. The security functions for each subsystem are described. The subsystem interfaces are defined and the externally visible interfaces are identified.

Assurance Requirement	Assurance Measures	Assurance Rationale
ADV_RCR.1	EAL 2 Design Documentation F5 Networks BIG-IP® , 06-948-R-0011.	The informal correspondence document maps the security functionality as described in the FSP and ST and as described in the FSP and HLD.
ALC_FLR.1	EAL 2 Basic Flaw Remediation F5 Networks BIG-IP® Traffic Manager 6400 High Availability pair (qty 2), 06-948-R-0064	Flaw Remediation outlines the sponsor's process to address security related product issues
AGD_ADM.1	BIG-IP® Network and System Management Guide version 9.2.3 MAN-0185-02 Configuration Guide for Local Traffic Management version 9.2.0 MAN-0182-00 Platform Guide: 1500, 3400, 6400, and 6800 MAN-0183-00 August 16, 2006. Configuration Worksheet PUB-0090-02 0905 Common Criteria Supplement EAL2 F5 Networks BIG-IP® Local Traffic Manager 6400 High Availability pair (qty 2) Document ID: 05-948-R-0134	The Administrator guidance documents provide complete administrative guidance for the TOE, including all security features and configuration items.
AGD_USR.1	*N/A*	*The only users of the TOE are Administrative users therefore, separate User level Guidance is not applicable
ATE_COV.1	Tests Activity ATE F5 Networks BIG-IP® Traffic Manager 6400 High Availability pair (qty 2) EAL 2,06-948-R-0041	The test coverage document provides a mapping of the test cases performed against the TSF.
ATE_FUN.1	Tests Activity ATE F5 Networks BIG-IP® Traffic Manager 6400 High Availability pair (qty 2) EAL 2,06-948-R-0041.	The functional testing document includes the test plans, test procedures, and associated test cases of the TOE functional testing effort.
ATE_IND.2	F5 Networks BIG-IP® Traffic Manager 6400 High Availability Pair (qty2) Independent Testing Test Plan 06-948-R-0065	The TOE hardware, software, guidance, and testing documentation were made available to the CC testing laboratory for independent testing.

Assurance Requirement	Assurance Measures	Assurance Rationale
AVA_SOF.1	EAL 2 Strength of Function Analysis F5 Networks BIG-IP® Local Traffic Manager 6400 High Availability pair (qty 2), 06-948-R-0012	The strength of function analysis document provides the SOF argument for the password mechanism.
AVA_VLA.1	F5 Networks BIG-IP® Local Traffic Manager 6400 High Availability pair (qty 2) Common Criteria Vulnerability Analysis AVA_VLA.1 EAL 2, 05-948-R-0148	The vulnerability analysis document identifies and describes the process used to discover obvious vulnerabilities, the results of the vulnerability analysis, and the mitigation of each identified obvious vulnerability.

Table 17: Rationale for Security Assurance Measures

***Product usage is transparent to network users therefore this requirement (AGD_USR.1) requirement is vacuously satisfied (ref: PD-0106: Situations Where AGD_USR May Be Vacuously Satisfied)**

7 Protection Profile Claims

This Security Target does not claim conformance to any Protection Profiles.

8 Rationale

This Security Target does not claim conformance to any Protection Profiles.

8.1 Security Objectives Rationale

Sections 4.3 - 4.6 provide the security objectives rationale.

8.2 Security Requirements Rationale

Sections 5.7 - 5.11 provide the security requirements rationale.

8.3 TOE Summary Specification Rationale

Sections 6.3 - 6.5 provide the TOE summary specification rationale.

8.4 Protection Profile Claims Rationale

This Security Target does not claim conformance to any Protection Profiles.

9 Appendix A – OpenSSL Ciphers available for use for SSL Traffic

The BIG-IP appliance when set for SSL offloading of backend servers, provides SSL negotiation and termination on behalf of backend web servers, but does not (by default) provide more restrictive control over SSL sessions than the web servers themselves. Based on this any SSLv2, SSLv3 or TLS cipher suites can be processed by the TOE.

CIPHER SUITE NAMES

The following lists give the SSL or TLS cipher suites names from the relevant specification and their OpenSSL equivalents. The BIG-IP Appliance utilizes OpenSSL for generation of SSL session keys.

SSL v3.0 cipher suites.

SSL or TLS cipher suites names	OpenSSL equivalents
SSL_RSA_WITH_NULL_MD5	NULL-MD5
SSL_RSA_WITH_NULL_SHA	NULL-SHA
SSL_RSA_EXPORT_WITH_RC4_40_MD5	EXP-RC4-MD5
SSL_RSA_WITH_RC4_128_MD5	RC4-MD5
SSL_RSA_WITH_RC4_128_SHA	RC4-SHA
SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5	EXP-RC2-CBC-MD5
SSL_RSA_WITH_IDEA_CBC_SHA	IDEA-CBC-SHA
SSL_RSA_EXPORT_WITH_DES40_CBC_SHA	EXP-DES-CBC-SHA
SSL_RSA_WITH_DES_CBC_SHA	DES-CBC-SHA
SSL_RSA_WITH_3DES_EDE_CBC_SHA	DES-CBC3-SHA
SSL_DH_DSS_EXPORT_WITH_DES40_CBC_SHA	Not implemented.
SSL_DH_DSS_WITH_DES_CBC_SHA	Not implemented.
SSL_DH_DSS_WITH_3DES_EDE_CBC_SHA	Not implemented.
SSL_DH_RSA_EXPORT_WITH_DES40_CBC_SHA	Not implemented.
SSL_DH_RSA_WITH_DES_CBC_SHA	Not implemented.
SSL_DH_RSA_WITH_3DES_EDE_CBC_SHA	Not implemented.
SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA	EXP-EDH-DSS-DES-CBC-SHA
SSL_DHE_DSS_WITH_DES_CBC_SHA	EDH-DSS-CBC-SHA
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA	EDH-DSS-DES-CBC3-SHA
SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA	EXP-EDH-RSA-DES-CBC-SHA

SSL_DHE_RSA_WITH_DES_CBC_SHA	EDH-RSA-DES-CBC-SHA
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA	EDH-RSA-DES-CBC3-SHA
SSL_DH_anon_EXPORT_WITH_RC4_40_MD5	EXP-ADH-RC4-MD5
SSL_DH_anon_WITH_RC4_128_MD5	ADH-RC4-MD5
SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA	EXP-ADH-DES-CBC-SHA
SSL_DH_anon_WITH_DES_CBC_SHA	ADH-DES-CBC-SHA
SSL_DH_anon_WITH_3DES_EDE_CBC_SHA	ADH-DES-CBC3-SHA
SSL_FORTEZZA_KEA_WITH_NULL_SHA	Not implemented.
SSL_FORTEZZA_KEA_WITH_FORTEZZA_CBC_SHA	Not implemented.
SSL_FORTEZZA_KEA_WITH_RC4_128_SHA	Not implemented.

TLS v1.0 cipher suites

TLS_RSA_WITH_NULL_MD5	NULL-MD5
TLS_RSA_WITH_NULL_SHA	NULL-SHA
TLS_RSA_EXPORT_WITH_RC4_40_MD5	EXP-RC4-MD5
TLS_RSA_WITH_RC4_128_MD5	RC4-MD5
TLS_RSA_WITH_RC4_128_SHA	RC4-SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5	EXP-RC2-CBC-MD5
TLS_RSA_WITH_IDEA_CBC_SHA	IDEA-CBC-SHA
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA	EXP-DES-CBC-SHA
TLS_RSA_WITH_DES_CBC_SHA	DES-CBC-SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA	DES-CBC3-SHA
TLS_DH_DSS_EXPORT_WITH_DES40_CBC_SHA	Not implemented.
TLS_DH_DSS_WITH_DES_CBC_SHA	Not implemented.
TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA	Not implemented.
TLS_DH_RSA_EXPORT_WITH_DES40_CBC_SHA	Not implemented.
TLS_DH_RSA_WITH_DES_CBC_SHA	Not implemented.
TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA	Not implemented.
TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA	EXP-EDH-DSS-DES-CBC-SHA
TLS_DHE_DSS_WITH_DES_CBC_SHA	EDH-DSS-CBC-SHA
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	EDH-DSS-DES-CBC3-SHA
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA	EXP-EDH-RSA-DES-CBC-SHA

TLS_DHE_RSA_WITH_DES_CBC_SHA	EDH-RSA-DES-CBC-SHA
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	EDH-RSA-DES-CBC3-SHA
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5	EXP-ADH-RC4-MD5
TLS_DH_anon_WITH_RC4_128_MD5	ADH-RC4-MD5
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA	EXP-ADH-DES-CBC-SHA
TLS_DH_anon_WITH_DES_CBC_SHA	ADH-DES-CBC-SHA
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA	ADH-DES-CBC3-SHA

Additional Export 1024 and other cipher suites

Note: these ciphers can also be used in SSL v3.

TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA	EXP1024-DES-CBC-SHA
TLS_RSA_EXPORT1024_WITH_RC4_56_SHA	EXP1024-RC4-SHA
TLS_DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA	EXP1024-DHE-DSS-DES-CBC-SHA
TLS_DHE_DSS_EXPORT1024_WITH_RC4_56_SHA	EXP1024-DHE-DSS-RC4-SHA
TLS_DHE_DSS_WITH_RC4_128_SHA	DHE-DSS-RC4-SHA

SSL v2.0 cipher suites.

SSL_CK_RC4_128_WITH_MD5	RC4-MD5
SSL_CK_RC4_128_EXPORT40_WITH_MD5	EXP-RC4-MD5
SSL_CK_RC2_128_CBC_WITH_MD5	RC2-MD5
SSL_CK_RC2_128_CBC_EXPORT40_WITH_MD5	EXP-RC2-MD5
SSL_CK_IDEA_128_CBC_WITH_MD5	IDEA-CBC-MD5
SSL_CK_DES_64_CBC_WITH_MD5	DES-CBC-MD5
SSL_CK_DES_192_EDE3_CBC_WITH_MD5	DES-CBC3-MD5