
# McAfee Firewall Enterprise v8.3.2 and McAfee Firewall Enterprise Control Center v5.3.2 Security Target

17 December 2013

Version 1.5

Prepared By:

Primasec Ltd

For

McAfee Inc

2340 Energy Park Drive

St. Paul, MN  55108

USA

# Contents

# 1 Introduction

## 1.1 ST Introduction

This section presents the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE is McAfee Firewall Enterprise 8.3.2 and McAfee Firewall Enterprise Control Center 5.3.2.

Within this ST, “McAfee Firewall” is used to identify the combination hardware and software required to manage and operate the TOE. There are two possible configurations, reflecting two separate management options.

*Configuration A* comprises:

- the McAfee Firewall Enterprise software, including its SecureOS operating system,
- the McAfee Firewall Admin Console client software,
- the hardware or virtual platform for running the firewall software.

*Configuration B* comprises:

- the McAfee Firewall Enterprise software, including its SecureOS operating system,
- the McAfee Firewall Enterprise Control Center (“Control Center”) Management server software,
- the hardware or virtual platform for running the Control Center Management server software,
- the Control Center client software.

The specific firewall software version and management tool versions to be evaluated are all specified in Section 1.2.

McAfee Firewall is a firewall and access control security platform for the enterprise; McAfee Firewall configured in its operational environment delivers strong security while maintaining performance and scalability. It provides access control of communication and information flow between two or more networks, usually the Internet and internal networks, using application-level proxy and packet filtering technology. The operational environment for the McAfee Firewall software is a dedicated McAfee appliance platform or virtual appliance, supporting a typical Intel-based instruction architecture. The configured McAfee Firewall provides the highest levels of security by using SecureOS ™, an enhanced UNIX operating system that employs McAfee's patented Type Enforcement™ security technology. Type Enforcement technology protects McAfee Firewall by separating all processes and services on the firewall.

McAfee Firewall supports user identification and authentication (I&A) where "user" is defined to be a human user acting in an Administrative role, an authenticated proxy user, or an authorized IT entity. It provides the capability to pass and block information flows based on a set of rules defined by the Administrator. Additionally, it enforces security policies which restrict host-to-host connections to common Internet services such as: Telnet, File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP and HTTPS), and Simple Mail Transfer Protocol (SMTP). McAfee Firewall supports encryption for remote administration, remote proxy users and authorized IT entities (e.g. certificate server, NTP server), and generates audit data of security relevant events. McAfee Firewall also provides VPN capability to encrypt out-going traffic flowing to a geographically separated enclave and decrypt in-coming traffic from such an enclave.

This ST contains the following additional sections:

- TOE Description (Section 2)
- Security Problem Definition (Section 3)
- Security Objectives (Section 4)
- Security Requirements (Section 5)
- TOE Summary Specification (Section 6)
- Rationale (Section 8).

## 1.2 Security Target, TOE and CC Identification

ST Title –McAfee Firewall Enterprise v8.3.2 and McAfee Firewall Enterprise Control Center 5.3.2 P01 Security Target

ST Version – 1.5

ST Date – 17 December 2013

TOE Identification – McAfee Firewall Enterprise 8.3.2 and McAfee Firewall Enterprise Control Center 5.3.2

Software: McAfee Firewall 8.3.2, together with **either** McAfee Firewall Enterprise (Sidewinder) Admin Console 5.09 (Configuration A) **or** McAfee Firewall Enterprise Control Center 5.3.2 (Configuration B)

The TOE runs on any 64 bit hardware or virtual platform for which a license can be purchased from McAfee (see list of platforms in section 2.3.4.1).

TOE Developer – McAfee

Evaluation Sponsor – McAfee

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 3.1r3

## 1.3 Conformance Claims

### 1.3.1 Common Criteria

This TOE and ST are conformant to the following CC specifications:

[CC_PART2] Extended

[CC_PART3] Conformant

Assurance Level: EAL 4 augmented with ALC_FLR.3

### 1.3.2 Protection Profile

This TOE and ST are conformant to [FWPP] (Augmented).

The TOE type is a firewall, and the TOE type in the PP is stated to be a firewall. The TOE type is therefore consistent with the PP.

The statement of security problem definition in the ST is consistent with that in the PP. All threats, assumptions and organizational security policies in the PP are included in the ST. One threat has been added to address confidentiality and integrity of network traffic in support of claims made in relation to VPNs.

The statement of security objectives in the ST is consistent with that in the PP. The security objectives for the TOE in the ST include all those in the PP. One security objective for the TOE has been added, covering use of VPN. This does not conflict with the other objectives. One of the security objectives for the TOE has been repeated in the statement of security objectives for the environment, to reflect use of an external single-use authentication server. Some of the security objectives for the environment have been reworded for clarity, but in each case the objective is unaltered.

The statement of security requirements in the ST is consistent with that in the PP. Additional security functional requirements have been added to reflect use of VPN. These additional security functional requirements are consistent with those from the PP. An additional security functional requirement has been added to reflect use of an external authentication server. This approach was validated with the PP authors during evaluation of an earlier version of the TOE in 2007.

The security assurance requirements in the ST are hierarchical to those in the PP. The PP calls up EAL2 augmented with ALC_FLR.2, whereas the TOE uses EAL4 augmented with ALC_FLR.3.

## 1.4 Conventions

Since this security target is claiming compliance with a protection profile, the conventions used are intended to highlight the completion of operations made within this security target. While this security target will include the operations made by the protection profile upon the CC requirements it is not the author's intent to highlight those operations (i.e., use bold, italics or special fonts). Therefore, keywords (e.g. selection, assignment and refinement) and formatting (e.g., special fonts) used within the protection profile to designate operations are being removed by this ST. The brackets used by the protection profile to designate operations completed by the PP are left in the requirements.

The following conventions have been applied to indicate operations that this ST is making to the requirements in the protection profile:

☐ **Security Functional Requirements** – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.

- Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a number in brackets placed at the end of the component. For example FDP_ACC.1 (1) and FDP_ACC.1 (2) indicate that the ST includes two iterations of the FDP_ACC.1 requirement, 1 and 2.
- Assignment: allows the specification of an identified parameter. Assignments are indicated using **bold** and are surrounded by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g. [***[selected-assignment]***]).
- Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
- Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ big things …").

☐ **Other sections of the ST** – Other sections of the ST use **bolding** to highlight text of special interest, such as captions.

## 1.5 Terminology & Acronyms

In the Common Criteria, many terms are defined in Section 4 of [CCPART1]. The following terms are a subset of those definitions. They are listed here to aid the user of the Security Target.

| | |
|---|---|
| **External Entity** | Any entity (human or IT) outside the TOE that interacts (or may interact) with the TOE. |
| **User** | Same as External Entity |
| **Authorized User** | A user who may, in accordance with the SFRs, perform an operation. |
| **Role** | A predefined set of rules establishing the allowed interactions between a user and the TOE. |
| **Identity** | A representation (e.g., a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym. |
| **Authentication data** | Information used to verify the claimed identity of a user. |

In addition to the above general definitions, this Security Target provides the following specialized definitions:

**Administrator** – Any human user who has been identified and authenticated to act in the administrative role defined in the ST. An “authorized administrator” is an administrator who may, in accordance with the SFRs, perform an operation. A “non-administrator” is, obviously, someone who is not an administrator.

**Application-Level Proxy** – A proxy server acts on behalf of the user. All requests from clients to the Internet go to the proxy server first. The proxy evaluates the request, and if allowed, re-establishes it on the outbound side to the Internet. Likewise, responses from the Internet go to the proxy server to be evaluated. The proxy then relays the message to the client. Both client and server think they are communicating with one another, but, in fact, are dealing only with the proxy. Proxy servers are available for common Internet services; for example, an HTTP proxy is used for Web access, and an FTP proxy is used for file transfers. Such proxies are called "application-level proxies” because they are dedicated to a particular application and protocol, and are aware of the content of the packets being sent.

**Authenticated Proxy User** – A user who has been identified and authenticated to satisfy the requirements for using a proxy according to the authenticated policy enforced by the TOE. A “proxy user” is any user, either authenticated or not, who is sending traffic through a proxy according to any security policy enforced by the TOE. A “remote proxy user” is a proxy user who is also a remote user.

**Authorized IT entity** – Any IT entity outside the TOE that may, in accordance with the SFRs, perform an operation on the TOE.

**Local Administration Console** – This is a physically connected, generic hardware platform (part of the IT environment) running the McAfee Firewall Administration Console client (part of the TOE). Both the local administration console hardware and its network connection to the McAfee Firewall are physically protected. McAfee Firewall must be configured to accept administrative commands from the local administration console.

**Local Administrator** – This is an administrator who uses a local administration console to manage McAfee Firewall.

**Remote Administration Console** – This is also a generic hardware platform running the McAfee Firewall Administration Console client; it has a network connection to McAfee Firewall, but it is not a local administration console. McAfee Firewall must be configured to accept administrative commands from such a remote administration console.

**Remote User** - A user that communicates with the TOE by means of a network connection. Since administrators are users, a “remote administrator” is an administrator who is also a remote user.

**Remote Administrator** – This is an administrator who uses a remote administration console or Control Center to manage the McAfee Firewall.

**Single-Use Authentication** –Data for single-use authentication can be something the user has or knows, but not something the user is. Examples of single-use authentication data include single-use passwords, encrypted time-stamps, and/or random numbers from a secret lookup table.

The following abbreviations are used in this Security Target:

| | |
|---|---|
| AES | Advanced Encryption Standard |
| ANSI | American National Standards Institute |
| BSD | Berkley Software Distribution |
| CC | Common Criteria for Information Technology Security Evaluation |
| CD | Compact Disk |
| CLSOS | Cryptographic Library for SecureOS |
| CPU | Central Processing Unit |
| DSA | Digital Signature Algorithm |
| EAL | Evaluation Assurance Level |
| ECB | Electronic Codebook |
| ESP | Encapsulating Security Payload |
| FIPS | Federal Information Processing Standard |
| FIPS PUB | Federal Information Processing Standard Publication |
| FLR | Flaw Remediation |
| FTP | File Transfer Protocol |
| GHz | Gigahertz |

| | |
|---|---|
| GUI | Graphical User Interface |
| HTTP | Hypertext Transfer Protocol |
| HTTPS | Hypertext Transfer Protocol Secure |
| I&A | Identification and Authentication |
| ICMP | Internet Control Message Protocol |
| IKE | Internet Key Exchange |
| IPSEC | Internet Protocol Security |
| IT | Information Technology |
| KCLSOS | Kernel Cryptographic Library for SecureOS |
| LAN | Local Area Network |
| MB | Megabyte |
| MMU | Memory Management Unit |
| NAT | Network Address Translation |
| NTP | Network Time Protocol |
| OS | Operating System |
| OSP | Organizational Security Policy |
| PC | Personal Computer |
| PP | Protection Profile |
| PS/2 | Personal System/2 |
| RAM | Random Access Memory |
| RDSA | RSA Digital Signature Algorithm |
| RFC | Request For Comment |
| RNG | Random Number Generator |
| SA | Security Association |
| SAR | Security Assurance Requirement |
| SFP | Security Function Policy |
| SFR | Security Functional Requirement |
| SHA | Secure Hash Algorithm |
| SMTP | Simple Mail Transfer Protocol |
| SSL | Secure Sockets Layer |
| ST | Security Target |
| SVGA | Super Video Graphics Array |
| TCP/IP | Transmission Control Protocol/Internet Protocol |
| TLS | Transport Layer Security |

| | |
|---|---|
| TOE | Target of Evaluation |
| TSC | TSF Scope of Control |
| TSF | TOE Security Functions |
| TSP | TOE Security Policy |
| URL | Uniform Resource Locator |
| US | United States |
| VPN | Virtual Private Network |

## 1.6 References

The following documentation was used to prepare this ST:

| | |
|---|---|
| [CC_PART1] | Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated July 2009, version 3.1 revision 3, CCMB-2009-07-001. |
| [CC_PART2] | Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated July 2009, version 3.1 revision 3, CCMB-2009-07-002. |
| [CC_PART3] | Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated July 2009, version 3.1 revision 3, CCMB-2009-07-003. |
| [CEM] | Common Methodology for Information Technology Security Evaluation – July 2009, version 3.1 revision 3, CCMB-2009-07-004. |
| [FWPP] | U.S. Government Protection Profile for Application-level Firewall in Basic Robustness Environments Version 1.1, July 25, 2007. |
| [FIPS 140-2] | Security Requirements for Cryptographic Modules, Federal Information Processing Standard , May 2001 |
| [FIPS 180-3] | Secure Hash Standard (SHS), Federal Information Processing Standard, Oct 2008 |
| [FIPS 197] | Advanced Encryption Standard, Federal Information Processing Standard, Nov 2001 |
| [SP 800-57] | Recommendation for Key Management, NIST Special Publication, March 2007 |

# 2 TOE Description

This section provides context for the TOE evaluation by identifying the product type and describing the evaluated configuration.

## 2.1 Product Type

The McAfee Firewall, operating with two or more network interfaces, provides a hybrid firewall solution that supports both application-level proxy and packet filtering. The McAfee Firewall software version consists of a collection of integrated firewall applications and SecureOS, a secure operating system. This OS is an extended version of the FreeBSD UNIX operating system. It includes McAfee's patented Type Enforcement security technology, additional network separation control, network-level packet filtering support and improved auditing facilities. SecureOS also provides the secured computing environment in which all McAfee Firewall application layer processing is done. McAfee Firewall also provides VPN capability between separated network enclaves.

In addition to the McAfee Firewall hardware or virtual platform running the firewall application with SecureOS, the TOE also includes one of the following two configurations:

Configuration A

The Admin Console client software (McAfee Firewall Enterprise (Sidewinder) Admin Console). The Admin Console is separately installed on a generic Windows platform that is part of the IT environment: it is used to manage McAfee Firewall.

*Configuration B*

The McAfee Firewall Enterprise Control Center (“Control Center”) Management server software, the FIPS compliant hardware or virtual platform for running the Control Center Management server software, and the Control Center client software.

## 2.2 Application Context

McAfee Firewall operates in an environment where it provides a single point of connectivity between at least two networks. Typically one network is viewed as the inside of an organization, where there is some assumption of control over access to the computing network. The other network is typically viewed as an external network, similar to the Internet, where there is no practical control over the actions of its processing entities. McAfee Firewall's role is to limit and control all information flow between the networks.

## 2.3 Physical and Logical Boundaries

### 2.3.1 Evaluation Application Context

The following contextual assumptions apply to the TOE:

a) It shall be newly installed and configured in accordance with the directives contained in the supplied guidance documentation;
b) Physical access to the configured McAfee Firewall shall be controlled;
c) The configured McAfee Firewall shall be connected only to networks between which it controls information flow;
d) The configured McAfee Firewall shall manage traffic for at least two (2) networks, at least one of which is designated as internal and one is designated as external;

e) The configured McAfee Firewall shall support administrative operations via a GUI application, known as Admin Console, running on a Windows system, or via Control Center;
f) If the configured McAfee Firewall is connected to an administrative workstation either directly or remotely, the communications are encrypted using TLS and the workstation is physically protected;
g) If the configured McAfee Firewall is connected to Control Center, the communications between the McAfee Firewall and the Control Center Management server, and between the Control Center Management server and the Control Center client are encrypted using TLS, and Control Center client and server are physically protected;
h) Only authorized administrators shall be allowed physical access to the McAfee Firewall hardware computing platform, or to the administrative workstation, or to Control Center Management Server and Client, for such purposes as starting the system.

### 2.3.2 Proxy agents to be Evaluated

The FTP, HTTP, HTTPS, SMTP, Telnet, and Generic proxy agents are all included within the scope of the evaluation. Other protocol-aware proxy agents and services provided by McAfee Firewall are excluded from the scope of the evaluation.

### 2.3.3 Features not to be Evaluated

McAfee Firewall provides additional capabilities by means of optional “add-on” features that require additional equipment and/or licensing. The following extra functionality of this type is specifically excluded from the scope of this evaluation:

a) Anti-Virus;
b) SmartFilter (URL Filtering);
c) Signature based IPS;
d) Policy Acceleration Network Cards;
e) SSL Termination;
f) Network analysis capability;
g) Security Reporter (optional tool to view audit).

McAfee Firewall includes functions that are explicitly excluded from the scope of the evaluation:

a) Built-in servers other than ICMP;
b) Trusted Source (reputation service for email senders);
c) Use of the command line to manage the TOE (disabled in the evaluated configuration).

### 2.3.4 Physical Scope and Boundary

The TOE consists of McAfee Firewall software version 8.3.2, which includes the firewall application and the SecureOS operating system, running on a dedicated McAfee appliance platform or virtual appliance.

The TOE includes the Admin Console client software (the McAfee Firewall Enterprise (Sidewinder) Admin Console version 5.09). This software is provided with every McAfee Firewall appliance, and it is also provided as a separate part of every McAfee Firewall software product distribution. The administration client software runs on a generic

computing platform with a Windows operating system. However, the platform and Windows OS are not part of the TOE.

The TOE also includes the Control Center Management Server version 5.3.2, its dedicated McAfee (FIPS compliant) hardware platform or virtual appliance, and the Control Center Client software version 5.3.2. The Control Center Client software runs on a generic computing platform with a Windows operating system. However, the client platform and Windows OS are not part of the TOE.

#### 2.3.4.1 TOE Environment Requirements

The McAfee Firewall appliance is configured to control the flow of TCP/IP traffic between two network interfaces. McAfee offers a family of appliance models with various hardware combinations to address a wide range of customer performance needs.

In addition, a generic hardware platform is required in the IT environment to run the McAfee Firewall Admin Console software for remote or local administration, or the Control Center client software for remote administration. The evaluated configuration must include at least one administration console. The minimum configuration required for this platform is as follows:

- CPU: Intel, 3GHz
- RAM: 1 GB
- OS: MS Windows 2008 Server, Windows XP Professional, Windows Vista or Windows 7
- Media:
  - Minimum of 750 MB of available disk storage
  - CD drive
- Network: One network interface
- USB port
- SVGA video and display
- PS/2 or Serial Mouse
- Keyboard

The McAfee Firewall is available in two virtual forms: the Multi-Firewall Edition, provided in partnership with VMware, and the Virtual Appliance. The Multi-Firewall Edition appliance models come preinstalled on the same Dell or Intel hardware used for non-virtual appliances, preloaded with either 4, 8, 16 or 32 virtual firewalls, VMware vSphere Hypervisor (ESXi) operating system, and a virtual instance of McAfee Firewall Enterprise Control Center. The Virtual Firewall is delivered as software only, and is intended to be installed on existing VMware infrastructure installed on ESXi Hypervisor.

The current McAfee Firewall Enterprise platforms are:

- McAfee appliances: S1104, S2008, S3008, S4016, S5032, S6032, S7032, 1100F, 2150F, 4150F, 1100E, 2100E, 2150E, 4150E,
- Virtual: VMware vSphere Hypervisor (ESXi) version 5.0

The current McAfee Firewall Enterprise Control Center platforms are:

- McAfee appliances: C1015, C2050 and C3000
- Virtual: VMware vSphere Hypervisor (ESXi) version 5.0

The current CloudShield platform is:

- CloudShield CS-4000

All specific TOE or TOE Environment settings and requirements are documented in guidance supplied with the TOE.

#### 2.3.4.2 Hardware Security Considerations

No extraordinary security demands are placed upon the hardware platforms and peripheral equipment used by the McAfee Firewall software. This equipment is expected to meet the customary demands for reliable operation of typical Unix or Microsoft Servers as provided by standard Intel PC computing platforms. The security features assumed to be present and operational on the hardware platforms include:

- The CPU must provide a two-state processing model to support the separation of the kernel processing from the application processing.
- The CPU and /or the supporting motherboard must provide a Memory Management Unit (MMU) to support separate memory spaces for the kernel and each process.
- The system motherboard must provide a battery backup for the clock to maintain time information when the system is shut down. Also the CPU or ancillary hardware must provide a periodic timer to support the internal time management within the kernel.
- If any of the network interface cards support features such as wake-on LAN, special external command features, or special protocol processing, the hardware connections to support those features should not be connected. In the evaluated configuration, McAfee Firewall will not enable any such special features.

For those instances of the TOE that run on VMware, the virtual environment is assumed to emulate these hardware security features. Secure isolation of the virtual environments is the responsibility of the VMware environment, and is outside the scope of this ST.

### 2.3.5 Logical Scope and Boundary

The TOE with support from the IT environment provides the following security features:

a) Security Management [SF_FMT]
b) Identification and Authentication [SF_FIA]
c) User Data Protection [SF_FDP]
d) Protection of Security Functions [SF_FPT]
e) Audit [SF_FAU]
f) Cryptographic support [SF_FCS]

#### 2.3.5.1 Security Management

Management of the McAfee Firewall may be carried out using either the McAfee Firewall Admin Console or McAfee Firewall Enterprise Control Center.

An administrator can use the McAfee Firewall Admin Console client (part of the TOE) to communicate with the McAfee Firewall remotely or via a locally connected network. All administration consoles, whether they are local or remote, use the same management interface and encrypted communications.

Alternatively, an administrator can use the Control Center client, running on a Windows computer (part of the IT environment), to perform management functions on the McAfee Firewall. This interface modifies firewall configurations stored on the Control Center Management server, and these are then deployed to the specified firewalls. All communications are encrypted.

#### 2.3.5.2 Identification and Authentication

The McAfee Firewall TOE, along with support from the IT environment, supports standard UNIX password authentication. Identification attributes are assigned to each administrative user and each authenticated proxy user. McAfee Firewall gathers data from the user and the associated service connection, and consults the rules to determine what form of authentication is required for the service (including use of an external authentication server). McAfee Firewall consults its stored user information, determines the password's validity, and enforces the result of the validity check.

McAfee Firewall provides a mechanism for managing user access following authentication failures. McAfee Firewall also strictly limits the actions it will perform on behalf of a user before the user is authenticated.

When establishing VPNs, McAfee Firewall will exchange identities and perform device-level authentication of the remote device (peer McAfee Firewall or remote VPN gateway). Device-level authentication is performed using authentication techniques specified in RFC 2409 and RFC 4306. Peers will mutually authenticate themselves to each other before establishing the secure channel.

#### 2.3.5.3 User Data Protection

McAfee Firewall allows an administrator to define security attributes to permit or deny information flows to or through the TOE. The set of security attributes will include items such as source and destination identification, application signatures, application level commands and user authentication. The TOE Administrator uses the security attributes to construct one or more access control rules. Packets arriving at the TOE interface are compared to the security attributes in the rules. When the packet attributes "match" the rules security attributes, that packet or connection is explicity approved or disapproved; otherwise the packet is dropped and the connection disallowed. In addition to restricting access via the rules, the TOE must generate and maintain "state" information for all approved connections mediated by the TOE. The TOE utilizes the "state" information to monitor the status of an approved connection and validate incoming packets purporting to be part of an approved connection.

McAfee Firewall restricts information flows via application level commands by incorporating application proxies. Proxies understand the operation of a particular application protocol and can filter the application data portion of a packet according to Administrator defined security attributes (e.g. commands, data types, etc.). Proxies originate all proxy controlled information flows through the TOE on behalf of the communicating end points, which are not allowed to establish a direct connection through the TOE. In the evaluated configuration, McAfee Firewall provides 4 application proxies that can be configured to require user authentication: FTP, Telnet, HTTP and HTTPS. McAfee Firewall also provides a proxy for SMTP and a generic proxy that don't require user authentication. In the evaluated configuration, the FTP, Telnet, HTTP and HTTPS proxies can also be configured without requiring user authentication.

McAfee Firewall uses the same security attributes discussed above to control access to its own services. McAfee Firewall supports Internet Control Message Protocol (ICMP) as an unauthenticated information flow, which can be enabled or disabled.

McAfee Firewall also allows an administrator to establish a VPN policy to control data flows with remote VPN devices. McAfee Firewall provides for authentication to and from the

remote device, agreement on cryptographic keys and algorithms, secure generation and distribution of session keys, and encryption of network traffic in accordance with the policy.

User data is protected by different facilities depending upon the protocol and stage of processing. While user data is within the network stack, it is part of the kernel memory space, and as such is protected from all user state processing elements on the system. While user data is in the control of a proxy process, it is protected by the SecureOS processing model and Type Enforcement facilities.

McAfee Firewall network stack processing ensures that there is no leakage of residual information from previous packets to new packets as they are transferred through the firewall. The memory system zeros storage blocks before they are reused to prevent residual information leakage.

#### 2.3.5.4 Protection of Security Functions

McAfee Firewall, with its SecureOS operating system, has been designed to be highly resistant to both malicious and accidental attack. It includes system elements that provide several levels of protection for its security functions.

The lowest level of protection is provided by the computing platform Central Processing Unit (CPU). The CPU provides a two-state processing model that limits access to certain privileged instructions to the SecureOS kernel. The SecureOS kernel provides a second layer of protection by limiting user mode access to kernel memory. SecureOS also extends the normal FreeBSD UNIX network stack processing with additional separation control to restrict inter-process communication to certain interfaces.

SecureOS includes McAfee's patented Type Enforcement facilities that enforce mandatory security policy control over all user state processing. The Type Enforcement policy data is loaded onto the system during installation and cannot be modified on an operational system. Type Enforcement ensures that critical data is accessible only via programs designed to use the data and that the impact of any failure will be confined in scope.

McAfee Firewall also provides a reliable time stamp that is used by its audit mechanism.

#### 2.3.5.5 Audit

SecureOS supplements the normal UNIX Syslog Facilities by providing an audit device to which all processes and the kernel may write audit data. The SecureOS audit device adds security relevant information, such as the time and the identity of the generating process, to the audit data when it passes through the device within the kernel.

The Administrator can view the contents of the audit records, and delete the audit trail. McAfee Firewall provides a sort and search capability to improve audit analysis.

The Administrator can configure auditable events, and can configure the TOE to take appropriate actions in the event that the audit trail is close to being exhausted. The TOE provides the Administrator with a configurable audit trail threshold to track the storage capacity of the audit trail. As soon as the threshold is met, the TOE generates an audit record and displays a message on the console. In addition to displaying the message, the Administrator may configure the TOE to prevent all auditable events except for those performed by the Administrators, or may configure the TOE to overwrite the oldest audit records in the audit trail.

#### 2.3.5.6 Cryptographic support

McAfee Firewall establishes encrypted communications (acting as the initiator or responder) with authorized remote users and external IT entities. McAfee Firewall includes a software cryptographic module that is validated to FIPS 140-2 (Level 1) as a minimum. McAfee Firewall performs data encryption/decryption using the Advanced Encryption Standard (AES) algorithm with a minimum key size of 128 bits. McAfee Firewall also performs digital signature generation/verification, random number generation and cryptographic hashing.

McAfee Firewall implements VPN mechanisms using cryptography and key management, using algorithms that have been validated to FIPS 140-2 (Level 1) as a minimum.

## 2.4 TOE Documentation

McAfee offers a series of documents that describe the installation of McAfee Firewall as well as guidance for subsequent use and administration of the applicable security features.

# 3 Security problem definition

This section sets out the threats, assumptions and organisational security policies for the TOE. These are all taken from [FWPP].

## 3.1 Assumptions

The following conditions are assumed to exist in the operational environment.

| | |
|---|---|
| A.PHYSEC | The TOE is physically secure. |
| A.LOWEXP | The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low. |
| A.GENPUR | There are no general-purpose computing capabilities (e.g. the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE. |
| A.PUBLIC | The TOE does not host public data. |
| A.NOEVIL | Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error. |
| A.SINGEN | Information cannot flow among the internal and external networks unless it passes through the TOE. |
| A.DIRECT | Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE. |
| A.NOREMO | Human users who are not authorized administrators cannot access the TOE remotely from the internal or external networks.[1] |
| A.REMACC | Authorized administrators may access the TOE remotely from the internal and external networks. |

## 3.2 Threats

The following threats are addressed either by the TOE or the environment.

### 3.2.1 Threats Addressed by the TOE

The threat agents are either unauthorized persons or external IT entities not authorized to use the TOE itself.

| | |
|---|---|
| T.NOAUTH | An unauthorized person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE. |
| T.REPEAT | An unauthorized person may repeatedly try to guess authentication data in order to use this information to launch attacks on the TOE. |

[1] All assumptions in this ST are taken from [FWPP]. The assumption is interpreted to refer to direct access to TOE administrative functions, rather than to send traffic via the TOE. As such, the assumption is unnecessary, since such access is controlled via TOE identification and authentication controls, and also requires access to the management application.

| | |
|---|---|
| T.REPLAY | An unauthorized person may use valid identification and authentication data obtained to access functions provided by the TOE. |
| T.ASPOOF | An unauthorized person on an external network may attempt to by-pass the information flow control policy by disguising authentication data (e.g. spoofing the source address) and masquerading as a legitimate user or entity on an internal network. |
| T.MEDIAT | An unauthorized person may send impermissible information through the TOE, which results in the exploitation of resources on the internal network. |
| T.OLDINF | Because of a flaw in the TOE functioning, an unauthorized person may gather residual information from a previous information flow or internal TOE data by monitoring the padding of the information flows from the TOE. |
| T.PROCOM | An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete security related information that is sent between a remotely located authorized administrator and the TOE. |
| T.AUDACC | Persons may not be accountable for the actions that they conduct because the audit records are not reviewed, thus allowing an attacker to escape detection. |
| T.SELPRO | An unauthorized person may read, modify, or destroy security critical TOE configuration data. |
| T.AUDFUL | An unauthorized person may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attackers actions. |
| T. LOWEXP | The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low. |
| T.NETSEC | An unauthorised person or unauthorised external I T entity may be able to view or modify private information that is sent between the TOE and another TOE or trusted IT product. |

### 3.2.2 Threat to be Addressed by Operating Environment

The threat possibility discussed below must be countered by procedural measures and/or administrative methods.

| | |
|---|---|
| T.TUSAGE | The TOE may be inadvertently configured, used, and administered in an insecure manner by either authorized or unauthorized persons. |

## 3.3 Organisational security policies

US Federal agencies are required to protect sensitive but unclassified information with cryptography. The following organisational security policy must be met:

| | |
|---|---|
| P.CRYPTO | AES (Advanced Encryption Standard as specified in FIPS 197) encryption (as specified in SP 800-67) must be used to protect remote administration functions, and the associated cryptographic module must comply, at a minimum, with [FIPS 140-2] (level 1). |

# 4 Security objectives

## 4.1 Security objectives for the TOE

The following are the IT security objectives for the TOE:

| | |
|---|---|
| O.IDAUTH | The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to TOE functions or, for certain specified services, to a connected network. |
| O.SINUSE | The TOE must prevent the reuse of authentication data for users attempting to authenticate to the TOE from a connected network. |
| O.MEDIAT | The TOE must mediate the flow of all information between clients and servers located on internal and external networks governed by the TOE, and must ensure that residual information from a previous information flow is not transmitted in any way. |
| O.SECSTA | Upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE must not compromise its resources or those of any connected network. |
| O.ENCRYP | The TOE must protect the confidentiality of its dialogue with an authorized administrator through encryption, if the TOE allows administration to occur remotely from a connected network. |
| O.SELPRO | The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions. |
| O.AUDREC | The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search and sort the audit trail based on relevant attributes. |
| O.ACCOUN | The TOE must provide user accountability for information flows through the TOE and for authorized administrator use of security functions related to audit. |
| O.SECFUN | The TOE must provide functionality that enables an authorized administrator to use the TOE security functions, and must ensure that only authorized administrators are able to access such functionality. |
| O.LIMEXT | The TOE must provide the means for an authorized administrator to control and limit access to TOE security functions by an authorized external IT entity. |
| O.EAL | The TOE must be structurally tested and shown to be resistant to obvious vulnerabilities. |
| O.NETSEC | The TOE must provide a means to maintain the confidentiality and integrity of information sent between itself and another instance of the TOE or other trusted IT product. |

For a detailed mapping between threats and the IT security objectives listed above, see section 7.1 of the Rationale.

## 4.2 Security objectives for the environment

All of the assumptions stated in section 3.1 are considered to be security objectives for the environment. The following are the security objectives that, in addition to those assumptions, are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

| | |
|---|---|
| OE.PHYSEC | The TOE is physically secure. |
| OE.LOWEXP | The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low. |
| OE.GENPUR | There are no general-purpose computing capabilities (e.g. the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE. |
| OE.PUBLIC | The TOE does not host public data. |
| OE.NOEVIL | Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error. |
| OE.SINGEN | Information cannot flow among the internal and external networks unless it passes through the TOE. |
| OE.DIRECT | Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g. a console port) if the connection is part of the TOE. |
| OE.NOREMO | Human users who are not authorized administrators cannot access the TOE remotely from the internal or external networks. |
| OE.REMACC | Authorized administrators may access the TOE remotely from the internal and external networks. |
| OE.GUIDAN | The TOE must be delivered, installed, administered, and operated in a manner that maintains security. |
| OE.ADMTRA | Authorized administrators must be trained as to establishment and maintenance of security policies and practices. |
| OE.SINUSE | The TOE must prevent the reuse of authentication data for users attempting to authenticate to the TOE from a connected network. [2] |

For a detailed mapping between threats, assumptions, and the security objectives listed above see section 7.1 of the Rationale.

[2] This objective for the environment is included to reflect the use in this ST of an authentication server in the environment.

# 5 Security requirements

This section provides functional and assurance requirements that must be satisfied by the TOE. These requirements are expressed using functional components from Part 2 of the CC, and assurance components, including Evaluation Assurance Level (EAL), taken from Part 3 of the CC.

## 5.1 Security functional requirements

The security functional requirements for the TOE are summarised in the table below. They are a superset of [FWPP], with additions for VPN, use of an external authentication server and key management. Extended components are indicated by (X). Additions to the PP are indicated by *.

| | |
|---|---|
| FMT_SMR.1 | Security roles |
| FIA_ATD.1 | User attribute definition |
| FIA_UID.2 | User identification before any action |
| FIA_AFL.1 | Authentication failure handling |
| FIA_UAU.5 | Multiple authentication mechanisms |
| FIA_UAU.8 (x)* | Invocation of authentication mechanism |
| FIA_SOS.2* | TSF generation of secrets |
| FDP_IFC.1 (1) | Subset information flow control (1) |
| FDP_IFC.1 (2) | Subset information flow control (2) |
| FDP_IFC.1 (3)* | Subset information flow control (3) |
| FDP_IFF.1 (1) | Simple security attributes (1) |
| FDP_IFF.1 (2) | Simple security attributes (2) |
| FDP_IFF.1 (3)* | Simple security attributes (3) |
| FDP_UCT.1* | Basic data exchange confidentiality |
| FTP_ITC.1* | Inter-TSF trusted channel |
| FMT_MSA.1 (1) | Management of security attributes (1) |
| FMT_MSA.1 (2) | Management of security attributes (2) |
| FMT_MSA.1 (3) | Management of security attributes (3) |
| FMT_MSA.1 (4) | Management of security attributes (4) |
| FMT_MSA.1 (5) | Management of security attributes (5) |
| FMT_MSA.1 (6) | Management of security attributes (6) |
| FMT_MSA.3 | Static attribute initialization |
| FMT_MTD.1 (1) | Management of TSF data (1) |
| FMT_MTD.1 (2) | Management of TSF data (2) |
| FMT_MTD.2 | Management of limits on TSF data |

| | |
|---|---|
| FDP_RIP.1 | Subset residual information protection |
| FCS_COP.1 (1) | Cryptographic operation |
| FCS_COP.1 (2)* | Cryptographic operation |
| FCS_COP.1 (3)* | Cryptographic operation |
| FCS_COP.1 (4)* | Cryptographic operation |
| FCS_CKM.1 (1)* | Cryptographic key generation |
| FCS_CKM.1 (2)* | Cryptographic key generation |
| FCS_CKM.4* | Cryptographic key destruction |
| FPT_STM.1 | Reliable time stamps |
| FAU_GEN.1 | Audit data generation |
| FAU_SAR.1 | Audit review |
| FAU_SAR.3 | Selectable audit review |
| FAU_STG.1 | Protected audit trail storage |
| FAU_STG.4 | Prevention of audit data loss |
| FMT_MOF.1 (1) | Management of security functions behaviour (1) |
| FMT_MOF.1 (2) | Management of security functions behaviour (2) |

**Table 5.1**

### 5.1.1 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the role [authorized administrator].

FMT_SMR.1.2 The TSF shall be able to associate users with the authorized administrator role.

### 5.1.2 FIA_ATD.1 User attribute definition

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

a) identity;

b) association of a human user with the authorized administrator role;

**c) hashed value of password**

**d) login specific data**].

### 5.1.3 FIA_UID.2 User identification before any action

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

### 5.1.4 FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when [a non-zero number determined by the authorized administrator] **of** unsuccessful authentication attempts occur related to [authorized TOE administrator access or authorized TOE IT entity access].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [prevent the offending user from successfully authenticating until an authorized administrator takes some action to make authentication possible for the user in question].

### 5.1.5 FIA_UAU.5 Multiple authentication mechanisms

FIA_UAU.5.1 The TSF shall provide [password and single-use authentication mechanisms] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [following multiple authentication mechanism rules:

a) single-use authentication mechanism shall be used for authorized administrators to access the TOE remotely such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that authorized administrator;

b) single-use authentication mechanism shall be used for authorized external IT entities accessing the TOE such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that authorized external IT entity;

c) single-use authentication mechanism shall be used for human users sending or receiving information through the TOE using **HTTP, HTTPS,** FTP or Telnet such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that human user;

d) reusable password mechanism shall be used for authorized administrators to access the TOE via a directly connected terminal such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that authorized administrator].

*Application Notes:*
*1. In the above list a) refers to remote administration, b) relates to VPN, c) relates to proxy users, and d) relates to local console access.*
*2. Under item c) it should be noted that the requirement for FTP, HTTP and HTTPS authentication is a configurable option in the TOE. This also applies to item c) under FIA_UAU.8.*
*3. The single-use authentication mechanism is provided in conjunction with the following requirement, FIA_UAU.8, which invokes a single-use authentication mechanism from the TOE operating environment. This approach is consistent with the industry view that a firewall supplier should not mandate selection of a single (possibly weak) single-use authentication product, but should allow choice of state of the art products from a range of third party vendors. The "directly connected terminal" for authorized administrator access is provided by an administration workstation connected to the TOE via a protected local area network.*

### 5.1.6 FIA_UAU.8 (X) Invocation of authentication mechanism

FIA_UAU.8.1 (X) The TSF shall invoke the external single-use authentication server to authenticate a user's claimed identity according to [**the following rules:**

**a) single-use authentication mechanism shall be used for authorized administrators to access the TOE remotely such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that authorized administrator;**

**b) single-use authentication mechanism shall be used for authorized external IT entities accessing the TOE such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that authorized external IT entity;**

**c) Single-use authentication mechanism shall be used for human users sending or receiving information through the TOE using HTTP, HTTPS, FTP or Telnet such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that human user**].

### 5.1.7 FIA_SOS.2 TSF Generation of secrets

FIA_SOS.2.1 The TSF shall provide a mechanism to generate secrets that meet [**random number generation (RNG) services in accordance SP 800-90A, seeded by one or more independent software-based entropy sources**].

FIA_SOS.2.2 The TSF shall be able to enforce the use of TSF generated secrets for [**all applicable cryptographic services**].

Requirements Overview: This Security Target includes multiple information flow control Security Function Policies (SFPs). The CC allows multiple policies to exist, each having a unique name. This is accomplished by iterating FDP_IFC.1 for each of the three named information flow control policies. The first policy identified is called the UNAUTHENTICATED SFP. The subjects under control of this policy are external IT entities on an internal or external network sending information through the TOE to other external IT entities. The second policy identified is called the AUTHENTICATED SFP. The subjects under control of this policy are human users on an internal or external network who must be authenticated at the TOE before using the services in FIA_UAU.5 and FIA_UAU.8. The third policy identified is called the VPN SFP. The subjects under control of this policy are network interfaces for the TOE or other IT products. The information flowing between subjects in all policies is traffic with attributes, defined in FDP_IFF.1.1, including source and destination addresses. The rules that define each information flow-control SFP are found in FDP_IFF.1.2. Component FDP_IFF.1 is iterated three times to correspond to each of the three iterations of FDP_IFC.1.

### 5.1.8 FDP_IFC.1 Subset information flow control (1)

Note: This first policy identified is called the UNAUTHENTICATED SFP. The subjects under control of this policy are external IT entities on an internal or external network sending information through the TOE to other external IT entities.

FDP_IFC.1.1(1) The TSF shall enforce the [UNAUTHENTICATED SFP] on:

a) [subjects: unauthenticated external IT entities that send and receive information through the TOE to one another;

b) information: traffic sent through the TOE from one subject to another;

c) operation: pass information].

### 5.1.9 FDP_IFC.1 Subset information flow control (2)

Note: This second policy is called the AUTHENTICATED SFP. The subjects under control of this policy are human users on an internal or external network who must be authenticated to the TOE.

FDP_IFC.1.1(2) The TSF shall enforce the [AUTHENTICATED SFP] on:

a) [subjects: a human user or external IT entity that sends and receives FTP**, HTTP, HTTPS** and Telnet information through the TOE to one another, only after the human user initiating the information flow has authenticated at the TOE per FIA_UAU.5 **and FIA_UAU.8(X)**;

b) information: FTP**, HTTP, HTTPS** and Telnet traffic sent through the TOE from one subject to another;

c) operation: initiate service and pass information].

### 5.1.10 FDP_IFC.1 Subset information flow control (3)

Note: This third policy is called the VPN SFP. The subjects under control of this policy are interfaces of the TOE or other trusted IT products on an internal or external network where private communication is required.

FDP_IFC.1(3) The TSF shall enforce the [**VPN SFP**] on:[

**a) source subject: TOE or other IT product interface on which information is received;**
**b) destination subject: TOE or other IT product interface to which information is destined;**
**c) information: network packets;**
**d) operations:**

**i) pass packets without modifying;**

**ii) send IPSEC encrypted and authenticated packets to a peer TOE or other IT product using ESP in tunnel mode;**

**iii) decrypt, verify authentication and pass received packets from a peer TOE or other IT product in tunnel mode using ESP**].

### 5.1.11 FDP_IFF.1 Simple security attributes (1)

FDP_IFF.1.1(1) The TSF shall enforce the [UNAUTHENTICATED SFP] based on at least the following types of subject and information security attributes:

[a) subject security attributes:

•presumed address,

•no other subject security attributes;

b) information security attributes:

•presumed address of source subject;

•presumed address of destination subject;

•transport layer protocol;

•TOE interface on which traffic arrives and departs;

•service **(application signature);**

•**destination service port range**].

FDP_IFF.1.2(1) The TSF shall permit an information flow between a controlled subject and another controlled subject via a controlled operation if the following rules hold:

[a) Subjects on an internal network can cause information to flow through the TOE to another connected network if:

•all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;

•the presumed address of the source subject, in the information, translates to an internal network address;

•and the presumed address of the destination subject, in the information, translates to an address on the other connected network.

b) Subjects on the external network can cause information to flow through the TOE to another connected network if:

•all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;

•the presumed address of the source subject, in the information, translates to an external network address;

•and the presumed address of the destination subject, in the information, translates to an address on the other connected network.]

FDP_IFF.1.3(1) The TSF shall enforce the [none].

FDP_IFF.1.4(1) The TSF shall explicitly authorize an information flow based on the following rules: [none].

FDP_IFF.1.5(1) The TSF shall explicitly deny an information flow based on the following rules:

[a) The TOE shall reject requests for access or services where the information arrives on an external TOE interface, and the presumed address of the source subject is an external IT entity on an internal network;

b) The TOE shall reject requests for access or services where the information arrives on an internal TOE interface, and the presumed address of the source subject is an external IT entity on the external network;

c) The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on a broadcast network;

d) The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on the loopback network;

e) The TOE shall reject requests in which the subject specifies the route in which information shall flow en route to the receiving subject; and

f) For the **FTP, HTTP, HTTPS and SMTP application protocols** ~~supported by the TOE (e.g., DNS, HTTP, SMTP, and POP3)~~, the TOE shall deny any access or service requests that do not conform to its associated published protocol specification (e.g. RFC). This shall be accomplished through protocol filtering proxies that are designed for that purpose.

*Application Note: The generalized wording of the FDP_IFF.1.5f) requirement has been modified from the PP to make it clear that only HTTP, HTTPS and SMTP are included in the TOE (while DNS and POP3 application-level proxies are not included in the TOE).*

### 5.1.12 FDP_IFF.1 Simple security attributes (2)

FDP_IFF.1.1(2) The TSF shall enforce the [AUTHENTICATED SFP] based on at least the following types of subject and information security attributes:

[a) subject security attributes:

- presumed address;
- no other subject security attributes;

b) information security attributes:

- user identity;
- presumed address of source subject;
- presumed address of destination subject;
- transport layer protocol;
- TOE interface on which traffic arrives and departs;
- service (i.e. FTP, Telnet**, HTTP and HTTPS**);
- security-relevant service command;
- **destination service port range;**
- **application signature**].

FDP_IFF.1.2(2) The TSF shall permit an information flow between a controlled subject and another controlled subject via a controlled operation if the following rules hold:

[a) Subjects on an internal network can cause information to flow through the TOE to another connected network if:

• the human user initiating the information flow authenticates according to FIA_UAU.5 **and FIA_UAU.8**;

• all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;

• the presumed address of the source subject, in the information, translates to an internal network address;

• and the presumed address of the destination subject, in the information, translates to an address on the other connected network.

b) Subjects on the external network can cause information to flow through the TOE to another connected network if:

• the human user initiating the information flow authenticates according to FIA_UAU.5 **and FIA_UAU.8**;

• all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;

• the presumed address of the source subject, in the information, translates to an external network address; and

• the presumed address of the destination subject, in the information, translates to an address on the other connected network.]

FDP_IFF.1.3(2) The TSF shall enforce the [none].

FDP_IFF.1.4(2) The TSF shall explicitly authorize an information flow based on the following rules: [none].

FDP_IFF.1.5(2) The TSF shall explicitly deny an information flow based on the following rules:

[a) The TOE shall reject requests for access or services where the information arrives on an external TOE interface, and the presumed address of the source subject is an external IT entity on an internal network;

b) The TOE shall reject requests for access or services where the information arrives on an internal TOE interface, and the presumed address of the source subject is an external IT entity on the external network;

c) The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on a broadcast network;

d) The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on the loopback network;

e) The TOE shall reject requests in which the subject specifies the route in which information shall flow en route to the receiving subject; and

f) The TOE shall reject Telnet, FTP**, HTTP and HTTPS** command requests that do not conform to generally accepted published protocol definitions (e.g., RFCs). This must be accomplished through protocol filtering proxies designed for that purpose.

*Application Note: The TOE can make no claim as to the real address of any source or destination subject, and therefore the TOE can only suppose that these addresses are accurate. Therefore, a "presumed address" is used to identify source and destination addresses.*

### 5.1.13 FDP_IFF.1 Simple security attributes (3)

FDP_IFF.1.1(3) The TSF shall enforce the [**VPN SFP**] based on the following types of subject and information security attributes:

[**a) Source subject security attributes: set of source subject identifiers;**

**b) Destination subject security attributes: set of destination subject identifiers;**

**c) Information security attributes: presumed identity of source subject,identity of destination subject**].

FDP_IFF.1.2(3) The TSF shall permit an information flow between a source subject and a destination subject via a controlled operation if the following rules hold:

[**a) the presumed identity of the source subject is in the set of source subject identifiers;**

**b) the identity of the destination subject is in the set of source destination identifiers;**

**c) the information security attributes match the attributes in an information flow policy rule (contained in the information flow policy rule set defined by the Authorized Administrator) according to the following algorithm {rules are examined in order, once a match is found, the specified action is taken}; and**

**d) the selected information flow policy rule specifies that the information flow is to be permitted, and what specific operation from FDP_IFC.1 (3) is to be applied to that information flow**].

FDP_IFF.1.3(3) The TSF shall enforce the [**Authorized Administrator shall have the capability to view all information flows allowed by the information flow policy rule set before the rule set is applied**].

FDP_IFF.1.4(3) The TSF shall explicitly authorize an information flow based on the following rules: **[none]**.

FDP_IFF.1.5(3) The TSF shall explicitly deny an information flow based on the following rules:

[**a) The TOE shall reject requests for access or services where the presumed source identity of the information received by the TOE is not included in the set of source identifiers for the source subject;**

**b) The TOE shall reject requests for access or services where the presumed source identity of the information received by the TOE specifies a broadcast identity;**

**c) The TOE shall reject requests for access or services where the presumed source identity of the information received by the TOE specifies a loopback identifier;**

**d) The TOE shall reject requests in which the information received by the TOE contains the route (set of host network identifiers) by which information shall flow from the source subject to the destination subject)**].

*Application Note: In FDP_IFF.1.2(3) c) and d)* the information flow policy rule is equivalent to the VPN security association.

*Application Note:* FDP_IFF.1 in [CC_PART2] now contains one less element than was used in [PP]. This has been removed in this ST, but as the element was not used to specify functional requirements in [PP] there is no impact.

### 5.1.14 FDP_UCT.1 Basic data exchange confidentiality

FDP_UCT.1.1 The TSF shall enforce the **[VPN SFP]** to [***transmit and receive***] user data in a manner that is protected from unauthorised disclosure.

### 5.1.15 FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit *the **[TSF or another trusted IT product]*** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [**establishment of VPNs**].

### 5.1.16 FMT_MSA.1 Management of security attributes (1)

FMT_MSA.1.1 (1) The TSF shall enforce the [UNAUTHENTICATED_SFP] to restrict the ability to [delete attributes from a rule, modify attributes in a rule, add

attributes to a rule] the security attributes [listed in section FDP_IFF1.1(1)] to [the authorized administrator].

### 5.1.17 FMT_MSA.1 Management of security attributes (2)

FMT_MSA.1.1(2) The TSF shall enforce the [AUTHENTICATED_SFP] to restrict the ability to [delete attributes from a rule, modify attributes in a rule, add attributes to a rule] the security attributes [listed in section FDP_IFF1.1(2)] to [the authorized administrator].

### 5.1.18 FMT_MSA.1 Management of security attributes (3)

FMT_MSA.1.1(3) The TSF shall enforce the [**VPN_SFP**] to restrict the ability to [**delete attributes from a rule, modify attributes in a rule, add attributes to a rule**] the security attributes [**listed in section FDP_IFF1.1(3)] to [the authorized administrator**].

### 5.1.19 FMT_MSA.1 Management of security attributes (4)

FMT_MSA.1.1(4) The TSF shall enforce the [UNAUTHENTICATED_SFP] to restrict the ability to [delete [and create]] the security attributes [information flow rules described in FDP_IFF.1(1)] to [the authorized administrator].

### 5.1.20 FMT_MSA.1 Management of security attributes (5)

FMT_MSA.1.1(5) The TSF shall enforce the [AUTHENTICATED_SFP] to restrict the ability to [delete and [create]] the security attributes [information flow rules described in FDP_IFF.1(2)] to [the authorized administrator].

### 5.1.21 FMT_MSA.1 Management of security attributes (6)

FMT_MSA.1.1(6) The TSF shall enforce the [**VPN_SFP**] to restrict the ability to [***delete and [create]***] the security attributes [**information flow rules described in FDP_IFF.1(3)**] to [**the authorized administrator**].

### 5.1.22 FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1 The TSF shall enforce the [UNAUTHENTICATED_SFP and AUTHENTICATED_SFP **and VPN_SFP**] to provide *restrictive* default values for information flow security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow [the authorized administrator] to specify alternative initial values to override the default values when an object or information is created.

*Application Note: Following TOE installation, the default configuration is to allow no traffic through the firewall. The default values for the information flow control security attributes appearing in FDP_IFF.1 (1), FDP_IFF.1 (2) and FDP_IFF.1 (3) are intended to be restrictive in the sense that both inbound and outbound information is denied by the TOE until the default values are modified by an authorized administrator.*

### 5.1.23 FMT_MTD.1 Management of TSF data (1)

FMT_MTD.1.1(1) The TSF shall restrict the ability to *query, modify, delete,* [and assign] the [user attributes defined in FIA_ATD.1.1] to [the authorized administrator].

### 5.1.24 FMT_MTD.1 Management of TSF data (2)

FMT_MTD.1.1(2) The TSF shall restrict the ability to [set] the [time and date used to form the timestamps in FPT_STM.1.1] to [the authorized administrator].

### 5.1.25 FMT_MTD.2 Management of limits on TSF data

FMT_MTD.2.1 The TSF shall restrict the specification of the limits for [the number of authentication failures] to [the authorized administrator].

FMT_MTD.2.2 The TSF shall take the following actions, if the TSF data are at, or exceed, the indicated limits: [actions specified in FIA_AFL.1.2].

### 5.1.26 FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the *allocation of the resource to* [all objects].

*Application Note: This requirement is met by zeroing all newly allocated memory pages and by ensuring that the network traffic packet processing is based upon the actual packet size as reported by the NIC hardware.*

### 5.1.27 FCS_COP.1 Cryptographic operation (1 data encryption)

FCS_COP.1.1(1) The TSF shall perform [encryption of remote authorized administrator sessions **and virtual private networks**] in accordance with a specified cryptographic algorithm [AES (Advanced Encryption Standard as specified in FIPS 197) encryption (as specified in SP 800-67)] and cryptographic key sizes [that are at least 128 binary digits in length] that meet the following: [FIPS PUB 140-2 (Level 1)].

### 5.1.28 FCS_COP.1 Cryptographic operation (2 cryptographic signature services)

FCS_COP.1.1(2) The TSF shall perform [**cryptographic signature services**] in accordance with a specified cryptographic algorithm [**Digital Signature Algorithm (DSA) and RSA Digital Signature Algorithm (RDSA)**] and cryptographic key sizes [ **(modulus) of 1024 bits**] that meet the following: [**NIST Special Publication 800-57, 'Recommendation for Key Management' and FIPS PUB 140-2 (Level 1)**].

### 5.1.29 FCS_COP.1 Cryptographic operation (3 cryptographic hashing)

FCS_COP.1.1(3) The TSF shall perform [**cryptographic hashing services**] in accordance with a specified cryptographic algorithm [**SHA-1, SHA-224[3], SHA-256, SHA-384, SHA-512**] and cryptographic key sizes [**not applicable**] that meet the following: [**FIPS PUB 180-3 and FIPS PUB 140-2 (Level 1)**].

### 5.1.30 FCS_COP.1 Cryptographic operation (4 cryptographic key agreement)

FCS_COP.1.1(4) The TSF shall perform [**cryptographic key agreement services**] in accordance with a specified cryptographic algorithm [**Discrete Logarithm Cryptography (Diffie-Hellman)**] and cryptographic key sizes [**(modulus) of 1024 bits**] that meet the following: [NIST SP 800-56A and **FIPS 140-2 (Level 1)**].

[3] SHA-224 is supported on Control Center only, and not on the firewall

### 5.1.31 FCS_CKM.1 Cryptographic key generation (1)

FCS_CKM.1.1(1) The TSF shall generate **symmetric** cryptographic keys in accordance with a specified key generation algorithm [**FIPS Approved random number generator**] and specified cryptographic key sizes [**up to 256 bits AES**] that meet the following: [**SP 800-90A**].

### 5.1.32 FCS_CKM.1 Cryptographic key generation (2)

FCS_CKM.1.1(2) The TSF shall generate **asymmetric** cryptographic keys in accordance with a specified key generation algorithm [**FIPS Approved random number generator**] and specified cryptographic key sizes [**up to 1024 bits**] that meet the following: [**SP 800-90A**].

### 5.1.33 FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified key destruction method [**overwriting**] that meets the following: [**FIPS 140-2**].

### 5.1.34 FPT_STM.1 Reliable time stamps

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

*Application Note: The word "reliable" in the above requirement means that the order of the occurrence of auditable events is preserved.*

### 5.1.35 FAU_GEN.1 Audit data generation

FAU_GEN.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) [the events listed in Table 5.2].

FAU_GEN.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, 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, [information specified in column three of Table 5.2].

| Functional Component | Auditable Event | Additional Audit Record Content |
|---|---|---|
| FMT_SMR.1 | Modifications to the group of users that are part of the authorized administrator role. | The identity of the authorized administrator performing the modification and the user identity being associated with the authorized administrator role |
| FIA_UID.2 | All use of the user identification mechanism. | The user identities provided to the TOE |

| | | |
|---|---|---|
| FIA_UAU.5 | Any use of the authentication mechanism. | The user identities provided to the TOE |
| FIA_AFL.1 | The reaching of the threshold for unsuccessful authentication attempts and the subsequent restoration by the authorized administrator of the user's capability to authenticate**.** | The identity of the offending user and the authorized administrator |
| FDP_IFF.1 | All decisions on requests for information flow. | The presumed addresses of the source and destination subject. |
| FCS_COP.1 | Success and failure, and the type of cryptographic operation | The identity of the external IT entity attempting to perform the cryptographic operation |
| FPT_STM.1 | Changes to the time. | The identity of the authorized administrator performing the operation |
| FMT_MOF.1 | Use of the functions listed in this requirement pertaining to audit. | The identity of the authorized administrator performing the operation |

**Table 5.2**

### 5.1.36 FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide [an authorized administrator] with the capability to read [all audit trail data] from the audit records.

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

### 5.1.37 FAU_SAR.3 Selectable audit review

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

a) [user identity;

b) presumed subject address;

c) ranges of dates;

d) ranges of times;

e) ranges of addresses].

### 5.1.38 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 *prevent* modifications to the audit records.

### 5.1.39 FAU_STG.4 Prevention of audit data loss

FAU_STG.4.1 The TSF shall *prevent auditable events, except those taken by the authorized administrator* and [shall limit the number of audit records lost] if the audit trail is full.

### 5.1.40 FMT_MOF.1 Management of security functions behaviour (1)

FMT_MOF.1.1(1) The TSF shall restrict the ability to *enable, disable* the functions:

a) [operation of the TOE;

b) multiple use authentication functions described in FIA_UAU.5 **and FIA_UAU.8**]

to [an authorized administrator].

*Application Note: By "Operation of the TOE" in a) above, we mean having the TOE start up (enable operation) and shut down (disable operation). By "multiple use authentication" in b) above, we mean the management of password and single use authentication mechanisms.*

### 5.1.41 FMT_MOF.1 Management of security functions behaviour (2)

FMT_MOF.1.1(2) The TSF shall restrict the ability to *enable, disable, determine and modify the behaviour* of the functions:

a) [audit trail management;

b) backup and restore for TSF data, information flow rules, and audit trail data; and

c) communication of authorized external IT entities with the TOE]

to [an authorized administrator].

*Application Note: Determine and modify the behaviour of element c (communication of authorized external IT entities with the TOE) is intended to cover functionality such as providing a range of addresses from which the authorized external entity can connect.*

## 5.2 Security assurance requirements

The TOE assurance requirements are EAL4 augmented by ALC_FLR.3 as shown in the table below.

| Assurance Class | Assurance Component ID | Assurance Component Name |
|---|---|---|
| ADV: Development | ADV_ARC.1 | Security architecture description |
| | ADV_FSP.4 | Complete functional specification |
| | ADV_IMP.1 | Implementation representation of the TSF |
| | ADV_TDS.3 | Basic modular design |
| AGD: Guidance | AGD_OPE.1 | Operational user guidance documents |
| | AGD_PRE.1 | Preparative procedures |

| | | |
|---|---|---|
| ALC: Life-cycle support | ALC_CMC.4 | Production support, acceptance procedures and automation |
| | ALC_CMS.4 | Problem tracking CM coverage |
| | ALC_DEL.1 | Delivery procedures |
| | ALC_DVS.1 | Identification of security measures |
| | ALC_FLR.3 | Systematic flaw remediation |
| | ALC_LCD.1 | Developer defined life-cycle model |
| | ALC_TAT.1 | Well-defined development tools |
| ASE: Security Target evaluation | ASE_CCL.1 | Conformance claims |
| | ASE_ECD.1 | Extended components definition |
| | ASE_INT.1 | ST introduction |
| | ASE_OBJ.2 | Security objectives |
| | ASE_REQ.2 | Derived security requirements |
| | ASE_SPD.1 | Security problem definition |
| | ASE_TSS.1 | TOE summary specification |
| ATE: Tests | ATE_COV.2 | Analysis of coverage |
| | ATE_DPT.1 | Testing: basic design |
| | ATE_FUN.1 | Functional testing |
| | ATE_IND.2 | Independent testing – sample |
| AVA: Vulnerability | AVA_VAN.3 | Focused vulnerability analysis |

**Table 5.3**

## 5.3 Definition of Extended Components

For this evaluation the Security Functional Requirements in CC Part 2 have been extended to cover part of the TOE functionality that cannot otherwise clearly be expressed.

One additional component has been defined. This has been placed in an existing Family UAU: User authentication within the Class FIA: Identification and authentication. This choice has been made as the new component is related to the provision of user authentication.

Single use authentication is in the operational environment in this ST, and an extended component FIA_UAU.8 has been added to cover invocation of this external service. This requirement ensures that the authentication server will successfully authenticate a user's claimed identity (e.g. humans using FTP and Telnet) before allowing any other TSF-mediated actions on behalf of that user.

**Invocation of authentication mechanisms (FIA_UAU.8)**

Management: FIA_UAU.8

The following actions could be considered for the management functions in FMT:

a) Management of the authentication mechanism.

Audit: FIA_UAU.8

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: Invocation of the single-use authentication mechanism.

b) Basic: The final decision on authentication.

**FIA_UAU.8** **Invocation of authentication mechanisms**

Hierarchical to: No other components

Dependencies: FIA_UAU.5

FIA_UAU.8.1 The TSF shall invoke a single-use authentication server to authenticate a user's claimed identity according to the following rules: [assignment: *rules for invocation of single-use authentication mechanism*].

# 6 TOE Summary Specification

This section describes the security functions provided by the TOE to meet the security functional requirements.

## 6.1 Security audit (SF-FAU)

The Security audit function is designed to satisfy the following security functional requirements:

Audit

- FAU_GEN.1, FPT_STM.1:

Audit information is generated by affected McAfee Firewall processes as they experience security relevant events listed in the “auditable events” table (Section 5.1.35). Audit is generated to capture pertinent information related to the use of the authentication facilities, use of network communication services, establishment of administrative connections, changes to the security policy and security relevant changes to the system configuration. The audit records include type of event, date/time, subject identity (if applicable), identity of the generating process, and outcome for the events. Audit is also generated to mark the start and stop of auditing services.

The audit event generator provides information to identify the type of auditable event and entities related to the event. The audit generator writes the audit event to the McAfee Firewall audit device. The SecureOS kernel augments that audit event with a time stamp, identification information about the audit generator, such as the process ID value, the process’s TE security attributes, and the name of the command that generated the audit event. The audit event is then made available to the audit logging and audit monitor processes via the audit device.

- FAU_SAR.1, FAU_SAR.3:

McAfee Firewall administrators may use the Administrative Console audit viewing screens to review, search and sort audit data. Access to the audit trail is restricted to administrators.

McAfee Firewall provides the ability to search and sort audit data based upon user, source subject, destination subject and rule. In addition, searching and sorting can be based upon ranges of dates, time, user identities and subject service identities. In particular, user identity ranges for human users are arrived at by specifying a string with wildcard, while a range of IT entities is defined by specifying a subnet (e.g.10.10.10.*). A range of subject service identifiers or transport layer protocols is defined by specifying a range of ports. The Administrator may select one of the predefined record filters, or define their own filter to select the record they want to review. A range of predefined reports is also provided.

- FAU_STG.1:

McAfee Firewall provides an audit-logging daemon, named auditd, which reads all audit events from the audit device and records them into log files. Administrators may remove audit files to manage the storage space but they may not modify the content of the audit files.

Access to the McAfee Firewall audit files and audit database are controlled by the Type Enforcement security policy. Audit files are given Type Enforcement attributes that limit access to those processing elements with need to access the data.

McAfee Firewall's Type Enforcement mechanism prevents any process from modifying stored audit records. Only the Administrator is permitted to delete from the audit trail. The Administrator can also configure the TOE to overwrite the oldest audit records in the event that the audit trail is full.

- FAU_STG.4:

The McAfee Firewall audit facilities monitor the state of the audit storage area to minimize the risk of loss of data. On a daily basis it will "roll" the data files. This means that the current audit file is compressed (zipped) and aged, named by date, and a new current log file is created. This frees up disk space and allows more audit data to be stored. The audit "roll" mechanism is implemented so that no data is lost during the transition from the current audit file to the new audit file.

Every 5 minutes McAfee Firewall checks the status of the available audit space. When the used storage space exceeds a defined threshold it triggers an audit event. When the used storage exceeds a second threshold the system will, by default, stop inter-network communications to avoid loss of audit data.

## 6.2 Cryptographic support (SF-FCS)

The Cryptographic support function is designed to satisfy the following security functional requirements:

Validated Cryptographic Module

The McAfee Firewall cryptographic module has been validated to FIPS 140-2 (CMVP certificate [to be supplied[4]]) with a minimum rating of level 1.

- FCS_COP.1 (1), FCS_COP.1 (2), FCS_COP.1 (3), FCS_COP.1 (4), FCS_CKM.1 (1), FCS_CKM.1 (2), FCS_CKM.4:

McAfee Firewall contains the following FIPS 140-2 validated cryptographic functions: AES operating in CBC and ECB mode for key lengths of 128, 192, and 256 bits for encryption and decryption; DSA with key sizes (modulus) of 1024- and 2048 bits, and RSA with key sizes of 1024-, 1536-, 2048-, 3072-, 4096-bit for signature services; SHA-1, SHA-256, SHA-384 and SHA-512 for hashing services; and 1024 bits for Diffie-Hellman key agreement services.

- FIA_SOS.2, FCS_CKM.1 (1):

Random number generation in McAfee Firewall is done using an X9.31 RNG, which is seeded from an entropy gathering mechanism in the kernel using the Yarrow algorithm. The OpenSSL library uses a NIST Special Publication 800-90 AES CRT Deterministic RBG. This DRBG is seeded by the kernel X9.31 RNG.

Internet Key Exchange

- FCS_COP.1 (4):

As defined in RFC 2409 and RFC 4306, McAfee Firewall implements the following: cryptographic key establishment techniques for IPSEC; signature and pre-shared key authentication methods; digital signature authentication using RSA and DSA algorithms

[4] At time of issue of this Security Target, the evidence for FIPS 140-2 module validation has been submitted to Block 2 review.

using X.509 certificates; administrator selectable configuration for perfect forward secrecy for Quick Mode exchanges. The Administrator manages the certificates on McAfee Firewall and initiates certification revocation list validation.

**MFE Algorithm Certificate Numbers for Cryptographic Libraries**

| Approved security functions | CLSOS 64-bit | CLSOS 32-bit | KCLSOS (physical) | Virtual[5] 64-bit | Virtual[5] 32-bit | KCLSOS (virtual) |
|---|---|---|---|---|---|---|
| **Symmetric Key Algorithm** | | | | | | |
| Advanced Encryption Standard (AES) 128-, 192-, 256-bit in CBC, CFB128, OFB, CTR and ECB modes | 2713 | 2711 | | 2714 | 2712 | |
| AES 128-, 192-, 256-bit in CBC, ECB modes | | | 1833 | | | 1963 |
| Triple Data Encryption Standard (DES) 3-key option in CBC, ECB, OFB, CFB64 modes, KO 1, 2 | 1630 | 1628 | | 1631 | 1629 | |
| Triple-DES 3-key option in CBC mode | | | 1185 | | | 1275 |
| **Secure Hashing Algorithm (SHA)** | | | | | | |
| SHA-1, SHA-256, SHA-384, and SHA-512 | 2278 | 2276 | 1612 | 2279 | 2277 | 1722 |
| **Message Authentication Code (MAC) Function** | | | | | | |
| HMAC using SHA-1, SHA-256, SHA-384, and SHA-512 | 1692 | 1690 | 1086 | 1693 | 1691 | 1184 |
| **Random Bit Generator** | | | | | | |
| SP 800-90 Counter-based DRBG | 450 | 448 | | 451 | 449 | |
| ANSI X9.31 Appendix A.2.4 PRNG | | | 964 | | | 1032 |
| **Asymmetric Key Algorithm** | | | | | | |
| RSA PKCS #1 sign/verify: 1024-, 1536-, 2048-, 3072-, 4096-bit | 1409 | 1407 | | 1410 | 1408 | |
| RSA ANSI X9.31 key generation: 1024-, 1536-, 2048-, 3072-, 4096- | 1409 | 1407 | | 1410 | 1408 | |

[5] VMWare ESXi 5.0

| | | | | | | |
|---|---|---|---|---|---|---|
| bit | | | | | | |
| Digital Signature Algorithm (DSA) sig verify – 1024-bit | 830 | 828 | | 831 | 829 | |

**MFECC Algorithm Certificate Numbers for Cryptographic Libraries**

| Approved security functions | Crypto-J Physical | Crypto-J Virtual | OpenSSL Physical | OpenSSL Virtual |
|---|---|---|---|---|
| **Symmetric Key Algorithm** | | | | |
| Advanced Encryption Standard (AES) 128-, 192-, 256-bit in CBC, CFB128, OFB and ECB modes | 2703 | 2702 | 2486 | 2487 |
| Triple Data Encryption Standard (DES) 3-key option in CBC, ECB, OFB, CFB64, KO 1,2 modes | 1622 | 1621 | 1524 | 1525 |
| **Secure Hashing Algorithm (SHA)** | | | | |
| SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512 | 2270 | 2269 | 2104 | 2105 |
| **Message Authentication Code (MAC) Function** | | | | |
| HMAC using SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512 | 1683 | 2269 | 1528 | 1529 |
| **Deterministic Random Bit Generator** | | | | |
| HMAC Based DRBG: SP800-90A | 445 | 444 | | |
| **Asymmetric Key Algorithm** | | | | |
| RSA PKCS #1 sign/verify: 1024-, 2048-, 3072-, 4096[6]-bit | 140 | 1400 | 1275 | 1276 |
| RSA ANSI X9.31 key generation: 1024-, 2048-, 3072-, 4096[6]-bit | 1401 | 1400 | 1275 | 1276 |
| Digital Signature Algorithm (DSA) sig gen/verify – 1024- and 2048-bit | 824 | 823 | 766 | 767 |

## 6.3 User data protection (SF-FDP)

For information protocols supported by McAfee Firewall, the information flow is determined by the relevant network protocol connection attributes established by the Administrator. Authentication requirements can be specified for HTTP, HTTPS, FTP and Telnet.

[6] 4096-bit is supported by OpenSSL only.

On McAfee Firewall, the flow of information through the system is affected by key information security attributes. In particular, the flow rules depend upon the presumed source and destination addresses, the McAfee Firewall interface (zone) on which the traffic arrives or departs, and the requested service. McAfee Firewall employs the zone concept as a convenience that allows Administrators to refer to one or more network interfaces from the same security point of view when defining flow rules. On McAfee Firewall there is no mandatory distinction between internal networks and external networks; they are just separate zones. The allowed flow between any two networks is determined by the services enabled and the state of the rules in the firewall security policy.

The McAfee Firewall rule mechanism implements a site's security policy and determines the flow of user data. Each rule requires an application, which identifies the type of traffic matched by the rule. An application can be as general as a protocol and port(s), or targeted at a particular web application using signature information. The McAfee® AppPrism™ mechanism provides application discovery and control that allows applications running through a network to be monitored, and to allow or deny them based on policy settings. AppPrism can be used to create policy that protects against specific threats and reduces bandwidth usage by restricting the use of non-business applications. Application Discovery, when enabled, identifies which applications are traversing the network, and Application Control allows determination of which applications are allowed and denied. The Administrator may use applications provided by McAfee Labs, firewall applications, or may create custom applications. Access control rules can be based on individual applications, application groups, or application category filters that block all applications belonging to a specified category.

When an internal or external user requests a network connection, the appropriate ipfilter proxy or server checks the rules to determine whether to allow the requested connection. The rules can be configured to allow access from one zone to another, where a zone is a type enforced network area used to isolate network interfaces from each other.

In addition to specific rules, McAfee Firewall uses these security attributes to enforce some general flow rules that are described in subsequent paragraphs.

McAfee Firewall deals with address spoofing issues at two levels. First the kernel validates that a source address matches the zone from which the packet is received. Failures of this check are reported as an attack audit event.

Also the proxies can determine the zone associated with the connection socket and make policy decisions based on this information independent of the stated source address.

By default the McAfee Firewall IP stack processing rejects IP packets that have a broadcast address as their source address. The McAfee Firewall IP stack processing rejects IP packets that have a source address on a loop-back network, but were received on a non loop-back device.

The McAfee Firewall rejects all IP packets containing source route information and generates a net-probe audit message.

McAfee Firewall processing for HTTP, HTTPS, FTP and Telnet connections provides controls to check for bad service requests. For HTTP, HTTPS and FTP, the rules can specify which specific protocol service requests are allowed.

The McAfee Firewall provides two means of controlling network communications. The first is the detailed application level session based control. The second is a general packet filtering mechanism that operates at the IP network layer of the network stack.

The Administrator determines which form of control to use for various communication flows when they establish the firewall security policy.

McAfee Firewall includes the network protocol proxies and network protocol servers required to transfer communication between networks. These elements are responsible for establishing the network connections, transferring or arranging for the transfer of data between networks, and enforcing firewall security policy decisions.

McAfee Firewall also provides proxies for controlling connections to standard network services.

McAfee Firewall supports and controls transfer of data between connected networks via a wide range of Internet application layer protocols. No connection is allowed unless all of the criteria specified in the firewall security policy rules are satisfied. All protocol proxies must support network address translation and service address translation as specified in the rules. This supports hiding the structure of one McAfee Firewall zone from another. The McAfee Firewall installation includes proxies that support the application layer protocols. It also provides generic TCP and UDP proxies.

McAfee Firewall supports Network Address Translation (NAT).

The User data protection function is designed to satisfy the following security functional requirements.

**Unauthenticated Information Flow Policy**

- FDP_IFC.1 (1), FDP_IFF.1 (1):

McAfee Firewall enforces an unauthenticated information flow policy based upon the source, destination, and content of network packets (protocol connection attributes) without requiring subject authentication. Based on this policy, McAfee Firewall can either discard or pass information. Information can be passed directly or via an application proxy. Specifically, McAfee Firewall implements this policy by means of an SMTP proxy, as well as a Generic Proxy and IP Filter capability that can be applied to the wide spectrum of information protocols. McAfee Firewall's HTTP, HTTPS and FTP proxies can also be used to enforce the unauthenticated information flow policy. In this case, they are configured so no authentication is required. Of course, the HTTP, HTTPS and FTP proxies can also be configured to require authentication and thereby enforce the authenticated information flow policy.

McAfee Firewall supports all of the SMTP commands, FTP subcommands, HTTP and HTTPS request methods and Stateful packet attributes as specified in FDP_IFF.1 (1).

McAfee Firewall's AdminConsole and Control Center display the Administrator-defined information flow rule set, allowing for the Administrator to review changes prior to activating the rule set. Once activated, McAfee Firewall enforces flow control by requiring an explicit match to an Administrator defined flow rule, based on the source, destination, protocol and service identifiers, plus service commands used for SMTP, HTTP, HTTPS and FTP. McAfee Firewall examines the flow rules in order; once a match is found, the specified action is taken. Information flows not matching an explicitly allowed flow are denied by

McAfee Firewall. McAfee Firewall also denies information flows with inappropriate source identities or route information.

**Authenticated Information Flow Policy**

- FDP_IFC.1 (2), FDP_IFF.1 (2):

McAfee Firewall enforces an authenticated information flow policy based upon the source, destination, and content of network packets (protocol connection attributes); in order for information to flow, subjects must first successfully authenticate to McAfee Firewall. Based on this policy, McAfee Firewall can either discard or pass information. Information is passed via an application proxy. Specifically, McAfee Firewall implements this policy by means of FTP, HTTP, HTTPS and Telnet proxies which can be configured to require user authentication as a condition for using the service. In this case, an Administrator must define the service users in the user database and establish rules that specify that the service is contingent upon successful authentication. The rule specifies the particular type of single-use authentication mechanism that is to be used. The McAfee Firewall and its proxies validate the protocol, including the stateful packet attributes listed in FDP_IFF.1 (2).

McAfee Firewall's AdminConsole and Control Center display the Administrator-defined information flow rule set, allowing for the Administrator to review changes prior to activating the rule set. Once activated, McAfee Firewall enforces flow control by requiring an explicit match to an Administrator defined flow rule, based on the source, destination, protocol and service identifiers, plus service commands used for FTP, HTTP, HTTPS and Telnet. McAfee Firewall examines the flow rules in order; once a match is found, the specified action is taken. Information flows not matching an explicitly allowed flow are denied by McAfee Firewall.

**VPN Policy**

- FDP_IFC.1 (3), FDP_IFF.1 (3), FDP_UCT.1, FTP_ITC.1:

McAfee Firewall enforces a VPN policy based on source and destination identifiers from the network packet. Based on VPN policy, McAfee Firewall can either pass information without modification, decrypt, or encrypt. The VPN cryptographic operations are accomplished by means of the McAfee Firewall Cryptographic Module which has been validated against FIPS 140-2[7].

McAfee Firewall matches packets against VPN policy using the source and destination attributes of the packet and matching those attributes against the selections made in the VPN policy rules. Information security attributes, including the presumed identity of the source subject are bound to the VPN policy rules by requiring authenticated IKE connections to be established before allowing traffic to flow through the matching VPN policy rule.

McAfee Firewall's AdminConsole displays the Administrator-defined information flow rule set, allowing for the Administrator to review local changes prior to activating the rule set. Thereafter, McAfee Firewall enforces flow control by requiring an explicit match to an Administrator defined flow rule, based on the source and destination identifiers and presumed identity of the source. Information flows not matching an explicitly allowed flow are denied by McAfee Firewall. McAfee Firewall also denies information flows with inappropriate source identities or route information.

[7] Currently in Block 2 under the CMVP.

Residual Information Protection

- FDP_RIP.1:

When a user data packet is processed by the proxy, it resides within memory buffers in that proxy's memory space. The McAfee Firewall virtual memory system ensures that, as physical memory pages are taken from a free list and added to a given process's memory space, they are zeroed so that no residual data passes between processes.

A second situation arises when using kernel message buffers for managing data read from or written to the network. Since these buffers have previously been allocated, they are not zeroed again. Rather the avoidance of data leakage from one network message to another is managed by keeping track of the amount of data placed in the message. The network interface controller provides the data count to the driver. This information is maintained in the message buffer header information, separate from the message data. The kernel network stack code maintains the integrity of this critical data element and ensures that when a subsequent message is transmitted on another network interface card or the message is transferred to a memory buffer in user space, the correct number of data bytes is moved.

## 6.4 Identification and authentication (SF-FIA)

The Identification and authentication function is designed to satisfy the following security functional requirements:

Authentication Failure Handling

- FIA_AFL.1, FMT_MTD.2:

An Administrator can define an authentication failure limit. After that defined number of consecutive unsuccessful authentication attempts by a user trying to establish a remote Administrator connection or trying to employ an authenticated protocol service connection, McAfee Firewall prevents that user from successfully authenticating. McAfee Firewall also enforces the authentication failure limit on external IT entities attempting to authenticate. The denied user, either human or IT, is prevented from successful authentication until an authorized Administrator takes action to restore the user's rights.

User Identification

- FIA_ATD.1:

McAfee Firewall supports two classes of users: those who are Administrators and those who are proxy users. The identification information for each McAfee Firewall administrative user includes the following information:

- The user's login name;
- The hashed version of the password required to authenticate, assuming the relevant rules call for password authentication;
- The administrative role in which the user is allowed to operate;
- Login specific data including home directory, default login shell, etc.

Proxy users are those individuals identified within the Firewall user database for the purpose of defining control over who may utilize specific firewall inter-network communication services. These users cannot log into the McAfee Firewall and have no direct access to the McAfee Firewall. In response to specific access control rules, the McAfee Firewall may

interact with these users to require an authentication action before the user is allowed to utilize the communication protocol through the firewall. For authenticated proxy users, the following information is retained:

- The user's name;
- User's password, which is stored in an encrypted form (multi-use passwords only).

Only Administrative users that may connect to the McAfee Firewall via the Admin Console GUI can directly control the behaviour of McAfee Firewall.

Authentication

- FIA_UID.2, FIA_UAU.5, FIA_UAU.8 (X):

McAfee Firewall provides support for both single use and multi-use passwords. The decision on which form to use is dictated by the content of the rule associated with the service being accessed. This is the same for administrative access as for proxy services. In either case, the service providing the function consults the appropriate authentication mechanism “warder” which operates on the McAfee Firewall being accessed. (FIA_UAU.5)

In the case of reusable passwords, the warder consults the user information maintained on the McAfee Firewall to determine if the provided password matches the user’s valid password. Reusable passwords are implemented by means of a permutational mechanism. In the case of single use passwords, the relevant warder consults the remote authentication server to determine if the provided authentication data is valid. (FIA_UAU.5, FIA_UAU.8) Note that compliance with the PP requires the TOE to be configurable to provide use of single –use and multi-use authentication in certain specified cases. The TOE can be configured to meet this requirement, but also provides flexibility to switch between the two if required.

Authentication control is supported for all forms of administrative access to the McAfee Firewall, and for the FTP and Telnet proxies.

For TOE services over the network, McAfee Firewall allows negotiation of IP-based network state, including TCP session establishment and ICMP discovery/error handling to occur in order to establish necessary transport protocols. After the necessary network state is established, authentication can be performed. Only upon successful authentication, will the McAfee Firewall allow TSF-mediated actions on behalf of the user.

McAfee Firewall evaluates each information flow request against the Administrator-defined access control policies. If the flow request matches a rule requiring authentication for the service (e.g. HTTP, HTTPS, FTP, Telnet), the remote proxy user is required to successfully authenticate to McAfee Firewall before traffic is allowed to flow on behalf of that user. If the flow request matches a rule not requiring authentication, no user authentication will be performed, and traffic will flow as defined by the policy. In the later case, no other TOE mediated actions will be allowed on behalf of that unauthenticated user.

All users (human and IT) must provide identification before McAfee Firewall will allow any mediated actions on their behalf. McAfee Firewall requires that Administrators and authorized IT entities must be successfully authenticated before it will allow any TSF-mediated actions on their behalf. For proxy services configured to require authentication (HTTP, HTTPS, FTP, and Telnet), the proxy user is required to authenticate before McAfee Firewall allows traffic to flow on their behalf.

McAfee Firewall provides a password-based authentication mechanism. The user name and credentials are maintained locally by McAfee Firewall.

Upon a successful Administrator authentication, McAfee Firewall binds an immutable log id with the Administrator's session and associated process. All subsequent processes acting on behalf of the Administrator inherit the Administrator's unique log id. McAfee Firewall's Type Enforcement mechanism prevents user security attributes from being modified within the context of an Administrator's authenticated session.

Similarly, for authenticated proxy users and authorized IT entities, a unique session id is used to bind subjects to that user's security attributes. Again, the attributes are set for the initial subject and new subjects inherit the attributes from the creating subject. And, user attributes associated with a subject do not change within the session.

## 6.5 Security management (SF-FMT)

Security Management is carried out using either the Admin Console or Control Center.

The Admin Console graphical user interface (GUI) provides the external interfaces required for an Administrator to manage the McAfee Firewall and utilize its security features. AdminConsole windows-oriented, point-and-click features are used to turn services on or off and to select configuration options. A keyboard is used enter configuration parameters to augment the point-and-click Admin Console operation. Remote communications with the firewall are encrypted using TLS 1.0[8].

Control Center is an enterprise-class management tool for creating and applying security policies across multiple firewalls. Network administrators can remotely manage, maintain, and monitor firewalls for one or more domains.

The Control Center consists of the following entities:

• Control Center Client application — An application that resides on a desktop computer that is running a Windows operating system. The application provides the user interface to configure, manage, and monitor supported firewalls, and to perform Control Center administrative tasks.

• Control Center Management Server — A hardened Linux platform that provides the firewall management and monitoring capabilities that are required to centrally implement security policy. It manages the framework for secure communication between the server, Client, and supported firewalls. The Management Server requires at least one installation of the Control Center Client.

The Client and tiers of firewalls securely communicate with the Management Server by using SOAP over HTTPS. TLS 1.0, using Client Certificates generated by the built-in Certificate Authority, is used to encrypt and authenticate the client/server communication.

The Security Management function is designed to satisfy the following security functional requirements:

- FMT_SMR.1:

McAfee Firewall provides support for the administrative role. All Administrators can use the Admin Console to administer McAfee Firewall locally or remotely.

[8] By default the Admin Console uses TLS v1.2. The CCECG provides details of how to configure the Admin Console to use TLS v1.0

- FMT_MOF.1 (1), FMT_MOF.1 (2):

Only Administrators can alter the behaviour of the security auditing function. Administrators are the only individuals that may initiate management functions which enable and disable the various operational features of the McAfee Firewall.

- FMT_MSA.1 (1), FMT_MSA.1 (2), FMT_MSA.1 (3), FMT_MSA.1 (4), FMT_MSA.1 (5), FMT_MSA.1 (6):

McAfee Firewall protects the rule database via Type Enforcement and Administrator roles. Only an authenticated Administrator may establish a connection to McAfee Firewall and affect a change to the information flow policies and their security attributes.

- FMT_MSA.3:

McAfee Firewall installation provides a minimal set of rules sufficient to support administration of the system. This set does not allow any inter-network traffic through the firewall and it does not make any TOE services available to unauthenticated users. Only an Administrator is allowed to set up new rules which override the default values to allow for information flow or unauthenticated TOE services.

- FMT_MTD.1 (2):

McAfee Firewall controls access to the operations such as changing the system time and date via the Type Enforcement policy. That action is restricted to software that may be initiated by input from an Administrator or an authorized IT entity.

- FMT_MTD.1 (1), FIA_ATD.1:

Only an Administrator can take actions to query, modify, revoke or assign a user's role which controls the means whereby a user can administer McAfee Firewall or use its services and information flow policies as permitted by that role. Once changes are made, the effect is immediate.

## 6.6 Protection of the TSF (SF-FPT)

The Protection of the TSF function is designed to satisfy the following security functional requirement:

Reliable Time Stamp

- FPT_STM.1:

The McAfee Firewall hardware platform provides the battery-backed real-time clock and the CPU cycle counters that allow the SecureOS kernel to reliably maintain the time. For the virtual appliance this function is provided through VMware.

# 7 Rationale

## 7.1 Rationale for TOE security objectives

| | |
|---|---|
| O.IDAUTH | This security objective is necessary to counter the threat: T.NOAUTH because it requires that users be uniquely identified before accessing the TOE. |
| O.SINUSE | This security objective is necessary to counter the threats: T.REPEAT and T.REPLAY because it requires that the TOE prevent the reuse of authentication data so that even if valid authentication data is obtained, it will not be used to mount an attack. |
| O.MEDIAT | This security objective is necessary to counter the threats: T.ASPOOF, T.MEDIAT and T.OLDINF which have to do with getting impermissible information to flow through the TOE. This security objective requires that all information that passes through the networks is mediated by the TOE and that no residual information is transmitted. |
| O.SECSTA | This security objective ensures that no information is compromised by the TOE upon start-up or recovery and thus counters the threats: T.NOAUTH and T.SELPRO. |
| O.ENCRYP | This security objective is necessary to counter the threats and policy: T.NOAUTH, T.PROCOM and P.CRYPTO by requiring that an authorized administrator use encryption when performing administrative functions on the TOE remotely. |
| O.SELPRO | This security objective is necessary to counter the threats: T.SELPRO, T.AUDFUL and T.NOAUTH because it requires that the TOE protect itself from attempts to bypass, deactivate, or tamper with TOE security functions. |
| O.AUDREC | This security objective is necessary to counter the threat: T.AUDACC by requiring a readable audit trail and a means to search and sort the information contained in the audit trail. |
| O.ACCOUN | This security objective is necessary to counter the threat: T.AUDACC because it requires that users are accountable for information flows through the TOE and that authorized administrators are accountable for the use of security functions related to audit. |
| O.SECFUN | This security objective is necessary to counter the threats: T.NOAUTH, T.REPLAY and T.AUDFUL by requiring that the TOE provide functionality that ensures that only the authorized administrator has access to the TOE security functions. |
| O.LIMEXT | This security objective is necessary to counter the threat: T.NOAUTH because it requires that the TOE provide the means for an authorized administrator to control and limit access to TOE security functions. |
| O.EAL | This security objective is necessary to counter the threat: T.LOWEXP because it requires that the TOE is resistant to penetration attacks performed by an attacker possessing minimal attack potential. |
| O.NETSEC | This security objective is necessary to counter the threat: T.NETSEC. The TOE must be able provide confidentiality and integrity protection for information being transferred between itself and another TOE or trusted IT product in order to counter the threat of unauthorised access or modification. |

| | T.NOAUTH | T.REPEAT | T.REPLAY | T.ASPOOF | T.MEDIAT | T.OLDINF | T.PROCOM | T.AUDACC | T.SELPRO | T.AUDFUL | T.LOWEXP | T.NETSEC | P.CRYPTO |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| O.IDAUTH | X | | | | | | | | | | | | |
| O.SINUSE | | X | X | | | | | | | | | | |
| O.MEDIAT | | | | X | X | X | | | | | | | |
| O.SECSTA | X | | | | | | | | X | | | | |
| O.ENCRYP | X | | | | | | X | | | | | | X |
| O.SELPRO | X | | | | | | | | X | X | | | |
| O.AUDREC | | | | | | | | X | | | | | |
| O.ACCOUN | | | | | | | | X | | | | | |
| O.SECFUN | X | | X | | | | | | | X | | | |
| O.LIMEXT | X | | | | | | | | | | | | |
| O.EAL | | | | | | | | | | | X | | |
| O.NETSEC | | | | | | | | | | | | X | |

**Table 7.1: Summary of Mappings Between Threats and IT Security Objectives**

## 7.2 Rationale for security objectives for the environment

OE.PHYSEC The TOE is physically secure.

OE.LOWEXP The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.

OE.GENPUR There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.

OE.PUBLIC The TOE does not host public data.

OE.NOEVIL Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.

OE.SINGEN Information cannot flow among the internal and external networks unless it passes through the TOE.

OE.DIRECT Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE.

OE.NOREMO Human users who are not authorized administrators cannot access the TOE remotely from the internal or external networks.

OE.REMACC Authorized administrators may access the TOE remotely from the internal and external networks.

OE.GUIDAN This non-IT security objective is necessary to counter the threat: T.TUSAGE and T.AUDACC because it requires that those responsible for the TOE ensure that it is delivered, installed, administered, and operated in a secure manner.

OE.ADMTRA This non-IT security objective is necessary to counter the threat: T.TUSAGE and T.AUDACC because it ensures that authorized administrators receive the proper training.

OE.SINUSE This IT environment security objective is necessary to counter the threats: T.REPEAT and T.REPLAY because it requires that the TOE prevent the reuse of authentication data so that even if valid authentication data is obtained, it will not be used to mount an attack.

| | T.TUSAGE | T.AUDACC | T.REPEAT | T.REPLAY |
|---|---|---|---|---|
| OE.GUIDAN | X | X | | |
| OE.ADMINTRA | X | X | | |
| OE.SINUSE | | | X | X |

**Table 7.2: Summary of Mappings between Threats and Security Objectives for the Environment**

Since the rest of the security objectives for the environment are, in part, a re-statement of the security assumptions, those security objectives trace to all aspects of the assumptions.

## 7.3 Rationale for security requirements

The security requirements are derived according to the general model presented in Part 1 of the Common Criteria. Specifically, Table 7.3 illustrates the mapping between the security requirements and the security objectives and Table 7.1 demonstrates the relationship between the threats, policies and IT security objectives. The functional and assurance requirements presented in this security target are mutually supportive and their combination meets the stated security objectives.

The objective O.EAL is not mapped to any security functional requirements. It is an objective for the development process, and is therefore verified through the evaluation process.

FMT_SMR.1 Security roles

Each of the CC class FMT components in this security target depends on this component. It requires the ST writer to choose a role(s). This component traces back to and aids in meeting the following objective: O.SECFUN.

FIA_ATD.1 User attribute definition

This component exists to provide users with attributes to distinguish one user from another, for accountability purposes and to associate the role chosen in FMT_SMR.1 with a user. This component traces back to and aids in meeting the following objectives: O.IDAUTH and O.SECFUN.

FIA_UID.2 User identification before any action

This component ensures that before anything occurs on behalf of a user, the user's identity is identified to the TOE. This component traces back to and aids in meeting the following objectives: O.IDAUTH and O.ACCOUN.

FIA_AFL.1 Authentication failure handling

This component ensures that human users who are not authorized administrators cannot endlessly attempt to authenticate. After some number of failures that the authorized administrator decides, that must not be zero, the user becomes unable from that point on in attempts to authenticate. This goes on until an authorized administrator makes authentication possible again for that user. This component traces back to and aids in meeting the following objective: O.SELPRO.

FIA_UAU.5 Multiple authentication mechanisms

This component was chosen to ensure that multiple authentication mechanisms are used appropriately in all attempts to authenticate at the TOE from an internal or external network. This component traces back to and aids in meeting the following objective: O.SINUSE and O.IDAUTH.

FIA_UAU.8 Invocation of authentication mechanism

This extended component was included to ensure that the TOE invokes the authentication server to authenticate all human users using HTTP, HTTPS, FTP and Telnet. This component traces back to and aids in meeting the following objectives: O.IDAUTH, O.SINUSE and O.SELPRO.

FIA_SOS.2 Generation of secrets

This component provides generation of random numbers in support of cryptographic operations. This component traces back to and aids in meeting the following objective: O.NETSEC.

FDP_IFC.1 Subset information flow control (1)

This component identifies the entities involved in the UNAUTHENTICATED information flow control SFP (i.e., users sending information to other users and vice versa). This component traces back to and aids in meeting the following objective: O.MEDIAT.

FDP_IFC.1 Subset information flow control (2)

This component identifies the entities involved in the AUTHENTICATED information flow control SFP (i.e., users of the services HTTP, HTTPS, FTP or Telnet sending information to servers and vice versa). The users of these services must be authenticated at the TOE. This component traces back to and aids in meeting the following objective: O.MEDIAT.

FDP_IFC.1 Subset information flow control (3)

This component identifies the entities involved in the VPN information flow control SFP. This component traces back to and aids in meeting the following objectives: O.MEDIAT, O.NETSEC.

FDP_IFF.1 Simple security attributes (1)

This component identifies the attributes of the users sending and receiving the information in the UNAUTHENTICAED SFP, as well as the attributes for the information itself. Then the policy is defined by saying under what conditions information is permitted to flow. This component traces back to and aids in meeting the following objective: O.MEDIAT.

FDP_IFF.1 Simple security attributes (2)

This component identifies the attributes of the users sending and receiving the information in the AUTHENTICAED SFP, as well as the attributes for the information itself. Then the policy is defined by saying under what conditions information is permitted to flow. This component traces back to and aids in meeting the following objective: O.MEDIAT.

FDP_IFF.1 Simple security attributes (3)

This component identifies the attributes of the users sending and receiving the information in the VPN information flow control SFP. Then the policy is defined by saying under what

conditions information is permitted to flow. This component traces back to and aids in meeting the following objectives: O.MEDIAT, O.NETSEC.

FDP_UCT.1

This component specifies the requirement for the TOE to provide confidentiality while transmitting and receiving user data via a VPN. This component traces back to and aids in meeting the following objective: O.NETSEC.

FTP_ITC.1

This component specifies the requirement for establishing a trusted channel between the TOE and another trusted IT entity that will safeguard the data against modification or disclosure. This component traces back to and aids in meeting the following objective: O.NETSEC.

FMT_MSA.1 Management of security attributes (1)

This component ensures the TSF enforces the UNAUTHENTICATED_SFP to restrict the ability to delete, modify, and add within a rule those security attributes that are listed in section FDP_IFF1.1(1). This component traces back to and aids in meeting the following objectives: O.MEDIAT, O.SECSTA, and O.SECFUN.

FMT_MSA.1 Management of security attributes (2)

This component ensures the TSF enforces the AUTHENTICATED_SFP to restrict the ability to delete, modify, and add within a rule those specified security attributes that are listed in section FDP_IFF1.1(2). This component traces back to and aids in meeting the following objectives: O.MEDIAT, O.SECSTA, and O.SECFUN.

FMT_MSA.1 Management of security attributes (3)

This component ensures the TSF enforces the VPN_SFP to restrict the ability to delete, modify, and add within a rule those specified security attributes that are listed in section FDP_IFF1.1(3). This component traces back to and aids in meeting the following objectives: O.MEDIAT, O.SECSTA, and O.SECFUN.

FMT_MSA.1 Management of security attributes (4)

This component ensures the TSF enforces the UNAUTHENTICATED_SFP to restrict the ability to create or delete rules for security attributes that are listed in FDP_IFF.1(1). This component traces back to and aids in meeting the following objectives: O.MEDIAT, O.SECSTA, and O.SECFUN.

FMT_MSA.1 Management of security attributes (5)

This component ensures the TSF enforces the AUTHENTICATED_SFP to restrict the ability to create or delete rules for security attributes that are listed in FDP_IFF.1(2). This component traces back to and aids in meeting the following objectives: O.MEDIAT, O.SECSTA, and O.SECFUN.

FMT_MSA.1 Management of security attributes (6)

This component ensures the TSF enforces the VPN_SFP to restrict the ability to create or delete rules for security attributes that are listed in FDP_IFF.1(3). This component traces back to and aids in meeting the following objectives: O.MEDIAT, O.SECSTA, and O.SECFUN.

FMT_MSA.3 Static attribute initialization

This component ensures that there is a default deny policy for the information flow control security rules. This component traces back to and aids in meeting the following objectives: O.MEDIAT and O.SECSTA.

FMT_MTD.1 Management of TSF data (1)

This component ensures that the TSF restrict abilities to query, modify, delete and assign certain user attributes as defined in FIA_ATD.1.1 to only the authorized administrator. This component traces back to and aids in meeting the following objective: O.SECFUN.

FMT_MTD.1 Management of TSF data (2)

This component ensures that the TSF restrict abilities to set the time and date used to form timestamps to only the authorized administrator. This component traces back to and aids in meeting the following objective: O.SECFUN.

FMT_MTD.2 Management of limits on TSF data

This component ensures that the TSF restrict the specification of limits of the number of unauthenticated failures to the authorized administrator and specifies the action be taken if limits on the TSF data are reached or exceeded. This component traces back to and aids in meeting the following objective: O.SECFUN.

FDP_RIP.1 Subset residual information protection

This component ensures that neither information that had flowed through the TOE nor any TOE internal data are used when padding is used by the TOE for information flows. This component traces back to and aids in meeting the following objective: O.MEDIAT.

FCS_COP.1 Cryptographic operation (1)

This component ensures that AES is used to encrypt traffic when authorized administrators communicate with the TOE remotely from an internal or external network. This component traces back to and aids in meeting the following objective: O.ENCRYP. [9]

FCS_COP.1 Cryptographic operation (2)

This component provides cryptographic signature services that are used in support of the VPN service. This component traces back to and aids in meeting the following objectives: O.ENCRYPT and O.NETSEC.

FCS_COP.1 Cryptographic operation (3)

This component provides hashing services that are used in support of the VPN service. This component traces back to and aids in meeting the following objectives: O.ENCRYPT and O.NETSEC.

FCS_COP.1 Cryptographic operation (4)

This component provides key agreement services that are used in support of the VPN service. This component traces back to and aids in meeting the following objectives: O.ENCRYPT and O.NETSEC.

FCS_CKM.1 Cryptographic key generation (1)

This component provides key generation services that support use of AES. This component traces back to and aids in meeting the following objectives: O.ENCRYPT and O.NETSEC.

FCS_CKM.1 Cryptographic key generation (2)

This component provides key generation services that support use of DSA and RDSA. This component traces back to and aids in meeting the following objectives: O.ENCRYPT and O.NETSEC.

FCS_CKM.4 Cryptographic key destruction

[9] In [FWPP] FCS_COP.1 is also mapped to O.EAL. However, no rationale is given for this mapping, and the text in the PP is inconsistent with the table. This is assumed to be an error in the PP, and the mapping is not made here.

This component provides key destruction services that support use of AES, DSA and RDSA. This component traces back to and aids in meeting the following objectives: O.ENCRYPT and O.NETSEC.

ADV_ARC.1 Security architecture description

This component must describe how the architecture ensures that the TSF are always invoked. ADV_ARC.1 must describe how the architecture ensures that the TSF have a domain of execution that is separate and that cannot be violated by unauthorized users. This component traces back to and aids in meeting the following objective: O.SELPRO and O.SECSTA.

FPT_STM.1 Reliable time stamps

FAU_GEN.1 depends on this component. It ensures that the date and time on the TOE is dependable. This is important for the audit trail. This component traces back to and aids in meeting the following objective: O.AUDREC.

FAU_GEN.1 Audit data generation

This component outlines what data must be included in audit records and what events must be audited. This component traces back to and aids in meeting the following objectives: O.AUDREC and O.ACCOUN.

FAU_SAR.1 Audit review

This component ensures that the audit trail is understandable. This component traces back to and aids in meeting the following objective: O.AUDREC.

FAU_SAR.3 Selectable audit review

This component ensures that a variety of searches and sorts can be performed on the audit trail. This component traces back to and aids in meeting the following objective: O.AUDREC.

FAU_STG.1 Protected audit trail storage

This component is chosen to ensure that the audit trail is protected from tampering, the security functionality is limited to the authorized administrator and that start-up and recovery does not compromise the audit records. This component traces back to and aids in meeting the following objectives: O.SELPRO, O.SECFUN and O.SECSTA.

FAU_STG.4 Prevention of audit data loss

This component ensures that the authorized administrator will be able to take care of the audit trail if it should become full. But this component also ensures that no other auditable events as defined in FAU_GEN.1 occur. Thus the authorized administrator is permitted to perform potentially auditable actions though these events will not be recorded until the audit trail is restored to a non-full status. This component traces back to and aids in meeting the following objectives: O.SELPRO, O.SECFUN and O.SECSTA.

FMT_MOF.1 Management of security functions behaviour (1)

This component was to ensure the TSF restricts the ability of the TOE start up and shut down operation and multiple authentication function to the authorized administrator. This component traces back to and aids in meeting the following objectives: O.SECFUN, O.LIMEXT, and O.SECSTA.

FMT_MOF.1 Management of security functions behaviour (2)

This component was to ensure the TSF restricts the ability to modify the behaviour of functions such as audit trail management, back and restore for TSF data, and communication of authorized external IT entities with the TOE to an authorized administrator. This component traces back to and aids in meeting the following objectives: O.SECFUN, O.LIMEXT, and O.SECSTA.

| | O.IDAUTH | O.SINUSE | O.MEDIAT | O.SECSTA | O.ENCRYP | O.SELPRO | O.AUDREC | O.ACCOUN | O.SECFUN | O.LIMEXT | O.NETSEC |
|---|---|---|---|---|---|---|---|---|---|---|---|
| FMT_SMR.1 | | | | | | | | | X | | |
| FIA_ATD.1 | X | | | | | | | | X | | |
| FIA_UID.2 | X | | | | | | | X | | | |
| FIA_AFL.1 | | | | | | X | | | | | |
| FIA_UAU.5 | X | X | | | | | | | | | |
| FIA_UAU.8 | X | X | | | | X | | | | | |
| FIA_SOS.2 | | | | | | | | | | | X |
| FDP_IFC.1(1) | | | X | | | | | | | | |
| FDP_IFC.1(2) | | | X | | | | | | | | |
| FDP_IFC.1(3) | | | X | | | | | | | | X |
| FDP_IFF.1(1) | | | X | | | | | | | | |
| FDP_IFF.1(2) | | | X | | | | | | | | |
| FDP_IFF.1(3) | | | X | | | | | | | | X |
| FDP_UCT.1 | | | | | | | | | | | X |
| FTP_ITC.1 | | | | | | | | | | | X |
| FMT_MSA.1(1) | | | X | X | | | | | X | | |
| FMT_MSA.1(2) | | | X | X | | | | | X | | |
| FMT_MSA.1(3) | | | X | X | | | | | X | | |
| FMT_MSA.1(4) | | | X | X | | | | | X | | |
| FMT_MSA.1(5) | | | X | X | | | | | X | | |
| FMT_MSA.1(6) | | | X | X | | | | | X | | |
| FMT_MSA.3 | | | X | X | | | | | | | |
| FMT_MTD.1(1) | | | | | | | | | X | | |

| | O.IDAUTH | O.SINUSE | O.MEDIAT | O.SECSTA | O.ENCRYP | O.SELPRO | O.AUDREC | O.ACCOUN | O.SECFUN | O.LIMEXT | O.NETSEC |
|---|---|---|---|---|---|---|---|---|---|---|---|
| FMT_MTD.1(2) | | | | | | | | | X | | |
| FMT_MTD.2 | | | | | | | | | X | | |
| FDP_RIP.1 | | | X | | | | | | | | |
| FCS_COP.1(1) | | | | | X | | | | | | X |
| FCS_COP.1(2) | | | | | X | | | | | | X |
| FCS_COP.1(3) | | | | | X | | | | | | X |
| FCS_COP.1(4) | | | | | X | | | | | | X |
| FCS_CKM.1 (1) | | | | | X | | | | | | X |
| FCS_CKM.1 (2) | | | | | X | | | | | | X |
| FCS_CKM.4 | | | | | X | | | | | | X |
| ADV_ARC.1 | | | | X | | X | | | | | |
| FPT_STM.1 | | | | | | | X | | | | |
| FAU_GEN.1 | | | | | | | X | X | | | |
| FAU_SAR.1 | | | | | | | X | | | | |
| FAU_SAR.3 | | | | | | | X | | | | |
| FAU_STG.1 | | | | X | | X | | | X | | |
| FAU_STG.4 | | | | X | | X | | | X | | |
| FMT_MOF.1(1) | | | | X | | | | | X | X | |
| FMT_MOF.1(2) | | | | X | | | | | X | X | |

**Table 7.3: Summary of Mappings between Security Functional Requirements and TOE Security Objectives**

## 7.4 Dependency rationale

The following table is provided as evidence that all dependencies have been satisfied in this ST.

| SFR | Dependencies | Satisfied? |
|---|---|---|

| SFR | Dependencies | Satisfied? |
|---|---|---|
| FAU_GEN.1 | FPT_STM.1 | Yes |
| FAU_SAR.1 | FAU_GEN.1 | Yes |
| FAU_SAR.3 | FAU_SAR.1 | Yes |
| FAU_STG.1 | FAU_GEN.1 | Yes |
| FAU_STG.4 | FAU_STG.1 | Yes |
| FCS_COP.1 | FDP_ITC.1 or<br>FDP_ITC.2 or<br>FCS_CKM.1<br>FCS_CKM.4 | Yes (by inclusion of FCS_CKM.1 and FCS_CKM.4) |
| FCS_CKM.1 | FCS_CKM.2 or<br>FCS_COP.1<br>FCS_CKM.4 | Yes (by inclusion of FCS_COP.1 and FCS_CKM.4) |
| FCS_CKM.4 | FCS_ITC.1 or<br>FCS_ITC.2 or<br>FCS_CKM.1 | Yes (by inclusion of FCS_CKM.1) |
| FDP_IFC.1 | FDP_IFF.1 | Yes (all iterations of IFC.1) |
| FDP_IFF.1 | FDP_IFC.1<br>FMT_MSA.3 | Yes<br>Yes |
| FDP_RIP.1 | None | N/A |
| FDP_UCT.1 | FTP_ITC.1 or<br>FTP_TRP.1<br>FDP_ACC.1 or<br>FDP_IFC.1 | Yes<br><br><br>Yes |
| FIA_AFL.1 | FIA_UAU.1 | No, however FIA_UAU.5 provides the mechanism that is referred to in AFL.1 and can be used to satisfy the dependency. |
| FIA_ATD.1 | None | N/A |
| FIA_SOS.2 | None | N/A |
| FIA_UAU.5 | None | N/A |
| FIA_UAU.8 (X) | FIA_UAU.5 | Yes |
| FIA_UID.2 | None | N/A |
| FMT_MOF.1 | FMT_SMR.1 | Yes (all iterations) |

| SFR | Dependencies | Satisfied? |
|---|---|---|
| | FMT_SMF.1 | No (see note below) |
| FMT_MSA.1 | FDP_ACC.1 or<br>FDP_IFC.1<br>FMT_SMR.1<br>FMT_SMF.1 | <br>Yes (all iterations)<br>Yes<br>No (see note below) |
| FMT_MSA.3 | FMT_MSA.1<br>FMT_SMR.1 | Yes<br>Yes |
| FMT_MTD.1 | FMT_SMR.1<br>FMT_SMF.1 | Yes (all iterations)<br>No (see note below) |
| FMT_MTD.2 | FMT_SMR.1<br>FMT_MTD.1 | Yes<br>Yes |
| FMT_SMR.1 | FIA_UID.1 | Yes, FIA_UID.2 |
| FPT_STM.1 | None | N/A |
| FTP_ITC.1 | None | N/A |

**Table 7.4: Dependencies**

Note: Common Criteria includes a dependency for FMT_MOF.1, FMT_MSA.1 and FMT_MTD.1 requirements on FMT_SMF. This ST does not include that requirement. The ST was written to be consistent with [FWPP], which does not include the extra requirement. The PP was originally written before FMT_SMF.1 was added to the CC, and when the PP was updated the authors chose not to add it. In each case, the MOF.1, MSA.1 and MTD.1 requirements “restrict” certain management functions to an authorized administrator and this has been interpreted within this ST as requiring that those management functions exist in the TOE. The TOE Summary Specification (section 6.5) includes these management functions.

## 7.5 Rationale for TOE summary specification

This section demonstrates that the TOE security functions are suitable to meet the security functional requirements.

The specified TOE security functions work together to satisfy the TOE security functional requirements. Section 6 includes in the descriptions of security functions a mapping to SFRs to show that each security function is traced to at least one SFR. The table below demonstrates that each SFR is covered by at least one security function.

| SFR | Name | Security Function |
|---|---|---|
| FMT_SMR.1 | Security roles | SF_FMT |
| FIA_ATD.1 | User attribute definition | SF_FIA, SF_FMT |
| FIA_SOS.2 | Generation of secrets | SF_FCS |
| FIA_UID.2 | User identification before any action | SF_FIA |
| FIA_AFL.1 | Authentication failure | SF_FIA |

| | | |
|---|---|---|
| | handling | |
| FIA_UAU.5 | Multiple authentication mechanisms | SF_FIA |
| FIA_UAU.8 (X) | Invocation of authentication mechanisms | SF_FIA |
| FDP_IFC.1 | Subset information flow control (1) | SF_FDP |
| FDP_IFC.1 | Subset information flow control (2) | SF_FDP |
| FDP_IFC.1 | Subset information flow control (3) | SF_FDP |
| FDP_IFF.1 | Simple security attributes (1) | SF_FDP |
| FDP_IFF.1 | Simple security attributes (2) | SF_FDP |
| FDP_IFF.1 | Simple security attributes (3) | SF_FDP |
| FDP_UCT.1 | Basic data exchange confidentiality | SF_FDP |
| FTP_ITC.1 | Inter-TSF trusted channel | SF_FDP |
| FMT_MSA.1 | Management of security attributes (1) | SF_FMT |
| FMT_MSA.1 | Management of security attributes (2) | SF_FMT |
| FMT_MSA.1 | Management of security attributes (3) | SF_FMT |
| FMT_MSA.1 | Management of security attributes (4) | SF_FMT |
| FMT_MSA.1 | Management of security attributes (5) | SF_FMT |
| FMT_MSA.1 | Management of security attributes (6) | SF_FMT |
| FMT_MSA.3 | Static attribute initialization | SF_FMT |
| FMT_MTD.1 | Management of TSF data (1) | SF_FMT |
| FMT_MTD.1 | Management of TSF data (2) | SF_FMT |
| FMT_MTD.2 | Management of Limits on TSF data | SF_FIA |
| FDP_RIP.1 | Subset residual information protection | SF_FDP |
| FCS_COP.1 | Cryptographic operation (1) | SF_FCS |
| FCS_COP.1 | Cryptographic operation (2) | SF_FCS |
| FCS_COP.1 | Cryptographic operation (3) | SF_FCS |
| FCS_COP.1 | Cryptographic operation (4) | SF_FCS |
| FCS_CKM.1 | Cryptographic key generation (1) | SF_FCS |
| FCS_CKM.1 | Cryptographic key generation (2) | SF_FCS |
| FCS_CKM.4 | Cryptographic key destruction | SF_FCS |
| FPT_STM.1 | Reliable time stamps | SF_FAU, SF_FPT |
| FAU.GEN.1 | Audit data generation | SF_FAU |
| FAU_SAR.1 | Audit review | SF_FAU |
| FAU_SAR.3 | Selectable audit review | SF_FAU |
| FAU_STG.1 | Protected audit trail storage | SF_FAU |
| FAU_STG.4 | Prevention of audit data loss | SF_FAU |
| FMT_MOF.1 | Management of security | SF_FMT |

| | | |
|---|---|---|
| | functions behaviour (1) | |
| FMT_MOF.1 | Management of security functions behaviour (2) | SF_FMT |

**Table 7.5: Rationale for security functions (1)**

The table below provides a rationale that the security functions are suitable to meet the SFRs.

| Security Function | SFRs | Rationale |
|---|---|---|
| SF_FMT | FMT_SMR.1<br>FMT_MSA.1 (1)<br>FMT_MSA.1 (2)<br>FMT_MSA.1 (3)<br>FMT_MSA.1 (4)<br>FMT_MSA.3<br>FMT_MTD.1 (1)<br>FMT_MTD.1 (2)<br>FMT_MOF.1 (1)<br>FMT_MOF.1 (2) | The SF_FMT security function provides an authorized administrator, as appropriate, with the capability to manage the operation of the firewall. A user acting in the administrator role is allowed to control the operation of the TOE, manage user attributes, set the system time and date, and manage authentication failure responses. Authorized administrators are also provided with the capability to manage the flow of information through the firewall. This includes complete control of all information flow security attributes and setting the limit for authentication failure handling. Authorized administrators are provided the capability to selectively review audit data and may remove old audit records. |
| SF_FCS | FCS_COP.1(1)<br>FCS_COP.1(2)<br>FCS_COP.1(3)<br>FCS_COP.1(4)<br>FCS_CKM.1(1)<br>FCS_CKM.1(2)<br>FCS_CKM.4<br>FIA_SOS.2 | The SF_FCS security function provides a set of cryptographic services, including symmetric and asymmetric encryption and decryption, together with associated key generation and destruction. |
| SF_FIA | FIA_ATD.1<br>FIA_UID.2<br>FIA_AFL.1<br>FIA_UAU.5<br>FIA_UAU.8 (X)<br>FMT_MTD.2 | The SF_FIA security function provides the capability to determine and verify the identity of users, determine their authority to interact with the TOE, and associate the proper security attributes for each authorized user. Also, it ensures that user identification and authentication precede any TSF-mediated actions on behalf of a user, responds to unsuccessful authentication attempts, and provides for both password and single-use authentication mechanisms. |

| | | |
|---|---|---|
| SF_FDP | FDP_IFC.1 (1)<br>FDP_IFC.1 (2)<br>FDP_IFC.1 (3)<br>FDP_IFF.1 (1)<br>FDP_IFF.1 (2)<br>FDP_IFF.1 (3)<br>FDP_UCT.1<br>FTP_ITC.1<br>FDP_RIP.1 | The SF_FDP security function implements the information flow and mediates all flows through the firewall. It controls traffic flows from unauthenticated IT entities and also controls FTP and Telnet flows which require the human user initiating the flow to be authenticated. Safeguards are provided to ensure that residual data from a previous packet is not leaked to new packets as they flow through the firewall. |
| SF_FPT | FPT_STM.1 | The SF_FPT security function provides a reliable time stamp. |
| SF_FAU | FAU_GEN.1<br>FAU_SAR.1<br>FAU_SAR.3<br>FAU_STG.1<br>FAU_STG.4 | The SF_FAU security function generates audit records related to security relevant events. It provides the capability to review audit logs using tools for searching and sorting. Audit records are protected from modification and unauthorized deletion. If the audit trail becomes full, appropriate safeguards are applied to prevent audit data loss. |

**Table 7.6: Rationale for security functions (2)**

## 7.6 Rationale for security assurance requirements

The security assurance requirements have been selected firstly to encompass those contained in the [FWPP] to ensure compliance with that standard, and secondly to reflect the common marketplace requirement for firewalls to be assured to EAL4. The augmentation of ALC_FLR.3 was selected to provide assurance to purchasers of the firewall that identified flaws will be addressed in a timely manner.

## 7.7 Loss of audit data

[FWPP] requires the Security Target writer to provide, as part of the rationale, an analysis of the maximum amount of audit data that can be expected to be lost in the event of audit storage failure, exhaustion, and/or attack.

The McAfee Firewall audit subsystem is designed to minimize the amount of audit data that will be lost in the event of audit storage failure, exhaustion, and/or attack. All audit data is written to log files by the audit daemon immediately as they are created by the system. If the audit daemon fails to write the message, the system will enter failure mode until the problem is resolved. The audit daemon also monitors the amount of space left on the drive. The system will be put into failure mode in advance of running out of audit storage space. In failure mode, of course, no traffic is allowed to flow and no mediation takes place. At that point, there are no new traffic flow audit records to be lost.

In the event of catastrophic failures, such as a power failure, audit data loss is limited to the audit records which have not yet been written to the disk. Lost audit data in these cases is

limited to audit records that the audit daemon has not yet read from the audit device and audit records that are in the process of being written to disk.