F5 Networks

FirePass® 4100 Version 5.5.2

Security Target

EAL 2 + ALC_FLR.1, ADV_SPM.1

Release Date:	December 19, 2007
Document ID:	**06-1023-R-0018**
Version:	1.3

Prepared By: InfoGard Laboratories, Inc.

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

Table of Contents

List of Tables

List of Figures

Document History

Release Number	Date	Author	Details
1.3	12/19/07	M. McAlister	Final Release Version

1 Introduction

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

1.1 Identification

TOE Identification:	FirePass 4100 Version 5.5.2 + Hotfix HF-552-10
ST Identification:	F5 Networks FirePass® 4100 Version 5.5.2 Security Target EAL 2 + ALC_FLR.1, ADV_SPM.1
ST Publication Date:	December 19, 2007
ST Version Number:	Version 1.3
Authors:	M. McAlister (InfoGard)

1.2 CC Conformance Claim

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

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

The TOE is also compliant with all International interpretations with effective dates on or before September 1, 2006.

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

1.3 Overview

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

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

servers & 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.

1.4 Organization

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

Table 1: ST Organization and Description

1.5 Document Conventions

The CC defines four operations on security functional and assurance requirements. The conventions below define the conventions used in this ST to identify these operations. When

NIAP interpretations are included in requirements, the changes from the interpretations are displayed as refinements.

Assignment: **indicated with bold text**

Selection: indicated with underlined text

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

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

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

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

1.6 Document Terminology

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

1.6.1 ST Specific Terminology

Admin (full access) This refers to the top Administrative role with full privileges, access and control over all FirePass functions.

Administrator Console This refers to the Administrator GUI which allows Administrative Users to manage the appliance through a Administrator Workstation in the IT Environment via the Administrator Management port on the FirePass appliance.

Client Within the context of this security target, the Client refers to the External VPN User role, located outside of the internal network, who establishes VPN sessions through the TOE to allocated internal network resources. Synonymous with External VPN User.

Controller Within this document, the term Controller is used in the context of FirePass Controller and is synonymous with the appliance term. The FirePass Controller, FirePass Appliance and FirePass TOE all represent the TOE product.

Web Applications Mode Web Applications Mode access is supported through a layer 7 connection for public secure access to Internal Web Portals and Intranet applications. Dynamic parsing and patching of HTML, JavaScript, and other content is performed as part of this function.

Application Access Mode

Application Access mode allows for specific application access such as Oracle or Exchange Servers. This mode is not part of the CC evaluation configuration.

Network Access Mode

Network Access Mode is supported through a layer 3 connection through PPP over SSL techniques. This allows for a secure tunnel to be established to network resources. This mode requires FirePass Client Plug-Ins.

Internal Appliance Users

For the purposes of this ST, Users who are managed on the FirePass product (stored in the internal database) authenticated internal to the appliance.

External VPN Users

For the purposes of this security target, Users of the FirePass VPN functionality. These accounts are managed on the FirePass product (stored in the appliance internal database) and authenticated external to the appliance through an external authentication server.

Failover

This describes the processes of switching FirePass functions from one unit to another redundant unit when configured in the high availability redundant pair configuration (CC evaluated configuration).

Host Client Network

This describes the Private Network Resources that are accessed by outside (External) Users through the FirePass TOE.

Master Groups

A master group is a collection of users. It contains authentication settings, overall security configuration settings for groups of users, network access filtering policies, user experience.

Pre-login Sequence

A named set of inspectors, rules, and actions, which evaluates each endpoint system presented for log on to the FirePass controlled network.

Post-login Protection

Configurable protection features that run after the user logs on to the FirePass appliance. You can configure to download an ActiveX control to support various kinds of post-logon protection.

Protected Configurations

A set of safety checks to protect resources (Endpoint Security). These focus on a specific aspect of protection, such as unauthorized access, information leaks, virus attacks, and keystroke loggers. For each criterion, FirePass provides specific safety measures.

Realm

An administrative realm is a complete set of roles, master groups, and resource groups.

Resource Group

A resource group is a collection of resources, which includes your company intranet servers, applications, and network shares.

Reverse Proxy

Reverse proxy within the context of this ST refers to the mapping of internal network addresses to external URLs within the FirePass appliance during Web Application mode sessions, thereby preventing disclosure of network address information to users outside the network.

RSA SecureID

A (token based) mechanism developed by RSA Security for authenticating a user to a network resource.

VASCO Digipass

Digipass is a security product from VASCO, providing strong user authentication and e-Signatures via small hardware keys carried by users, or in software on mobile telephones, portable devices or PCs.

1.6.2 Acronyms

AD	Active Directory (Authentication Server)
CA	Certificate Authority
CC	Common Criteria
CLI	Command Line Interface
DLL	Dynamic Link Library
FTP	File Transfer Protocol
NAT	Network Address Translation
RNG	Random Number Generator
SFP	Security Function Policy
SSL	Secure Socket Layer (denotes SSLv2 or SSLv3 only)
TCP	Transport Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TOE Security Function Interface

TSP	TOE Security Policy
OS	Operating System
VPN	Virtual Private Network

2 TOE Description

2.1 Overview

The TOE is a VPN Appliance that enables secure network access to remote Users. The FirePass Appliance provides network access based on various access modes. Network Access Mode allows secure network layer access from trusted resources through a VPN tunnel established using PPP over SSL techniques. Network Access mode sessions are established through a browser in conjunction with plug-in modules which are downloaded during the initial session. Point to Point Protocol (PPP) is used as a data link layer which is used to establish communications between two network nodes. This session through FirePass is secured through a Secure Socket Layer (SSL) session, which encrypts these communications to avoid disclosure or modification of data. Utilizing the plug-in module functionality a series of endpoint security checks are executed on the External VPN client workstation prior to and during Network Access mode sessions, to assure required security settings are in place.

Web Applications Mode allows for secured public access to internal web portals and intranet applications especially suited for access from public (untrusted) resources. This mode features clientless application layer session access which allows SSL secured access to allocated resources. This mode includes special functions to ascertain security status and modify access based on established security profiles.

These operational modes refer to the method by which connections are made through the TOE by the Client; the TOE supports both options simultaneously. The TOE evaluated configuration includes a network appliance (hardware/software) that applies to both modes of operation and Client plug-ins (software) for the Network Access Mode capability. The Common Criteria evaluated configuration requires that the TOE be installed in a high redundancy pair (qty 2) configuration.

2.2 Architecture Description

The following figures describe the FirePass TOE architecture, TOE Boundary and internal TOE subsystem arrangement used within this Security Target.

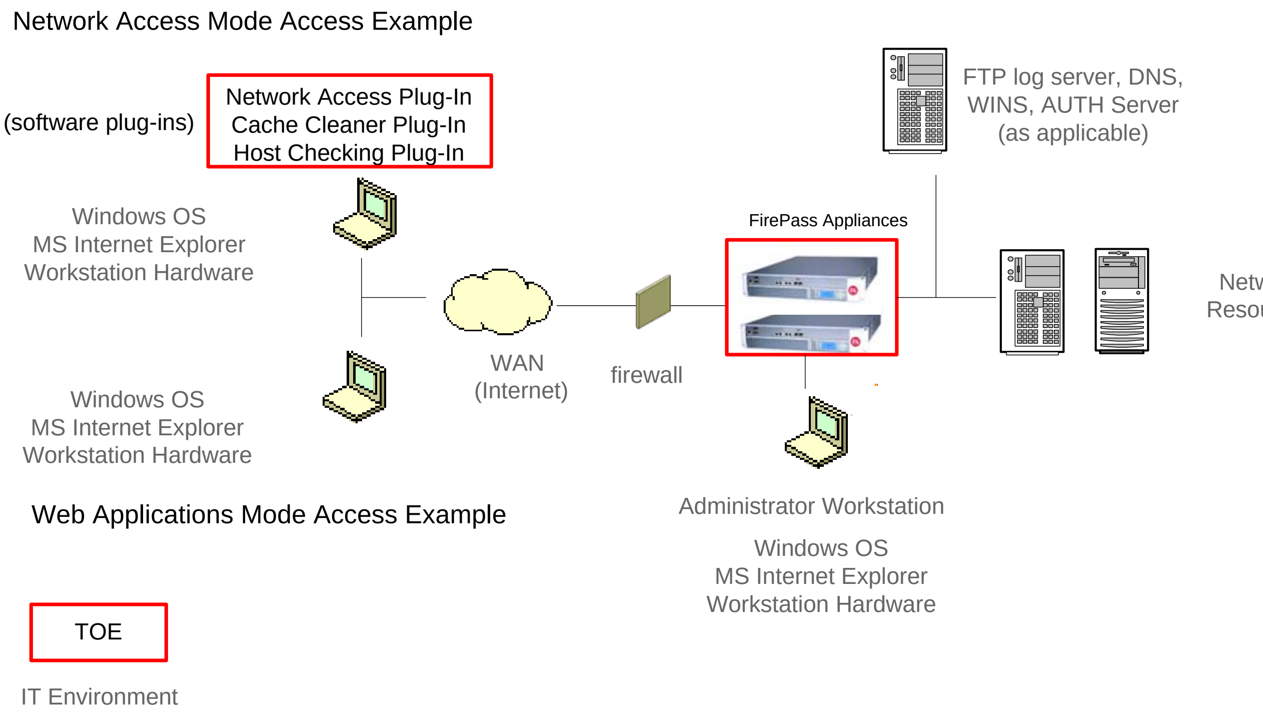

Figure 1: FirePass TOE Network Diagram/Boundaries

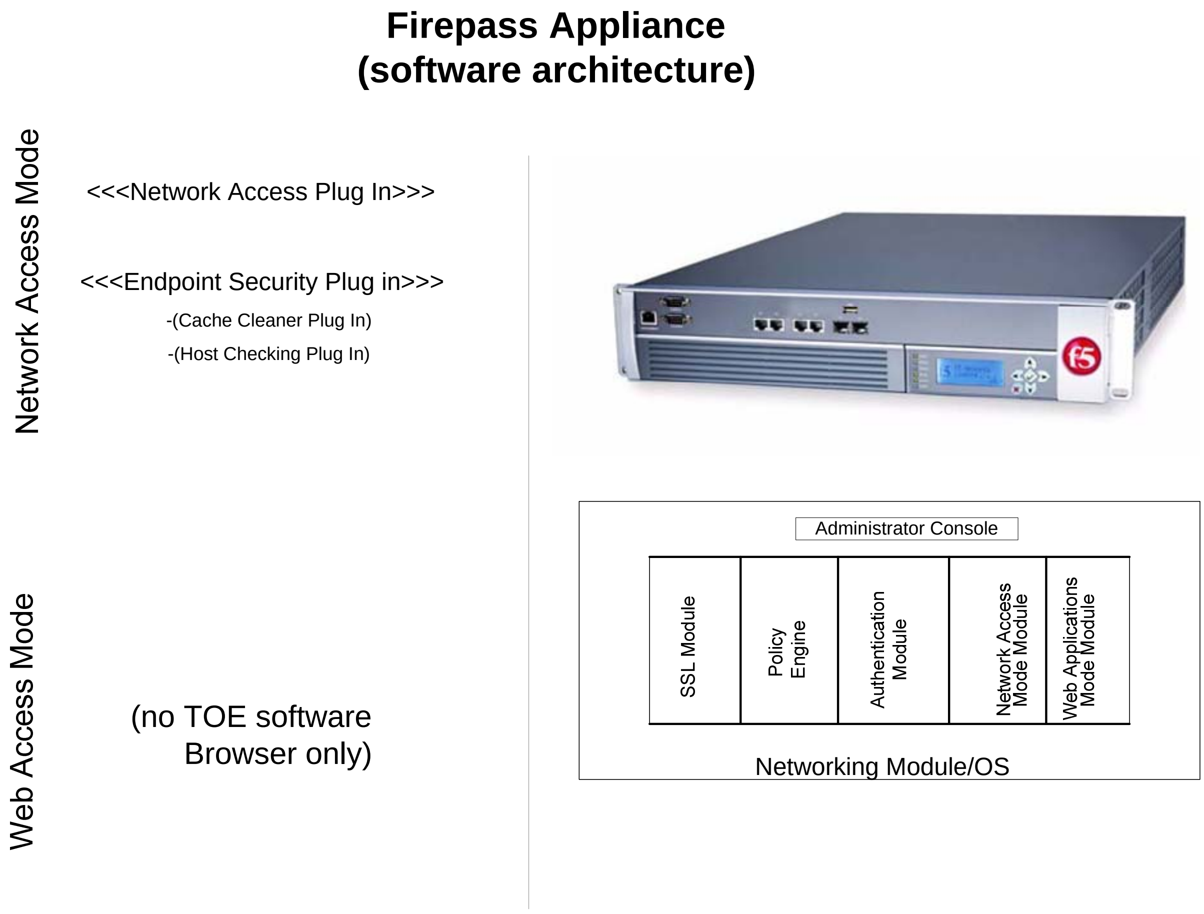

Figure 2: TOE Internal Architecture

The following section describes the FirePass TOE subsystems as depicted in Figure 2. These subsystems provide a design abstraction for the purpose of describing the method used for providing the security functionality described in Section 2.4, Logical Boundaries. A detailed description of how the listed subsystems implement the TOE security functions is provided in Section 6: TOE Summary Specification.

2.2.1 SSL Module

The SSL module negotiates the secure connections with the Client and coordinates identification, authentication requests and certificate exchange services with the Authentication Module. Within this module is the certificate store that maintains certificates and key management information. The SSL module utilizes a Secure Socket Layer (SSL) secure protocol which negotiates and establishes a key/certificate exchange among the two parties to result in cryptographic encryption of traffic traveling between the two parties to avoid intercept or disclosure. The TOE leverages an open-source SSL module that is part of the Apache Web Server software within the TOE software suite. The Common Criteria Evaluated Configuration requires the high grade security setting which determines acceptable ciphers and the TLS only settings which accepts only TLS session protocols.

2.2.2 Policy Engine

The Policy Engine provides enforcement of traffic flow policies within the FirePass Appliance to assure that security is maintained during Network Access Mode and Web Applications Mode sessions. This includes routing rules created by administrative user settings by connection type and rules for establishing connections based on security attributes and Administrative user configured session parameters.

2.2.3 Web Applications Mode Module

The Web Applications Mode Module manages a layer 7 connection that supports secure access to intranet applications and internal web portals. This module provides secure access through reverse-proxy techniques. A reverse proxy takes connections from the internet and translates the routed address to actual internal network locations. Traffic routed from within the LAN to outside locations is mapped to different addresses and routed outside the network. This provides a “proxy” between the WAN and protected network and manages different IP addresses for the WAN from the Internal Network and provides the translation within the FirePass appliance. Through this, the true internal network IP addresses are not disclosed outside the network. In addition to concealing IP addresses, the FirePass appliance fronts cookies on behalf of network resources. By fronting cookies, the appliance is actually accepting and managing cookies on behalf of protected network servers to outside resource requiring session cookies. The Web Applications Mode Module allows External VPN users to access internal web portal and intranet applications from a public access device after successful identification and authentication. Prior to transferring content to the client, conversion to HTML is executed within this module to allow for viewing using a browser. The Apache Web Server component, which is part of the TOE software suite, supports this functionality. This provides remote Users with secure (SSL encrypted) access to intranet resources such as corporate email servers.

2.2.4 Authentication Module

The Authentication Module manages both internal and external authentication mechanisms for the TOE appliance. Internal authentication for the TOE allows for users to be authenticated within the appliance. For the TOE, internally authenticated users are limited to Administrative Users; External VPN Users are authenticated via an external authentication server. This module contains an internal database which stores FirePass controller user data: name, logon designation, password (stored as cryptographically strong hashes), email address, and group name. Password management features for internal authentication are integrated in this module with authentication validation processes. If an external authentication server is used, the Authentication Module interacts with the external authentication server to forward credentials and manage access to the appliance.

2.2.5 Application Access Mode Module

The Application Access Mode Module manages Application Access Mode features. This functionality is not included in the evaluated configuration for Common Criteria and is not shown in Figures 1 and 2.

2.2.6 Network Access Mode Module

The Network Access Mode Module manages the Network Access Mode features for layer 3 connections. This module provides the capability for the TOE to establish PPP over SSL connections through a secure VPN tunnel, allowing secure access to FirePass protected network resources.

2.2.7 Networking Module/Operating System

The Networking Module provides FirePass Networking features implemented through the FirePass Operating System functionality. The Networking Module functions include the TCP/IP stack, advanced Policy Based Resource Management, Network Address Translation (NAT), SQL database and packet filtering operations.

2.2.8 Administrator Console

The Administrator Console manages the Administrative user access to the TOE for both local and remote types of access through a dedicated local Administrator management port for remote web access through a GUI using Apache software functionality. The Administrator Console interacts with the Authentication Module to assure users are identified and authenticated by FirePass as Administrative user prior to access.

2.2.9 Network Access Plug-In

The Network Access Plug-In, in association with the supported Microsoft® Internet Explorer browser, provides the Client functionality to establish a secure Network Access Mode tunnel via PPP over SSL. This subsystem only applies to Network Access Mode. Web Applications Mode is clientless and does not require specific FirePass Client software.

2.2.10 Endpoint Security Plug-In

This module includes the Cache Cleaning Plug-in and the Host Checking Plug-in used by the FirePass Network Access Plug-In (Active-X), in association with the supported Microsoft® Internet Explorer browser, to provide security features for the Client machine. The cache cleaning plug-in assures that cache is cleaned following a secure session to ensure that sensitive data does not remain following a secure session. The Host Checking Plug-in activates functions that verify the status of the Client computer through scans which detect suspect running processes, virus checker status, and firewall in use to assure adequate security is supported on the client. Based on the results of these scans, access can be modified to limit exposure to insecure clients.

2.2.11 FirePass Hardware

The FirePass 4100 appliance platform provides the hardware device upon which the software described above is implemented. This hardware platform features a standard 2U rack mounted chassis with 4 10/100/1000 LAN ports and a single 160 GB hard drive. The appliance features 4 GB of RAM and is upgradeable to 8 GB as needed. The 4100 platform supports a single AMD® dual-core processor and supports clustering and appliance fail-over protections. A single appliance is designed to accommodate 500 concurrent users and supports up to a maximum of 2000 users. The Common Criteria evaluated configuration requires 2 appliances arranged in a redundant pair configuration.

2.2.12 Statement of Non-Bypassibility of the TSF

TOE security functions cannot be bypassed. All access to TOE security management functions requires Administrative user level access to the TOE. The FirePass Controller authentication process ensures that a secure user name and password combination must be entered prior to allowing any changes to TSF settings.

2.3 Physical Boundaries

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

2.3.1 Hardware Components

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

TOE or Environment	Component Name	Description of Component
TOE	FirePass Hardware 4100	4100 2U rack mounted chassis, Single AMD Dual-Core Processor, 4 LAN ports, 160 GB hard drive, 4 GB RAM
Environment	Authentication Server	Applicable Auth. Server (A.D., LDAP, RADIUS)
Environment	Application Servers	Application servers – Web Servers
Environment	Firewall	Firewall appliance
Environment	Remote PC	PC or Laptop for remote Administrator access

Table 2: Physical Scope and Boundary: Hardware

2.3.2 Software Components

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

TOE or Environment	Component Name	Description of Component
TOE	FIREPASS OBJECT CODE - WYVERN (5.5.2) + Hotfix HF-552-10 FirePass Appliance software	FirePass software suite installed on Appliance includes: FirePass OS (Linux 2.4.31) –Operating System with F5 FirePass Kernel, FirePass Client Endpoint Security Plug-In (Cache Cleaner Plug-in (Client) Host Checking Plug-in (Client))
TOE	OBJECT CODE, BOOTSTRAP, BUFFALO JUMP FAMILY SCCP RELEASE A ECO-1366 Switch Card software	Secondary switch card software loaded during manufacturing
(Client & Administrator workstation) Environment	Microsoft Internet Explorer 6.0 SP2 or later	Web Browser Component (required for client side features – Network Access Mode) and for Administrator workstation machine
(Client & Administrator workstation) Environment	Client Operating System for Network Access Mode	Supported client operating systems include Windows 2000 SP4, Windows XP SP2 and for Administrator workstation machine

Table 3: Physical Scope and Boundary: Software

2.4 Logical Boundaries

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

2.4.1 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 records generated by the TOE are managed by the following categories for administrative user access:

App logs User related log which reflect user session origin and action taken during the session

Logins login statistics including success/failure of login attempt

Session log session details by session type, duration and current status

HTTP log Exclusively, HTTP protocol related events & classification

System log System level events such as session details, prelogin check messages, system status, reboot, failover etc.

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. Once offloaded to an external server, the audit logs are no longer accessible for review during FirePass administrative sessions.

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

2.4.2 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 account assignments. Master Groups provide the FirePass Administrative User with a convenient mechanism to specify identical access privileges to resources within the internal network among multiple External VPN User accounts. Access to specific network resources are configured to Master Groups during initial configuration and include what network resource can be accessed, the type of session allowed to that resource and what actions are allowed during a session. Additional security provisions can also be required for sessions on a resource by resource basis such as protected workspace.

For example, a Sales Master Group may be created to allow access to Sales web servers within the internal network to members of the group. These resources may also be configured for a Marketing Master Group as well, potentially with different access levels or privileges. External VPN Users may be assigned to multiple groups within FirePass. In order to access a given internal network resource, at least one group assignment held by the user must have the desired access explicitly allowed.

Master Group access assignments specify allowed access, therefore, absence of an explicit access assignment represents access denied to a given resource or session type.

Explicit access restrictions are primary enforced through session pre-requisites such as pre-login checks, where if a series of security pre-requisites on the Client machine are not met, access to the session type is denied on a global basis.

Master Groups are also used as the means of establish access privileges for Administrative Users through roles i.e.: the Admin (Full Access) role is assigned by placing the administrative user in the “Full Access” group assignment. Administrative Master Group configuration allows configuration of access to FirePass appliance configuration objects through the GUI.

Administrative Users (local Users) are identified and authenticated internal to the FirePass TOE using values stored internal to the appliance within an SQL database. FirePass requires that the Admin (full access) be authenticated within the appliance to assure Administrator level access to the Appliance is dependant on authentication server resources in the IT Environment.

External VPN users access the FirePass appliance exclusively to initiate VPN sessions with supported backend network resources. Once login processes are completed, FirePass functionality is transparent to these users as they access network resources in much the same manner as when residing within the internal network. These users hold accounts within the appliance which specify their FirePass VPN access privileges and session settings but are authenticated using an external authentication server. The FirePass appliance requires validation of login credentials by an external authentication server for External VPN users prior to allowing initiation of a FirePass VPN session. 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.

2.4.3 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 (presence of anti-virus software running on client)
- personal firewalls (presence of firewall software running on client)

- 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.

Some Endpoint Security features are realized through the Client software, which may be installed on the Client machine (i.e.: for Network Access Mode) in clientless mode; that is, when the inspection process does not download any controls or plug-ins, the Endpoint Security process inspects the HTTP headers to gather the information. For example, FirePass will restrict downloads if caching is not disabled or cache cleanup is not enabled so, following a session, residual information does not remain on a public access computer.

Examples of post-login protection features include:

Activate cache cleanup to allow attachment downloads in Mobile E-Mail and downloads from Web Applications.

Activate cache cleanup to allow file downloads in Windows Files. If this option is not checked, the user can only download .zip archives.

End the FirePass session if the user closes the browser or webtop.

Uninstall FirePass client components.

Remove dial-up entries once used by Network Access clients.

Uninstall ActiveX components downloaded during the session.

Empty the Windows Recycle Bin.

Clean forms and passwords auto-complete data.

Close Google desktop search.

Inherit caching policy settings from Portal Access Web Applications configuration.

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.

Through the Secure Virtual Keyboard feature, (a part of the Client Security Module), login data can be entered from client resources with a mouse versus a keyboard for enhanced security. This technique is intended to obfuscate keystroke observation.

2.4.4 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 as described in Section 2.1 (Overview). 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 listed in Section 2.4.3, which enhances session security through Endpoint Security checks and cleanup functions following session closure.

2.4.5 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 (see Section 2.1, Overview), 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.

2.4.6 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. This functionality is provided by the Policy Engine in concert with the Networking Module.

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.

2.4.7 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.

2.4.8 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. Cryptography strength of function is not included within the scope of this ST.

2.4.9 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 2.4.8.

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.

2.5 Items Excluded from the TOE

This section identifies any items that are specifically excluded from the TOE.

- Application Access Mode of Operation & Application Access Mode Module software component
- Web Access Mode: File Share Access feature incl. usage of SMB protocol
- The use of the standalone VPN client for Network Access Mode sessions (browser use required)
- SSL accelerator hardware option
- Cache cleanup usage and activation for Web Applications Mode which allows file downloads in Windows Files. If this option is not checked, the user can only download .zip archives.
- Linux and Macintosh Client usage for Network Access Mode
- The use of FirePass in a cluster configuration
- The use of a self remediation network for suspect connections
- Internal authentication of External VPN users
- The use of FirePass for load balancing
- Password-less “auto-authentication” through FirePass Appliance
- Certificate based authentication through FirePass Appliance
- Online Software updates
- Anti-Virus capability represented by the Clam AV component for scanning of traffic traversing the FirePass appliance.
- Service account usage/access to CLI console (disabled in TOE)

3 TOE Security Environment

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

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

3.1 Assumptions

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

3.1.1 Personnel Assumptions

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

3.1.2 Physical Environment Assumptions

A.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.

3.1.3 Operational Assumptions

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

3.2 Threats

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

T.SEC_FUNC Administrators may make changes to TOE security functionality without accountability.

T.FLAW_CONFIG Unintentional errors in implementation of the TOE deployment may occur, leading to flaws which may be exploited by a malicious User or program.

T.MASK An unauthorized User may masquerade as an authorized User or an authorized IT entity to gain access to data or TOE resources.

T.AUDIT_ COMP A user or process may gain unauthorized access to the audit trail and cause audit records to be lost or modified or prevent future audit records from being recorded, thus masking a security relevant event.

T.TSF_COMP An attacking user or process may cause, through an unsophisticated attack, TSF data or executable code to be inappropriately accessed (viewed, modified, or deleted).

T.UNID_ACTION An administrator may not have the ability to notice potential security violations, thus limiting the administrator's ability to identify and take action against a possible security breach.

T.UNSEC_CLIENT The IT Environment in Clients may not be securely configured or may lack firewall or anti-virus protection, leading to potential security exploits remaining within the system and/or compromised ability to connect to FirePass in a secure manner.

T.UNSEC_DATA Data Transfer between the FirePass Appliance and FirePass Clients (Network Access Mode)/Untrusted IT resources (Web Applications Mode) or between the TOE and applicable authentication servers may be modified or disclosed in transit.

T.RESIDUAL Session related Data or User Information may remain within the Client IT Environment following a session, leading to disclosure (Network Access Mode).

T.TOE_FAIL The failure of a TOE appliance may result in loss of traffic and/or failure to meet the TSF.

3.3 Organizational Security Policies

There are no Organizational Security Policies for this TOE.

4 Security Objectives

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

4.1 Security Objectives For The TOE

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

O.AUDIT_GEN The TOE will support creation of audit records of security relevant events.

O.AUDIT_PROTECT The TOE will provide the capability to protect audit information.

O.AUDIT_REVIEW The TOE will provide the capability to read audit information from the audit records in a manner suitable for the user to interpret the information

O.AUDIT_STOR The TOE will provide a means for secure storage of the TOE audit log files.

O.CLIENT_TEST The TOE will provide functionality to evaluate the Client IT Environment to assure that the Client IT Environment is operating in a secure mode.

O.MANAGE The TOE will provide all the functions and facilities necessary to support the Administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.

O.RESIDUAL The Network Access Mode Client of the TOE will provide mechanisms to remove residual data from the Client IT Environment to prevent disclosure (Cache Cleaner).

O.SELF_PROT The FirePass appliance will maintain a domain for its own execution that protects its resources from external interference, tampering or unauthorized disclosure through its own interfaces.

O.TIME_STAMPS The TOE shall provide reliable time stamps and the capability for the Administrator to set the time used for these time stamps.

O.ROBUST_TOE The TOE will provide mechanisms that control a User's logical access to the TOE and to explicitly deny access to specific Users when appropriate.

O.SECURE_DATA The TOE will establish SFPs to ensure secure and unmodified data transfer between the FirePass appliance and FirePass Client Software (Network Access Mode) /Untrusted IT Resources (Web Applications Mode) and External Authentication Servers, as applicable.

O.SAFE_FAIL The TOE will protect the TSF in the event of the failure of a single TOE appliance and preserve correct operations during such events.

4.2 Security Objectives for the Environment

OE.AUTH_SUPPORT The IT Environment will provide authentication verification mechanisms for the TOE and send the authentication result to the FirePass appliance when required.

OE.NO_BYPASS The IT Environment will ensure that the TOE security mechanisms cannot be bypassed in order to gain access to the TOE resources.

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

OE.ADMIN Sites using the TOE will ensure that the authorized administrators are appropriately trained, not careless, not willfully negligent, non-hostile and follow all instructions within administrative guidance.

OE.DEDICATED Administrators will assure that the FirePass Appliance is dedicated to its primary function and does not provide any general purpose computing or storage capabilities.

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

4.3 Mapping of Security Environment to Security Objectives

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

	T.SEC_FUNC	T.FLAW_CONFIG	T.MASK	T.AUDIT_COMP	T.UNID_ACTION	T.RESIDUAL	T.TSF_COMP	T.UNSEC_CLIENT	T.UNSEC_DATA	T.TOE_FAIL	A.ADMIN	A.DEDICATED	A.PHYSICAL
O.AUDIT_GEN	☑				☑								
O.AUDIT_REVIEW					☑								
O.AUDIT_STOR					☑								
O.AUDIT_PROTECT				☑	☑		☑						
O.MANAGE		☑											
O.CLIENT_TEST								☑					
O.SELF_PROT				☑			☑						
O.TIME_STAMPS	☑				☑								
O.RESIDUAL						☑							
O.ROBUST_TOE			☑										
O.SECURE_DATA									☑				
O.SAFE_FAIL										☑			
OE.NO_BYPASS							☑						
OE.AUTH_SUPPORT			☑										
OE.ADMIN											☑		
OE.DEDICATED												☑	
OE.PHYSEC													☑

Table 4: Threats & IT Security Objectives Mappings

4.4 Rationale For Threat Coverage

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

T.SEC_FUNC	O.AUDIT_GEN mitigates this threat by providing audit record data for any changes to TSF related functions and/or security related events. O.TIME_STAMPS supports the audit function by assuring that reliable time stamps are provided by the TOE when they are needed for audit records generated and/or stored in the Environment.
T.FLAW_CONFIG	O.MANAGE ensures that the functions and facilities needed for secure configuration are provided by the TOE, and TSF is protected from unauthorized use.
T.MASK	O.ROBUST_TOE mitigates this threat by providing mechanisms that effectively control access to the TOE and deny access to specific Users when appropriate. OE.AUTH_SUPPORT mitigates this threat by providing authentication support for the TOE to authenticate users when requested by the TOE.
T.AUDIT_COMP	O.AUDIT_PROTECT mitigates this threat by restricting access to audit records to authorized personnel. O.SELF_PROT mitigates this threat by maintaining a domain within the FirePass Appliance for its own execution that protects its resources from external interference, tampering or unauthorized disclosures through its own interfaces.
T.UNID_ACTION	O.AUDIT_GEN mitigates this threat by creating audit record data for any changes to TSF related functions and/or security related events. O.AUDIT_REVIEW mitigates this threat by providing a means to review audit records thereby supporting the administrator's ability to detect potential security violations. O.AUDIT_STOR mitigates this threat by storing all audit record outputs from the TOE relating to security function related events within the TOE. O.AUDIT_PROTECT mitigates this threat by restricting access to audit records to authorized personnel. O.TIME_STAMPS supports the audit function by providing a reliable time stamp for audit records generated within the TOE.
T.TSF_COMP	O.SELF_PROT mitigates this threat by maintaining a domain for the FirePass Appliance's execution that protects its resources from external

interference, tampering or unauthorized disclosures through its own interfaces.

O.AUDIT_PROTECT further mitigates this threat by restricting access to audit records to authorized personnel.

OE_NO_BYPASS further mitigates this threat by assuring that TOE security mechanisms cannot be bypassed through the IT Environment.

T.UNSEC_CLIENT O.CLIENT_TEST mitigates this threat by providing functionality to test the Client IT Environment to assure that the Client Environment is operating in a secure fashion prior to and during a secure session.

T.UNSEC_DATA O.SECURE_DATA mitigates this threat by implementation of the FirePass Network Access Mode SFP/FirePass Web Applications Mode SFP to ensure secure and unmodified data transfer of TOE Client software to TOE Clients and secure and unmodified data transfer between the FirePass appliance and applicable authentication servers.

T.RESIDUAL O.RESIDUAL mitigates this threat by providing mechanisms that the Client TSF utilizes to perform cleanup activities following a Network Access Mode session to prevent disclosure of session related information.

T.TOE_FAIL O.SAFE_FAIL mitigates this threat by preserving correct TSF operations and/or protecting the TSF in the event of a failure of a single appliance in a redundant pair configuration.

4.5 Rationale For Organizational Policy Coverage

There are no Organizational Policies for this TOE.

4.6 Rationale For Assumption Coverage

This section provides a justification for how security objectives cover each assumption.

A.ADMIN This assumption is restated in the form of OE.ADMIN, which specifies that the Administrators are appropriately trained, not careless, not willfully negligent, non hostile and follow and abide by the instructions provided in the guidance documentation.

A.DEDICATED This assumption is restated in the form of OE.DEDICATED, assuring that the FirePass Appliance is dedicated to its primary function.

A.PHYSICAL This assumption is restated in the form of OE.PHYSEC, which states that the TOE is physically secure and physical access is controlled to assure only authorized Administrators have access.

5 IT Security Requirements

The security requirements that are levied on the TOE and the IT environment are specified in this section of the ST. These security requirements are defined in Sections 5.1 - 5.8.

TOE Security Functional Requirements (from CC Part 2)	
FAU_GEN.2	User Identity association
FAU_SAR.1	Audit review
FAU_SAR.3a	Selectable Audit Review – HTTP Logs
FAU_SAR.3b	Selectable Audit Review – System Logs
FAU_STG.1	Protected audit trail storage
FCS_CKM.1a	Cryptographic key generation – symmetric keys
FCS_CKM.1b	Cryptographic key generation-asymmetric keys
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1	Cryptographic operation
FDP_IFC.1a	Subset information flow control-***Network Access Mode***
FDP_IFC.1b	Subset information flow control-***Web Applications Mode***
FDP_IFF.1a	Simple security attributes-- ***Network Access Mode***
FDP_IFF.1b	Simple security attributes-***Web Applications Mode***
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User Attribute Definition
FIA_UID.1	Timing of identification-***External VPN users***
FIA_UAU.2	User authentication before any action– ***Internal appliance users***
FIA_UID.2	User identification before any action– ***Internal appliance users***
FIA_SOS.1	Verification of Secrets
FMT_MOF.1	Management of security functions behavior
FMT_MSA.1a	Management of security attributes- ***Network Access Mode***
FMT_MSA.1b	Management of security attributes-***Web Applications Mode***
FMT_MSA.2	Secure security attributes
FMT_MSA.3a	Static Attribute Initialisation- ***Network Access Mode***

FMT_MSA.3b	Static Attribute Initialisation-***Web Applications Mode***
FMT_MTD.1a	Management of TSF data – *Query, Modify*
FMT_MTD.1b	Management of TSF data- *Query, Delete*
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security Roles
FPT_FLS.1	Failure with preservation of secure state
FPT_RVM.1a	Non-bypassability of the TSP
FPT_SEP.1a	TSF Domain Separation-*FirePass Appliance*
FPT_STM.1	Reliable Time Stamps
FRU_FLT.2	Limited fault tolerance
FTA_SSL.3	TSF-initiated termination
TOE Explicitly Stated Security Functional Requirements	
FAU_GEN_EXP.1	Audit data generation
FAU_STG_EXP.1	Use of remote log server
FDP_NAM_EXP.1	Level 3 VPN Sessions – Network Access mode
FDP_WAM_EXP.1	Level 7 VPN Session – Web Applications mode
FIA_UAU_EXP.2	User authentication via External Authentication Server – *External VPN users*
FPT_SEP_EXP.1	*Partial* TSF domain separation-*Client*
FPT_TST_EXP.1	Client IT Environment testing and cleanup

Table 5: Functional Requirements

5.1 TOE Security Functional Requirements

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

5.1.1 Class FAU: Security audit

FAU_GEN.2 User identity association

FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide **Realm_admin (administrator) and Admin (full access)** with the capability to read **all audit information** from the audit records.

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

FAU_SAR.3a Selectable audit review – HTTPS Logs

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

a) Class
b) IP address
c) ID
d) Text

FAU_SAR.3b Selectable audit review – System Logs

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

a) Period (month)
b) Source

FAU_STG.1 **Protected audit trail storage**

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

FAU_STG.1.2 The TSF shall be able to <u>prevent</u> unauthorized modifications to the audit records in the audit trail.

5.1.2 Class FCS: Cryptographic key management

FCS_CKM.1a **Cryptographic key generation – symmetric keys**

FCS_CKM.1.1a The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **a software random number generator (RNG)** and specified cryptographic key sizes **168 bits (3DES) or 256 bits (AES)** that meet the following: **FIPS 140-1/2 approved Diffie-Hellman key exchange.**

FCS_CKM.1b Cryptographic key generation-asymmetric keys

FCS_CKM.1.1b The TSF shall generate *asymmetric* cryptographic keys in accordance with a specified cryptographic key generation algorithm **RSA, Diffie-Hellman** and specified cryptographic key sizes **1024, 2048** that meet the following: **ANSI X9.31 (RSA), RFC 2631 (DH)**.

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **Block Level Overwrite of all plaintext cryptographic keys and other critical security parameters within the device** that meets the following**: none.**

FCS_COP.1 Cryptographic operation

FCS_COP.1.1 The TSF shall perform **Session Data Encryption/Decryption** in accordance with a specified cryptographic algorithm **TDEA (Triple Data Encryption Algorithm) or AES** and cryptographic key sizes **168 bits (3DES) or 256 bits (AES) - 1024, 2048 bit (RSA)** that **meet the following: FIPS 46-3, PKCS #10 (RSA).**

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

5.1.3 Class FDP: User data protection

FDP_IFC.1a Subset information flow control-*Network Access Mode*

FDP_IFC.1.1a The TSF shall enforce the **FirePass Network Access Mode information flow control SFP** on

a. **Subject: All IT entities that send/receive information through the TOE to assigned Network Access Mode Resources**
b. **Information: Traffic sent through the TOE from one subject to another**
c. **Operation: Pass Traffic**

FDP_IFC.1b **Subset information flow control-*Web Applications Mode***

FDP_IFC.1.1b The TSF shall enforce the **FirePass Web Applications Mode information flow control SFP** on

a. **Subject: All IT entities that send/receive information through the TOE to assigned Web Application Mode Resources**

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

c. **Operation: Pass Traffic**

FDP_IFF.1a **Simple security attributes-*Network Access Mode***

FDP_IFF.1.1a The TSF shall enforce the **FirePass Network Access Mode information flow control SFP** based on the following types of subject and information security attributes:

a. **Subject Security Attributes: FirePass Network Access Mode policy settings for evaluated security score based on pre-session endpoint testing, Configured Packet Filter Rules**

b. **Information Security Attributes: Presumed IP address of source subject, Presumed IP address of destination subject, User ID/Group Assignment**

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

a. **the subject is explicitly allowed to send information, if based on the Network Access Mode policy settings:**
   1. **The evaluated security based on pre-session endpoint testing score meets the minimum requirements for access to the information source**
   2. **The information flow is permitted based on Administrative User Configured Packet Filter Rules**

3. **The source address is explicitly allowed to send information**
4. **The User is explicitly allowed to initiate session activities based on User ID/Group Assignment**
5. **The information flow is permitted based on Administrative User Configured Access Scopes which are enforced by Master Group membership.**

b. the subject is explicitly allowed to receive information, if based on the Network Access Mode policy settings:

1. **The evaluated security based on pre-session endpoint testing score meets the minimum requirements for access to the information source**
2. **The information flow is permitted based on Administrative User Configured Packet Filter Rules**
3. **The source address is explicitly allowed to receive information**
4. **The User is explicitly allowed to initiate session activities based on User ID/Group Assignment**
5. **The information flow is permitted based on Administrative User Configured Access Scopes which are enforced by Master Group membership.**

FDP_IFF.1.3a The TSF shall enforce the **FirePass Network Access Mode information flow control SFP to assure that only valid PPP protocol sessions are routed to Network Access Mode resources.**

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

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

FDP_IFF.1.6a The TSF shall explicitly deny an information flow based on the following rules: **no other rules**

FDP_IFF.1b **Simple security attributes-*Web Applications Mode***

FDP_IFF.1.1b The TSF shall enforce the **FirePass Web Applications Mode information flow control SFP** based on the following types of subject and information security attributes:

a. Subject Security Attributes: FirePass Web Applications Mode policy settings for evaluated security score based on pre-session endpoint testing, Master Group Assignment

b. **Information Security Attributes: Presumed IP address of source subject, Presumed IP address of destination subject, User ID/Group Assignment**

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

a. **the subject is explicitly allowed to send information, if based on the Web Applications Mode policy settings:**

1. **The evaluated security based on pre-session endpoint testing score meets the minimum requirements for access to the information source**
2. **The information flow is permitted based on Administrative User Configured Access Scopes which are enforced by Master Group membership.**
3. **The source address is explicitly allowed to send information**
4. **The User is explicitly allowed to initiate session activities based on User ID/Group Assignment.**

b. **the subject is explicitly allowed to receive information, if based on the Web Applications Mode policy settings:**

1. **The evaluated security based on pre-session endpoint testing score meets the minimum requirements for access to the information source**

2. **The information flow is permitted based on Administrative User Configured Access Scopes which are enforced by Master Group membership.**

3. **The source address is explicitly allowed to receive information**
4. **The User is explicitly allowed to initiate session activities based on User ID/Group Assignment.**

FDP_IFF.1.3b The TSF shall enforce the **FirePass Web Applications Mode information flow control SFP to enforce that only valid HTTPs protocol traffic attempts are allowed to connect to a Web Applications Mode resources.**

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

FDP_IFF.1.5b The TSF shall explicitly authorize an information flow based on the following rules: **no other rules**.

FDP_IFF.1.6b The TSF shall explicitly deny an information flow based on the following rules: **no other rules**.

5.1.4 Class FIA: Identification and authentication

FIA_AFL.1 **Authentication failure handling**

FIA_AFL.1.1 The TSF shall detect when an administrator configured value of consecutive unsuccessful authentication attempts occur ***within an administrator configured time period in minutes*** related to **FirePass session initiation.**

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall **generate an "HTTP log" record and deactivate the subject account.**

FIA_ATD.1 **User attribute definition**

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: **User Identifier, Group Memberships, Authentication Data, Assigned Roles.**

FIA_SOS.1 **Verification of secrets – Passwords**

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet **Administrative User configured Password Management settings – Minimum of 8 characters. Must start with an alphabetical character; contain at least one numeric and one special character (neither the numeric nor the special character should be in the last character position of the password).**

FIA_UID.1 Timing of identification-***External VPN users***

FIA_UID.1.1 The TSF shall allow **initiation of the log-in process, and access to the online knowledge base** on behalf of the user to be performed before the user is identified.

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

FIA_UAU.2 **User authentication before any action – *Internal appliance users***

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

FIA_UID.2 **User identification before any action – *Internal appliance users***

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

5.1.5 Class FMT: Security management

FMT_MOF.1 **Management of security functions behaviour**

FMT_MOF.1.1 The TSF shall restrict the ability to modify the behaviour of, disable, or enable the functions

a. **Auditing**
b. **Failover**
c. **Server Certificate Management**
d. **Remote Interface Configuration (GUI)**
e. **Restart Services**
f. **Restart Controller**
g. **Shutdown Controller**
h. **Authentication Failure Handling**
i. **Password policy enforcement**

to the **Realm_admin (administrator) and Admin (full access)*.**

***realm_admin can only access assigned realms**

FMT_MSA.1a **Management of security attributes-*Network Access Mode***

FMT_MSA.1.1a The TSF shall enforce the **FirePass Network Access Mode information flow control SFP** to restrict the ability to query, modify, delete the security attributes **Information Flow Rules contained in FDP_IFF.1a** to **Realm_admin (administrator) and Admin (full access).**

FMT_MSA.1b **Management of security attributes-*Web Applications Mode***

FMT_MSA.1.1b The TSF shall enforce the **FirePass Web Applications information flow control SFP** to restrict the ability to query, modify, delete the security attributes **Information Flow Rules contained in FDP_IFF.1b** to the **Realm_admin (administrator) and Admin (full access).**

FMT_MSA.2 **Secure security attributes**

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

FMT_MSA.3a **Static attribute initialisation-*Network Access Mode***

FMT_MSA.3.1a The TSF shall enforce the **FirePass Network Access Mode information flow control SFP** to provide restrictive default values for security attributes used to enforce the SFP.

FMT_MSA.3.2a The TSF shall allow the **Realm_admin (administrator) and Admin (full access)** to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3b **Static attribute initialisation-*Web Applications Mode***

FMT_MSA.3.1b The TSF shall enforce the **FirePass Web Applications information flow control SFP** to provide restrictive default values for security attributes used to enforce the SFP.

FMT_MSA.3.2b The TSF shall allow the **Realm_admin (administrator) and Admin (full access)** to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1a **Management of TSF data –*Query, Modify***

FMT_MTD.1.1a The TSF shall restrict the ability to query, modify, the

a) Failover settings
b) Administrator authentication data
c) Master group settings
d) Resource group settings
e) Remote Interface Settings (GUI)

to the **Realm_admin (administrator) and Admin (full access)**.

***realm_admin can only access assigned realms**

FMT_MTD.1b **Management of TSF data – *Query, Delete***

FMT_MTD.1.1b The TSF shall restrict the ability to query , delete the

a) Appliance audit logs
b) Server Certificate properties

to the**, Realm_admin (administrator) and Admin (full access)**.

FMT_SMF.1 **Specification of Management Functions**

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

a) Restart Services, Restart FirePass Appliance and Shutdown FirePass appliance

b) Create, Modify, Delete user accounts

c) Create and configure master groups (users)

d) Create and configure resource groups (IT entities)

e) Update and manage Server Certificates

f) Review appliance audit logs

g) Enable auditing

h) Modify logging levels

i) Enable/disable Failover

j) Manage information flow rules

k) Delete audit logs

FMT_SMR.1 **Security roles**

FMT_SMR.1.1 The TSF shall maintain the roles **External VPN user**, **realm_admin (administrator) and admin (full access)*.**

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

*note: the terms in parentheses refer to the realm used. The TOE manages roles as realms

5.1.6 Class FPT: Protection of the TSF

FPT_FLS.1 Failure with preservation of secure state

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

a. **Power Supply Failure of the active appliance**
b. **Hard Drive Failure of the active appliance**
c. **Memory based Failure of the active appliance**
d. **Software failure of the active appliance**
e. **Processor failure of the active appliance**
f. **>200mSec delay between heartbeats (sync signal)**

FPT_RVM.1a Non-bypassability of the TSP

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

FPT_SEP.1a TSF domain separation-

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

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

FPT_STM.1 Reliable time stamps

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

5.1.7 Class FRU: Resource Utilisation

FRU_FLT.2 Limited fault tolerance

FRU_FLT.2.1 The TSF shall ensure the operation of **all the TOE's capabilities** when the following failures occur:

a. **Power Supply Failure of the active appliance**
b. **Hard Drive Failure of the active appliance**

c. **Memory based Failure of the active appliance**
d. **Software failure of the active appliance**
e. **Processor failure of the active appliance**
f. **>200mSec delay between heartbeats (sync signal)**

5.1.8 Class FTA - TOE Access

FTA_SSL.3 TSF-initiated termination

FTA_SSL.3.1 The TSF shall terminate an interactive session after **an Admin (full access) configurable time interval of session inactivity**.

5.2 Explicitly Stated TOE Security Functional Requirements

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

5.2.1 Class FAU: Security Audit (Explicitly Stated)

FAU_GEN_EXP.1.1 The TSF shall be able to generate an audit record of the following auditable events:
~~**a) Start-up and shutdown of the audit functions;**~~
b) All auditable events for the not specified level of audit; and
c) **Additional Events: Events listed in Table 6.**

FAU_GEN_EXP.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST**.**

Audited Event	**Audit Data**
App logs: Time	**start/stop time of session**
App logs: Source IP	**Origin of session IP**
App logs: Logon	**Username of logged on user**
App logs: Session ID	**Unique ID of session**
App logs: Record	**Each single action taken recorded results in single record Includes administrative user action (query, modify, delete) such as:**

	Security Management Functions listed in FMT_SMF.1, **TSF data access as listed in FMT_MTD.1a,b** **Security attributes access, modification as listed in FMT_MSA.1a, b.** **Includes External VPN user actions such as:** **Access attempts to backend servers, actions taken during access and success/failure of attempted operations.**
App logs: User agent string	**Browser ID string**
App logs: Message	**Type of activity**
Logons: Logon	**Name of User that originated session**
Logons: valid user?	**Yes or No (recognized as valid user)**
Logons: passed?	**Yes or No (logon success/failure)**
Logons: name	**First and last name of user if avail.**
Logons: time	**Start date and time of logon**
Logons: user agent	**Returns the browser type and ID**
Logons: From	**IP address when logon originated**
Session log: User	**Session Username**
Session log: start time	**Session start time**
Session log: end time	**Session end time**
Session log: duration	**Session time duration**
Session log: From	**IP address when session originated**
Session log: To	**Type of connection requested**
Session log: Status	**Current session status –“server session in progress”, “logged out from server”**
HTTP log : Date	**Date of HTTP related event**
HTTP log : Class	**Classification of event (where applicable)**
HTTP log : IP	**IP address relating to HTTP event**
HTTP log : ID	**Identification number indicating event type**
HTTP log : Text	**Text description of event**
System log : Date	**Date of system event**
System log : Time	**Time of system event**
System log : Source	**Source of event**
System log : Message	**Text description of event**

Table 6: Audit Events

FAU_STG_EXP.1 **Use of a remote log server**

FAU_STG_EXP.1.1 The TSF shall provide the ability to use a remote log server for the storage of system audit log records generated by the TSF.

5.2.2 Class FDP: User Data Protection (Explicitly Stated)

FDP_NAM_EXP.1	Level 3 VPN Sessions – Network Access mode
FDP_NAM_EXP.1.1	The TSF shall provide the ability to establish secure Level 3 VPN sessions between external VPN Users and administrator configured network resources utilizing PPP over SSL techniques.
FDP_WAM_EXP.1	Level 7 VPN Session – Web Applications mode
FDP_WAM_EXP.1.1	The TSF shall provide the ability to establish secure Level 7 VPN sessions between external VPN Users and administrator configured network resources and render requested content to external VPN users in HTML utilizing HTTPS techniques.

5.2.3 Class FIA: Identification and authentication (Explicitly Stated)

FIA_UAU_EXP.2 User authentication via External Authentication Server – *External VPN users*

FIA_UAU_EXP.2.1 The TSF of the FirePass Appliance will deny an external user access to the TSF until the FirePass Appliance has requested and obtained the username and password and had the credentials validated by the IT Environment.

5.2.4 Class FPT: Protection of the TSF (Explicitly Stated)

FPT_SEP_EXP.1 *Partial* TSF domain separation-*Client*

FPT_SEP_EXP.1.1 The ***FirePass Client*** TSF shall maintain a security domain that protects it from interference and tampering by untrusted subjects initiating actions through its own TSFI.

FPT_SEP_EXP.1.2 The ***FirePass Client*** TSF shall enforce separation between the security domains of subjects in the TSC.

FPT_TST_EXP.1 Client IT Environment testing and cleanup

FPT_TST_EXP.1.1 The TSF shall run a suite of self tests at the condition_Session Startup, Session Intervals, as configured, to demonstrate the correct operation and secure configuration of the Client IT Environment.

FPT_TST_EXP.1.2 The TSF shall run a suite of operations at the condition Post-Session, as configured**,** to eliminate residual information within the IT Environment.

5.3 IT Environment Security Functional Requirements

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

IT Environment Security Functional Requirements	
FPT_RVM.1b	Non-bypassability of the TSP-***Client***
FPT_SEP.1b	TSF domain separation-***Client***
IT Environment Explicitly Stated Security Functional Requirements	
FIA_AUT_EXP.2	User authentication verification via External Authentication Server **–** ***External VPN users***

5.3.1 Class FPT: Protection of the TSF

FPT_RVM.1b Non-bypassability of the TSP - ***Client***

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

FPT_SEP.1b TSF domain separation - ***Client***

FPT_SEP.1.1b The ~~***TSF***~~ ***IT Environment*** shall maintain a security domain for the ~~***TOE's***~~ ***its own*** execution that protects ~~***the TOE***~~ ***it*** from interference and tampering by untrusted subjects.

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

5.4 Explicitly Stated IT Environment Security Functional Requirements

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

5.4.1 Class FIA: Identification and authentication

FIA_AUT_EXP.2 User authentication verification via External Authentication Server – *External VPN users*

FIA_AUT_EXP.2.1 The IT Environment shall perform authentication verification for the TOE and send the authentication result to the FirePass appliance.

5.5 TOE Strength of Function Claim

The only probabilistic or permutational mechanisms in the product are the password mechanism used to authenticate users and the cryptographic mechanisms. Strength of cryptographic algorithms is outside the scope of the Common Criteria.

The claimed minimum strength of function is SOF-basic. FIA_UAU.2, FIA_UAU_EXP.2 are the only non-cryptographic TOE security functional requirements that contain a permutational or probabilistic function.

5.6 TOE Security Assurance Requirements

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

Assurance Class	Assurance Components	
ACM: Configuration management	ACM_CAP.2	Configuration items
ADO: Delivery and operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation, and start-up procedures

Assurance Class	Assurance Components	
ADV: Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.1	Descriptive high-level design
	ADV_RCR.1	Informal correspondence demonstration
	ADV_SPM.1	Informal TOE security policy model
AGD: Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
ATE: Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
AVA: Vulnerability assessment	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis
ALC: Life Cycle Support	ALC_FLR.1	Basic Flaw Remediation

Table 7: Assurance Requirements: EAL2 Augmented ALC_FLR.1, ADV_SPM.1

5.6.1 ACM_CAP.2 Configuration items

Developer action elements:

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

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

ACM_CAP.2.3D The developer shall provide CM documentation.

Content and presentation of evidence elements:

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

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

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

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

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

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

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

Evaluator action elements:

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

5.6.2 ADO_DEL.1 Delivery procedures

Developer action elements:

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

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

Content and presentation of evidence elements:

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

Evaluator action elements:

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

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

Developer action elements:

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

Content and presentation of evidence elements:

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

Evaluator action elements:

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

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

5.6.4 ADV_FSP.1 Informal functional specification

Developer action elements:

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

Content and presentation of evidence elements:

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

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

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

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

Evaluator action elements:

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

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

5.6.5 ADV_HLD.1 Descriptive high-level design

Developer action elements:

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

Content and presentation of evidence elements:

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

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

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

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

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

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

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

Evaluator action elements:

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

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

5.6.6 ADV_RCR.1 Informal correspondence demonstration

Developer action elements:

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

Content and presentation of evidence elements:

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

Evaluator action elements:

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

5.6.7 ADV_SPM.1 Informal TOE security policy model

Developer action elements:

ADV_SPM.1.1D The developer shall provide a TSP model.

ADV_SPM.1.2D The developer shall demonstrate correspondence between the functional specification and the TSP model.

Content and presentation of evidence elements:

ADV_SPM.1.1C The TSP model shall be informal.

ADV_SPM.1.2C The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled.

ADV_SPM.1.3C The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled.

ADV_SPM.1.4C The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model.

Evaluator action elements:

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

5.6.8 AGD_ADM.1 Administrator guidance

Developer action elements:

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

Content and presentation of evidence elements:

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

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

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

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

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

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

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

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

Evaluator action elements:

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

5.6.9 AGD_USR.1 User guidance

Developer action elements:

AGD_USR.1.1D The developer shall provide user guidance.

Content and presentation of evidence elements:

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

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

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

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

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

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

Evaluator action elements:

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

5.6.10 ATE_COV.1 Evidence of coverage

Developer action elements:

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

Content and presentation of evidence elements:

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

Evaluator action elements:

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

5.6.11 ATE_FUN.1 Functional testing

Developer action elements:

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

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation of evidence elements:

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

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

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

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

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

Evaluator action elements:

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

5.6.12 ATE_IND.2 Independent testing - sample

Developer action elements:

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

Content and presentation of evidence elements:

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

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

Evaluator action elements:

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

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

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

5.6.13 AVA_SOF.1 Strength of TOE security function evaluation

Developer action elements:

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

Content and presentation of evidence elements:

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

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

Evaluator action elements:

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

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

5.6.14 AVA_VLA.1 Developer vulnerability analysis

Developer action elements:

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

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

Content and presentation of evidence elements:

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

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

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

Evaluator action elements:

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

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

5.6.15 ALC_FLR.1 Basic flaw remediation

Developer action elements

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

Content and presentation of evidence elements

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

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

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

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

Evaluator action elements

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

5.7 Rationale For TOE Security Requirements

5.7.1 TOE Security Functional Requirements

	O.AUDIT_GEN	O.AUDIT_PROTECT	O.AUDIT_REVIEW	O.AUDIT_STOR	O.MANAGE	O.CLIENT_TEST	O.RESIDUAL	O.SELF_PROT	O.TIME_STAMPS	O.ROBUST_TOE	O.SECURE_DATA	O.SAFE_FAIL
FAU_GEN_EXP.1	X											
FAU_GEN.2	X											
FAU_SAR.1			X									
FAU_SAR.3a			X									
FAU_SAR.3b			X									
FAU_STG.1		X		X								
FCS_CKM.1a											X	
FCS_CKM.1b											X	
FCS_CKM.4											X	
FCS_COP.1											X	
FDP_IFC.1a											X	
FDP_IFC.1b											X	
FDP_IFF.1a											X	
FDP_IFF.1b											X	
FIA_AFL.1										X		
FIA_ATD.1										X		
FIA_SOS.1										X		
FIA_UID.1										X		
FIA_UAU.2										X		

	O.AUDIT_GEN	O.AUDIT_PROTECT	O.AUDIT_REVIEW	O.AUDIT_STOR	O.MANAGE	O.CLIENT_TEST	O.RESIDUAL	O.SELF_PROT	O.TIME_STAMPS	O.ROBUST_TOE	O.SECURE_DATA	O.SAFE_FAIL
FIA_UID.2										X		
FMT_MOF.1					X							
FMT_MSA.1a					X							
FMT_MSA.1b					X							
FMT_MSA.2											X	
FMT_MSA.3a					X							
FMT_MSA.3b					X							
FMT_MTD.1a					X							
FMT_MTD.1b					X							
FMT_SMF.1					X							
FMT_SMR.1					X							
FPT_FLS.1												X
FPT_RVM.1a								X				
FPT_SEP.1a								X				
FPT_STM.1									X			
FRU_FLT.2												X
FTA_SSL.3								X				
FAU_STG_EXP.1		X										
FDP_NAM_EXP.1											X	
FDP_WAM_EXP.1											X	
FIA_AUT_EXP.2										X		
FIA_UAU_EXP.2										X		
FPT_SEP_EXP.1								X				
FPT_TST_EXP.1						X	X					

Table 8: SFR and Security Objectives Mapping

Security Objective	Mapping Rationale
O.AUDIT_GEN	FAU_GEN_EXP.1 specifies that the TOE generates audit records of security relevant events and information as detailed in Table 6 FAU_GEN.2 is selected to ensure that the audit records associate a user identity with the event audited.
O.AUDIT_PROTECT	FAU_STG.1 ensures that the TOE provides for the storage of audit data in a manner that protects the data from unauthorized deletion and prevents unauthorized modification of TOE audit records. FAU_STG_EXP.1 specifies that the TSF has the capability to offload audit records to an external FTP server.
O.AUDIT_REVIEW	FAU_SAR.1 specifies that Administrators are explicitly given the capability to read all audit information from the audit records, and the records are provided in a suitable manner for interpretation. FAU_SAR.3a specifies that HTTPS logs may be sorted by Class, IP, ID, Text. FAU_SAR.3b specifies that System logs may be sorted by Period (month) and Source.
O.AUDIT_STOR	FAU_STG.1 ensures that the TOE provides for the storage of audit data in a manner that protects the data from unauthorized deletion and prevents unauthorized modification of TOE audit records.
O.MANAGE	FMT_MOF.1 provides that the TOE's management function can only be accessed and utilized by authorized personnel. FMT_MTD.1a, FMT_MTD.1b specifies the TSF data that can be queried, modified or deleted by use of the TOE's management functions. FMT_SMR.1 defines the roles provided by the TOE. FMT_SMF.1 specifies the management functions supported by the TOE. FMT_MSA.1a specifies that the TOE enforces the FirePass Network Access Mode information flow control SFP to restrict the ability to query, modify, or delete the applicable security attributes to the Admin (full access). FMT_MSA.1b specifies that the TOE enforces the FirePass Web Applications information flow control SFP to restrict the ability to query, modify, or delete the applicable security attributes to the Admin (full access). FMT_MSA.3a specifies that the TOE enforces the FirePass Network Access Mode information flow control SFP to provide restrictive default values for security attributes that are used to enforce the SFP and that the Administrator can specify alternative default values. FMT_MSA.3b specifies that the TOE enforces the FirePass Web Applications Mode information flow control SFP to provide restrictive default values for security attributes that

	are used to enforce the SFP and that the Administrator can specify alternative default values.
O.CLIENT_TEST	FPT_TST_EXP.1 specifies testing of Client IT Environment security status during session initiation and periodically during the session to assure the security of the Client Environment.
O.SELF_PROT	FPT_SEP.1a specifies that the TOE will provide a secure domain for its execution and will enforce separation between subjects in the TSC. FPT_SEP_EXP.1 specifies that the IT Environment supporting the TOE will provide a secure domain for it's execution which further ensures that the TOE is protected from unauthorized users. FPT_RVM.1a specifies that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed. FTA_SSL.3 specifies that the TOE will terminate an interactive session with the TOE after an Admin (full access) configured time interval of inactivity.
O.RESIDUAL	FPT_TST_EXP.1 specifies the cleanup of session related data following the completion of a Network Access Mode session to assure data is not disclosed.
O.TIME_STAMPS	FPT_STM.1 specifies that the TOE provides reliable time stamps for use in audit records.
O.ROBUST_TOE	FIA_UID.1 specifies that may initiate the log-in process and access the online knowledge base prior to being identified by the TOE but all other access requires identification prior to accessing the TSF. FIA_UAU.2 specifies that the TOE requires authentication before allowing access to TSF resources for internal appliance users (admins). FIA_UID.2 specifies that the TOE requires identification before allowing access to TSF resource for internal appliance users (admins) FIA_ATD.1 specifies that the TOE will maintain security attributes belonging to individual users to include: User Identifier, Group Memberships, Authentication Data, and Assigned Roles. FIA_SOS.1 specifies that the TOE will enforce a password policy which requires at least 8 characters and the details contained in FIA_SOS.1. FIA_AFL.1 specifies that the TOE will detect when a Admin (full access) specified number of failed logon attempts within a Admin (full access) specified period of time occurs and will generate an HTTP log record of the event and deactivate the subject account (when so configured) FIA_AUT_EXP.2 specifies that the IT Environment shall perform authentication verification for the TOE and send the authentication result to the FirePass appliance. FIA_UAU_EXP.2 specifies that the TOE will deny an external user access to the TSF until the FirePass Appliance has requested and obtained the username and password and have the credentials validated by the IT Environment.

O.SECURE_DATA	FCS_CKM.1a, FCS_CKM.1b, FCS_CKM.4, FCS_COP.1, FMT_MSA.2 FCS_CKM.1a, FCS_CKM.1b requires that key generation utilize RNG based key generation with key sizes of 128 bit (AES), 160 bit (3DES), (RSA) 1024bits that meets the requirements of FIPS 140. FCS_CKM.4 specifies that key destruction is completing by a block level overwrite of configuration data. FCS_COP.1 establishes that strong cryptography, utilizing 3DES or AES will be used for session encryption for all Network Access Mode or Web Applications mode sessions. FMT_MSA.2 specifies that the TSF accepts only secure values for security attributes which support aspects such as the use of cryptography for protection of data transfer during FirePass sessions. FDP_IFC.1a and FDP_IFC.1b specifies the Subject and Objects controlled by the FirePass Network Access Mode SFP and FirePass Web Application Mode SFP and FDP_IFF.1a and FDP_IFF.1b specifies the rules that are invoked by the SFPs established in FDP_IFC.1a & FDP_IFC.1b FDP_NAM_EXP.1 specifies that the TSF provides the capability to establish secure level 3 connections to specified network resources using PPP over SSL techniques. FDP_WAM_EXP.1 specifies that the TSF provides the capability to establish secure level 7 connections to specified network resources and render content to external VPN users in HTML using HTTPS.
O.SAFE_FAIL	FPT_FLS.1 specifies that the TOE protects the TSF during the following failures: Power Supply Failure, Hard Drive Failure, Memory based Failure, Software failure, Processor failure of the active appliance, or no heartbeat response within <200mSec. FRU_FLT.2 specifies that the TOE meets all SFR requirements in the event of the following failures: Power Supply Failure, Hard Drive Failure, Memory based Failure, Software failure, Processor failure of the active appliance, or no heartbeat response within <200mSec when installed in a redundant pair configuration.

5.8 Rationale For IT Environment Security Requirements

	OE.AUTH_SUPPORT	OE.NO_BYPASS
FPT_RVM.1b		☑
FPT_SEP.1b		☑
FIA_AUT_EXP.2	☑	

Table 9: SFR and Security Objectives Mapping

Environment Security Objective	Mapping Rationale
OE.AUTH_SUPPORT	FIA_AUT_EXP.2 ensures that the IT Environment provides authentication of passwords for external VPN users when requested by the TOE.
OE.NO_BYPASS	FPT_RVM.1b Non-bypassability of the IT Environment Security Policy ensures that TSP enforcement functions are invoked and succeed before TSF access is allowed. FPT_SEP.1b specifies that the IT Environment will provide a secure domain for the TOE client's execution and will enforce separation between subjects in the TSC.

5.9 Rationale for Explicitly Stated Security Requirements

The follow paragraphs details the rationale for the inclusion of the explicit requirements found in this Security Target.

Explicit Requirement	Identifier	Rationale
FAU_GEN_EXP.1	Logging of Audit Function activation/inactivation	This requirement is explicitly stated because the TOE does not allow audit function de-activation. Audit functions run by default and may not be deactivated. (Logging levels can be modified by the Admin (full access), however, the audit function cannot be disabled.
FAU_STG_EXP.1	Use of a remote log server	This component defines the TSF function of offloading audit records to a FTP server in the IT Environment. This explicit is required since this is done during operation and not only when the audit queue is filled as possible as available in FAU_STG.4.
FIA_UAU_EXP.2	User authentication via External Authentication Server – External VPN users	This explicit SFR was required to specify that External VPN Users must be authenticated via an External Authentication Server prior to gaining access to TSF protected resources.
FPT_SEP_EXP.1	Partial TSF domain separation-Client	This explicit was required as FPT_SEP.1 does not allow the revisions necessary to specify that the TOE Client software requires the IT Environment of the Client machine to provision essential domain separation through the operating system to assist in TOE Protection.
FPT_TST_EXP.1	Client IT Environment testing and cleanup	This explicit SFR was required to specify a version of TOE self testing that did not fit adequately within the constraints of FPT_TST.1. The TOE tests the IT Environment of the client for security risks prior to connecting and then provides a clean up process after the session is complete.
FIA_AUT_EXP.2	User authentication verification via External Authentication Server – External VPN users	This explicit SFR was required to specify the IT Environment requirement for authentication verification by an external authentication server when requested by the TOE appliance. Since External VPN users must be authenticated via the external authentication server the TOE and external authentication server must coordinate this process. Existing Part 2 SFRs were unsuitable for this purpose.

Table 10: Explicitly Stated SFR Rationale

5.9.1 TOE Security Assurance Requirements

EAL2 (Augmented ALC_FLR.1, ADV_SPM.1) was chosen to provide a low to moderate level of independently assured security. The chosen assurance level is consistent with the threat environment. Specifically, the threat of malicious attacks is not greater than moderate and the product will have undergone a search for obvious flaws. ALC_FLR.1 was selected to provide extra assurance relating to Flaw Remediation practices employed by F5 Networks for the

FirePass product. These processes support timely corrective actions and customer support in the event a security flaw is detected following product release. ADV_SPM.1 was selected to demonstrate the Security Policy Model enforced by the product through design was included as a required dependency for SFRs FMT_MSA.2 and FPT_FLT.1.

5.10 Rationale For IT Security Requirement Dependencies

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

Functional Component	Dependency	Included/Rationale
FAU_GEN_EXP.1	FPT_STM.1	Yes
FAU_GEN.2	FAU_GEN.1, FIA_UID.1	Yes via FAU_GEN_EXP.1
FAU_SAR.1	FAU_GEN.1	Yes via FAU_GEN_EXP.1
FAU_SAR.3a	FAU_GEN.1	Yes via FAU_GEN_EXP.1
FAU_SAR.3b	FAU_GEN.1	Yes via FAU_GEN_EXP.1
FAU_STG.1	FAU_GEN.1	Yes
FCS_CKM.1a	FCS_COP.1, FCS_CKM.4 FMT_MSA.2	Yes
FCS_CKM.1b	FCS_COP.1, FCS_CKM.4 FMT_MSA.2	Yes
FCS_CKM.4	FCS_CKM.1, FMT_MSA.2	Yes
FCS_COP.1	FCS_CKM.1, FCS_CKM.4 FMT_MSA.2	Yes
FDP_IFC.1a	FDP_IFF.1	Yes
FDP_IFC.1b	FDP_IFF.1	Yes
FDP_IFF.1a	FDP_IFC.1, FMT_MSA.3	Yes
FDP_IFF.1b	FDP_IFC.1, FMT_MSA.3	Yes
FIA_AFL.1	FIA_UID.1	Yes, FIA_UID.2
FIA_ATD.1	None	Yes
FIA_SOS.1	None	Yes
FIA_UAU.2	FIA_UID.1	Yes, FIA_UID.2
FIA_UID.2	None	Yes

Functional Component	Dependency	Included/Rationale
FMT_MOF.1	FMT_SMF.1, FMT_SMR.1	Yes
FMT_MSA.1a	FMT_SMR.1, FMT_SMF.1, FDP_IFC.1	Yes
FMT_MSA.1b	FMT_SMR.1, FMT_SMF.1, FDP_IFC.1	Yes
FMT_MSA.2	ADV_SPM.1, FDP_IFC.1 FMT_MSA.1, FMT_SMR.	Yes
FMT_MSA.3a	FMT_MSA.1, FMT_SMR.1	Yes
FMT_MSA.3b	FMT_MSA.1, FMT_SMR.1	Yes
FMT_MTD.1a	FMT_SMR.1, FMT_SMF.1	Yes
FMT_MTD.1b	FMT_SMR.1, FMT_SMF.1	Yes
FMT_SMF.1	None	Yes
FMT_SMR.1	FIA_UID.1	Yes
FPT_FLS.1	ADV_SPM.1	Yes, see Section 6.1.9 “Changes in State related to Failover process
FPT_RVM.1a	None	Yes
FPT_SEP_EXP.1	None	Yes
FPT_SEP.1a	None	Yes
FPT_STM.1	None	Yes
FRU_FLT.2	FPT_FLS.1	Yes
FTA_SSL.3	None	Yes
FAU_STG_EXP.1	FAU_GEN.1	Yes via FAU_GEN_EXP.1
FDP_NAM_EXP.1	FDP_IFC.1a, FDP_IFF.1a	Yes
FDP_WAM_EXP.1	FDP_IFC.1b, FDP_IFF.1b	Yes
FIA_UAU_EXP.2	FIA_UID.1	Yes
FPT_SEP_EXP.1	None	Yes
FPT_TST_EXP.1	None	Yes

Table 11: SFR Dependencies

***ADV_SPM.1 satisfied within Security Target, Section 6.1.9 “Changes in State related to Failover process”**

5.11 Rationale For Internal Consistency and Mutually Supportive

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

The selected requirements together form a mutually supportive whole by:

- satisfying dependencies as demonstrated in **Table 11: SFR** Dependencies
- tracing security functional requirements to security objectives and justifying that tracing as demonstrated in Section 5.7
- including the SFRs FPT_RVM.1a and FPT_SEP.1a to protect the TSF
- including audit requirements to detect security-related actions and potential attacks
- including security management requirements to ensure that the TOE is managed and configured securely

5.12 Rationale For Strength of Function Claim

The rationale for choosing SOF-basic is based on the low to moderate attack potential of the threats identified in this ST. The security objectives provide probabilistic security mechanisms, and the strength of function claim is satisfied by the password management features provided by the TOE.

6 TOE Summary Specification

6.1 TOE Security Functions

The TOE consists of 9 Security Functions:

- Security Audit
- Identification and Authentication
- Endpoint Security
- Network Access Mode
- Web Applications Mode Access
- Policy Based Resource Management
- Security Management
- Secure Communications
- TOE Protection

6.1.1 Security Audit

The TOE provides an audit capability that generates audit records and provides 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 parameters or applicable recorded aspects of session activity. The FirePass Appliance has a report function that allows for various reports to be created from the Audit records, allowing Administrative user access to specific information based on report configuration. The audit logging function is enabled by default and cannot be disabled by any user.

Audit Record Generation (FAU_GEN_EXP.1, FAU_GEN.2, FPT_STM.1)

The FirePass appliance generates detailed audit records for configuration settings such as appliance management, user/group management and association of backend server resources with FirePass to facilitate VPN sessions. All access attempts and actions taken by external VPN users using FirePass produce detailed logs which allow Administrative users to monitor access statistics and assure that a thorough audit trail is managed for all FirePass mediated activities. Administrative user sessions also produce an audit trail using these functions, detailing all aspects of the session, access attempts and changes made to FirePass appliance settings.

The audit generation function allows Administrative users to specify the amount of information to record in audit records and has the capability to record detailed session related activity through the appliance. Logging levels are configurable within the appliance that supports Administrative users efforts to tailor the depth and detail of audit logs generated by the appliance based on the deployment and potential threats.

FirePass logs are categorized into types of logs which allows the Administrative user to quickly access the type of information and detail required. Reports can also be generated through the GUI which results in a collection of logs based on specified criteria using pull-down menus. FirePass log categories include: Session logs (for detailed session based data), App logs for a detailed report based on user of activity during a FirePass session, HTTP logs which focus on server access attempts and error messages and System logs which provide an audit trail of appliance level events such as failure, boot cycles etc.

Session log include session details which allow the Administrative User to view reports which detail the types of sessions FirePass is supporting and access attempts during those sessions. These logs include connection type, FirePass Operational Access Mode type (Network Access Mode/Web Applications Mode), identity of client (including client machine parameters), and detailed session activities.

Logons (logs) specifically log logon attempts, success/failure and originating IP address.

App logs include detailed records by user of actions taken during FirePass sessions. This includes external VPN users accessing backend resources and administrative users accessing FirePass GUI pages and executing various administrative functions such as creating new FirePass users, management of authentication failure handling, password policy enforcement, and configuration of attributes which enforce FirePass SFPs.

The HTTP log category includes records relating to HTTP/HTTPS server access attempts and error notices and also includes the SSL engine log which reports SSL related events. Each entry in the HTTP Logs report contains data that describes the HTTP commands that the FirePass controller runs.

System Logs cover areas that are managed at the appliance level by the underlying Linux based operating system. This includes User session log messages, Application logs that tracks favorites (web servers configured for FirePass access), Pre-login check messages (response messages from clients during pre-login checks) and system level events such as system up monitors, system down monitors and reboot cycles. This category of logs may be pushed to a syslog server in the IT Environment; however, this option is not part of the Common Criteria evaluated configuration.

Audit records include a time stamp provided by a clock within the appliance to assure time based audit records of events as they occur during a session. Identified within the audit records are: date and time of the event, type of event, subject identification, and outcome of the event.

Audit records can only be accessed by the Admin (full access), or Realm_admin (administrator) roles through the Administrator Console.

Examples of audit event data by log category include:

App Logs:	Start/Stop time of session, origin IP address, username, Session ID, Action, Browser ID, Message
Logons:	Logon name, valid user yes/no, success/failure, user name, start date/time, browser ID, Origin IP address

Session log:	Username, start time, end time, duration, IP origin, connection type, current status
HTTP log:	Date of event, Class of event, related IP address, Event type ID, Text description of event
System log:	Date of event, Time of system event, Source of event, Text description of event

Audit logs are configured on the appliance to be kept for 1 hr., 6 hr., 12 hr., 1 day, 7 days or 30 days. Logs are kept for 7 days by default. Once this setting has been reached audit logs are deleted. When the archive checkbox is selected, these records are saved to an archive file prior to deletion. Audit logs are offloaded to an FTP Server in the IT Environment for archiving.

Audit records may be deleted through the Administrator GUI by the Admin (full access) user.

Audit Record Review - (FAU_SAR.1, FAU_SAR.3a,b)

Through the Administrator console, the Admin (full access) can review audit records using a Graphical User Interface (GUI) which allows Audit records stored on the FirePass appliance to be reviewed by user with an Administrator role. Reports of audit activity may be configured to identify various aspects of access and session activities. Administrator roles (Admin (full access), Realm_Admin (administrator) privileges are required to access and review audit records on the FirePass appliance. The HTTPS audit logs may be sorted by Class, IP address, ID, or Text columns. The System logs may be sorted by Period (month) or Source. The Application logs do not provide a sort function.

The Administrative GUI presents these records in a table format and the aforementioned sort categories are indicated by the column name being linked to the sort command. Upon clicking the column name, the records are sorted based on that category. For example, clicking on the IP column name in the HTTPS audit logs results in those records being sorted by IP address.

Audit Record Storage and Protection - (FAU_STG.1)

Explicit access is required to access and view audit records within the Administrator console. Only users with Administrator privileges (Administrator (Full Access), Realm_Admin) can access and view audit records.

Audit records are stored and protected within the TOE and may be exported manually or automatically as configured by the TOE Administrator. The TSF prohibits modification to the audit trail by design; no GUI object or command is available for editing. The FirePass appliance does not provide a facility for editing of audit records, as this is not allowed on the appliance.

Use of a remote log server – (FAU_STG_EXP.1)

The FirePass appliance has a provision for using a remote log server in the IT Environment for system logs. The administrator may configure the FTP server address and settings through the Administrative GUI and the TOE will forward log records to this server resource for storage external to the FirePass appliance at the interval set by the Admin (full access) user. This results in the archiving of these FirePass logs so when the scheduled purge occurs audit logs are not permanently lost. Once offloaded external to the FirePass appliance, these log records are no longer included for review using the GUI log report interface, during FirePass Admin workstation sessions.

6.1.2 Identification and Authentication

The primary Administrator of the appliance (Admin (full access) must be authenticated within the appliance to assure that the Administrator can always access the appliance. All other users may either authenticate internal to the appliance or use an external authentication server based on configuration. The CC Evaluated Configuration utilizes authentication within the appliance for FirePass Administrators (internal appliance users), and external VPN users are authenticated using an external authentication server (LDAP, RADIUS or Active Directory). The FirePass logon process enforces an Admin (full access) configurable delay following failed logon attempts to thwart brute force attacks on the logon interface. By default, this delay is set to 6 seconds.

Authentication Failure Handling during session logon (FIA_AFL.1)

The TOE has a provision for reporting repeated logon failures as a possible attack. The Admin (full access) configures how many consecutive failures are allowed within a configured period of time through the FirePass GUI. For Common Criteria, this value is stipulated to be 10 failed logins with 5 minutes. Upon reaching the specified maximum (10) login attempts in a configured period of time (5 minutes), the TSF generates an HTTP log record indicating a possible attack. In addition, the Admin (full access) may select an additional option to deactivate the User’s account upon exceeding the maximum number of logon attempts. This option is required to be selected for the Common Criteria Evaluated configuration. These settings apply to actual TOE login processes managed by the TOE appliance; external authentication servers used for External VPN users may enforce various policies based on methods used.

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

The FirePass Appliance maintains security attributes by user within the SQL database used in the identification and authentication process. The following attributes are maintained at a minimum to support the TSF:

- User Identifier,
- Group Memberships,
- Authentication Data,
- Assigned Roles

These attributes allow the TOE to determine assigned roles and group memberships to resource groups and access to TSF and TSF mediated resources.

Dynamic group mapping supports the authentication process. The group mapping table serves as a framework to ensure that the FirePass controller correctly authenticates external VPN users or local users authenticated externally, and that those users get access to the appropriate resources. A lookup to this table ensures that the authentication request is appropriately routed based on the appropriate authentication resource.

User Identification by FirePass (FIA_UID.1, FIA_UID.2)

Internal appliance users must be successfully identified prior to gaining access to the FirePass appliance. External VPN Users may initiate the log-in process and access the online knowledge base prior to being identified by the TOE. All other access for External VPN Users requires successful identification by the TOE. Internal appliance users and External VPN users are identified through the FirePass Appliance by comparison of login information to an internal SQL database. If the User is successfully identified, the authentication data is forwarded to an external authentication server for external VPN users or authenticated locally by the FirePass appliance for local (administrator) Internal appliance users in the Common Criteria Evaluated Configuration.

User authentication by TSF-local administrator (FIA_UAU.2, FIA_SOS.1)

FirePass local Administrators (Internal appliance users) are authenticated internal to the FirePass appliance. Administrators with the roles (Admin (full access) and Realm_admin (administrator)), are considered the sole local Users of the TOE and are identified and authenticated locally within the FirePass TOE. Authentication credentials are stored within the TOE in an MD5 hash, which is compared to local values entered and verified prior to allowing access to TSF resources. The password mechanism utilized satisfies the Strength of Function claim of SOF-Basic.

The TOE as configured for the Common Criteria Evaluated configuration (enables “enforce strong password for authentication against internal database” option) enforces the following password policy for passwords created on the FirePass appliance: Minimum of 8 characters. Must start with an alphabetical character; contain at least one numeric and one special character (neither the numeric nor the special character should be in the last character position of the password).   Also enforced is that the password cannot:

- Contain more than 3 consecutive occurrences of the same character
- Contain the employee name or logon
- Contain 5 consecutive numeric characters. For example, Test@12345

The password authentication mechanism is realized by a probabilistic or permutational security mechanism.

User authentication by authentication server –External VPN users (FIA_UAU_EXP.2)

External VPN users are authenticated by an external authentication server in order to gain access to Network Access mode or Web Application mode resources through FirePass. Username and Authentication is entered from the Client computer, the External VPN User is identified through the FirePass internal database and, if the identification is valid, a request is made to the authentication server to validate the credentials. If the authentication is successful, the External VPN User is logged on to the FirePass Appliance with access to the appropriate resources. If the authentication attempt is unsuccessful, the FirePass appliance requests new authentication data from the Client and repeats this process until authentication is successful or the maximum login attempts threshold has been reached.

The password mechanism utilized satisfies the Strength of Function claim of SOF-Basic.

The password authentication mechanism is realized by a probabilistic or permutational security mechanism.

6.1.3 Endpoint Security

The Endpoint Security features provide essential verification and protection tools that are implemented on the Client computer requesting access through FirePass.

Upon negotiation of a Network Access Mode session, the FirePass appliance utilizes the Client portion of the TOE to evaluate the operating environment of the client computer to assess various security related settings. These results are returned to the FirePass appliance and used as input for the Policy Based Resource Management security function.

Upon negotiation of a Web Applications Mode session, the FirePass appliance inspects HTML header information to evaluate the Operating System and Browser settings and evaluates this information in the same manner as Network Access Mode. The Web Applications Mode may be used in a clientless fashion where the available tests performed via the Endpoint security function are more limited than tests available for Network Access Mode. Pre-logon sequences can be enabled for either Network Access or Web Application Modes of operation, allowing for client-side components to perform full client data analysis/collection. If this is enabled for Web Application Mode, then the pre-logon processing is not clientless, but the Web Application Mode access will be clientless.

The TOE can identify the applicable Access Mode type on which the client is attempting to establish a HTTPs based SSL session (Web Access Mode) or PPP over SSL (Network Access Mode). By identifying the protocol requested, the TOE can determine the VPN access type requested.

These options are highly configurable and allow the Admin (full access) to set pre-requisites for establishing secure sessions and actions to take at the completion of sessions to assure information security is maintained on the Client. The configuration options and related action settings are termed Protected Configurations. Endpoint Security checks provide input to Protected Configurations, which in turn, enforces information flow policy as described in Policy Based Resource Management, Section: 6.16.

This functionality ensures the client configuration meets the organization's security policy for remote access. These assessments are performed in Collection, Remediation and Protection phases as information is collected from the prospective client and action taken based on Admin (full access) pre-configured options.

The FirePass Controller maintains the following protection options available for Admin (full access) configuration for Network Mode Access sessions; settings within these categories allow the Administrator to evaluate the Client.

- Anti-Virus & Firewall detection (presence of this software running on the Client)
- OS system type/version detection
- File Version Detection – i.e.: anti-virus binaries, signature files etc
- MD5 signature verification on Client - Inspects the MD5 signature of a file on a client system to ensure that the file has not been tampered with or corrupted
- Scanning – initiates Scan on Client computer to Admin (full access) set values

Endpoint Security – Network Access Mode (FPT_TST_EXP.1)

In both Network Access Mode and Web Applications Mode, Client Integrity Checking can be configured to assure firewalls, virus scan software or other process are running prior to granting access 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 other 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. In order for endpoint security to be used in this way for Web Applications Mode clients, a client component must be downloaded.

Examples of post-login protection features include (all required to be enabled for CC evaluated configuration:

- Activate cache cleanup to allow attachment downloads in Mobile E-Mail and downloads from Web Applications (Note: Applies only to Web Applications Mode)
- End the FirePass session if the user closes the browser or webtop
- Uninstall FirePass client components
- Remove dial-up entries that Network Access clients use
- Uninstall ActiveX components downloaded during the session
- Empty the Windows Recycle Bin
- Clean forms and passwords auto-complete data
- Close Google Desktop Search
- Inherit caching policy settings from Web Applications Mode configuration

Through the Secure Virtual Keyboard feature (a part of the Client Security Module), login data can be entered from client resources with a mouse versus a keyboard for enhanced security. This technique is intended to obfuscate keystroke observation.

Endpoint Security – Web Applications Mode (FPT_TST_EXP.1)

One of the endpoint security features available for Web Applications Mode is cache cleaning following session completion. Since this requires download of the Plug-In it may not be utilized, especially if on a public computer resource. In Web Applications Mode *if* the cache clean capability is *not* loaded into the client machine, downloads are blocked that would result in temporary file creation. This assures that information is not inadvertently left on a public access machine through cache cleaning or blocking of temporary file creation.

If Web Applications Mode is operated in a clientless fashion, the following actions are available without the need for downloaded plug-ins:

- Send email
- Check the time on the system
- Check the Browser Type and Version
- Check the type of device
- Check the operating system
- Check the client certificate
- Write content to the Logon log

If a client component is downloaded to the Web Application Mode client machine then pre-login sequences may be executed in a similar fashion to Network Access Mode noted above.

6.1.4 Network Access Mode

Level 3 VPN Access – FDP_NAM_EXP.1

Network Access Mode offers secure access to network resources. External VPN users can initiate secure sessions with the FirePass appliance, and after being identified and authenticated, can download client software to allow the establishment of PPP over SSL sessions to protected resources.

Network Access mode requires the use of Endpoint Security (see 6.1.3) to assure that clients computing resources are adequately secure prior attempting to established a Network Access Mode session.

Pre-login sequences

In a pre-logon sequence, inspectors are configured to gather the information required about the client computing environment. The inspectors create session variables containing the detected information. The FirePass controller passes the information to the protected configuration to determine access to protected resources. Rules and criteria are applied to the information collected to determine is session initiation requirements are met. By default, if the system does not meet the requirements, the FirePass Controller denies the user access. A pre-login sequence is a prerequisite to the use of protected configurations and is required to be enabled and utilized for the Common Criteria Evaluated Configuration.

Protected Configurations

The FirePass controller for Common Criteria uses protected configurations to control access to network resources. A protected configuration is a definition of criteria that users' systems must meet in order to be granted access to specific resources. Once you have determined the client information you plan to gather, you create protected configurations, named sets of safety checks and security measures, to assign to resources, applications, and files.

Protected configurations represent the conditions that control access to resources under their protection. Controlled conditions include what antivirus software the endpoint system is running, whether a logon comes from a company-issued computer, what time of day the logon occurs, which certificate the client is using, and others.

The following chart lists available Endpoint Security measures and settings required for the Common Criteria Evaluated configuration:

Risk factor	Available protection
Information Leaks	**Trusted Windows Version** Restricts access to users running specific Windows versions or hot-fixes, as specified in properties. If you specify Trusted Windows version, make sure also to configure the versions you want to accept. CC REQUIRED CONFIGURATION: Trusted Windows versions specified as: Windows 2000 SP4, Windows XP SP2 **Cache Cleaner** Removes content from the cache when users log out. CC REQUIRED CONFIGURATION: CACHE CLEANER = ENABLED **Trusted Browser**
	Requires use of a browser specified in properties. CC REQUIRED CONFIGURATION: Trusted Browser specified as: Microsoft Internet Explorer 6.0 SP1 or later
Loggers	The following protection criteria are available for preventing access by key-logging programs: **Virtual Keyboard** Specifies that passwords be entered using mouse clicks on a screen representation of a keyboard. CC REQUIRED CONFIGURATION: ENABLED
Virus Attack	The following protection criteria are available for preventing virus attacks: **Antivirus** Requires the presence of specific antivirus software, as specified in properties. CC REQUIRED CONFIGURATION: Norton Antivirus, McAfee Anti-Virus or Kaspersky (detected in client pre-login sequence) **Firewall** Requires the presence of specific firewall software, as specified in properties. CC REQUIRED CONFIGURATION: Windows Firewall, Norton Firewall software, McAfee Firewall software, ZoneAlarm software

Protected Configurations can be assigned on the following basis:

- **Webtop**

Protects all types of resource favorites.

- **Resource type**

Protects a class of resource favorites (for example, Web Applications or Network Access favorites). Overrides webtop-level protection.

- **Individual**

Protects a single resource (for example, the Sales Intranet). Overrides resource-type-level protection.

<u>Specification of Applications running on Clients</u>

The FirePass appliance provides configuration options that allow the administrator to specify what applications are allowed to be running on a client machine prior to allow a Network Access Mode session to initiate or continue. During session initiation, if an application is running on the client that is not explicitly in the allowed list, the session request is rejected. During an active session, if an application that is not in the allowed list, executes the session is immediately dropped by the FirePass appliance. These session related configuration settings are established by the TOE Administrator and stored within the FirePass appliance. The Common Criteria Evaluated Configuration requires the configuration of this feature; however, the specific applications allowed to run are determined by the Administrator at the time of installation based on what network resource and application types FirePass is supporting.

Post Logon Protection

Post Logon Protection features below must be enabled for Network Access Mode sessions for the Common Criteria Evaluated Configuration as indicated in Section 6.1.3.

Network Access Mode encrypted sessions using FirePass

(FCS_COP.1, FCS_CKM.1a, FCS_CKM.1b, FMT_MSA.2)

The Network Access Mode feature allows the FirePass Appliance to establish secure, layer 3 connections with clients using PPP over SSL VPN tunneling techniques. FirePass sessions are encrypted to assure that session data transfer is secured from intercept or information disclosure during FirePass sessions. The TSF generates session keys utilizing a software based random number generator with a key length of 160 bits in association with a Diffie-Helman key exchange per the requirements of FIPS 140-2. The High Grade security setting for Common Criteria assures that only AES (256) or 3DES (168) are used for SSL session encryption. The “Accept only TLS” protocol security selection on FirePass assures that only properly negotiated TLS sessions are accepted for Network Access Mode sessions.

The FirePass TOE allows the establishment of secure VPN network connections without requiring pre-installed client software. Required client plug-ins and security module software is installed on the Client from the FirePass appliance during the first session establishment. Using a standard HTTPs protocol, connection can be made through standard infrastructure components used in private LANs, proxies and ISPs.

Routing in Network Access Mode establishment

Network Access global settings specify IP address pools that the FirePass controller uses to assign IP addresses to a client computer’s point-to-point protocol (PPP) adapter. When the end user opens the address of the FirePass controller in their web browser, the browser opens an SSL connection to the FirePass controller. The user can then log on to the FirePass controller.

Flow Control Rules for Network Mode Access are detailed under Policy Based Resource Management, Section 6.1.6.

6.1.5 Web Applications Mode Access

Level 7 VPN Access – FDP_WAM_EXP.1

The Web Application Mode on the FirePass appliance allows access to specified intranet resources via a browser. The FirePass establishes secure sessions via SSL with a user that has been successfully identified and authenticated as indicated in Section 6.1.2. The FirePass appliance converts selected content from the network to HTML format to allow for viewing from a computer resource using just a browser. This mode is typically reserved for access to Intranet Web Servers or Email resources from public terminals where Client software is not available. FirePass offers various mechanisms in this mode to assure that the network is protected, content is restricted based on this mode of operations, and information is not cached or is thoroughly deleted following a session.

Web Applications Mode encrypted sessions using FirePass

((FCS_COP.1, FCS_CKM.1a, FCS_CKM.1b, FMT_MSA.2)

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 network 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 FirePass Appliance enforces the Web Applications Mode information flow SFP by requiring that the SSL session is appropriately established by only specified cryptographic key generation and exchange. All information transferred in Web Application mode is encrypted/decrypted through the SSL session parameters. SSL settings and usage within FirePass is identical to that described above for Network Access mode sessions.

The Web Application mode also fronts cookies on behalf of the network, providing insulation from potential security risks contained in cookies from the public computing resource. FirePass also can 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.

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. This setting is required for the Common Criteria Evaluated Configuration.

Flow Control Rules for Web Applications Mode Access are detailed under Policy Based Resource Management, Section 6.1.6.

6.1.6 Policy Based Resource Management

The FirePass Appliance enforces the FirePass Network Access Mode and Web Application Mode information flow control policies in establishing authorization for routing of traffic to client users based on the IP of the client, the IP address of the resource requested, authentication credentials of the user, and the satisfaction of administrator configured security prerequisites enforced by the Endpoint Security features. The Endpoint Security features provide input through testing to Protected Configurations, which characterize the Policy Based Resource Management security function. Administrators can establish the rule set to be used for Protected Configurations to support the FirePass Network Access Mode and Web Application Mode information flow control policies.

Protected Configurations provide criteria for specified security related events with restrictions or actions, which take effect based on the security situation assessed through Endpoint Security checks. Protected configurations can be applied in the following ways:

- To the entire feature: Users must meet certain requirements to use the functionality.
- To one or more resources: Users must meet certain requirements to access a specific server.
- To the master group: Users must belong to a specific master group to get access to certain resources.
- To applications and files: Users must meet certain requirements to have access to specific applications or files.

Access Mode Restrictions - FMT_MSA.3a, FMT_MSA.3b

Information Flows through the FirePass device are restrictive by default in that User's must be explicitly authorized to initiate either a Network Access Mode or Web Applications Mode session and explicitly allow access to specified resources based on Policy Based Resource Management decisions.

Information Flow Control – Network Access Mode

(FDP_IFC.1a FDP_IFF.1a, FMT_MSA.1a, FDP_NAM_EXP.1))

The FirePass Appliance enforces the FirePass Network Access Mode information flow control

SFP by assuring that information transferred during sessions is encrypted between the FirePass appliance and the Client upon initiation of the PPP over SSL session and that traffic is only routed to the session established IP addresses. If session security requirements are not met, either during session initiation or during the session (as administrator configured), the information flow will be explicitly denied.

Within the FirePass Appliance, the Admin (full access) or Realm_admin (administrator) uses configuration options to establish routing rules and permissions based on the performance of the Client in the Endpoint pre-session security checks as detailed in Section 6.1.3. Only FirePass administrators assigned to these role can query or modify these rules. Upon initiating a session, the FirePass appliance can use these Endpoint test results to enforce information flow rules by granting or limiting access to specific network resources. These flow control attributes are accessible only by the aforementioned roles and allow for configuration of access to network locations based on the rules established. The FirePass appliance will either permit or restrict information flow based on these attributes. By default, the FirePass appliance applies a restrictive flow control policy, Network Access Mode SFP, as access to network resources is not granted unless explicitly permitted by matching a configured rule.

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, resources that do not successfully pass all Endpoint Security checks are restricted to a limited (administrator specified) level of access to protect TOE resources.

Global packet filter rules can be customized by administrator users listed above for Network Access Mode to allow for isolation of specific protocol types and route traffic based on factors such as source, destination and type of service requested. Without packet filtering enabled, the FirePass appliance accepts all packets by default. Once packet filter rules are established and packet filtering is enabled, these rules are enforced upon service startup.

FirePass can implement this function in one of two ways.

1. Applying the filtering rules to run all global filtering rules, specifying rules to allow packets and, upon completion, execute a "Drop All" packets command that drops all packets not meeting the established "Pass" rule sets.
2. Alternatively, if rules are established relating to which packets are filtered out, then upon completion of the "Drop" rule set, an "Accept All" rule is executed, thereby accepting all packets that have not been explicitly filtered out.

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).

Information Flow Control – Web Applications Mode

(FDP_IFC.1b FDP_IFF.1b, FMT_MSA.1b, FDP_WAM_EXP.1)

FirePass has features that may be configured to limit the level of access to the TOE and Host Network resources based on the browser used, cache settings and the ability to download plug-in for cache cleaning. Web Application mode is intended for untrusted (typically public) resources and is therefore restricted to a limited (administrator specified) level of access to protect TOE resources. Since Web Applications Mode allows only browser based HTML access to allocated resources, the resources available for access are restricted by use of this mode through FirePass. In addition, based on Administrator configured options (as listed above) for Network Access Mode, additional restrictions may apply based on the results of the Endpoint Security checks performed by the FirePass appliance during session initiation.

The application of these configured flow control rules through the FirePass Appliance enforces the Web Applications Mode SFP. Only FirePass administrators (assigned to roles Admin (full access), or Realm_admin (administrator)s) can query or modify these rules. An example of these restrictions is that FirePass will not allow for download of files if the “clear cache” option can not be instituted for the Client IT Environment. These rules for Web Applications mode provide security by either deleting files used during a session or restricting the download of such files to assure that data is not left on a public access point, where Web Applications Mode is typically used.

6.1.7 Security Management

The Security Management security function provides Realm_admin (administrator) and Administrator’s (SuperUser) with a GUI based administrative console to view and manage TSF functions and data. The graphic user interface provides the ability to make appliance configuration settings, create and manage FirePass users, install and manage Server certificates, view various appliance health monitors and session characteristics, and review appliance audit logs. These sessions are secured via TLS based sessions and are hosted by a dedicated Ethernet port, the Administrator Management Port.

The FirePass appliance also includes a menu driven serial interface which allows Administrative users to manage a limited set of functions such as resetting appliance settings, remove firewall rules, enable accounts for admin console access, disable SSH, modify access requirement for console access, perform diagnostic checks, create/restore the FirePass snapshot, FIPS card admin and enable disable failover mechanisms.

The FirePass appliance protects Administrator sessions by requiring proper authentication, secure sessions using TLS and has provision for restricting Administrative User access to a specific set of IP addresses or subnetworks. Typical configuration allows Administrator access only from within the trusted network.

Management of TSF Data

(FMT_MOF.1, FMT_MTD.1a, FMT_MTD.1b, FMT_SMF.1)

The TOE utilizes the Security Management security function to restrict the management of TSF data to authorized administrators with the roles Administrator(SuperUser) or Realm_admin (administrator). Based on the type of TSF data, various operations can be executed to query, modify, or delete TSF data to support security functionality. In addition, appliance health and session monitors provide detailed data on the session load, operational characteristics such as disk storage available, appliance temperature, database integrity, and related resource usage and availability.

The security management function of the TOE provides specific access controls based on the type of TSF data management by the appliance. The limited ability to only query appliance audit logs and installed Server certificate characteristics is restricted to authorized administrators (Realm_admin (administrator) and Admin (full access)**)**. Authorized administrators may query and modify the Failover settings that the appliance uses to determine how to transfer traffic to a standby unit in the event of a single appliance failure. Also using this interface, authorized users may stop or start specific services within the FirePass appliance and/or stop, start or restart the entire appliance.

Administrator User settings and authentication data is accessed through the administrator console and can only be viewed or modified by Admin (full access)s. Group settings are also accessed and may be modified through the administrator console. This allows the Admin (full access) to define master groups of users to configure users based on access requirements and other common characteristics and resource groups that configures specific resources by common function and access requirements.

The remote interface can also be configured through the administrator console, allowing authorized administrators to query and modify interface settings.

Security Management via FirePass Roles - (FMT_SMR.1)

The TOE uses Administrator Realms to structure specific roles and access levels based on assigned status within the TOE configuration. An administrative realm is a complete set of roles, master groups, and resource groups. Administrator Realms are established to define a subset of resource groups that can be managed by a FirePass Administrator. Realms are used by the TOE Administrator to segment the network to allow multiple Administrators to take charge of a given segment, thereby distributing Administrator duties.

The External VPN user represents the user which utilizes the FirePass appliance to establish Network Mode or Web Applications Mode access to network resources. This user's interface with the product is limited to logon dialogs and password establishment. The Admin (full access) is the top level Administrator for the FirePass Appliance with unrestricted privileges and access to all functions. Administrators (SuperUsers) can create Realm_admin (administrator)s, who can provide Administrator level services to all resources within their Administrator assigned realm. This allows Administrators (SuperUser) to assign responsibilities to Realm_admin (administrator)s by assigned subsets or Realms of the overall system. All roles can potentially access all security management functions, if so configured by the Admin (full access).

6.1.8 Secure Communications

The secure communication security function supports the implementation of the FirePass Network Access Mode and Web Applications information flow control SFP through the use of encryption via SSL sessions for all data transfers through the TOE. The FirePass appliance restricts all transmissions through the appliance to encryption through PPP over SSL protocols or HTTPs connections utilizing only authorized administrator (Realm_admin (administrator) and Admin (full access)**)** configured SSL cipher/hash combinations.

Secure Traffic and Communications

(FCS_COP.1, FCS_CKM.1a, FCS_CKM.1b, FMT_MSA.2)

All sessions established by and traveling through the FirePass appliance utilize SSL encryption through a TLS protocol to assure TSF or User data cannot be modified or disclosed during transmission to unauthorized parties. Network Access Mode establishes a secure tunnel using Point to Point Protocol over SSL techniques. This offers the most secure mode of operation for FirePass and allows for direct VPN network access to protected network resources as configured by the Administrator. Web Applications Mode sessions are secured using SSL encryption and is designed to establish a secure, HTML based connection using a browser, without the need to download plug-ins or client software. This mode is limited to access of specified resources only via HTML. In both cases, rules are established by the Administrator to alter access based on Endpoint security test results and established session prerequisites.

The SSL session is established during the initial login to the FirePass Appliance and requires successful authentication and key exchange. The TOE accepts only TLS based sessions with either AES (256bit) or 3DES (128bit) ciphers with SHA-1 that meet the requirements of FIPS 140-2 for the Common Criteria Evaluated Configuration. This requirement is enforced through the High Grade Security + accept TLS only settings configured on the TOE.

The following cipher-suites are allowed for use by the FirePass appliance in the high grade security setting:

DHE-RSA-AES256-SHA
DHE-DSS-AES256-SHA
AES256-SHA
EDH-RSA-DES-CBC3-SHA
EDH-DSS-DES-CBC3-SHA
DES-CBC3-SHA

All sessions are encrypted by default using TLS; data transfer during a session is not permitted to be sent in plain text.

The FirePass appliance can generate self-signed SSL server certificates with a 1024 bit key length. SSL server certificates can be imported to the FirePass appliance which is either 1024, 2048 or 4096 bit key length.

Key Destruction (FCS_CKM.4)

The FirePass appliance features a snapshot restoration utility that allows all configuration data within the box, including all plaintext keys and security parameters to be overwritten at the block level and be replaced with factory default configuration data. When the authorized administrator executes this command via a direct connection to the appliance (using the maintenance console) the existing security and configuration data is entirely overwritten at the block level with a stored (factory) configuration data set. This feature is used often when an appliance requires service and a customer wants to assure all security data is fully obliterated before returning.

Session keys which are used to secure Network Access and Web Application mode sessions are valid only for the active sessions. Following the session, the memory locations where these keys reside are reallocated through the underlying operating system function.

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

Secure Communications between the FirePass TOE and applicable Authentication Servers

Communications with the authentication server (trusted IT product) is secured through an SSL based connection using the methods described above to assure that TSF data such as username, passwords or other authentication data are not disclosed to unauthorized parties, modified or deleted.

The TOE receives the remote authentication request and routes that request to the remote authentication server for validation.

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

6.1.9 Protection of TOE Functions

Self Protection - (FPT_RVM.1a, FPT_SEP.1a, FPT_SEP_EXP.1)

The FirePass appliance institutes fundamental self protection functionality through physical protection of the appliance itself (including the physical locations assumptions listed in Section 3.1.2), use of tamper-labels and logical protection to assure security functionality cannot be bypassed or altered. The underlying FirePass Operating System and Identification and Authentication requirements (as discussed in Section 6.1.2) restrict access to TSF resource to authorized administrators.

The FirePass Client installed provides partial TSF Domain Separation by protecting the (Client) TSF from subjects initiating actions through its interfaces.

VPN Session Termination due to inactivity – (FTA_SSL.3)

The FirePass appliance allows the Admin (full access) to configure a time interval of inactivity by which the TSF will terminate the interactive VPN session (Network Access mode/Web Applications mode). Once the session has been inactive for the specified period of time, the TOE ends the session and requires a new authentication cycle prior to instituting a new VPN session through the TOE.

Client Plug-In Protection (FPT_SEP_EXP.1)

Client Plug-Ins downloaded onto the client machine maintain a TSF protected security domain and protect against tampering through its interfaces. The Client Plug-In supports the enforcement of separation between the TSF and subjects through its association with the authorized user session restrictions, post session cleanup activities and separation enforcement measures implemented on the appliance side.

Reverse Proxy Mode protection

The TOE dynamically maps internal URLs to external URLs and deletes URL information following the session through the Cache Cleaner function, when enabled. This protects IP addresses from eavesdropping by obscuring network IP addresses and reducing the potential for security exploitation in Web Applications Mode. This functionality is provided by the Policy Engine in concert with the Networking Module.

Failure in Secure State and Failover redundancy (FPT_FLS.1, FRU_FLT.2)

The Evaluated Configuration of the TOE is the High Availability Redundant Pair configuration, allowing for maximum availability under various failure conditions. This provides one unit as the active appliance to process traffic and a second (redundant) appliance, which does not process traffic until Failover occurs. This assures that a fully configured standby appliance is available so, in the event of failure of the active unit, traffic is immediately switched to the standby unit.
The TOE preserves a secure state during operational failure of a single TOE hardware device. Operational failure is defined as:

a. Power Supply Failure of the active appliance
b. Hard Drive Failure of the active appliance
c. Memory based Failure of the active appliance
d. Software failure of the active appliance
e. Processor failure of the active appliance
f. >200mSec delay between heartbeats (sync signal)

Failover is executed with minimal traffic interruption and established TSF protection features when configured in the Evaluated Configuration.

The TOE is protected from software or hardware failures via a “Failover” system facilitated by a hardwired Ethernet connection between two identical FirePass hardware units configured in redundant fail-over configuration.

The following redundant features are provided in the Common Criteria Evaluated Configuration:

- Failover – defines behavior relating to protection of availability via Failover redundancy functionality
- Configuration synchronization – defines behavior related to synchronizing the TOE’s redundant pair configuration
- System fail secure – provides TSF protection during failure

When properly configured by the administrator, the FirePass system will switch traffic from the failed unit to the Active Standby unit automatically.

When the system failover is configured, the FirePass system monitors various hardware components, as well as the heartbeat of various system services, and takes action if the system detects a failure.

Changes in State related to Failover process

The FirePass redundant-pair Failover process results in TOE state changes that relate to which appliance is in the active or standby mode. In the active mode, the appliance is actively passing traffic to Network Access Mode and Web Applications Mode resources enforcing all SFRs and the applicable SFP. During initial configuration, the Administrator assigns one appliance as “First” and the other as “Second”. This designation is used when both units are started simultaneously and priority has to be established. When an appliance is in the standby mode, it is powered up and fully configured, but not involved in the creation of or support of FirePass sessions. The standby and active appliances are connected by a crossover cable that provides a “heartbeat” monitor (activity indicator) that keeps both appliances in synch and aware of the status of the other pair member.

Each appliance is individually configured with a unique IP address, and both appliances are configured with a shared IP address. The active controller and the standby controller share this IP address, so either controller can assume the shared IP address when it is the active controller.

A web service is configured through the FirePass Administrator console by the Administrator by creating a synchronization agent which assures that the configuration is shared among both appliances and establishes that both devices are prepared to assume the active state when required.

Failover process

If the standby node does not receive a heartbeat within 200 milliseconds of the expected arrival time, the standby node considers its peer inactive, assumes its virtual IP address, and becomes the active member of the pair. Heartbeat settings specify the interface and port a controller uses while it is the active member of the Failover pair.

Re-initialization after Failover

If both Failover controllers are turned off, the first controller started automatically assumes the role of active controller, and the second controller started becomes the standby controller. The two controllers remain in this state until either the active controller fails and the standby controller takes over, or the active controller is restarted and the standby controller becomes the active controller.

If a pair of Failover controllers is started simultaneously, the controller configured as First on the Failover settings screen becomes the active controller, and the controller configured as Second on the Failover settings screen becomes the standby controller.

Identification of an appliance as either the Active or Standby controller can be determined by the Administrator by logging on to the appliance. The welcome screen includes the status as either Active or Standby during startup.

The following table illustrates the changes in state of the TOE appliances associated with the Failover process:

State Definitions	Action	State Change	Secure Result
Normal Operation “First” = active “Second = standby”	Active appliance manages Secure VPN traffic	None – both operational and configured First, Second priority in force	All SFRs & SFPs in effect – standby appliance is configured and available
Active Appliance Failure (hardware or software)“First” = failed “Second = active”	Fail-Over – traffic is switched to standby appliance	Active becomes off line – Standby appliance becomes active enforcing all SFPs	All traffic is transferred without interruption and all SFRs and SFPs remain in effect

Standby Appliance Failure (hardware or software)“First” = active “Second = failed”	No action – Traffic remains on Active Appliance, unaffected	Standby appliance goes from operational to failed – no effect on traffic	All SFRs & SFPs in effect – standby appliance has failed and can be serviced without affecting traffic
Both Appliances Fail (hardware or software) “First” = failed “Second = failed”	All traffic halted through device	Traffic halted due to failure – Fail-Over does not commence – both appliances go from operational to failed	Traffic is halted – protected resources secure
Standby Appliance Recovers “First” = failed “Second = active”	Traffic is processed by standby appliance	Active is off line – Standby appliance is active enforcing all SFPs	All traffic is processed normally upon startup and all SFRs and SFPs remain in effect
Active Appliance recovers “First” = active “Second = failed”	No action – Traffic remains on Active Appliance, unaffected	Active Appliance goes from failed to operational	All SFRs & SFPs in effect – standby appliance is down
Both Appliance recover/restart simultaneously “First” = active “Second = standby”	Active appliance manages Secure VPN traffic – Appliance with “First” configuration attribute assumes Active Role – Appliances are synchronized – heartbeat established	Both appliances go from failed to operational	All SFRs & SFPs in effect – standby appliance is configured and available

Table 12: TOE State Change during Failover process

Identification and Authentication Security Policy Model

The TOE enforces a policy of requiring positive identification and authentication for all users accessing the TOE either through direct access of the appliance or by conducting VPN sessions by which network data is access through FirePass VPN functionality. The TOE maintains two classes of users, Internal Appliance Users and External VPN Users. Internal Appliances users access the TOE for the primary purpose of managing FirePass users, operations and settings. Within this user class are Administrators termed Admin-full access and realm administrators termed realm-admin. External VPN users use the FirePass appliance as a conduit to access internal network resources from a remote location via a virtual private network (VPN). Separate URLs are used to host Internal Appliance Users and External VPN Users login screens. Identification and Authentication requirements are enforced during all operational states of the TOE.

The TOE enforces an identical Identification and Authentication policy for both classes of Users in that positive identification and authentication is required prior to access to TSF resources, whether these are actual FirePass appliance settings (Internal Appliance Users) or Backend Network Resources (External VPN Users). Both Username and Password are verified against either an internal FirePass appliance database (Admin-Full access) or through an external authentication server in the IT Environment (all other users). Regardless of method of validation of authentication credentials, Username/Password combinations must match a valid account for the FirePass appliance. Based on the role and group memberships associated with the validated Username/Password combination, appropriate access is granted following login processes as specified in the FirePass Information Flow Control SFP. The entry of invalid information results in a failed login attempt which is logged by the TOE. In addition, the TOE disables the User Account associated with a failed login after 10 attempts within a 5 minutes timeframe. Only the Admin-full access user may re-activate the account after deactivation.

The FirePass appliance also enforces Password usage to assure strong passwords are selected for use and thereby, enforced, by the TOE for all users except the Admin-full access user. This user is procedurally advised to follow the password policy as technical means of enforcement are not instituted. Passwords must meet a **minimum of 8 characters, must start with an alphabetical character; contain at least one numeric and one special character (neither the numeric nor the special character should be in the last character position of the password).**

Security Audit Security Policy Model

The FirePass TOE enforces a security audit policy which assures audit logs are generated for security related events and appliance configuration changes which could impact the TSF. As described in Section 6.1.1, logs are generated in support of the Identification and Authentication security function, detailing success and failure of logins and action taken once logged in to a FirePass VPN session. The audit trail provided also shows access attempts that are unsuccessful to provide the TOE Administrator (Admin-full access) with the ability to detect potential malicious access attempts. Information flows during sessions are logged in support of the FirePass Information Flow Control SFP. The audit policy enforces audit generation requirement for specified actions by all users regardless of role and does not allow audit records to be modified or deleted by any user. Auditing cannot be disabled on the appliance and system logs, indicating security related appliance configuration actions, are enabled by default. The audit policy is enforced entirely through technical means within the TOE appliance, although logging levels can be configured by the Admin – full access user to provide more detailed logging during troubleshooting or security event investigation. The policy enforces that only internal appliance users (realm admin, admin-full access) may access audit records for review through the security management security function. External VPN Users are explicitly denied access to all Administrative GUI/Configuration settings, including audit logs, by domain separation aspects of the appliance architecture. The common criteria evaluated configuration stipulates the use of an external FTP server, for audit log storage, to ensure that the FirePass audit trail is preserved under all conditions. The security audit policy is in force during all states of operation for the FirePass TOE, including failure of a single appliance, as described in Table 12: TOE State Change during Failover process.

Buffer Overflow protection through TOE Configuration options (Web Applications Mode only)

Buffer Overflow attacks can be prevented by TOE Administrator configuration of the following settings as required for the Common Criteria Evaluated Configuration:

- Restrict maximum upload size (32-1024 Mb)
  Constrains files that the User uploads to a specific size. The default value is 32 MB.
- Restrict maximum length of a GET query string
  Constrains the request string to the maximum specified. The default value is 2048 bytes.
- Restrict maximum length of POST data
  Constrains the response string to the maximum specified. The default value is 16384 bytes.

6.2 Security Assurance Measures

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

Assurance Requirement	Assurance Components
ACM_CAP.2	The description of the configuration items is provided in F5 Networks FirePass® 4100 High Availability pair (qty 2) EAL 2 Configuration Management Documentation, Version 1.0.
ADO_DEL.1	The description of the delivery procedures is provided in Common Criteria Supplement EAL2 Secure Delivery Document F5 Networks FirePass 4100 High Availability pair (qty 2) , Version 1.0.
ADO_IGS.1	The installation, generation, and start-up procedures are provided in Common Criteria User Guidance EAL2 F5 Networks FirePass 4100 High Availability pair (qty 2), Version 1.0
ADV_FSP.1	The informal functional specification is provided in EAL 2 Design Documentation Functional Specification and Implementation Representation F5 Networks FirePass®, Version 1.0.
ADV_HLD.1	The descriptive high-level design is provided in EAL 2 High Level Design Documentation F5 Networks FirePass®, Version 1.0.
ADV_RCR.1	The informal correspondence demonstration is provided in EAL 2 Design Documentation Functional Specification and Implementation Representation F5 Networks FirePass®, Version 1.0.
ADV_SPM.1	See Section 6.1.9 "Changes in State related to Failover process" & FIA, FAU policies
AGD_ADM.1	The administrator guidance is provided in the following documents: Common Criteria User Guidance EAL2 F5 Networks FirePass 4100 High Availability pair (qty 2), Version 1.0.
AGD_USR.1	The user guidance is provided in N/A
ATE_COV.1	The evidence of coverage is provided in Tests Activity ATE F5 Networks FirePass® 4100 Version 5.5.2 EAL 2, Version 1.0
ATE_FUN.1	The functional testing description is provided in Tests Activity ATE F5 Networks FirePass® 4100 Version 5.5.2 EAL 2, Version 1.0.
ATE_IND.2	The TOE and testing documentation were made available to the CC testing laboratory for independent testing. F5 Networks FirePass® 4100 Version 5.5.2 EAL 2 + ALC_FLR.1, ADV_SPM.1 Independent Test Plan (ATE_IND.2), Version 1.0.
AVA_SOF.1	The strength of function analysis performed is provided in EAL 2 Strength of Function Analysis F5 Networks FirePass® 4100 Version 5.5.2, Version 1.0.

Assurance Requirement	Assurance Components
AVA_VLA.1	The vulnerability analysis performed is provided in F5 Networks FirePass® 4100 Version 5.5.2 Common Criteria Vulnerability Analysis AVA_VLA.1 EAL 2, Version 1.0.
ALC_FLR.1	The Flaw Remediation description is provided in EAL 2 Basic Flaw Remediation F5 Networks FirePass® 4100 High Availability pair (qty 2), Version 1.0.

Table 13: Assurance Requirements: EAL2 Augmented ALC_FLR.1, ADV_SPM.1

6.3 Rationale for TOE Security Functions

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

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

	Security Audit	Identification and Auth.	Endpoint Security	Network Access Mode	Web Apps. Mode	Policy Based Resource Management	Security Management	Secure Communications	TOE Protection
FAU_GEN.2	X								
FAU_SAR.1	X								
FAU_SAR.3a	X								
FAU_SAR.3b	X								
FAU_STG.1	X								
FCS_CKM.1a				X	X			X	
FCS_CKM.1b				X	X			X	
FCS_CKM.4								X	
FCS_COP.1				X	X			X	
FDP_IFC.1a						X			
FDP_IFC.1b						X			
FDP_IFF.1a						X			
FDP_IFF.1b						X			
FIA_AFL.1		X							
FIA_ATD.1		X							
FIA_SOS.1		X							
FIA_UID.1		X							

	Security Audit	Identification and Auth.	Endpoint Security	Network Access Mode	Web Apps. Mode	Policy Based Resource Management	Security Management	Secure Communications	TOE Protection
FIA_UAU.2		X							
FMT_MOF.1							X		
FMT_MSA.1a						X			
FMT_MSA.1b						X			
FMT_MSA.2				X	X			X	
FMT_MSA.3a						X			
FMT_MSA.3b						X			
FMT_MTD.1a							X		
FMT_MTD.1b							X		
FMT_SMF.1							X		
FMT_SMR.1							X		
FPT_FLS.1									X
FPT_RVM.1									X
FPT_SEP.1									X
FPT_STM.1	X								
FRU_FLT.2									X
FTA_SSL.3									X
FAU_GEN_EXP.1	X								
FAU_STG_EXP.1	X								
FDP_NAM_EXP.1				X		X			
FDP_WAM_EXP.1					X	X			
FIA_UAU_EXP.2		X							

	Security Audit	Identification and Auth.	Endpoint Security	Network Access Mode	Web Apps. Mode	Policy Based Resource Management	Security Management	Secure Communications	TOE Protection
FPT_SEP_EXP.1									X
FPT_TST_EXP.1			X						

Table 14: TOE Security Function to SFR Mapping

6.4 Appropriate Strength of Function Claim

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

6.5 Rationale for Security Assurance Measures

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

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

Assurance Requirement	Assurance Measures	Assurance Rationale
ACM_CAP.2	F5 Networks FirePass® 4100 High Availability pair (qty 2) EAL 2 Configuration Management Documentation, Version 1.0	The configuration management documents defines the configuration items and contains the necessary information to demonstrate that a CM system is used and that there is a unique reference for the TOE.

Assurance Requirement	Assurance Measures	Assurance Rationale
ADO_DEL.1	Common Criteria Supplement EAL 2 Secure Delivery Document F5 Networks FirePass 4100 High Availability pair (qty 2) Version 1.0.	The delivery document describes the steps performed to deliver the TOE. It describes the process used to create distribution copies of the TOE software and the steps taken to ensure consistent, dependable delivery of the TOE to the customer.
ADO_IGS.1	Common Criteria User Guidance EAL2 F5 Networks FirePass 4100 High Availability pair (qty 2), Version 1.0.	The installation, documents describe the steps necessary for secure installation, generation and start-up of the TOE.
ADV_FSP.1	EAL 2 Design Documentation Functional Specification and Implementation Representation F5 Networks FirePass® Version 1.0.	The informal functional specification document identifies the external interfaces that completely represent the TSF and describes the purpose and method of use of all external TSF interfaces. It also describes the effects, exceptions, and error messages for each of the external TSF interfaces.
ADV_HLD.1	EAL 2 High Level Design Documentation F5 Networks FirePass® Version 1.0.	The descriptive high-level design describes the complete TSF in terms of subsystems. The security functions for each subsystem are described. The subsystem interfaces are defined and the externally visible interfaces are identified.
ADV_RCR.1	EAL 2 Design Documentation Functional Specification and Implementation Representation F5 Networks FirePass®, Version 1.0.	The informal correspondence document maps the security functionality as described in the FSP and ST and as described in the FSP and HLD.
ADV_SPM.1	Contained in Security Target – see section 6.1.9 Changes in State related to Failover process	The Security Target contains the ADV_SPM.1 informal Security Model to details state changes within the TOE given specified events.
ALC_FLR.1	EAL 2 Basic Flaw Remediation F5 Networks FirePass® 4100 High Availability pair (qty 2), Version 1.0.	Flaw Remediation outlines the sponsor’s process to address security related product issues

Assurance Requirement	Assurance Measures	Assurance Rationale
AGD_ADM.1	Common Criteria User Guidance EAL2 F5 Networks FirePass 4100 High Availability pair (qty 2), Version 1.0	The administrator guidance documents provide complete administrative guidance for the TOE, including all security features and configuration items.
AGD_USR.1	*Not applicable*	The user guidance describes the security functions and interfaces in a way that allows a user to interact with the TOE securely.
ATE_COV.1	Tests Activity ATE F5 Networks FirePass® 4100 Version 5.5.2 EAL 2, Version 1.0.	The test coverage document provides a mapping of the test cases performed against the TSF.
ATE_FUN.1	Tests Activity ATE F5 Networks FirePass® 4100 Version 5.5.2 EAL 2, Version 1.0.	The functional testing document includes the test plans, test procedures, and associated test cases of the TOE functional testing effort.
ATE_IND.2	F5 Networks FirePass® 4100 Version 5.5.2 EAL 2 + ALC_FLR.1, ADV_SPM.1 Independent Test Plan (ATE_IND.2), Version 1.0.	The TOE hardware, software, guidance, and testing documentation were made available to the CC testing laboratory for independent testing.
AVA_SOF.1	EAL 2 Strength of Function Analysis F5 Networks FirePass® 4100 Version 5.5.2, Version 1.0	The strength of function analysis document provides the SOF argument for the password mechanism.
AVA_VLA.1	F5 Networks FirePass® 4100 Version 5.5.2 Common Criteria Vulnerability Analysis AVA_VLA.1 EAL 2, Version 1.0	The vulnerability analysis document identifies and describes the process used to discover obvious vulnerabilities, the results of the vulnerability analysis, and the mitigation of each identified obvious vulnerability.

Table 15: Rationale for Security Assurance Measures

7 Protection Profile Claims

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

8 Rationale

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

8.1 Security Objectives Rationale

Sections 4.3 - 4.6 provide the security objectives rationale.

8.2 Security Requirements Rationale

Sections 5.7 - 5.12 provide the security requirements rationale.

8.3 TOE Summary Specification Rationale

Sections 6.3 - 6.5 provide the TOE summary specification rationale.

8.4 Protection Profile Claims Rationale

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