National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

F5® Networks

Big-IP® Local Traffic Manager Release: 10.2.2 Build 763.3 Hotfix 2 with Advanced Client Authentication and Protocol Security Modules

Report Number:	**CCEVS-VR-VID10408-2013**
Dated:	**21 April 2013**
Version:	**1.0**

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 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Mike Allen (Lead Validator)

The Aerospace Corporation
Columbia, Maryland

Daniel P. Faigin (Senior Validator)

The Aerospace Corporation
El Segundo, California

Common Criteria Testing Laboratory

Kenji Yoshino
Marvin Byrd
Michelle Ruppel

InfoGard Laboratories, Inc.
San Luis Obispo, California

Table of Contents

1 Executive Summary

This report is intended to assist the end-user of this product and any security certification Agent for that end-user in determining the suitability of this Information Technology (IT) product in their environment. End-users should review both the 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 tested and evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 4 and the Validator Comments in Section 10 where any restrictions are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the F5 Networks Big-IP® Local Traffic Manager Release: 10.2.2 Build 763.3 Hotfix 2 with Advanced Client Authentication and Protocol Security Modules. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This Validation Report applies only to the specific version and configuration of the product as evaluated and documented in the Security Target.

The evaluation of the F5 Networks Big-IP® Local Traffic Manager Release: 10.2.2 Build 763.3 Hotfix 2 with Advanced Client Authentication and Protocol Security Modules was performed by InfoGard Laboratories, Inc, the Common Criteria Testing Laboratory, in San Luis Obispo, California USA and was completed in March 2013.

The information in this report is largely derived from the Security Target (ST), Evaluation Technical Report (ETR) and associated test report. The ST was written by F5 Networks Inc. The ETR and test report used in developing this validation report were written by InfoGard Laboratories, Inc. The evaluation was performed to conform to the requirements of the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, dated July 2009 at Evaluation Assurance Level 2 (EAL 2) augmented with ALC_FLR.2. The Common Evaluation Methodology for IT Security Evaluation (CEM), Version 3.1, Revision 3, dated July 2009 was used for this evaluation. The product, when configured as specified in the installation guides, user guides, and Security Target satisfies all of the security functional requirements stated in the F5 Networks Big-IP® Local Traffic Manager Release: 10.2.2 Build 763.3 Hotfix 2 with Advanced Client Authentication and Protocol Security Modules Security Target. The evaluation team determined the product to be both Part 2 extended and Part 3 augmented compliant, and meets the assurance requirements of EAL 2 augmented by ALC_FLR.2. All security functional requirements are derived from Part 2 of the Common Criteria.

The Target of Evaluation (TOE) is a port-based, multilayer switch with multiple ports and a 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 OSI layers 2 and above. 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 also includes the Advanced Client Authentication and

Protocol Security Modules, which are included in appliance software and are enabled through licensing for the CC Evaluated configuration.

The BIG-IP system provides the ability to monitor the devices for which it manages traffic and to provide audit trails relating to the use of network resources. BIG-IP information flow control rules ensure that critical connections using IP protocols reach the correct destination server. The BIG-IP appliance supports HTTP, SMTP, and FTP routing and analysis and can be configured to perform analysis on all other Ethernet/IP based protocols using the iRules scripting feature. Using packet filtering and profile based routing provided by the Protocol Security Module (PSM), the TOE protects backend servers from unsolicited traffic and potentially malicious traffic flows. The PSM also performs security related checks and validations for HTTP, SMTP, and FTP traffic. Key Traffic Management features provided by BIG-IP include:

- Processing of SSL/TLS session authentication and SSL/TLS encryption to improve server performance.
- Client/Server Certificate based authentication of SSL/TLS traffic provided through the installed Advanced Client Authentication Module (ACA).
- Establishing and managing session and connection persistence.
- Handling application-traffic authentication and authorization functions based on User name/password and SSL/TLS certificate credentials.
- Protocol Sanitization – Terminates all TCP connections, preventing out-of-order packet floods, MSS tiny packet floods and TCP window tampering. Includes HTTP header evaluation, RFC violation matches, and protocol enforcement checks provided through the installed Protocol Security Module (PSM).
- Customizing the flow of application-specific traffic (such as HTTP and SSL/TLS traffic).
- Customizing the management of specific connections according to user-written scripts using iRules. iRules is based on the industry-standard Tool Command Language (TCL).

Note: The cryptography used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

1.1 Interpretations

There are no applicable Common Criteria interpretations.

2 Identification

The 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, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation conduct security evaluations.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology (IT) products, desiring a security evaluation, contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's 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 Protection Profile to which the product is conformant (if any); and
- The organizations and individuals participating in the evaluation.

Table 1 - Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	F5 Networks Big-IP® Local Traffic Manager Release: 10.2.2 Build 763.3 Hotfix 2 with Advanced Client Authentication and Protocol Security Modules
Protection Profiles	None.
Security Target	*F5 Networks Big-IP® Local Traffic Manager Release: 10.2.2 Build 763.3 Hotfix 2 with Advanced Client Authentication and Protocol Security Modules Security Target EAL2 augmented ALC_FLR.2*, Version 4.6, March 8, 2013
Dates of evaluation	June 2010 through March 2013
Evaluation Technical Report	*Evaluation Technical Report for the Big-IP® Local Traffic Manager 12-2020-R-0013* V1.2, March 8, 2013
Conformance Result	Part 2 extended conformant and EAL2 Part 3 augmented with ALC_FLR.2
Common Criteria version	Common Criteria for Information Technology Security Evaluation Version 3.1R3, July 2009 and all applicable NIAP and International Interpretations effective on June 19, 2010
Common Evaluation Methodology (CEM) version	CEM version 3.1R3 dated July2009and all applicable NIAP and International Interpretations effective on June 19, 2010
Sponsor	F5 Networks, Inc, 401 Elliott Avenue West, Seattle, WA 98119
Developer	F5 Networks, Inc, 401 Elliott Avenue West, Seattle WA 98119
Common Criteria Testing Lab	InfoGard Laboratories Inc., San Luis Obispo, CA
Evaluators	Kenji Yoshino, Marvin Byrd, and Michelle Ruppel
Validation Team	Daniel Faigin and Mike Allen, The Aerospace Corporation

3 Security Policy

This section contains the product features and denotes which are within the logical boundaries of the TOE. The following Security Functions are supported by the TOE:

- Security Audit
- Identification and Authentication
- Security Management
- Secure Communications
- Secure Traffic
- Protection of the TSF
- User Data Protection
- Email alerts (if configured)

3.1 Security Audit

The TOE generates 5 types of logs as part of this security function: System Events, Packet Filter Events, Local Traffic Events, Audit, and Application Security (PSM) logs. Audit records are stored local to the appliance and may be exported to a Syslog server in the operational environment.

Audit records within the TOE may be selectively filtered and searched based on various characteristics. Audit records are accessed through the Administrator Console GUI or tmsh (CLI). Audit records can only be deleted or overwritten by users with the Administrator role. Protection of the audit system is provided by the underlying BIG-IP TMOS and TOE identification and authentication mechanisms.

3.2 Identification and Authentication

The TOE authenticates administrative users using a username/password combination. The TOE enforces failed authentication attempt lockouts for each user and stores the role assigned to each user. For locally authenticated users, the TOE enforces password complexity restrictions.

The TOE can authenticate traffic users using a username/password combination or X.509 certificate authentication. When X.509 certificate authentication is performed the TOE uses an OCSP server to verify that certificates have not been revoked.

Both administrative and traffic users can be defined on the TOE (local) or on a remote authentication server. The TOE supports LDAP and RADIUS authentication servers.

3.3 Security Management

The TOE provides a web-based GUI and a CLI security management interface. The TOE enforces role based access control and validates each command against the user's role. In addition to roles, the TOE also permits further refinement of Administrative-users access to objects through the use of Administrative partitions. Administrative partitions are logical groupings of objects.

3.4 Secure Traffic

The TOE secures traffic using a hardware based security processor for SSL/TLS traffic, the software based Traffic Management Module within the BIG-IP operating system for SSL/TLS handshaking, and an OpenSSL library for supporting local X.509 certificate verification.

To increase availability and capacity within the supported backend servers, the TOE may be configured to terminate SSL/TLS at the appliance. Through this function, called SSL/TLS Termination, the TOE establishes and terminates SSL/TLS traffic on behalf of the backend server pools using Client, Server, or both Client and Server Profiles with certificate based authentication requirements.

3.5 Protection of the TSF

Physical and logical protection of the TOE appliance is required to assure that TOE related security functions are not bypassed or altered.

The TOE provides logical separation between Administrator-user sessions and traffic domains to assure traffic flowing through the device to backend server resource cannot access TSF security management interfaces and configuration mechanisms. The TOE requires Administrator-user access to TSF data through a dedicated management port through which HTTPS or SSH is used to secure communication with the Administrative-user.

TOE security functionality also mitigates DoS attacks by limiting the numbers of TCP connect requests allowed within a given period of time.

3.6 User Data Protection

The BIG-IP mediates network traffic by evaluating traffic destined for backend server resources and routing it based on a series of configured checks and flow control rules. The TOE supports unauthenticated flows for any protocol and authenticated flows for HTTP and HTTPS. The TOE protects backend servers within the internal network from unauthorized or malicious traffic flows through packet deconstruction and analysis.

Information Flow Control policies are configured through security profiles in the TOE. The combination of configured security checks and routing rule enforcement assures that traffic is fully inspected and identified threats addressed (by discarding the traffic) prior to routing to resources in the Operational Environment.

BIG-IP traffic processing options include: SSL/TLS secure traffic, Content based compression of HTTP traffic, and Rules based Pool selection to assure highest availability and processing speed.

Backend Servers are managed in resource Pools and flow control policies are deployed and enforced according to Pool memberships.

3.7 E-mail Alerts

Administrative-users with the administrator role with tmsh access may configure an e-mail notification for eligible alerts.

4 Assumptions and Clarification of Scope

4.1 Assumptions

The following assumptions are made about the usage of the TOE:

- The TOE is physically secure.
- There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.
- The TOE does not host public data.
- Administrative-users are non-hostile and follow all administrator guidance; however, they are capable of error.
- The TOE is configured and connected such that information cannot flow among the internal and external networks unless it passes through the TOE.
- Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port).
- An OSCP Server will be available in the Operational Environment for the purpose of verifying the revocation status of certificates on behalf of the TOE.
- If remote syslog is used in the operational environment, the remote syslog server and its connection to the TOE are physically secure.

4.2 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation and how the TOE needs to be configured to ensure it operates in the evaluated configuration.

- Additional software licenses are required to operate the TOE in the evaluated configuration (see Section 5.1.2).
- The following security relevant items associated with the product were excluded from the evaluated configuration and should not be used:

  a. Application templates. Configurations are restricted to manual approaches (procedurally enforced)

  b. The following modules, as they are separately licensed and not included in the CC Evaluated Configuration:

     i. BIG-IP Global Traffic Manager.

     ii. BIG-IP Link Controller.

     iii. BIG-IP Application Security Manager.

iv. BIG-IP WebAccelerator System.

v. BIG-IP WAN Optimization Module.

vi. BIG-IP Access Policy Manager.

vii. BIG-IP Message Security Module.

c. Application Security Policy Editor role. This role is not included in a BIG-IP configuration except as part of the Application Security Module.

d. Always-On Management (AOM). SSH access to AOM is disabled unless configured, and the Common Criteria evaluated configuration does not configure SSH for AOM. Serial console access to AOM is procedurally excluded from the Common Criteria Evaluated Configuration.

e. bash shell. This is disabled by Appliance mode.

f. Bigpipe Utility Command Line Interface (CLI) and Bigpipe Shell (bpsh). These are deprecated in this release and procedurally excluded. Note that:

i. Users must not be created with the capability to access the bigpipe shell, either through the GUI or tmsh.

ii. The bigpipe shell must not be accessed through the tmsh “run /util bigpipe shell“ command.

iii. The bigpipe utility commands must not be accessed through the “run /util bigpipe <command>” command.

g. SNMP for Remote Management of BIG-IP. This is disabled via configuration script; therefore references to SNMP in the environment do not apply. However, email notification of alerts relies on modifying the alertd configuration file, which uses the snmptrap statement format to define the alert. References to snmptrap in that context do apply.

h. FIPS hardware, including hardware-based SSL offloading.

i. iSessions (relates to data center to data center deployment models). This requires the BIG-IP® WAN Optimization Module, which is not included in TOE.

j. Editing the configuration files specified in the TMOS Management Guide. The GUI or tmsh must be used for all system configurations.

k. IMI and VTY shells.

l. Configuration of the TOE via the appliance LCD display. This is disabled except during initial configuration.

m. Serial port.

n. Kerberos server. This is not enabled unless configured, and the Common Criteria evaluated configuration does not configure Kerberos. Note that the default Kerberos profile says that it is enabled, but without fully configuring the profile and attaching it to a virtual server, Kerberos itself is not configured and not usable. Thus, by default, Kerberos itself is not enabled.

o. iControl interface. This is procedurally excluded since all of the function it provides is also provided with the GUI and tmsh interfaces.

p. Use of CRLs and CRLDPs. As CRLs can quickly become outdated, their use and that of CRLDPs is excluded from the TOE. Therefore, an OCSP server is required in the Operational Environment for certificate revocation checks.

q. The following profiles (based on the list in the Configuration Guide for BIG-IP Local Traffic Manager, Chapter 5 (Understanding Profiles), section “Profile Types”):

    i. Services profiles: RTSP, Diameter, and iSession.

    ii. Persistence profiles: Microsoft Remote Desktop.

    iii. Protocol profiles: SCTP.

    iv. SSL profiles: *(No SSL profiles are excluded)*

    v. Authentication profiles: Kerberos Delegation.

    vi. Other profiles: NTLM and Stream.

r. Protocol sanitization for protocols other than HTTP, FTP, and SMTP.

s. Ciphers other than those specified in Appendix A of the Security Target. Note that the CCMODE script described in Section 3.9 changes the cryptographic defaults as they are described in guidance documents and supersedes those documents. The CCMODE script enforces the algorithm restrictions and the symmetric key length restrictions; however, the administrator must procedurally enforce the RSA key lengths in X.509 certificates used to authenticate to the TOE.

t. Cryptographic-related protocols other than SSHv2, SSLv3, and TLSv1.0.

u. Any features requiring root access to configure. This is because access to root is disabled via Appliance Mode. This includes, for example, remote encrypted logging since Appliance Mode precludes the ability to configure the SSH tunnel required for that function.

v. The gencert utility. This is excluded since it is only accessible through excluded shells. Key and certificate generation should be accomplished through the GUI instead.

w. CORBA, which is not used in BIGIP.

x. TACACS+. This is excluded as a remote authentication server.

y. Network boot.

z. Software updates to the Common Criteria evaluated configuration.

aa. Batch mode tmsh transactions.

- The following non-security relevant items associated with the product were excluded from the evaluated configuration and should not be used:

  a. The following modules and capabilities that are separately licensed and not included with the TOE:

     - WebAccelerator™ Module (WAM).
     - Link Controller (LC).
     - Global Traffic Manager (GTM).
     - Application Policy Module (APM).
     - Enterprise Manager.
     - F5 Management Pack.
     - Advanced Routing.

  b. Optimization of network and application traffic; load balancing.

  c. HTTP compression.

  d. Caching.

  e. Aggregation of client requests.

  f. Routing around slower or degraded routes.

  g. Selective data compression.

  h. Windows NT LAN Manager authentication protocol (NTLM). The BIG-IP passes this protocol through, but does not itself perform NTLM authentication.

  i. Network resource monitoring.

  j. Trunk (link aggregation).

  k. Spanning Tree Protocols.

  l. Network Tunnels.

  m. Bigtop utility. This utility provides statistical monitoring only.

  n. SNAT. “Source NAT”. BIG-IP implements SNAT as mapping a source client IP address to a translation address defined on the BIG-IP system.

  o. Booting from different volumes. The BIG-IP may be configured with multiple volumes but only booting from the slot containing the Common Criteria-evaluated configuration is recommended.

5 Architectural Information

The TOE is classified as Router/Switch for Common Criteria purposes. The TOE is made up of hardware and software components.

5.1 Architecture Overview

The TOE consists of a redundant pair of appliances. The management port is physically separate from general purpose network ports. The BIG-IP LTM software is based on the following open source distributions:

- CentOS 5.4, Linux kernel 2.6
- openssl 0.9.8e (non-FIPS validated version)
- openssh 4.3p2
- Apache Httpd 2.2.3
- Tomcat 6.0.20
- Java 1.6.0

5.1.1 TOE Hardware

BIG-IP hardware appliance: Hardware Chassis Model 11050, 8900, or 6900 hardware platform (quantity 2):

- Model: 6900
  SKU: F5-BIG-LTM-6900-8G-R
  PN: 200-0300-01
- Model: 8900
  SKU: F5-BIG-LTM-8900-R
  PN: 200-0308-01
- Model: 11050
  SKU: F5-BIG-LTM-11050-R
  PN: 200-0299-00

5.1.2 TOE Software

Software for the BIG-IP platform consists of the following F5 components:

a. BIG-IP® Local Traffic Manager Release 10.2.2 Build 763.3 with Hotfix-BIGIP-10.2.2-911.0-HF2.

Licenses required to operate in the CC Evaluated configuration are:

a. Protocol Security Module (PSM) (F5-ADD-BIG-PSM)

b. Advanced Client Authentication (ACA) module (F5-ADD-BIG-ACA)

c. BIG-IP ADD-ON: Appliance Mode License (restricts the CLI to tmsh only; no bash access and no ability to login as root) (F5-ADD-BIG-MODE)

6 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. In these tables, the following conventions are used:

- Documentation that is delivered to the customer is shown with **bold** titles.
- Documentation that was used as evidence but is not delivered is shown in a normal typeface.
- Documentation that is delivered as part of the product but was not used as evaluation is shown with a hashed background.

The TOE is shipped to end users and a link to the documentation download page is emailed to customers. The guidance documents are provided via secure HTTP download and apply to the CC Evaluated configuration.

6.1 Design Documentation

Document	Revision	Date	Security Relevant
EAL 2 Design Documentation F5 Networks BIG-IP® v10.2.2	1.3.6	March 8, 2013	X
Local Traffic Control Descriptions	N/A	March 7, 2011	X
Network Control Descriptions	N/A	March 7, 2011	X
Overview Control Descriptions	N/A	March 7, 2011	X
Templates and Wizards Control Descriptions	N/A	March 7, 2011	X
Master List of iRule Events	N/A	May 13, 2011	X
iRule Operators	N/A	June 3, 2011	X
Master list of iRule Commands	N/A	May 19, 2011	X
iRule Functions	N/A	June 3, 2011	X
iRule Statements	N/A	June 3, 2011	X
EAL2 ADV mapping document	1.0	December 2,2011	X
Error Messages	N/A	February 28, 2012	X
RFCs	N/A	Multiple	X
Protocol Security Control Descriptions	N/A	July 29, 2011	X

Document	Revision	Date	Security Relevant
System Control Descriptions	N/A	November 23, 2011	X
Network Time Protocol Version 4: Protocol and Algorithms Specification	N/A	June 1, 2010	X
The hash function RIPEMD-160	N/A	February 13, 2012	X

6.2 Guidance Documentation

Document	Revision	Date	Security Relevant
Common Criteria Supplement EAL2 F5® Networks BIG-IP® Local Traffic Manager Release: 10.2.2	3.1	March 8, 2013	X
Configuration Worksheet BIG-IP® Local Traffic Manager	PUB-0090-02 0905	N/A	
BIG-IP® Systems: Getting Started Guide	MAN-0300-00	February 4, 2010	X
Platform Guide: 11050	MAN-0322-01	N/A	
Platform Guide: 6900	MAN-0329-00	March 8, 2011	
Platform Guide: 8900	MAN-0330-00	March 8, 2011	
Declaration of Conformity (11000 Series)	N/A	April 11, 2011	
Declaration of Conformity (6900, 8900, 8950)	PUB-0209-02 Rev A	March 31, 2011	
Configuration Guide for BIG-IP® Local Traffic Manager™	MAN-0292-01	August 4, 2010	X
Configuration Guide for BIG-IP® Protocol Security Module™	MAN-0284-02	April 1, 2010	X
6900/8900/8950 Platform Hazardous Substance Table	DOC-0300-01	May 11, 2011	
11050 Platform Hazardous Substance Table	DOC-0306-00	March 10, 2010	
Traffic Management Shell (tmsh) Reference Guide	MAN-0306-01	July 30, 2011	X
European Union Battery Notice	PUB-0186-01 Rev A	N/A	
11000 Series Platform Packing List	PUB-0200-02 Rev A	N/A	
6900/8900/8950 Platform Packing List	PUB-0201-02 Rev A	N/A	
Setting Up the 6900/8900/8950 Platform	MAN-0288-02	February 11, 2011	
Setting Up 11000 Series Platforms	MAN-0323-02	N/A	
Need a Quick Start? Visit the AskF5™ Knowledge Base	N/A	N/A	
SOL10025	N/A	October 12, 2011	X
Common Criteria Certification for BIG-IP version 10.2.2 (cc_documentation_readme.txt)	N/A	N/A	X
SOL10737: SSL Renegotiation vulnerability	N/A	December 11, 2012	X

Document	Revision	Date	Security Relevant
END USER SOFTWARE LICENSE 2011-05-16	N/A	May 16, 2011	X
F5 Networks, Inc. Terms of License and Sale	PUB-0024-04 Rev. B	N/A	
TMOS® Management Guide for BIG-IP® Systems	MAN-0294-01	May 25, 2010	X
SOL6319: TCL commands that have been disabled within BIG-IP 9.x iRules	N/A	May 7, 2010	X
Tcl and the Tk Toolkit, Second Edition [1]	ISBN-13: 978-0321336330	N/A	X

6.3 Life Cycle

Document	Revision	Date	Security Relevant
F5® Networks BIG-IP® Local Traffic Manager High Availability pair (quantity 2) Release: 10.2.2 Configuration Management ALC_CMS.2/ALC_CMC.2	1.3	March 7, 2013	X
Common Criteria Supplement Secure Delivery Document F5® Networks BIG-IP® Local Traffic Manager High Availability pair (quantity 2) Release: 10.2.2	0.9	February 7, 2013	X
Flaw Reporting Procedures ALC_FLR.2 BIG-IP® Local Traffic Manager High Availability pair (quantity 2) Release: 10.2.2	0.6	February 7, 2013	X
SOL4602: Overview of the F5 security vulnerability response policy	N/A	August 16, 2012	X
F5 Support Contact Information	PUB-0093-03	N/A	X

6.4 Testing

Document	Revision	Date	Security Relevant
F5® Networks BIG-IP® Local Traffic Manager Release: v10.2.2 build 763.3 hotfix 2 with Advanced Client Authentication and Protocol Security Modules Tests Activity ATE EAL 2 augmented ALC_FLR.2	1.9	December 12, 2012	X
ATE Interface Mappings	N/A	May 21, 2012	X

[1] The customer is instructed to separately purchase this book if they need to learn how to write iRules in the TCL language.

7 IT Product Testing

This section describes the testing efforts of the Developer and the Evaluation Team.

7.1 Developer Testing

The developer tests provided good coverage of the flow control, load balancing, authentication, and management functions; however, the Evaluators found that the developer testing was lacking in areas related to cryptography and security specific areas. The developer also provided the results to their standard testing procedures. These tests have not been documented to meet Common Criteria requirements; however, they do provide assurance to the scope of tests performed by the developer.

7.2 Evaluation Team Independent Testing

The Evaluators re-ran 83 of the developer's tests. The Evaluators wrote 110 independent tests to tests and verify TOE functionality in a different manner than the developer tests. The Evaluators developed the 'SFR coverage mapping.xlsx' document to map the requirements in the SFRs to the different tests and demonstrate the coverage achieved by the testing effort.

Note: The cryptography used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

7.3 Vulnerability Analysis

Information readily available to a potential attacker is limited to marketing and support related literature from the F5 web site and various Internet search domains and product information shipped with the TOE.

The Security Target, TOE documentation, and readily available public information were used to compile a list of keywords for conducting the search for obvious vulnerabilities. These keywords were used to search the SecurityFocus Vulnerability Database, the National Vulnerability Database, the Carnegie Mellon CERT Coordination Center, and AskF5 for known vulnerabilities.

Three potential vulnerabilities were identified for additional investigation. The three vulnerabilities were CVE-2012-2333, CVE-2011-3389, and CVE-2009-3555.

The CVE-2012-2333 vulnerability was later determined to be N/A, because the TOE does not support the affected protocols (i.e. TLSv1.1, TLSv1.2, DTLS).

The CVE-2011-3389 vulnerability is better known as the BEAST vulnerability and is present in SSLv3 and TLSv1.

The CVE-2009-3555 vulnerability is the SSL/TLS relegation vulnerability. The TOE is not vulnerable by default and the user is warned that enabling SSL renegotiation will make them vulnerable to this attack.

8 Evaluated Configuration

The Target of Evaluation (TOE) is the hardware and software of the F5 Networks Big-IP® Local Traffic Manager Release: 10.2.2 Build 763.3 Hotfix 2 with Advanced Client Authentication and Protocol Security Modules. The device is a port-based, multilayer switch with multiple ports and a host system for advanced processing.

9 Results of the Evaluation

InfoGard Laboratories, Inc. determined that the product meets the security criteria in the Security Target, which specifies an assurance level of EAL 2 augmented with ALC_FLR.2. A team of Validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation and validation efforts were finished in March 2013.

10 Validator Comments

The validation team's observations support the evaluation team's conclusion that F5 Networks Big-IP® Local Traffic Manager Release: 10.2.2 Build 763.3 Hotfix 2 with Advanced Client Authentication and Protocol Security Modules meets the claims stated in the Security Target. The following are additional clarifications from the validation team about the use of the product:

1. The cryptography used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.
2. The product appears to provide the ability to support CNSSI 1253 password complexity requirements for local passwords.
3. The evaluated configuration of the product is in conformance with the Application STIG.
4. The information sanitizing capabilities are based on simple pattern matching. Simple formatting changes would allow data to bypass the checks.
5. Users are reminded to not enable SSL Renegotiation, because that will open the vulnerability reported in CVE-2009-3555.
6. The product only supports SSLv3 and TLSv1, which are vulnerable to the BEAST attack reported in CVE-2011-2289.
7. The password complexity enforcement features provided by the TOE are limited. The password complexity rules are only enforced on *locally maintained accounts* that do not hold the Administrator or User Manager Roles. The rules *do not apply* to accounts maintained by an LDAP or RADIUS authentication server.
8. The Cookie Encryption Feature has a number of peculiar behaviors:
    a. The period (.) character is not allowed in cookie names. Only alphanumeric characters and the special characters dash and underscore (- and _) are allowed.
    b. Client cookies not able to be decrypted by the BIG-IP which have a length of 4*n (where n=[0,1,2,…]) cause the connection to be reset. Cookies of other lengths (decryptable or not) are passed through to the server.

11 Security Target

The Security Target is identified *F5 Networks Big-IP® Local Traffic Manager Release: 10.2.2 Build 763.3 Hotfix 2 with Advanced Client Authentication and Protocol Security Modules Security Target*, Version D4.6, dated March 8, 2013.

.

12 Glossary

The following acronyms and terms are used throughout this document:

12.1 Acronyms

ACA	Advanced Client Authentication (module)
ARP	Address Resolution Protocol
ASM	Application Security Module
CRL	Certificate Revocation List
CC	Common Criteria
CRC	Cyclic Redundancy Check
DoS	Denial of Service
FTP	File Transfer Protocol
GTM	Global Traffic Management
GUI	Graphical User Interface
HTTP	Hypertext Transport Protocol
HTTPS	Hypertext Transport Protocol (Secure)
LTM	Local Traffic Management
OCSP	Online Certificate Status Protocol
OS	Operating System
OSI	Open Systems Interconnection
PAM	Pluggable Authentication Module
PSM	Protocol Security Module
SNAT	Secure Network Address Translation
SSL	Secure Socket Layer
SMTP	Simple Mail Transfer Protocol
SPF	Sender Policy Framework
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TMOS	Traffic Management Operating System
VLANs	Virtual Local Area Networks
VNIC	Virtual Network Interface Card (driver)

12.2 Terminology

Administrative Partition
A logical container that Administrators can create, containing a defined set of BIG-IP system objects.

Backend Servers
A group of servers (aka pool members), organized in Pools, which are served by the BIG-IP appliance.

Content Server
A BIG-IP supported web or application (client) servers. Content servers are a subset of backend servers.

Certificate Revocation List
A listing of certificates that have been revoked by an applicable authority. An authenticating system checks a CRL to see if the SSL certificate that the requesting system presents for authentication has been revoked.

Data Guard™
An F5 Networks feature where data matching configured patterns is anonomized with characters to obscure sensitive data in transit.

iRules™
An F5 Networks scripting language included in the BIG-IP that may be used by users to develop scripts that control the behavior of a connection passing through the BIG-IP appliance.

iRules script
A script created using the iRules scripting language.

Local traffic management
The process of managing network traffic that comes into or goes out of a local area network (LAN), including an intranet.

Loopback network
In IPv4, the network with the CIDR prefix 127/8; ::1/128 in IPv6.

Node
An IP Address configured within BIG-IP as a destination.

OneConnect™
The F5 Networks OneConnect feature optimizes the use of network connections by keeping server-side connections open and pooling them for re-use.

Persistence
When load balancing, persistence means that once a client is connected to a specific server, future connections are always sent back to the specific server.

Persistence cookies
A method of using HTTP cookies to make connections persistent.

Pool
A grouping of backend servers.

Pool Member
This term refers to node-and-service pairs which are assigned to one or more Pools.

Protocol Security Module
The BIG-IP Protocol Security Module (PSM) runs on the BIG-IP traffic management platform, providing application security functionality.

Protocol Aware
This term refers to the fact that the TMM can readily identify protocols that flow on top of TCP, such as HTTP SMTP and protocols that flow under TCP such as routing protocols. Since TMM's functionality includes decoding these protocols, extra

	information about the traffic stream can be extracted and applied for firewall functionality.
Protocol Sanitization	Refers to Protocol RFC based compliance checks performed by BIG-IP. For the CC Evaluated configuration these are HTTP, FTP, and SMTP.
Server-side traffic	Refers to connections between the BIG-IP appliance and a target server system (backend server).
SSL	Secure Socket Layer. When used without a version number, this refers to the SSLv3/TLSv1.0/TLSv1.1 protocol support. Note that Profiles and iRules both refer to “SSL”; the support includes SSLv3/TLSv1.0/TLSv1.1 protocols even when the actual GUI page or command string is “SSL”.
TLS	Transport Layer Security. When used without a version number, this refers to the TLSv1.0/TLSv1.1 protocol support.
Traffic, Administrative	Traffic generated in order to manage the TOE (e.g. traffic from the administrative user to the GUI or tmsh).
Traffic user	Users sending traffic through the TOE; so named as to distinguish them from Administrative-users.
Traffic, User-generated	All traffic other than administrative traffic that flows through the TOE.
Virtual address	A virtual address is an IP address associated with one or more virtual servers managed by the BIG-IP system.
Virtual port	A virtual port is the port number or service name associated with one or more virtual servers managed by the BIG-IP system. A virtual port number should be the same TCP or UDP port number to which client programs expect to connect.
Virtual server	Virtual servers are a specific combination of virtual address and virtual ports, associated with a content site that is managed by a BIG-IP system or other type of host server. Also includes VLAN and protocol (TCP vs. UDP).
Virtual Local Area Network	A VLAN is a logical grouping of interfaces connected to network devices. A VLAN may be used to logically group devices that are on different network segments. Devices within a VLAN use Layer 2 networking to communicate and define a broadcast domain.

13 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1 R3, July 2009.

[2] Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements, Version 3.1 R3, July 2009.

[3] Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements, Version 3.1 R3, July 2009.

[4] Common Criteria Project Sponsoring Organisations. *Common Methodology for Information Technology Security Evaluation*, Version 3.1 R3, July 2009.

[5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 2.0, September 8, 2008.

[6] F5 Networks Big-IP® Local Traffic Manager Release: 10.2.2 Build 763.3 Hotfix 2 with Advanced Client Authentication and Protocol Security Modules Security Target, Version D4.6, March 8, 2013.

[7] InfoGard Laboratories, Inc., Evaluation Technical Report for the Big-IP® Local Traffic Manager, 12-2020-R-0013 V1.2, March 8, 2013.

[8] InfoGard Laboratories, Inc., Independent and Penetration Test Plan, 12-2020-R-0014 V1.4, December 6, 2012