Validation Report (VR)

F5 Networks

FirePass 4100 Version 5.5.2 + Hotfix HF-552-10

CCEVS-VR-VID10190-2007

December 19, 2007

Table of Contents

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 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 documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the FirePass 4100 Version 5.5.2 (+ Hotfix HF-552-10), 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 FirePass 4100 Version 5.5.2 (+ Hotfix HF-552-10) product was performed by InfoGard Laboratories, Inc., San Luis Obispo, CA in the United States and was completed on 28th September, 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, Evaluation Assurance Level 2 (EAL2) – augmented (ALC_FLR.1 and ADV_SPM.1), and the Common Evaluation Methodology for IT Security Evaluation (CEM), Version 2.2.

2 Identification of the TOE

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, 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.

Evaluation Scheme	United States Common Criteria Evaluation Validation Scheme
Evaluated Target of Evaluation	FirePass 4100 Version 5.5.2 + Hotfix HF-552-10
Protection Profile	Not applicable
Security Target	F5 Networks FirePass® 4100 Version 5.5.2 Security Target EAL 2 + ALC_FLR.1, ADV_SPM.1
Dates of evaluation	September 1, 2006 to September 28, 2007
Conformance result	Part 2 extended, Part 3 conformant, EAL 2 augmented with ALC_FLR.1 and ADV_SPM.1
Common Criteria version	CC version 2.2
Common Evaluation Methodology (CEM) version	CEM version 2.2
Evaluation Technical Report (ETR)	07-1023-R-0092 V1.0
Sponsor/Developer	F5 Networks 401 Elliot Avenue West Seattle, WA 98119
Common Criteria Testing Lab (CCTL)	InfoGard Laboratories, Inc.
CCTL Evaluators	Mark Plascencia, Clyde Sy
CCEVS Validators	Deborah Downs, Rick Murphy

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 TOE is also compliant with all International interpretations with effective dates on or before 09/01/06.

4 Security Policy

The TOE is a hardware and software based Virtual Private Networking (VPN) appliance that enables remote Users to access protected networks securely using the Microsoft® Internet Explorer™ web browser. The F5 FirePass® SSL VPN appliance establishes these secure connections using Secure Socket Layer (SSL) techniques and can proxy connections to file servers, email servers, web application servers and desktop PC applications. Since the FirePass manages the authentication of clients and coordinates the appropriate access, intranet resources are protected from direct access from the Internet.

FirePass has three operational modes based on the client/network relationship.

- Web Applications Mode denotes secure public application layer access to intranet web servers and web applications that allows access from various public client sources such as various desktop operating systems, airport kiosks, PDA, or cellular phones.
- Application Access Mode securely connects to specific application servers such as Oracle or Microsoft Exchange. This mode is not included in the Evaluated Configuration.
- Network Access Mode allows for secure network layer access using FirePass client plug-ins that establishes a layer 3 connection using Point to Point Protocol (PPP) over SSL techniques.

The FirePass appliances are also scalable, allowing clustering of multiple units to increase capacity. Maximum availability and reliability is assured through redundant pair configuration with two FirePass units in parallel operating in Active-Standby mode. The Common Criteria Evaluated configuration includes the FirePass 4100 appliance in a redundant pair configuration

The FirePass 4100 Version 5.5.2 + Hotfix HF-552-10 performs the following security functionality:

4.1 Security Audit

The TOE provides audit generation and review capability that produces an audit trail of TOE security function activities and logging of host network access attempts through the TOE. The audit function can be configured to log specific or all aspects of session activity. Audit records are maintained based on time and date of event and User identification. Audit records can only be accessed by authorized Administrators (Admin (full access) or Realm_admin (administrator)) through the Administrator Console. Audit log records are stored within an SQL database which is part of the Networking Module/Operating System TOE subsystem.

Audit records are stored and protected within the TOE and may be exported manually or automatically as configured by the Administrative User. The TOE has provisions to transfer system log records to an external ftp server in the IT Environment on a periodic basis as configured.

The TOE features an audit report generation function that may be configured to identify various aspects of session activity in a report format.

4.2 Identification and Authentication

All Users must be positively identified by username and authenticated by password or through certificate exchange prior to accessing TOE resources, TSF functions or supported TOE protected network servers. FirePass manages Users by creating Master Groups, which consist of groups of users, authentication settings, overall security configuration settings, network access filtering policies, and user accounts. As noted below, External VPN users are not managed internal to the appliance for the CC evaluated configuration.

Administrative Users (local Users) are identified and authenticated internal to the FirePass TOE. FirePass requires that the Admin (full access) be authenticated locally to assure Administrator level access to the Appliance. External VPN users are authenticated using an external authentication server. The TOE supports external authentication using LDAP, Active Directory and RADIUS.

Client certificate based authentication is also supported using external Certificate Authority or internally managed through the self-signed certificate function within FirePass. Two-factor authentication may also be enabled for authorization by groups, using methods such as RSA SecureID and VASCO Digipass. These options are not included in the CC evaluated configuration.

4.3 Endpoint Security

The Endpoint Security function can be used to evaluate security status on a Client requesting access to FirePass to initiate a session. This function can also execute tasks on the client machine to limit access to FirePass resource and/or remove content from the Client that could represent a security risk. The required plug-ins and Client Software are downloaded as part of the first session initiation process and signed using an F5 signing certificate to assure integrity during the download process (the client O.S. will verify the signature of all controls downloaded). Endpoint Security operates through a Collection step, where it obtains security related configuration information, including:

- virus scan
- personal firewalls
- OS patch levels
- registry settings
- absence of key logger

Following collection is a Remediation step, where it either actively corrects non-secure configurations or notifies the user to perform the needed steps, then a Protection step which implements the connection rules established by the administrator based on the resources being accessed.

Client Integrity checking verifies the security status of the client, and cache cleanup provides data removal upon the closing of a session. Integrity checking may be initiated as part of a Network Access Mode connection, Web Applications Mode connection (if client download is allowed) or during a Pre-logon sequence. In all cases controls must be loaded to the client.
Client Integrity Checking can be configured to assure firewalls, virus scan software or other process are running prior to granting or limiting access based on variables in this state. This host checking feature can be configured to recognize and alter access level granted based on whether client is a trusted entity (i.e.: corporate laptop) or untrusted IT entity.

Through the use of the Client Security Module, Pre-login sequences and Post-login protection features can be enabled as described above to establish required security status prior to login and during or after the session take actions to assure security data is protected.

Cache cleanup functions within Endpoint Security delete all cached items used during a FirePass session to assure that information does not remain on the computer, which may be a public access resource. This requires the download of a browser plug-in to facilitate the cleaning function.

4.4 Network Access Mode

The Network Access Mode feature allows the FirePass appliance to establish secure layer 3 connections with clients using PPP over SSL VPN tunneling techniques. A Network connection is established after the user has logged into the FirePass controller (authenticated), and receives an HTTP session cookie. When the user next clicks on the Network Access link after logging in, a client ActiveX control is either installed and activated (or just activated) in the user's browser. This ActiveX control will start the Network Access connection (PPP over SSL). The FirePass allows the establishment of secure, VPN Network Connection without requiring pre-installed client software. During the initial session, all required software is uploaded from the FirePass Appliance to the Client. Using a standard HTTPs protocol, connections can be made through standard infrastructure components used in private LANs, proxies and ISPs. Access functions to the Network Access Mode are orchestrated by the Authentication Module, which based on support from the Policy Engine, determines whether the User has the required credentials, forwards the credentials to the Authentication Server in the IT Environment for authentication, and determines which level of access to grant based on Endpoint Security Checking. Network Access Mode also includes the Endpoint Security functionality, which enhances session security through Endpoint Security checks and cleanup functions following session closure.

4.5 Web Applications Mode Access

The FirePass Web Applications Mode allows for network access through a layer 7 connection from public terminals utilizing a variety of operating systems and platforms. This mode allows secure access to internal web servers, email servers and intranet resources without installation of software on the client resource. Access to web applications can be closely tailored to specify which users and groups can access which resources. During the connection process, the FirePass Appliance remaps internal addresses to the client user so internal IP addresses are hidden from public view.

The Web Application mode also fronts cookies on behalf of the network, providing insulation from potential security risks contained in cookies from a public computing resource. FirePass can also prohibit caching and downloading of files if controls are not downloaded to the client, assuring that these files are safely deleted at the end of the session.

Access functions for the Web Applications Mode are orchestrated by the Authentication Module, which, based on support from the Policy Engine, grants access to applicable Intranet resources. Access to requested resources proceeds upon required credential verification using an external authentication server.

Users that access through a Windows XP/2000 operating system environment can be automatically switched to Protected Workspace mode, which restricts write access to only the protected area and deletes temporary files upon completion of the session.

4.6 Policy Based Resource Management

The TOE dynamically maps internal URLs to external URLs and deletes URL information following the session. This protects IP addresses for the internal network from eavesdropping and potential security exploitation in Web Applications Mode.

FirePass also has features that may be configured to limit the level of access to the TOE and Host Network resources based on the browser used, anti-virus and firewall status in the Client computer, and connecting computer origin. Therefore, untrusted resources are restricted to a limited (administrative user specified) level of access to protect TOE resources.

One aspect of how FirePass implements Policy Based Resource Management is the use of Resource Groups. Resource groups organize Network Resources (such as intranet servers, applications, and network shares) into groups within FirePass. The use of Resource Groups also allows the mapping of specific Master Groups of Users to specific groups of FirePass managed Network Resources.

The TOE automatically routes and quarantines suspect connections to a self remediation network to allow for analysis and appropriate response (self remediation network not included in the CC evaluated configuration). Packet filter rules can be customized by administrative users for Network Access Mode sessions to allow for isolation of specific protocol types and routes traffic based on factors such as source, destination or type of service requested. Policy Based Resource Management leverages the functionality of the Networking Module with the Policy Engine to determine appropriate routing based on configurable variables set by the Administrative User.

4.7 Security Management

The FirePass Appliance provides a comprehensive Security Management suite through the Administrator Console. This provides Administrative Users with GUI based tools to manage audit records, install the appliance, manage user and group enrollment, configure Failover, generate/install certificates, and customize the remote client user interface. Administrative users can tailor the function of the FirePass Appliance to the deployed environment and the network resource groups to be managed by the appliance. In addition, the Administrator interface is used to monitor security related events in appliance audit logs. An Administrator management (Ethernet) port is provided for dedicated Administrator GUI access.

The Security Management security function is supported by the Administrator Console, which provides the GUI interface and the Networking Module/OS which stores configuration data within an SQL database.

Security Management functions are accessible by Administrative Users only after successful identification and authentication as coordinated by the Authentication Module. Administrative Users are considered “Internal appliance users” and are authenticated by the TOE. A dedicated

Administrator Management Serial Port is provided for a limited set of appliance configuration activities. Remote administration is conducted through secure TLS sessions.

4.8 Secure Communications

Secure Communication techniques are available in the TOE for Administrative User access via SSLV2/3. Low, Medium and High Grade Security selections, which determine the cipher types, key sizes and SSL session security attributes, are available. The High Grade security selection is mandatory for the Common Criteria Evaluated Configuration in conjunction with the Accept TLS Only session setting. This assures that only 3DES or AES based ciphers are used within sessions using the TLS protocol, exclusively.

All communications are secured via Secure Socket Layer (SSL) encryption functionality provided by the SSL module. The SSL session is established during the initial login to the FirePass Appliance and requires successful authentication and key exchange. The TOE utilizes FIPS approved cipher suites through the high grade security setting; however, the FIPS 140-2 SSL Accelerator hardware option is not included in the Evaluated Configuration.

All traffic communicated through the FirePass TOE is encrypted using SSL techniques as described above, and TSF access is managed based on the FirePass Network Access Mode SFP/FirePass Web Applications Mode SFP. Access to these modes of operation is enforced by the Authentication Module functionality. FirePass Operating level support in establishing SSL sessions is coordinated through the Policy Module.

4.9 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 and Operating System Environment and through the secure communication methods described in previous section (4.8).

The TOE is installed in a redundant pair configuration, which applies a second FirePass appliance configured to automatically switchover in the event of failure of the primary appliance. This redundant pair is configured in an active-standby configuration. One appliance actively manages traffic and a standby unit provides redundancy. Upon failure of the active appliance, the standby unit is fully configured and able to process traffic immediately. Configuration settings established by the Administrative user ensure that the configuration and attributes established on the primary appliance are immediately in effect on the redundant appliance through the Failover functionality provided by the TOE.

5 Assumptions

5.1 Personnel Security 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.

5.2 Physical Security Assumptions

A.PHYSICAL 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 FirePass Appliance.

5.3 Operational Security Assumptions

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

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)
- Application Servers (Web Servers)

6.1 Architectural Information

. The FirePass appliance consists of the following components

- SSL Module
- Policy Engine
- Web Applications Mode Module
- Authentication Module
- Application Access Module
- Network Access Mode Module
- Networking Module/Operating System
- Administrator Console
- Network Access Plug-In
- Endpoint Security Plug-In

The high-level architecture of the TOE is shown in Figure 1

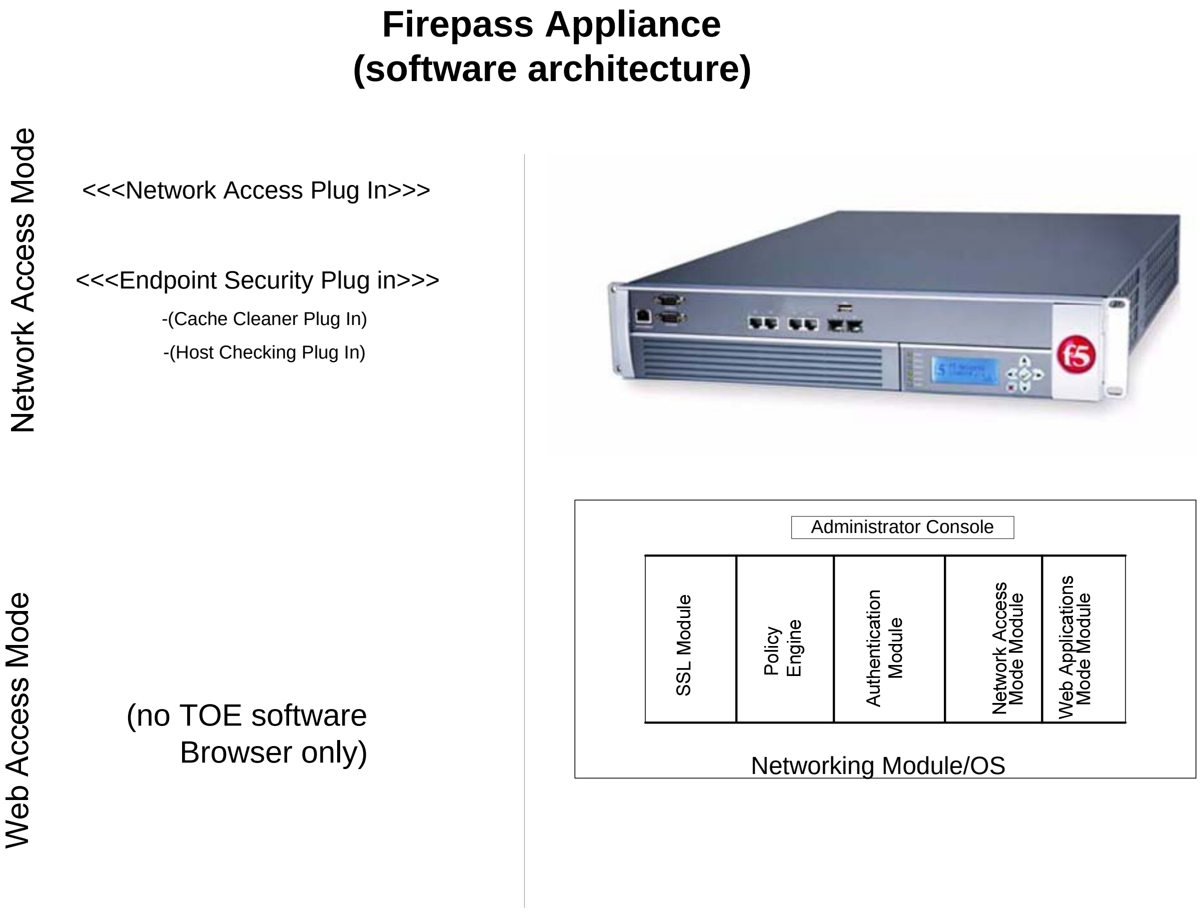

Figure 1: TOE internal architecture

6.2 TOE Hardware

The TOE hardware consist of the FirePass 4100 rack mounted chassis and dual AMD Opteron Processors.

6.3 TOE Software

The TOE software consist of the FirePass software suite installed on the Appliance includes: FirePass OS (Linux 2.4.31) – Operating System with F5 FirePass Kernel, FirePass Client, Endpoint Security Plug-In (Cache cleaner plug-in and host checking plug-in). Secondary switch card software is also loaded during manufacturing.

7 Documentation

Design Documentation

Document	Revision	Date
EAL 2 High Level Design Documentation F5 Networks FirePass® (ADV_HLD)	1.0	9/28/07
EAL 2 Design Documentation Functional Specification and Implementation Representation F5 Networks FirePass® (ADV_FSP)	1.0	9/28/07
EAL 2 Design Documentation Functional Specification and Implementation Representation F5 Networks FirePass®, Section 4 (ADV_RCR)	1.0	9/28/07
F5 Networks FirePass® 4100 Version 5.5.2 Security Target EAL 2 + ALC_FLR.1, ADV_SPM.1, Section 6.1.9 (ADV_SPM)	1.3	12/19/07

Guidance Documentation

Document	Revision	Date
FirePass® Controller Getting Started Guide		February 6, 2007
FirePass® Controller Administrator Guide		September 2005
FirePass Controller Remote Access Quick Setup Worksheet		
Common Criteria User Guidance EAL 2 F5 Networks FirePass 4100 High Availability pair (qty 2)	1.0	9/28/07
F5 Networks FirePass® 4100 Version 5.5.2 Security Target EAL 2 + ALC_FLR.1, ADV_SPM.1	1.3	12/19/07

Configuration Management and Lifecycle

Document	Revision	Date
F5 Networks FirePass® 4100 High Availability pair (qty 2) EAL 2 Configuration Management Documentation (ACM_CAP)	1.0	9/28/07
F5 Networks FirePass® 4100 Version 5.5.2 Security Target EAL 2 + ALC_FLR.1, ADV_SPM.1	1.3	12/19/07

Delivery and Operation Documentation

Document	Revision	Date
Common Criteria Supplement EAL 2 Secure Delivery Document F5 Networks FirePass 4100 High Availability pair (qty 2) (ADO_DEL)	1.0	9/28/07
F5 Networks FirePass® 4100 Version 5.5.2 Security Target EAL 2 + ALC_FLR.1, ADV_SPM.1	1.3	12/19/07

Test Documentation

Document	Revision	Date
Test Activity ATE F5 Networks FirePass® 4100 Version 5.5.2 EAL 2, Section 3 (ATE_COV.1)	1.0	9/28/07
EAL 2 High Level Design Documentation F5 Networks FirePass® (ADV_HLD)	1.0	9/28/07
EAL 2 Design Documentation Functional Specification and Implementation Representation F5 Networks FirePass®	1.0	9/28/07
F5 Networks FirePass® 4100 Version 5.5.2 Security Target EAL 2 + ALC_FLR.1, ADV_SPM.1	1.3	12/19/07

Vulnerability Assessment Documentation

Document	Revision	Date
F5 Networks FirePass® 4100 Version 5.5.2 Common Criteria Vulnerability Analysis AVA_VLA.1 EAL 2	1.0	9/28/07
F5 Networks FirePass® 4100 Version 5.5.2 Security Target EAL 2 + ALC_FLR.1, ADV_SPM.1	1.3	12/19/07
EAL 2 Strength of Function Analysis F5 Networks FirePass® 4100 Version 5.5.2	1.0	9/28/07
Common Criteria User Guidance EAL 2 F5 Networks FirePass 4100 High Availability pair (qty 2)	1.0	9/28/07
EAL 2 High Level Design Documentation F5 Networks FirePass® (ADV_HLD)	1.0	9/28/07

Security Target

Document	Revision	Date
F5 Networks FirePass® 4100 Version 5.5.2 Security Target EAL 2 + ALC_FLR.1, ADV_SPM.1	1.3	12/19/07

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 TOE 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 TOE consistent with the Common Criteria evaluated configuration identified in the ST. The Developer’s approach to testing is defined in the TOE Test Plan. The expected and actual test results (ATRs) are also included in the TOE Test Plan. Each test case was identified by a number that correlates to the expected test results in the TOE 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 TOE 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 TOE while performing work unit ATE_IND.2-2. The evaluation team confirmed that the TOE 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 TOE'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 70% 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 TOE Security Function was exercised at least once, and the evaluation team verified that each test passed.

8.3 Vulnerability analysis

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

The Developer performed a Vulnerability Analysis of the TOE to identify any obvious vulnerabilities in the product and to show that they are not exploitable in the intended environment for the TOE 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 TOE 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 five (5) penetration tests.

9 Evaluated Configuration

This section documents the configuration of the IT product during the evaluation. Typically, the administrator or installation guide will provide the necessary details for the correct configuration of the IT product. The IT product may be configurable in a number of different ways, depending on the environment it is used in or the security policies of the organization that it enforces.

The precise settings and configuration details with accompanying rationale for these choices are outlined in this section. Any additional operational notes and observations can also be included. This section is of particular importance, as it provides a baseline for the evaluated product installation.

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 TOE 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 and ADV_SPM.1. A team of Validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation was completed in September 2007.

11 Validator Comments/Recommendations

The TOE depends upon several devices in the IT environment. Reviewers should be aware of the fact that this evaluation does not include these devices. The authentication server, for example, is in the environment and was not evaluated. In addition, some features of the product are not included in the evaluated configuration. Some of these may be of interest to consumers, such as the use of dual-factor authentication devices. While the product provides this capability, it is not part of the evaluated configuration.

The Validation team reviewed the activities of the Evaluation team and concurred with their conclusion that issuance of an EAL4 rating is justified for the TOE.

12 Annexes

Not Applicable.

13 Security Target

F5 Networks FirePass® Version 5.5.2 Security Target EAL 2 + ALC_FLR.1, ADV_SPM.1, Version 1.3, December 19, 2007.

14 Glossary

The following definitions are used throughout this document:

- **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.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **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.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **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.
- **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.

15 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-2004-01-0001.

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 Technology 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 FirePass 4100 Version 5.5.2 Security Target EAL 2 + ALC_FLR.1, ADV_SPM.1, Version 1.3, December 19, 2007.

7.) InfoGard Laboratories, Evaluation Technical Report F5 Networks FirePass 4100 Version 5.5.2 EAL 2 + ALC_FLR.1, ADV_SPM.1, Version 1.0, September 28, 2007.