National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

F5 Networks
Seattle, WA

BIG-IP® Local Traffic Manager 6400 (v9.2.3)
High Availability pair (qty 2)

Hardware P/N: 200-0153-05 Rev. C

Software Version: 9.2.3 + Hotfix CR69440

Report Number:	**CCEVS-VR-07-0024**
Dated:	**16 April 2007**
Version:	**1.5**

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Mr. Daniel P. Faigin
Ms. Nicole M. Carlson

The Aerospace Corporation
El Segundo, California

Common Criteria Testing Laboratory

Mr. Mark Plascencia
Mr. Clyde Sy
Ms. Sherie Kim

InfoGard Laboratories, Inc.
641 Higuera St. 2nd floor
San Luis Obispo, CA 93401

Much of the material in this report was extracted from evaluation material prepared by the CCTL. The CCTL team deserves credit for their hard work in developing that material. Many of the product descriptions in this report were extracted from the F5 Big IP Security Target.

Table of Contents

List of Figures

List of Tables

1 Executive Summary

This report is intended to assist the end-user of this product with determining the suitability of this IT product in their environment. End-users should review both the F5 BIG-IP Local Traffic Manager 6400 High Availability pair (qty 2) Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR) which describes how those security claims were evaluated. *This report specifically applies to Hardware P/N: 200-0153-05 Rev. C, and LTM Software Version 9.2.3 + Hotfix CR69440v9.2.3 of the Local Traffic Manager.*

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the F5 BIG-IP Local Traffic Manager 6400 High Availability pair (qty 2), the target of evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This report is not an endorsement of the TOE by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation of the F5 BIG-IP Local Traffic Manager 6400 product was performed by InfoGard Laboratories, Inc., San Luis Obispo, CA in the United States and was completed on 16 April 2007. The information in this report is largely derived from the Security Target (ST), Evaluation Technical Report (ETR) and the functional testing report. The ST was written by InfoGard Laboratories. The evaluation was conducted in accordance with the requirements of the Common Criteria for Information Technology Security Evaluation, version 2.2, January 2004 Evaluation Assurance Level 2 (EAL2) - augmented, and the Common Evaluation Methodology for IT Security Evaluation (CEM), Version 2.2 January 2004.

The F5 BIG-IP Local Traffic Manager 6400 High Availability pair (qty 2)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 Secure Socket Layer (SSL) processing capabilities. Through effective implementation of the BIG-IP Appliance, users should be able to avoid additional infrastructure expense by effective use and traffic management of existing resources. The F5 BIG-IP appliance appears to provide efficiency gains through local traffic management techniques (LTM) and offloading processes, such as SSL processing, from back-end servers that should result in increased resource availability, thereby allowing increased traffic utilization from existing back-end server resources.

The BIG-IP product consists of the following components:

- **BIG-IP Hardware.** A hardware device, port-based, multilayer switch. 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.

- **Traffic Management MicroKernel (TMM).** This 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 Transmission Control Protocol (TCP), such as Hyper-Text Transfer Protocol (HTTP), File Transfer Protocol (FTP), and routing protocols over SSL or Online Certificate Status Protocol (OCSP). **Note:** Administrative documentation directs the administrator not to configure the system to use OCSP, and usage of an OCSP server is not evaluated as part of the Common Criteria Evaluated configuration.

- **Virtual Local Area Networks (VLANs).** VLANs are central to the functionality of the F5 BIG-IP appliance 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. There are two types of virtual servers configured for F5 BIG-IP appliance operation: Host and Network.

- **Pluggable Authentication Module (PAM).** This module runs under the BIG-IP operating system, and is a suite of shared libraries that enable the F5 BIG-IP appliance administrator to choose how applicable content server clients authenticate traffic. PAM allows separation of the authentication function from the core LTM system.

- **Virtual Network Interface Card (VNIC).** This is a BIG-IP operating system driver that transfers network packets to the TMM, where load balancing decisions are made.

- **Traffic Management Operating System (TM/OS)**. A customized implementation of a Linux OS. The security enhanced proprietary BIG-IP operating system proactively protects the operating system, services, modules and all applications from outsider or insider threats by restricting access to application functions only to those authorized. 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.

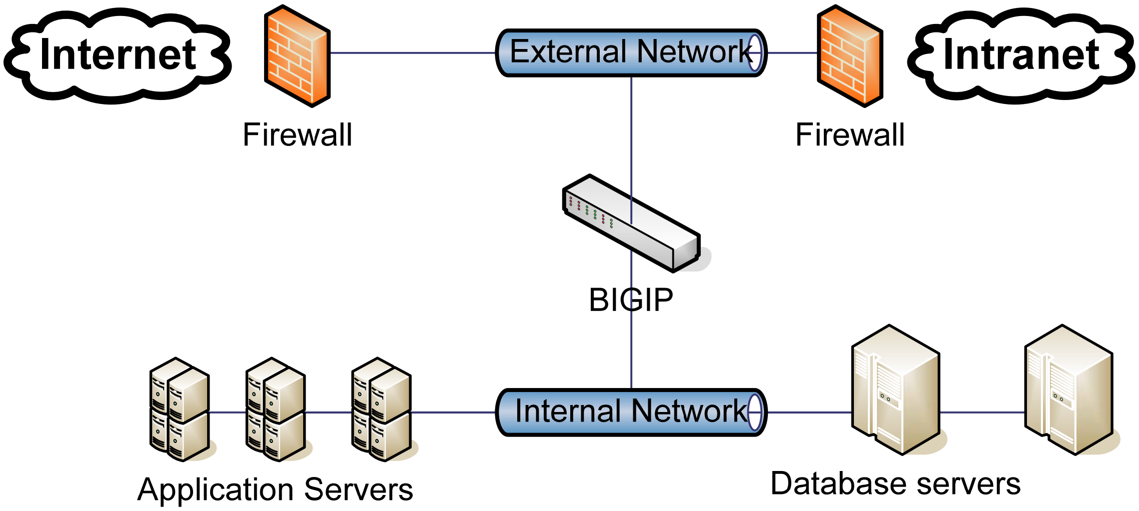

Figure 1. Use of the F5 BIG-IP Product in an Overall Network

It is important to note that the following components ***are included in the product but are excluded from the F5 BIG-IP appliance's evaluation***:

1. Application Security Module
2. Use of the Command Line Interface (CLI) (via console or Secure Shell (SSH)) for any purpose other than initial Internet Protocol (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:
    - Secure Network Management Protocol (SNMP) for 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)

The following components are present in the BIG-IP product and may provide significant functional capability, but are not security relevant and were not included in, or covered by, 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

2 Identification of the TOE

CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations.

Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for EAL 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL pay a fee for their product's NIAP Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The organizations and individuals participating in the evaluation.

Table 1. Product and Evaluation Identification

Evaluation Scheme	United States Common Criteria Evaluation Validation Scheme
Evaluated Target of Evaluation	BIG-IP® Local Traffic Manager 6400 (LTM v9.2.3) High Availability pair (qty 2) Hardware P/N: 200-0153-05 Rev. C Software Version: 9.2.3 + Hotfix CR69440
Protection Profile	Not applicable
Security Target	*BIG-IP® Local Traffic Manager 6400 High Availability pair (qty 2) Version 1.4, April 9, 2007*
Dates of evaluation	October 13, 2005 – April 16, 2007
Conformance result	Part 2 extended, Part 3 conformant, EAL 2 augmented with ALC_FLR.1
Common Criteria version	Common Criteria for Information Technology Security Evaluation Version 2.2
Common Evaluation Methodology (CEM) version	CEM version 2.2
Evaluation Technical Report (ETR)	Big-IP LTM 6400 ETR 06-948-R-0095 V1.4
Sponsor/Developer	F5 Networks 401 Elliot Avenue West Seattle, WA 98119
Common Criteria Testing Lab (CCTL)	InfoGard Laboratories
CCTL Evaluators	Mark Plascencia Clyde Sy Sherie Kim *InfoGard Laboratories*
CCEVS Validators	Daniel Faigin Nicole Carlson *The Aerospace Corporation*

3 Interpretations

The Evaluation Team performed an analysis of the international interpretations of the CC and the CEM and determined that none of the international interpretations issued by the Common Criteria Interpretations Management Board (CCIMB) identified below were applicable to this evaluation.

The F5 BIG-IP appliance is also compliant with all International interpretations with effective dates on or before October 13, 2005.

4 Security Policy

The Security Functional Policies (SFPs) implemented by the BIG-IP 6400 LTM provide a mechanism so that only identified/authenticated users have access to controlled resources, provide accountability for actions by logging security events, provide traffic flow policies, provide a mechanism to balance traffic flow when required and a protection mechanism that ensures the integrity of the security policies.

5 Assumptions

5.1 Physical Security Assumptions

A key environmental assumption is physical security, for it is assumed appropriate physical security protection will be applied to the BIG-IP 6400 LTM hardware and software commensurate with the value of the IT assets. This may be a facility with controlled access (which prevents unauthorized physical access), and the BIG-IP 6400 LTM can only be accessed by authorized users.

5.2 Personnel Security Assumptions

It is assumed that all authorized administrators are properly trained, not careless, not willfully negligent, or hostile, and will follow and abide by the instructions provided by the BIG-IP 6400 LTM documentation.

5.3 Operational Security Assumptions

It is also assumed that the operating environment will provide protection to the BIG-IP 6400 LTM and its related data, and that the TOE has access to all the IT System resources necessary to perform its functions. Lastly, it is assumed that the BIG-IP 6400 LTM is dedicated to its primary function and does not provide general purpose computing or storage capabilities.

5.4 Threats Countered and Not Countered

The BIG-IP 6400 LTM is designed to fully or partially counter the following threats:

- Administrators may make changes to BIG-IP 6400 LTM security functionality without accountability.
- An unauthorized user may masquerade as an authorized user or an authorized IT entity to gain access to data or BIG-IP 6400 LTM resources.
- Unintentional errors in implementation of the BIG-IP 6400 LTM deployment may occur, leading to flaws which may be exploited by a malicious User or program.

- Traffic may be routed to backend servers without prioritization, resulting in poor quality of service and loss of backend server availability for concurrent sessions.
- A malicious process or user may block others from BIG-IP 6400 LTM system resources (e.g., connection state tables) via a resource exhaustion denial of service attack.
- The failure of a BIG-IP 6400 LTM appliance may result in loss of traffic and/or failure to meet the appliance's security functions.
- An attacking user or process may cause, through an unsophisticated attack, BIG-IP 6400 LTM data or executable code to be inappropriately accessed (viewed, modified, or deleted).
- 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.
- Data Transfer between the BIG-IP Appliance and Administrator workstation may be modified or disclosed in transit.

5.5 Organizational Security Policies

There are no applicable organizational security policies

5.6 Clarification of scope

The BIG-IP 6400 LTM components that are excluded for the evaluated configuration are listed in the Executive summary in Section 1.

6 Evaluated configuration

The evaluated configuration consists of the appliance itself and requires the following components in the operating environment:

- Proper establishment of authentication servers (LDAP, RADIUS) (as required)
- Appropriate Firewall for WAN access (as required)

6.1 Architectural Information

The BIG-IP 6400 LTM is a configurable hardware and software solution that provides the ability to load balance and optimize network and application traffic. The BIG-IP system increases the speed and maximizes the availability of network resources by using compression, offloading SSL processes, caching data, using session persistence, and other traffic optimization techniques

The high-level architecture of the BIG-IP 6400 LTM is shown in Figure 2.

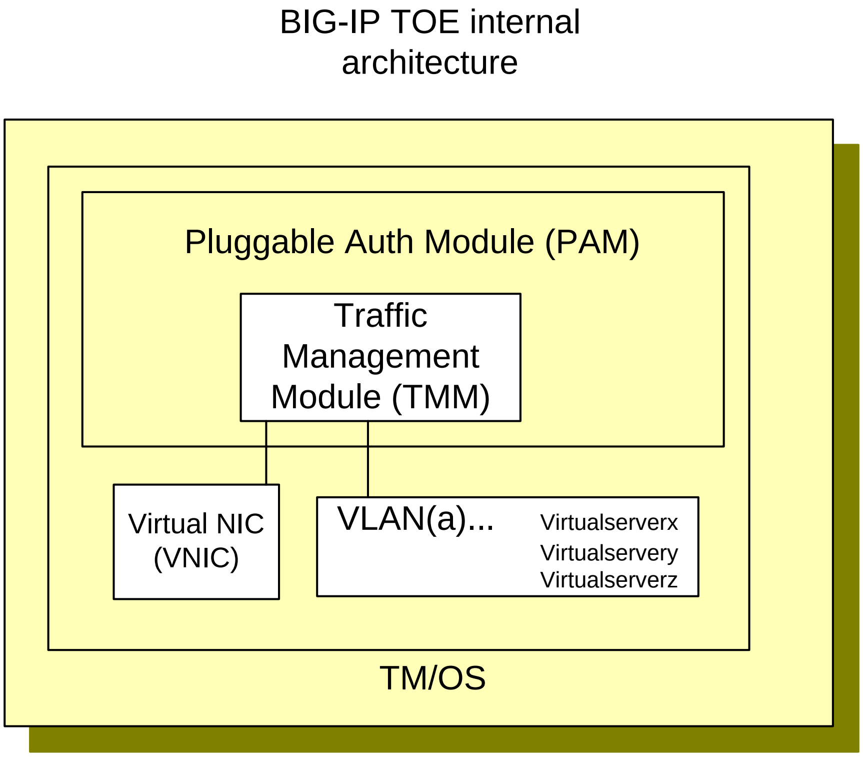

Figure 2. BIG-IP TOE High-Level Architecture

Note that the BIG-IP LTM 6400 is an appliance that includes an operating system and hardware components.

The BIG-IP Appliance consists of the following components

- **BIG-IP Hardware**. 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 sixteen (16) copper, Gigabit level ports and four (4) fiber optic Gigabit level ports. Additionally, a single Ethernet management network interface is included. A DB9 serial port is for console access. Another DB9 serial port is used for redundant pair communication. Layer 4 processing is accelerated using the F5 Packet Velocity™ Application Specific Integrated Circuit (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.
- **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 the Local Directory Authentication Protocol (LDAP) and RADIUS or SSL client certificate authentication via LDAP over SSL or OCSP. **Note: Usage of an OCSP server is not evaluated as part of the Common Criteria Evaluated configuration.**

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

- Balancing traffic to tune and distribute server load on the 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.

- **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.

  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.

- **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.

- **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.

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

6.2 TOE Boundaries

Figure 3 illustrates boundaries of evaluation for the F5 BIG-IP Local Traffic Manager . This figure attempts to show that the server pools, authentication server, switch and remote management workstation (shown in dashed boxes) are not part of the BIG-IP 6400 LTM for any of the four components (shaded boxes and circles). Additionally, other components of the BIG-IP product, as noted in the Introduction, are not part of the BIG-IP 6400 LTM evaluated product.

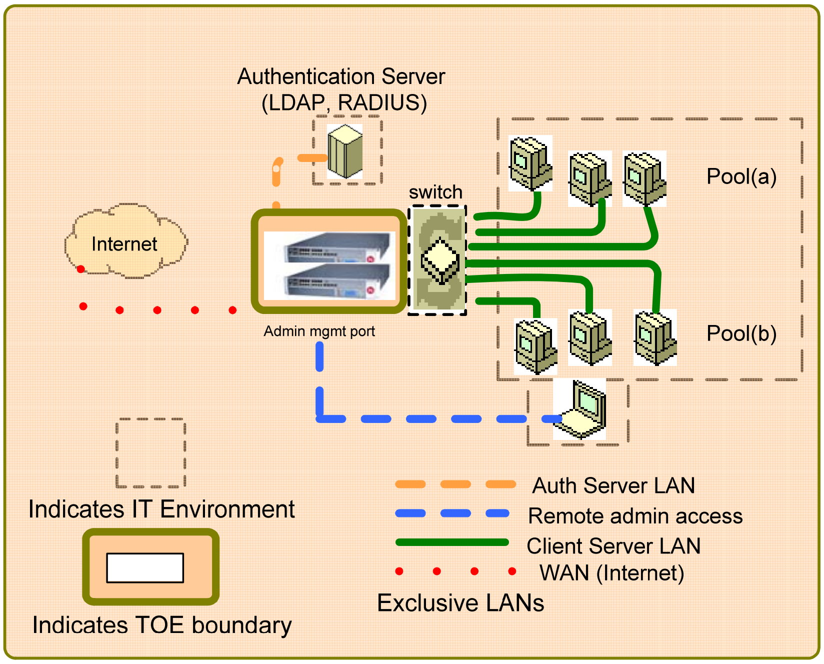

Figure 3. TOE Physical Boundaries

In terms of logical boundaries, Table 2 enumerates the division between services provided *by* the BIG-IP 6400 LTM and services provided *to* the BIG-IP 6400 LTM from the Operating Environment:

Table 2. TOE Logical Boundaries

Functional Area	**Services Provided *By* The** BIG-IP 6400 LTM	**Services Provided *To* The** BIG-IP 6400 LTM **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 BIG-IP 6400 LTM 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 BIG-IP 6400 LTM. These modules provide services to configure BIG-IP 6400 LTM 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 BIG-IP 6400 LTM 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 BIG-IP 6400 LTM 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 BIG-IP 6400 LTM	Storage of the certificates used for SSL communication.

7 Documentation

This section details the documentation that is (a) delivered to the customer, and (b) was used as evidence for the evaluation of the BIG-IP LTM 6400.[1] Note that not all evidence is available to customers. In these tables, the following conventions are used:

- Documentation that is delivered to the customer is shown with **bold** titles.
- Documentation that is available for download is shown with italicized titles.
- Documentation that was used as evidence but is *not* delivered is shown in a normal typeface.

[1] This documentation list is based on the lists provided in the Evaluation Technical Report developed by InfoGard.

- Documentation that is delivered as part of the product but was not used as evaluation is shown with a bold title, but a hashed background.

The BIG-IP 6400 LTM is physically delivered to the end user. Included in the delivery are the Quick Start Guide and Configuration worksheet. The remaining guidance is available online at the F5 website, https://tech.f5.com/home/solutions/sol7252.html.

7.1 Design documentation

Document	Revision	Date
EAL 2 Design Documentation F5 Networks BIG-IP®, 06-948-R-0011(ADV_FSP.1,ADV_HLD.1, ADV-RCR.1)	1.1	March 2, 2007
Big Pipe Man Pages for version 9.2.3		August 25, 2005
F5 Configuration Guide for Local Traffic Management, version 9.2, August 25, 2005.	9.2	August 25, 2005
F5 BIG-IP® Network and System Management Guide, version 9.2.3 .	9.2.3	February 27, 2006

7.2 Guidance documentation

Document	Revision	Date
Configuration Guide for Local Traffic Management version 9.2 MAN-0185-00	9.2	August 25, 2005
BIG-IP® Network and System Management Guide version 9.2.3 MAN-0185-02 *Configuration Worksheet PUB-0090-02 0905*	9.2.3	February 27, 2006
Platform Guide: 1500, 3400, 6400, and 6800 MAN-0183-00 August 16, 2006.		**August 16, 2006**

7.3 Configuration Management and Lifecycle

Document	Revision	Date
EAL 2 Configuration Management Documentation, 05-948-R-0145	1.1	March 2, 2007
Basic Flaw Remediation BIG-IP® Traffic Manager 6400 High Availability pair (qty 2) EAL 2, 06-948-R-0064 (ALC_FLR.1)	1.0	December 29, 2007

7.4 Delivery and Operation documentation

Document	Revision	Date
Installation, Licensing and Upgrades for BIG-IP version 9.2		August 25, 2005

Common Criteria Supplement EAL2 F5 Networks BIG-IP® Local Traffic Manager 6400 High Availability pair (qty 2), 05-948-R-0134	1.3	March 30, 2007
BIG-IP® Quick Start Instructions PUB-0089-03 1205		
Common Criteria Supplement EAL2 Secure Delivery Document F5 Networks BIG-IP® Traffic Manager 6400 High Availability pair (qty 2), 05-948-R-0144	1.1	December 1, 2005

7.5 Test documentation

Document	Revision	Date
Tests Activity ATE F5 Networks BIG-IP® Traffic Manager 6400 High Availability pair (qty 2) EAL 2, 06-948-R-0041(ATE_COV.1, ATE_FUN.1)	1.1	March 2, 2007
Tests Activity ATE – Test Evidence F5 Networks BIG-IP® Traffic Manager 6400 High Availability pair (qty 2) EAL 2, 06-948-R-0041	1.1	March 2, 2007

7.6 Vulnerability Assessment documentation

Document	Revision	Date
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 (AVA_VLA.1)	1.9	March 2, 2007
EAL 2 Strength of Function Analysis F5 Networks BIG-IP® Local Traffic Manager 6400 High Availability pair (qty 2), 06-948-R-0012 (AVA_SOF.1)	1.2	December 29, 2006
Common Criteria Supplement EAL2 F5 Networks BIG-IP® Local Traffic Manager 6400 High Availability pair (qty 2), 05-948-R-0134	1.3	March 30, 2007
EAL 2 Design Documentation F5 Networks BIG-IP®, 06-948-R-0011(ADV_FSP.1,ADV_HLD.1, ADV-RCR.1)	1.1	March 2, 2007
F5 Networks BIG-IP® Traffic Manager 6400 High Availability Pair (qty 2) Independent Testing Plan (ATE_IND.2)	1.2	April 2, 2007

7.7 Security Target

Document	Revision	Date

F5 Networks BIG-IP® Local Traffic Manager 6400 High Availability pair (qty 2) Security Target 05-948-R-0105	1.4	April 9, 2007

8 IT Product Testing

This section describes the testing efforts of the Developer and the evaluation team.

8.1 Developer testing

The test procedures were written by the Developer and designed to be conducted using manual interaction with the BIG-IP 6400 LTM interfaces. During the evaluation of the ATE_FUN.1, the evaluation team identified inconsistencies in the test cases and worked with the Developer to create accurate test cases.

The Developer tested the BIG-IP 6400 LTM consistent with the Common Criteria evaluated configuration identified in the ST. The Developer's approach to testing is defined in the Test Plan. The expected and actual test results (ATRs) are also included in the Test Plan. Each test case was identified by a number that correlates to the expected test results in the Test Plan.

The evaluation team analyzed the Developer's testing to ensure adequate coverage for EAL 2. The evaluation team determined that the Developer's actual test results matched the Developer's expected test results.

8.2 Evaluation team independent testing

The evaluation team conducted independent testing at the CCTL. The evaluation team installed the product according to vendor installation instructions and the evaluated configuration as identified in the Security Target.

The evaluation team confirmed the technical accuracy of the setup and installation guide during installation of the product while performing work unit ATE_IND.2-2. The evaluation team confirmed that the product version delivered for testing was identical to the version identified in the ST.

The evaluation team used the Developer's Test Plan as a basis for creating the Independent Test Plan. The evaluation team analyzed the Developer's test procedures to determine their relevance and adequacy to test the security function under test. The following items represent a subset of the factors considered in selecting the functional tests to be conducted:

- Security functions that implement critical security features
- Security functions critical to the product's security objectives
- Security functions that gave rise to suspicion regarding the behavior of the security features during the documentation evidence evaluation

- Security functions not tested adequately in the vendor's test plan and procedures

The evaluation team reran 30% of the Sponsor's test cases and specified additional tests. The additional test coverage was determined based on the analysis of the Developer test coverage and the ST.

Each evaluated Security Function was exercised at least once, and the evaluation team verified that each test passed.

The following were either not tested or were partially tested by the evaluation team. Note: Underlined items were not tested.

Not Tested

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

Partially Tested

- The iRule information flow was not tested in the following SFR:

  FDP_IFF.1.2a,b: 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.**

- The Reaper High Water Mark was not tested in the following SFR:

  FDP_IFF.1.6a,b: 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.**

- The iRules settings were not tested in the following SFR:

  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**.

- The iRules settings were not tested in the following SFR:

  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**

8.3 Vulnerability analysis

The evaluation team ensured that the product does not contain exploitable flaws or weaknesses in the TOE based upon the Developer Strength of Function analysis, the Developer Vulnerability Analysis, the evaluation team's Vulnerability Analysis, and the evaluation team's performance of penetration tests.

The Developer performed a Vulnerability Analysis of the product to identify any obvious vulnerabilities in the product and to show that they are not exploitable in the intended environment for the product's operation. In addition, the evaluation team conducted a sampling of the vulnerability sites claimed by the Sponsor to determine the thoroughness of the analysis.

Based on the results of the Developer's Vulnerability Analysis, the evaluation team devised penetration testing to confirm that the product was resistant to penetration attacks performed by an attacker with an expertise level of unsophisticated. The evaluation team conducted testing using the same test configuration that was used for the independent team testing. In addition to the documentation review used in the independent testing, the team used the knowledge gained during independent testing to devise the penetration testing. This resulted in a set of six (6) penetration tests.

9 Evaluated Configuration

The evaluated configuration of Big-IP 6400, as defined in the Security Target, consists of the following components:

- *BIG-IP® Local Traffic Manager 6400, High Availability pair (qty 2). Hardware P/N: 200-0153-05 Rev. C. Software Version: 9.2.3 + Hotfix CR69440.*

Big-IP 6400 LTM 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

10 Results of the Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The BIG-IP 6400 LTM was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 2.2. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 2.2.

InfoGard Laboratories has determined that the product meets the security criteria in the Security Target, which specifies an assurance level of EAL 2 augmented by ALC_FLR.1. A team of Validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation was completed in April 2007.

11 Validator Comments/Recommendations

1. The BIG-IP 6400 LTM makes use of cryptographic modules in order to fulfill some security functions. Cryptographic modules are evaluated under the National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) 140-2, a separate standard from the Common Criteria; the cryptographic functions were not evaluated further during this evaluation. Users should ensure that they select a product that meets their needs, including FIPS 140-2 compliance, if appropriate.

2. This evaluation excludes numerous security-relevant and non-security-relevant features. As these features are included in published product literature, users of the product should read this VR and the ST carefully to ensure that the capabilities critical to their usage are adequately covered.

3. This was an EAL2 evaluation. As such, there was no obligation on the part of the vendor or the CCTL to ensure that 100% of the SFRs or interfaces were covered by the security functional testing (ATE_FUN, ATE_IND). Section 8 of this report describes the testing that was performed and details what was not covered by evaluation testing. Users of this product should review this list to ensure that the features they depend upon where adequately tested. Users may need to perform additional product testing. Note that vulnerability testing (i.e., AVA_VLA) did look for obvious vulnerabilities in the entire product.

4. This product enforces a password construction policy on all users *except the Administrator*. The Administrator is assumed to follow the policy in the Administrative Guidance regarding password construction, but there is no automatic enforcement. Users are reminded of the importance of having strong passwords; it is recommended that the importance of following password policy be emphasized to all Administrators.

12 Security Target

BIG-IP® Local Traffic Manager 6400 High Availability pair (qty 2) Version 1.4, April 9, 2007.

13 Glossary

- **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. **The BIG-IP ASM is EXCLUDED from the Common Criteria Evaluated configuration.**
- **Authenticated 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 which is required to authenticate with through the TSF prior to access backend server resources. This is a role within the BIG-IP appliance and is a member of the traffic users grouping term.
- **Attack**. An attack is an exploited threat or an attempt to bypass security controls on a computer. The attack may alter, release, or deny data. Whether an attack will succeed depends on the vulnerability of the computer system and the effectiveness of existing countermeasures.
- **Authentication.** Verification of the identity of a user.
- **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.
- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Content Server** Within this ST, a content server refers to the BIG-IP application client servers which are grouped in Pools as illustrated in Figures 2 and 3.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **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, 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 user with limited access to the appliance. This role has read only access to TSF and beyond that may only enable/disable Nodes. Member of Administrative Users definition.

- **OCSP** A scheme for maintaining the security of a server and other network resources. **Use of OCSP is EXCLUDED from the Common Criteria Evaluated configuration.**

- **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** 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 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.

- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.

- **Threat**. In the Big-IP sense, this means through which the ability or intent of a threat agent to adversely affect the primary functionality of the TOE, facility that contains the TOE, or malicious operation directed towards the TOE. A potential violation of security.

- **Traffic Authentication** 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.

- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.

- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

- **Vulnerabilities**. A vulnerability is a hardware, firmware, or software flaw that leaves an Automated Information System (AIS) open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth that could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

14 Bibliography

[1] COMMON CRITERIA PROJECT SPONSORING ORGANISATIONS. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 2.2, January 2004. CCIMB-2004-01-001.

[2] COMMON CRITERIA PROJECT SPONSORING ORGANISATIONS. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 2.2, January 2004. CCIMB-2004-01-002.

[3] COMMON CRITERIA PROJECT SPONSORING ORGANISATIONS. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 2.2, January 2004. CCIMB-2004-01-003.

[4] COMMON CRITERIA PROJECT SPONSORING ORGANISATIONS. *Common Criteria Common Methodology for Information Technolgoy Security Evaluation*. January 2004 CCIMB-2004-01-004.

[5] COMMON CRITERIA EVALUATION AND VALIDATION SCHEME FOR INFORMATION TECHNOLOGY SECURITY, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, January 2002.

[6] INFOGARD LABORATORIES. *F5 Networks BIG-IP® Local Traffic Manager 6400 High Availability pair (qty 2) Security Target*, Version 1.4, April 9, 2007.

[7] InfoGard Laboratories. *Evaluation Technical Report for the Big-IP LTM 6400 Part I (Non-Proprietary)*, Version 1.2, March 27, 2007.