



# FI MU

---

Faculty of Informatics  
Masaryk University

## Application-Level Firewall Protection Profile for High Robustness Environments—Initial Considerations

by

M.J. Kelly  
V. Matyáš  
A. Patel

# Application-Level Firewall Protection Profile for High Robustness Environments – Initial Considerations

M.J. Kelly<sup>1</sup>, V. Matyáš<sup>1,2</sup>, A. Patel<sup>1</sup>

## Abstract

Firewalls act as access control policy mediators between networks. They either permit or block the exchange of data between networks. The ability to permit or block the transfer of data means firewalls can be used to selectively allow access to the resources it protects. Firewalls of varying security levels have been created to provide security that is adequate to the sensitivity of the data being protected. Firewalls are often formally evaluated to certify what level of security they are suitable for. They are evaluated against so-called security evaluation criteria – standardised descriptions of security measures. Common Criteria (CC) is the current global standard for evaluations. Firewall security attributes are described in a Protection Profile (PP) that defines an implementation-independent set of security requirements and objectives for a category of products or systems that meet similar consumers needs for IT security. Our project set out to produce a summary of security issues for an Application-Level Firewall Protection Profile (PP) for a High Robustness Environment. We started our work with the Basic-Level Firewall PP, the Medium-Level Firewall PP and the High-Level Mail Guard PP. The two firewall PPs and the Mail Guard PP are compared to give an insight into what the issues concerning the High-Level Firewall PP are. This High-Level Firewall PP is then discussed in terms of its major principles.

## 1 Introduction

This project endeavours to produce a summary of issues for an Application-level Firewall Protection Profile (PP) for a High Robustness Environment. In order to create this summary it is first necessary to ascertain what are Firewalls, what is Common Criteria (CC) and what is required in a PP. It is also necessary to look at previous lower-level firewall PPs and a High-Level PP. We provide only the very basic introduction to firewalls and security evaluations (against evaluation criteria) in this section; further information can be found, e.g., through [1, 2].

---

<sup>1</sup>University College Dublin, Ireland.

<sup>2</sup>Corresponding author, currently on sabbatical leave from FI MU. E-mail: matyas@fi.muni.cz.

## 1.1 Firewalls

Firewalls are systems that either permit or block traffic between external networks and an internal network. Traditionally particular firewalls were categorized as one of the following two types of firewalls. Traffic-Filter firewalls typically examine only a packet's headers to determine whether or not to allow the packet across the firewall. Application-Level proxies provide the firewall with greater security granularity by providing policy enforcement not only based on IP address or transport layer protocol, but on specific application e.g. HTTP. Both firewall types have positive and negative points. Traffic-Filter firewalls have higher throughput performance than Application-Level proxies. However Application-Level proxies have greater granularity than Traffic-Filter firewalls. Inevitably the boundary between these two firewall technologies disintegrated to produce hybrid firewalls. These hybrid firewalls combine the positive points to produce more effective and efficient firewalls.

## 1.2 Common Criteria

The Trusted Computer System Evaluation Criteria (TCSEC) started the history of evaluation criteria development in the early 1980's, and they are around the world known as the U.S. "Orange Book" since then. The first international evaluation criteria were published by France, Germany, the Netherlands, and the United Kingdom, as the Information Technology Security Evaluation Criteria (ITSEC), and the revised version of ITSEC was published in 1991 by the European Communities (EC) for trial use by the EC. The Canadian Trusted Computer Product Evaluation Criteria (CTCPEC) were developed during the early 1990's, with an intent to synthesize the developments in Europe and in the U.S. In the U.S., the draft of the Federal Criteria for Information Technology Security (FC) was published in 1993, with Canadian participation and using elements of the ITSEC. It was agreed to enforce a joint initiative to align the criteria approaches from the EC and North America between the European Commission and governments of Canada and United States. The backers of CTCPEC, FC and ITSEC pursued this initiative through the Common Criteria Editorial Board, output of which was the harmonized criteria called "Common Criteria" (CC). The CC was also endorsed by ISO as international criteria. Common Criteria [2] is the current global standard for evaluations. The Common Criteria is composed of three parts: Introduction and General Model (Part 1), Security Functional Requirements (P. 2), and Security Assurance Requirements (P. 3).

Target of Evaluation (TOE) denotes either a complete information technology system or a product that implements some security specifications. The TOE includes representation of all design refinements and evidence that the security requirements have been addressed. Definitions and descriptions of TOE security are to be covered in a set of documents characterizing the TOE security at all levels of abstraction. *Levelling* (of a security service) specifies the defined re-

quirements for granularity and/or strength addressing a specific set of threats. Each subsequent level of service provides a better countermeasure against the threats. Levels are mostly hierarchical regarding protection, but do not have to be proper subsets in all cases.

### 1.3 Protection Profile

A PP defines assumptions about the security aspects of the environment, threats, security objectives, functional and assurance requirements to meet those security objectives, and logic on how the requirements meet the objectives. The PP is split into six main areas:

- **Protection Profile Introduction** – This chapter gives an overview of the Protection Profile (PP). It gives definitions of terms used from the Common Criteria and a brief list of related PPs.
- **Target of Evaluation (TOE)** – A TOE is a system or part of a system that is under evaluation. This section describes the background, security policy, and users of the TOE, audit, VPN mechanisms, and the evaluation assurance level.
- **TOE Security Environment (TSE)** – The TSE describes the kind of environment that a PP compliant TOE will have to survive in. For example the Medium-Level Firewall TOE will have to be more robust than the Basic-Level Firewall TOE to repel the threats that exist in its proposed environment.
- **Security Objectives** – This section describes the security objectives for the TOE and the TOEs Operating Environment (OE). The OE is the location in which the TOE will work. The security objectives are divided into TOE Security Objectives and Security Objectives for the OE. The former are to be addressed by the TOE directly and the latter by the IT domain.
- **IT Security Requirements** – This area provides functional and assurance requirements that must be satisfied by a PP-compliant TOE. The functional components are taken from Part 2 and Part 3 of the CC.
- **Rationale** – This section describes the reasons and logic for the Security Objectives and Security Requirements.

### 1.4 Terminology

Both PPs use terms taken from the CC so in turn they provide definitions of the terms. This is to enable the user to more accurately follow the content of the

PPs. This interim report describes both Basic-Level and Medium-Level Firewalls so it is also necessary to include them here. The definitions are sourced from the Common Criteria Version 2.1 [2].

- Authentication Data – Information used to verify the claimed identity of a user.
- Authorized Administrator (AA) – A role which human users may be associated with to administer the security parameters of the TOE.
- Authorized External IT Entity – Any IT product or system, outside the scope of the TOE that may administer the security parameters of the TOE.
- Demilitarized Zone (DMZ) – A DMZ is a network that is mediated by the TOE.
- Evaluation Assurance Level (EAL) – An EAL is one of seven packages of security requirements from CC.
- Enclave – A collection of external IT entities protected by a TOE.
- External IT Entity – Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.
- Human User – Any person who interacts with the TOE.
- Identity – A representation (e.g., a string) uniquely identifying an authorized user.
- Operating Environment (OE) – The location and surroundings of where the TOE will work.
- Peer TOEs – Multiple, mutually authenticated TOEs that interact with each other.
- Protection Profile (PP) – It defines an implementation-independent set of security requirements and objectives for a category of products or systems that meet similar consumers' needs for IT security.
- Role – A predefined set of rules establishing the allowed interactions between a user and the TOE.
- Security Target – This is a specification of the security required by the TOE. The evaluation of the TOE considers this as the lowest target that the TOE has to achieve.
- Target Of Evaluation (TOE) – An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

- TOE Security Policy (TSP) – The TSP is a set of rules that regulate how assets are managed, protected and distributed within a TOE.
- TOE Security Functions (TSF) – A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.
- User – Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
- VPN – A Virtual Private Network (VPN) provides the ability to use a network (e.g., Internet, NIPRNET) as if it were a secure, private network [8].

## 1.5 Report Roadmap

Section 1, Introduction, provides a brief introduction to firewalls, Common Criteria (CC), Protection Profiles (PPs) and the terminology that is used in this report.

Section 2, Basic-Level FW PP, describes the security measures that appear in the U.S. Department of Defence (DOD) Firewall Protection Profile For Basic Robustness Environments [5].

Section 3, Basic-Level FW PP, Medium-Level FW PP and High-Level MG PP Contrasts, illustrates the comparisons and differences between the three papers studied.

Section 4, High-Level FW PP, provides a summary of the security measures that should be included in a High-Level Firewall PP.

Section 5, Observations and Conclusions, describes the conclusions that this project comes to and the future work that we plan to undertake in this area.

## 2 Basic-Level FW PP

This section describes the U.S. Department of Defence (DOD) Firewall Protection Profile For Basic Robustness Environments [5].

### 2.1 Protection Profile Introduction

The TOE described in the Basic-Level Firewall PP is a Boundary Gateway Device. A Boundary Gateway Device is a device that sits on the border between two networks and either permits the transfer of data or blocks it. The TOE is a firewall functional component that may either be a dedicated firewall gateway

device, or may be hosted on another device such as a router. The Basic-Level Firewall PP specifies the minimum-security requirements for firewalls used by the Department of Defence in basic robustness environments.

### **2.1.1 Protection Profile Overview**

This section contains mostly general information concerning the structure and organization of the PP. Apart from the general information, the relationship of the Basic-Level Firewall PP to other PPs is pointed out. The PPs that are listed below are precursors to the Basic-Level Firewall PP and can be considered as steps to its creation.

- U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments [4].
- U.S. Department of Defence Virtual Private Network (VPN) Boundary Gateway Protection Profile for Basic Robustness Environments Draft [6].

## **2.2 Target Of Evaluation**

The Target of Evaluation (TOE) is how the firewall is referred to from the TOE section on in the Basic-Level FW PP. This chapter describes the background, users and mechanisms of the TOE.

### **2.2.1 Background**

The development of the Basic-Level Firewall PP can be shown with the following steps.

1. Traffic-Filtering only examines a packet's header to determine whether it is permitted to traverse the firewall. This means high throughput.
2. Application-Level proxies can determine whether data can traverse the firewall based also on specific applications (e.g. HTTP). This means greater granularity.
3. Disintegration of the boundary between the two basic technological categories: Traffic-Filter and Application-Level (proxy) firewalls.
4. Hybrid firewall created.

### **2.2.2 TOE Security Policy**

This section provides descriptions of the different structures that a network can take and the flows of communication that are allowed.

- The TOE selectively routes information flows among internal and external networks according to security policy rules.
- The default is always to deny all inbound and outbound information flows.
- The AA has the authority to change the security policy rules.
- An information flow from an external network to an internal network must first be authenticated.
- Access to internal network services from external networks must use a VPN mechanism.
- The VPN provides individual user authentication and a secure communications path through external networks to the TOE and into the internal network.
- Technologies used by the Basic-Level TOE to authenticate the AA include one-time passwords, digital certificates or biometrics. Not constrained to these though.

### **2.2.3 Users of the TOE**

Users of the TOE include both humans and IT entities.

- Human users sending information from an external network to an internal network have to be identified and authenticated using a VPN mechanism.
- Only AAs may access the TOE through remote means from an internal or external network (also done with the use of VPNs).
- AAs may also access the TOE locally via a secure communications channel or a direct connection to a console port.
- External IT entities on internal network do not have to be identified and authenticated.
- External IT entities on external networks have to be identified and authenticated using VPN unless information is destined for DMZ.



#### 2.2.4 Audit

Audit events are collections of data that are recorded in case of security violation.

- Modifications to the individuals associated with AA role.
- Use of ID and authentication mechanisms.
- Changes made to TSP, mechanisms and data.
- Actions taken due to imminent security violations.
- Decisions made by TOE to enforce security policy rules.
- Changes to the TOE's date and time.
- Use of other security functions.

When the audit trail is 90% full, the AA events are recorded in the remaining 10% available.

#### 2.2.5 VPN Mechanisms

The Basic-Level Firewall TOE shall implement VPN mechanisms using technologies such as cryptography, key management, access control, authentication, and data integrity. The TOE meeting the Basic-Level Firewall PP has to meet or surpass a set of standards listed.

- TOE shall implement and conform to the Internet Engineering Task Force (IETF) Internet Protocol Security (IPSEC) Encapsulating Security Payload (ESP) protocol as specified in RFC 2406 [9].
- TOE encryption mechanisms shall conform to IETF ESP CBC-Mode Cipher Algorithms as specified in RFC 2451 [11].
- The TOE shall, at a minimum, implement the Triple DES (3DES) algorithms as specified in FIPS PUB 46-3 [7] and with usage for ESP outlined in RFC 2451 [11].
- TOE data integrity mechanisms shall conform to IETF Use of HMAC-SHA-1-96 within ESP and AH as specified in RFC 2404.
- The TOE shall use cryptographic modules that are compliant with FIPS PUB 140-2.
- The TOE shall perform key management and key exchange using the IETF-specified Internet Key Exchange (IKE) (RFC 2409) [10] which shall be FIPS PUB 140-2 compliant.

## 2.2.6 Evaluation Assurance Level

An EAL is one of seven packages of security requirements from CC. The numbers indicate which level along the scale they are. The TOE shall at a minimum, meet all of the assurance requirements defined by Part 3 of the CC for EAL2.

## 2.3 TOE Security Environment

The TOE Security Environment (TSE) is the surroundings of the TOE that contains all the threats, assumptions and policies of the TOE. Information systems are required by the Global Information Grid (GIG is a policy standard for the DOD) to be assigned a mission category that reflects the type of information processed by the system [3]. TOEs compliant with this PP can carry unclassified Mission Support or administrative data over any network, or Mission Critical data over an encrypted network. The information systems must employ mechanisms to ensure the level of robustness is relative to the sensitivity of the data and the threat agents involved.

### 2.3.1 Assumptions

These are conditions that are assumed to exist in Basic PP compliant TSE.

- A.CRYPTANALYTIC describes the standards that the cryptographic methods have to comply with. In the Basic-Level TOE they have to be evaluated to be FIPS 140-2 compliant.
- A.HARDENED. The operating system will have all mechanisms and services removed that are not required by the TOE.
- A.NO\_ENCLAVE\_PROTECTION deals with the flow of information between internal and external networks.
- A.NO\_EVIL states that AAs cannot intentionally be hostile, be properly trained and follow the guidelines set out.
- A.NO-GENERAL\_PURPOSE states that the TOE will have no general-purpose facilities like storage space available on it.
- A.NO\_PUBLIC\_DATA states that the TOE only holds TOE data and therefore does not hold public data.
- A.PHYSICAL\_SECURITY is just renamed A.PHYSEC in medium.
- A.REMOTE\_USERS states only AAs can access the TOE remotely from the internal or external network.

- A.SECURITY\_POLICY states that peer TOEs shall be administered to enforce compatible security policies.
- A.TOE\_ENTRY\_POINT states that information must pass through the TOE.

### 2.3.2 Threats to the TOE

Threat agents who are either unauthorized persons or external IT entities perpetrate the threats. The possible threats the TOE may face from a threat agent are listed below.

- T.ADDRESS\_SPOOFING. A threat agent masquerades as an AA, or an authorized external IT entity, or an external IT entity on the internal network by spoofing the source address.
- T.ATTACK\_CONFIGURATION\_DATA. A threat agent may try to read, modify, or destroy security-critical TOE configuration data.
- T.ATTACK\_POTENTIAL. In the basic the threat agent is only using obvious vulnerabilities to attempt to circumvent the TOE Security Functions (TSF).
- T.AUDIT\_FULL. A threat agent may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust storage capacity and therefore masking an attackers actions.
- T.AUDIT\_UNDETECTED. A threat agent may cause auditable events to go undetected.
- T.BRUTE\_FORCE. A threat agent tries to repeatedly guess authentication data in order to launch an attack against the TOE.
- T.CRYPTOGRAPHIC\_ATTACK. A threat agent, using a cryptographic attack may obtain information for which they it is not authorized.
- T.KEY\_COMPROMISE. A threat agent with the use of stolen or compromised cryptographic keys may decrypt sensitive data and gain unauthorized access to sensitive data.
- T.MASQUERADE. A threat agent through the use of stolen or compromised cryptographic keys may masquerade as a peer TOE and thus gain unauthorized access to sensitive data. Also, through the use of captured ID and authentication data, they could masquerade as an AA.
- T.REMOTE\_ATTACK. A threat agent may be able to view, modify, and/or delete security-related information that is sent between a remotely located AA and the TOE.

- T.REPLAY. A threat agent may replay valid ID and authentication information that has been captured to disguise itself as an AA or to use some of a TOEs other functions.
- T.RESIDUAL\_INFO. A threat agent may attempt to gather residual information from previous information flows or internal TOE data in order to gain authorized access to sensitive data.
- T.SERVICE\_MISUSE. A threat agent on the internal network may try to connect to services other than those expressly permitted. Additionally, a threat agent may attempt to send information through the TOE in order to exploit resources on the internal network.
- T.UNAUTHORIZED\_BYPASS. A threat agent 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.

### **2.3.3 Threats to the Operating Environment**

The following are possible threats to the environment that are not direct attacks on the system.

- T.CONFIGURATION. The TOE may be inadvertently configured, administered or used in an insecure manner by an AA.
- T.POOR\_MAINTENANCE. It states that AAs are not allowed to install software or hardware patches correcting known problems that may result in a compromise of confidentiality or integrity of TOE data.

### **2.3.4 Organizational Security Policies**

- P.ACCOUNTABILITY states that AAs will be held responsible for all security-relevant actions.
- P.ADMINISTRATION states that AAs shall administer the TOE locally or remotely through protected communications channels.
- P.AUDIT\_REVIEW states that audit data shall be reviewed, analyzed, and acted upon when necessary.
- P.CONFIDENTIALITY states that all traffic network sent to or received from an address associated with a peer TOE shall be encrypted or decrypted by the TOE where specified by the security policy. For inbound or outbound traffic with a peer TOE the local TOE shall create or use an existing secure channel between them.

- P.CRYPTO. The TOE shall support the IETF Internet Protocol Security Encapsulating Security Payload (IPSEC ESP) as specified in RFC 2406 [9]. The TOE shall utilize, at a minimum, the Triple DES (3DES) algorithm as specified in ESP CBC-Mode Cipher Algorithms (RFC 2451) [11]. The TOE shall utilize cryptographic modules that are compliant with FIPS PUB 140-2.
- P.INTEGRITY states that the TOE will support IETF IPSEC ESP as specified in RFC 2406 and that sensitive information transmitted to a peer TOE shall apply integrity mechanisms as specified in Use of HMAC-SHA-1-96 within ESP and AH (RFC 2404).
- P.KEY\_MANAGEMENT. The TOE shall support the IETF Internet Key Exchange (IKE) for key management and key exchange as specified in RFC 2409 [10].

## 2.4 Security Objectives

This section describes the security objectives for the TOE and the TOEs Operating Environment (OE).

### 2.4.1 Security Objectives for the TOE

- O.ACCOUNTABILITY. The TOE must provide user accountability for information flows through the TOE and for authorized administrator use of security functions related to audit.
- O.ADMINISTRATION. The TOE must provide tools for the AAs to manage and maintain itself. These have to be available remotely, through a direct connection or locally to the AA.
- O.AUDIT provides the means to accurately detect and record security-relevant events in audit records.
- O.CONFIDENTIALITY. Data flows between peer TOEs must be protected by encryption.
- O.EVALUATION\_ASSURANCE\_LEVEL. The TOE must meet all of the assurance requirements defined in EAL2 in Part 3 of the CC.
- O.INTEGRITY. Upon receipt of information from a peer TOE the data must be verified that it accurately represents the data that was originally transmitted.
- O.LIMIT\_EXTERNAL\_ACCESS. The TOE must provide the means for an AA to control and limit access to TOE Security Functions by an Authorized External IT Entity.

- O.MEDIATE. The TOE must mediate the flow of information between peer TOEs in accordance with their respective security policy and must ensure that residual information from a previous information flow is not revealed nor transmitted in any form or manner.
- O.SECURITY\_INFRASTRUCTURE. The TOE must protect the confidentiality and integrity of key management data and must ensure the proper exchange of keys.
- O.SELF\_PROTECT. The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.

#### **2.4.2 Security Objectives for the Operating Environment**

All of the Assumptions for the TSE from the Basic-Level FW PPs section 2.3.1 are considered to be security objectives for its environment. They are the security objectives that are to be defined by the IT domain or by non-technical or procedural means. That is they will be satisfied largely through application of procedural or administrative measures. They are all renamed here in this section with one addition that is not from 2.3.1.

- OE.CONFIGURATION states that the TOE, and any underlying operating system and hardware, must be installed, administered, and maintained in a manner that preserves the integrity and confidentiality of TOE data and data traversing the TOE.

### **2.5 IT Security Requirements**

This section documents the functional and assurance requirements that are to be satisfied by the Basic TOE. The requirements can be grouped into classes such as FIA, which deals with Identification and Authentication.

#### **2.5.1 TOE Functional Security Requirements**

The functional requirements are shown in the table (on the following pages, split into two parts) grouped into their general classes. They are all derived from the CC.

<b>Functional Component Class</b>	<b>Functional Component</b>	<b>Component Description</b>
Security Audit	FAU_ARP.1	Security alarms
	FAU_GEN.1	Audit data generation
	FAU_SAA.1	Potential violation analysis
	FAU_SAA.3	Simple attack heuristics
	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
	FAU_STG.1	Protected audit trail storage
	FAU_STG.3	Action in case of possible audit data loss
Cryptogr. Support	FAU_STG.4	Prevention of audit data loss
	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.2	Cryptographic key distribution
	FCS_CKM.4	Cryptographic key destruction
User Data Protection	FCS_COP.1	Cryptographic operation
	FDP_DAU.1	Basic data authentication
	FDP_IFC.1	Subset information flow control
	FDP_IFF.1	Simple security attributes
Identif. and Authentication	FDP_RIP.1	Subset residual information protection
	FIA_AFL.1	Authentication failure handling
	FIA_ATD.1	User attribute definition
	FIA_UAU.2	User authentication before any action
	FIA_UAU.4	Single-use authentication mechanisms
	FIA_UID.2	User identification before any action
	FMT_MOF.1	Management of security functions behaviour
	FMT_MSA.1	Management of security attributes
	FMT_MSA.2	Secure security attributes

Table 1, Part 1 – TOE Functional Security Requirements for the Basic-Level FW PP.

<b>Functional Component Class</b>	<b>Functional Component</b>	<b>Component Description</b>
Security Management	FMT_MSA.3	Static attribute initialisation
	FMT_MTD.1	Management of TSF data
	FMT_MTD.2	Management of limits on TSF data
	FMT_MTD.3	Secure TSF data
	FMT_SMR.1	Security roles
Protection of the TOE Security Functions	FPT_AMT.1	Abstract machine testing
	FPT_RPL.1	Replay detection
	FPT_RVM.1	Non-bypassability of the TSP
	FPT_SEP.1	TSF domain separation
	FPT_STM.1	Reliable time stamps
	FPT_TST.1	TSF testing

Table 1, Part 2 – TOE Functional Security Requirements for the Basic-Level FW PP.

### 2.5.2 TOE Security Assurance Requirements

The assurance requirements are shown grouped together in classes in the table on the following page, with descriptions of what they are necessary for.



Assurance Class	Assurance Component	Component Description
Configuration management	ACM_CAP.2	Configuration items
Delivery and operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation, and start-up procedures
Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.1	Descriptive high-level design
	ADV_RCR.1	Informal correspondence demonstration
Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability assessment	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

Table 2 – TOE Security Assurance Requirements for the Basic-Level FW PP.

## 2.6 Rationale

This section defines the reasons behind security measures being added or not added to the Basic PP. It describes the reasons for the following measures listed below.

- The TOE Security Objectives that are documented in section 2.4.1.
- The Security Objectives for the Environment that are documented in section 2.4.2.
- The Security Requirements that are in 2.5.1.
- The Assurance Requirements from 2.5.2.
- The non-addition of FMT\_MSA.2 and FMT\_MTD.3. This is because the PP is adequate for the Basic level without them.
- The choice of the level SOF-basic for this PP.

### **3 Basic-Level FW PP, Medium-Level FW PP and High-Level MG PP Contrasts**

The Basic-Level Firewall PP, Medium-Level Firewall PP and High-Level Mail Guard PP are all made for different levels of robustness. The Basic-Level FW PP forms the foundation for the Medium-Level FW PP. The Medium-Level FW PP improves on the security measures of the Basic-Level FW PP so that it can survive in a medium robustness environment. It is then assumed that the Medium-Level FW PP will form the foundation for the High-Level FW PP. Both Firewall PPs were sponsored by the same entity (National Security Agency (NSA)) so the comparisons and differences between the Basic-Level FW PP and Medium-Level FW PP will prove very informative about the kind of steps needed to make the step from one standard of firewall to another. Although the High-Level PP that has been reviewed is for a Mail Guard System it is useful for pointing out the security measures needed in a PP designed for a higher level. The High-Level MG PP was also sponsored by NSA for the U.S. Department of Defence (DoD) and gives a clear view of the updates for the higher security level because of its similar structure.

#### **3.1 Protection Profile Introduction**

This section is very similar in the three PPs. The Basic-Level FW PP, Medium-Level FW PP and High-Level MG PP describe their respective PP identification, their PP overview, their conventions in relation to CC (The three PPs use version 2.1 of CC), the CC terminology used and related PPs. The only difference between the Basic-Level FW PP and the Medium-Level FW PP is that the Medium-Level FW PP can list the Basic-Level FW PP as a related work because of its later development.

#### **3.2 Target Of Evaluation**

A very brief description of the TOE is conducted in the Medium-Level FW PP. The Basic-Level FW PP delves a lot deeper into the development of a hybrid firewall and its structure. The Basic-Level FW PP can be considered an introductory PP for the Medium-Level FW PP and thus explains the lack of information in the TOE section of the Medium-Level FW PP. The Medium-Level FW PP takes for granted that the reader has previous knowledge in the area of firewalls. A diagram can be provided to show where the Firewall devices mediate the flow of information. One is not included in the Medium-Level FW PP though they are present in the other two PPs studied.

In each PP AAs are described as being identified using such methods as one-time passwords, digital certificates or biometrics. The AAs can access the TOE

remotely in the Basic-Level and Medium-Level FW PPs after certain precautions are taken. In the High-Level MG PP this is not allowed. The AAs must administer the TOE locally via a physically protected direct connection to a console port.

In the Medium-Level FW PP when the audit trail is filled only auditable events made by the AAs are recorded. This same procedure is done in the Basic-Level FW PP and the High-Level MG PP when the data recorded exceeds 90%. However the extra feature that appears in the High-Level Mail Guard is the notifying of the AA when this happens.

The Basic-Level FW PP uses FIPS PUB 140-2 for its cryptographic modules. The Medium-Level FW PP uses FIPS PUB 140-1 for its cryptographic modules. The reason for the lower standards used in the Medium-Level FW PP is that it was produced before the Basic-Level FW PP. The High-Level MG PP uses FIPS PUB 186-2 to perform encryption/decryption and FIPS PUB 180-1 to compute a secure hash using the Hash Algorithm (SHA-1).

The Basic-Level FW PP must satisfy the requirements set out in EAL2. EAL is not mentioned in this section in the Medium-Level FW PP. The High-Level MG PP must at least satisfy the requirements for EAL4 and in most cases EAL6.

### **3.3 TOE Security Environment**

TOEs compliant with the Medium-Level FW PP must be able to fend off attackers that possess a moderate attack potential whereas the Basic-Level FW PP has to fend off attackers with a basic attack potential. Concordantly the High-Level MG PP has to fend off attackers with a high attack potential.

#### **3.3.1 Assumptions**

The following are the differences that have emerged when the corresponding three sections regarding the assumptions of security aspects from the three PPs studied are compared.

<b>Assumptions</b>	<b>Basic-Level FW PP</b>	<b>Medium- Level FW PP</b>	<b>High-Level MG PP</b>
A.CRYPTANALYTIC	Present		Updated to A.CRYPTO- GRAPHY
A.HARDENED	Present		
A.NO_ENCLAVE_PROTEC- TION	Present		
A.TOE_ENTRY_POINT	Present		Present
A.SINGEN		Present	
A.NO-GENERAL_PURPOSE	Present	Renamed A.GENPUR	
A.NO_PUBLIC_DATA	Present	Renamed A.PUBLIC	
A.PHYSICAL_SECURITY	Present	Renamed A.PHYSEC	Present
A.REMOTE_USERS	Present		
A.NOREMO		Present	
A.REMACC		Present	
A.SECURITY_POLICY	Present		
A.DIRECT		Present	
A.NO_EVIL	Present		Renamed A.NO_EV IL_USERS
A.NO_EVIL_PROGRAMS			Present

Table 3 – The TOE Security Environment Assumption contrasts between PPs.

### 3.3.2 Threats to the TOE

The difference between the sections relating to the threats in the three PPs is addressed below.

Threats	Basic-Level PP	Medium-Level PP	High-Level PP MG
T.ADDRESS_SPOOFING	Present	Renamed T.ASPROOF	T.ADDRESS_SPOOFING
T.ATTACK_CONFIGURATION NB in basic it does not take in modifying	Present	Renamed T.SELFPRO	Renamed T.MODIFY_DATA
T.ATTACK_POTENTIAL	Present	Updated to T.MODEXP	
T.AUDIT_FULL	Present	Renamed T.AUDFUL	T.AUDIT_FULL
T.AUDIT_UNDETECTED	Present	Renamed T.AUDACC	T.AUDIT_UNDETECTED
T.BRUTE_FORCE	Present	Renamed T.REPEAT	T.BRUTE_FORCE
T.CRYPTOGRAPHIC_ATTACK	Present		Present
T.KEY_COMPROMISE	Present		
T.MASQUERADE	Present		Present
T.REMOTE_ATTACK	Present	Renamed T.PROCOM	
T.REPLAY	Present	Present	
T.RESIDUAL	Present	Updated to T.OLDINF	
T.SERVICE_MISUSE	Present	Replaced by T.MEDIAT	
T.UNAUTHORIZED_BYPASS	Present	Renamed T.NOAUTH	Renamed T.BYPASS
T.ADMINISTRATION			Present
T.DISCLOSURE			Present
T.EXCESS_AUDIT			Present
T.HIGH_ATTACK_POTENTIAL			Present
T.IDENTIFICATION_AUTHENTICATION			Present
T.INCORRECT_LEVEL			Present
T.COVERT_CHANNEL			Present

Table 4 – The TOE Security Environment Threat contrasts between PPs.

### 3.3.3 Threats to the Operating Environment

The differences between the three PPs respective sections relating to the threats to the OE are shown below.

<b>Threats</b>	<b>Basic-Level PP</b>	<b>Medium-Level PP</b>	<b>High-Level PP MG</b>
T.CONFIGURATION	Present	Renamed T.USAGE	
T.POOR_MAINTENANCE	Present		
T.KEY_COMPROMISE			Present

Table 5 – The Operating Environment Threat contrasts between PPs.

### 3.3.4 Organizational Security Policies

The following table shows the organizational security policies that each PP must address.

<b>Security Policies</b>	<b>Basic-Level FW PP</b>	<b>Medium-Level FW PP</b>	<b>High-Level PP MG</b>
P.ACCOUNTABILITY	Present		
P.ADMINISTRATION	Present		
P.AUDIT_REVIEW	Present		
P.CONFIDENTIALITY	Present		
P.CRYPTO	Present	Updated Version Present	Updated version from Medium-Level
P.INTEGRITY	Present		
P.KEY_MANAGEMENT	Present		
P.MANDATORY_ACCESS_CONTROL			Present

Table 6 – The Organizational Security Policy contrasts between PPs.

### 3.3.5 Encryption Standards

The TOE that satisfies the Basic-Level FW PP shall support the IETF Internet Protocol Security Encapsulating Security Payload (IPSEC ESP) as specified in RFC 2406. The TOE shall utilize, at a minimum, the Triple DES (3DES) algorithm as specified in ESP CBC-Mode Cipher Algorithms (RFC 2451). The TOE shall utilize cryptographic modules that are compliant with FIPS PUB 140-2.

The Medium-Level FW PP will use triple DES encryption (as specified in FIPS 46-3 [4]) to protect remote administration functions and at a minimum the associated cryptographic must comply with FIPS 140-1 (level 1). Different specifications from the 3DES in the Basic-Level FW PP appear in the Medium-Level FW PP.

TOEs meeting the High-Level MG PP shall verify digital signatures according to the Digital Signature Algorithm (as specified in FIPS PUB 186-2), perform encryption/decryption using an NSA-certified high robustness algorithm, and compute a secure hash using the Secure Hash Algorithm (SHA-1) (as specified in FIPS PUB 180-1).

### **3.4 Security Objectives**

#### **3.4.1 TOE Security Objectives**

The following are the differences between the TOE Security Objectives of the three different PP levels.

Table 7 – following page – The TOE Security Objective contrasts between PPs.

<b>Security Objectives</b>	<b>Basic-Level PP</b>	<b>Medium-Level PP</b>	<b>High-Level PP MG</b>
O.ACCOUNTABILITY	Present	Split into O.ACCOUN & O.IDAUTH	O.ACCOUNT- ABILITY
O.ADMINISTRATION	Present		Present
O.AUDIT	Present	Updated to O.AUDREC	Present
O.CONFIDENTIALITY	Present	Replaced by O.ENCRYPT	O.CONFIDEN- TIALITY
O.EVALUATION_ ASSURANCE_LEVEL	Present	Replaced by O.EAL	
O.INTEGRITY	Present		O.DATA_IN-TEGRITY
O.LIMIT_EXTERNAL_ ACCESS	Present	Renamed O.LIMEXT	
O.MEDIATE	Present	Updated to O.MEDIAT	
O.SECURITY_ INFRASTRUCTURE	Present		
O.SELF_PROTECT	Present	Renamed O.SELFPRO	O.SELF_PRO-TECT
O.SINUSE		Present	
O.SECSTA		Present	
O.SECFUN		Present	
O.AUDIT_PROTECT			Present
O.AUDIT_SELECT			Present
O.AUTHENTICATION			Present
O.COVERT_CHANNEL			Present
O.CRYPTOGRAPHY			Present
O.DOMAIN_SEPARATION			Present
O.IMPERSONATE			Present
O.INFORMATION_FLOW			Present
O.MULTI_LEVEL_PORT			Not applicable
O.NON-BYPASSABILITYT			Present
O.RECOVERY			Present
O.ROLE_SEPARATION			Present
O.SELF_TEST			Present
O.SINGLE_LEVEL_PORT			Not applicable
O.SOF			Present



### 3.5 IT Security Requirements

#### 3.5.1 TOE Security Requirements

This section contains tables outlining the differences between the three different Protection Profiles Security Requirements section.

The following all appear in the Basic-Level FW PP but are absent from the Medium-Level FW PP.

<b>Functional Components</b>	
FAU_ARP.1	Security alarms
FAU_SAA.1	Potential violation analysis
FAU_SAA.3	Simple attack heuristics
FAU_STG.3	Action in case of possible audit data loss
FCS_CKM.1	Cryptographic key generation
FCS_CKM.2	Cryptographic key distribution
FCS_CKM.4	Cryptographic key destruction
FDP_DAU.1	Basic data authentication
FDP_RIP.1	Subset residual information protection
FIA_UAU.2	User authentication before any action
FIA_UAU.4	Single-use authentication mechanisms
FMT_MOF.1	Management of security functions behaviour
FMT_MSA.2	Secure security attributes
FMT_MTD.3	Secure TSF data
FPT_AMT.1	Abstract machine testing
FPT_RPL.1	Replay detection
FPT_TST.1	TSF testing

Table 8 – Functional Components that are present in the Basic-Level FW PP but are absent from the Medium-Level FW PP.

The following requirements are additions to the Medium-Level FW PP that are not present in the Basic-Level FW PP.

<b>Functional Components</b>	
FIA_UAU.5	Multiple authentication mechanisms
FMT_MSA.1	Management of security attributes (2)
FMT_MSA.1	Management of security attributes (3)
FMT_MSA.1	Management of security attributes (4)
FDP_RIP.1	Subset residual information protection
FMT_MOF.1	Management of security functions behaviour (1)
FMT_MOF.1	Management of security functions behaviour (2)

Table 9 – TOE Functional Security Requirements present in the Medium-Level FW PP but not in the Basic-Level FW PP.

The following table contains all the Functional Components that are present in the High-Level MG PP. It also notes if they are present in the Basic-Level and Medium-Level FW PPs or if they are new to the High-Level Mail Guard PP.

<b>Functional Component Class</b>	<b>Functional Component</b>	<b>Basic-Level FW PP</b>	<b>Medium-Level FW PP</b>	<b>High-Level MG PP</b>
Security Audit	FAU_GEN.1	Present	Present	
	FAU_SAA.1	Present		
	FAU_SEL.1			Present
	FAU_STG.1	Present	Present	
	FAU_STG.3	Present		
	FAU_STG.4	Present	Present	
Cryptographic Support	FCS_COP.1	Present	Present	
User Data Protection	FDP_ETC.1			Present
	FDP_ETC.2			Present
	FDP_IFC.1	Two subsets present	Two subsets present	
	FDP_IFF.2			Present
	FDP_IFF.3			Present
	FDP_ITC.1			Present
	FDP_ITC.2			Present
FDP_RIP.2			Present	
Identification and Authentication	FIA_AFL.1	Present	Present	
	FIA_ATD.1	Present	Present	
	FIA_UAU.2	Present		
	FIA_UAU.4	Present		
	FIA_UID.2	Present	Present	
Security Management	FMT_MOF.1	Present		
	FMT_MSA.1	Present	Present	
	FMT_MSA.2	Present		
	FMT_MSA.3	Present	Present	
	FMT_MTD.1	Present	Present	
	FMT_SMR.2			Present
	FMT_SMR.3			Present
Protection of the TOE Security Functions	FPT_AMT.1	Present		
	FPT_ITT.1			Present
	FPT_RCV.2			Present
	FPT_RPL.1	Present		
	FPT_RVM.1	Present	Present	
	FPT_SEP.2			Present
	FPT_STM.1	Present	Present	
	FPT_TDC.1			Present
	FPT_TST.1	Present		
	FTP_ITC.1			Present
FTP_TRP.1			Present	

Table 10 – All the TOE Functional Security Requirements that are present in the High-Level MG PP with indications if they are present in the Basic-Level and/or the Medium-Level FW PPs.

### **3.5.2 TOE Security Assurance Requirements**

The differences between the three PPs corresponding Assurance Requirements sections are documented below.

Assurance Class	Assurance Components	Basic-Level PP	Medium-Level PP	High-Level PP
Configuration Management	ACM_CAP.2	Present	Present	
	ACM_AUT.1			Present
	ACM_CAP.4			Present
	ACM_SCP.2			Present
Delivery and Operation	ADO_DEL.1	Present	Present	
	ADO_DEL.2			Present
	ADO_IGS.1	Present	Present	Present
Development	ADV_FSP.1	Present	Present	
	ADV_HLD.1	Present		
	ADV_RCR.1	Present	Present	
	ADV_HLD.2		Present	
	ADV_IMP.1		Present	
	ADV_LLD.1		Present	
	ADV_FSP.3			Present
	ADV_HLD.4			Present
	ADV_IMP.3			Present
	ADV_INT.2			Present
	ADV_LLD.2			Present
	ADV_RCR.2			Present
	ADV_SPM.2			Present
Guidance Documents	AGD_ADM.1	Present	Present	Present
	AGD_USR.1	Present	Present	Present
Life Cycle Support	ALC_DVS.2			Present
	ALC_FLR.3			Present
	ALC_LCD.1			Present
	ALC_TAT.1		Present	Present
Tests	ATE_COV.1	Present	Present	
	ATE_FUN.1	Present	Present	
	ATE_IND.2	Present	Present	Present
	ATE_COV.3			Present
	ATE_DPT.2			Present
	ATE_FUN.2			Present
Vulnerability Assessment	AVA_SOF.1	Present	Present	Present
	AVA_VLA.1	Present		
	AVA_VLA.3		Present	
	AVA_CCA.2			Present
	AVA_MSU.3			Present
	AVA_VLA.4			Present

Table 11 – TOE Security Assurance Requirements presence in the three Protection Profiles studied.

### **3.6 Rationale**

The rationale sections for the Basic-Level FW PP, Medium-Level FW PP and the High-Level MG PP all go through the reasoning behind including their respective IT Security Objectives, OE Security Objectives, Security Requirements and the Assurance Requirements. The Basic-Level FW PP and the High-Level MG PP both rationalise why they shoes their respective SOF level.

## **4 High-Level FW PP**

This section provides a summary of what should be included in an Application-Level Firewall Protection Profile for High Robustness Environments.

### **4.1 Protection Profile Introduction**

The High-Level Firewall PP will specify the minimum-security requirements for firewalls used by the Department of Defence in high robustness environments.

#### **4.1.1 Protection Profile Identification**

PP Identification will be updated to name the title as Application-level Firewall Protection Profile For High Robustness Environments. The Sponsor, Authors, Registration and PP Version fields can similarly be updated. There is only one section of real interest in the Identification, the CC Version that is to be used. The version that will be used for the High-Level Firewall PP will be CC Version 2.1 as it is used in its precursors and in the High-Level Mail Guard PP.

#### **4.1.2 Protection Profile Overview**

The target robustness level will be “high” as specified in the Guidance and Policy for the Department of Defence Global Information Grid Information Assurance (GIG) [3].

#### **4.1.3 Conventions**

The notation, formatting and conventions used in the High-Level FW PP will be largely consistent with those used in version 2.1 of the Common Criteria (CC). It will also retain the presentation choices that were made in the three PPs studied. These relate to the following operations; refinement, selection,

assignment, iteration and security target writer, which can be performed on the functional requirements.

#### **4.1.4 Terminology**

This section will have the union of terms mentioned in the respective sections of the Basic-Level FW PP and the Medium-Level FW PP.

#### **4.1.5 Related Protection Profiles**

This section will contain the following list of Protection Profiles.

- U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments [4].
- U.S Department of Defence Application-level Firewall Protection Profile for Basic Robustness Environments [5].
- U.S. Department of Defence Virtual Private Network (VPN) Boundary Gateway Protection Profile for Basic Robustness Environments [6].
- U.S. Department of Defence Traffic-Filter Firewall Protection Profile for Medium Robustness Environments [13].
- U.S Department of Defence Application-level Firewall Protection Profile for Medium Robustness Environments [14].
- U.S. Department of Defence Application-level Firewall Protection Profile for Basic Robustness Environments [15].

#### **4.1.6 Protection Profile Organization**

The High-Level FW Protection Profile will be split into the following sections.

- Section 1, Protection Profile (PP) Introduction.
- Section 2, Target of Evaluation (TOE) Description.
- Section 3, TOE Security Environment (TSE).
- Section 4, Security Objectives.
- Section 5, IT Security Requirements.
- Section 6, Rationale.
- References.
- Acronyms.

## 4.2 Target Of Evaluation

A diagram will be provided to show where the Firewall devices mediate the flow of information.

The AAs can access the TOE remotely in the Basic-Level and Medium-Level FW PPs after certain precautions are taken. In the High-Level FW PP this will not be allowed. The AAs must administer the TOE locally via a physically protected direct connection to a console port.

In the High-Level FW PP when the audit data recorded exceeds 90% only auditable events made by the AAs will be recorded. The AAs will also be notified when this event occurs.

The High-Level FW PP will use FIPS PUB 140-2 and FIPS PUB 180-1 to compute a secure hash using the Hash Algorithm (SHA-1).

The High-Level FW PP will state that TOEs meeting the requirements of this PP must at least satisfy the requirements for EAL4 and in some cases EAL6.

## 4.3 TOE Security Environment

High Robustness is defined in the GIG policy as: “security services and mechanisms that provide thorough rigorous analysis, the most confidence in the security countermeasures”. So the technical solutions that the High-Level Firewall must use that are required by the GIG are the following.

- Certified (e.g. NSA) high-robustness cryptography (algorithms and implementation) for encryption, key exchange, digital signature and hash.
- NSA-certified high-robustness cryptographically authenticated access control (e.g., digital signature, public key cryptography based, challenge/response identification and authentication).
- Approved (e.g. NSA) key management for symmetric key.
- Class 5 PKI certificates for asymmetric key.
- High Assurance security design that meets at a minimum Evaluated Assurance Level (EAL) 4, as defined in the Common Criteria (CC).

### 4.3.1 Assumptions

Below is the table of assumptions that will appear in the High-Level FW PP.



<b>Assumptions</b>	<b>Source of Assumption</b>
A.CRYPTOGRAPHY	High-Level MG PP
A.HARDENED	Basic-Level FW PP
A.NO_ENCLAVE_PROTECTION	Basic-Level FW PP
A.TOE_ENTRY_POINT	Basic-Level FW PP
A.SINGEN	Medium-Level FW PP
A.NO-GENERAL_PURPOSE	Basic-Level FW PP
A.NO_PUBLIC_DATA	Basic-Level FW PP
A.PHYSICAL_SECURITY	Basic-Level FW PP
A.SECURITY_POLICY	Basic-Level FW PP
A.DIRECT	Medium-Level FW PP
A.NO_EVIL	Basic-Level FW PP
A.NO_EVIL_PROGRAMS	High-Level MG PP

Table 12 – TOE Security Environment Assumptions for the High-Level FW PP.

#### 4.3.2 Threats to the TOE

The threats that will be addressed by the High-level FW PP are shown with their source as well. Table 13 – below – TOE Security Environment Threats for the High-Level FW PP.

<b>Threats</b>	<b>Source of Threat</b>
T.ADDRESS_SPOOFING	Basic-Level FW PP
T.ATTACK_CONFIGURATION	Medium-Level FW PP
T.HIGH_ATTACK_POTENTIAL	Updated to high attack potential
T.AUDIT_FULL	Basic-Level FW PP
T.AUDIT_UNDETECTED	Basic-Level FW PP
T.BRUTE_FORCE	Basic-Level FW PP
T.CRYPTOGRAPHIC_ATTACK	Basic-Level FW PP
T.KEY_COMPROMISE	Basic-Level FW PP
T.MASQUERADE	Basic-Level FW PP
T.REMOTE_ATTACK	Basic-Level FW PP
T.REPLAY	Basic-Level FW PP
T.OLDINF	Medium-Level FW PP
T.MEDIAT	Medium-Level FW PP
T.UNAUTHORIZED_BYPASS	Basic-Level FW PP
T.ADMINISTRATION	High-Level MG PP
T.DISCLOSURE	High-Level MG PP
T.EXCESS_AUDIT	High-Level MG PP
T.HIGH_ATTACK_POTENTIAL	High-Level MG PP
T.IDENTIFICATION_AUTHENTI-CATION	High-Level MG PP
T.INCORRECT_LEVEL	High-Level MG PP
T.COVERT_CHANNEL	High-Level MG PP

### 4.3.3 Threats to the Operating Environment

Threats	Source of Threat
T.CONFIGURATION	Basic-Level FW PP
T.POOR_MAINTENANCE	Basic-Level FW PP
T.KEY_COMPROMISE	High-Level MG PP

Table 14 – Threats to the Operating Environment for the High-Level FW PP.

### 4.3.4 Organizational Security Policies

Security Policies	Security Policy Source
P.ACCOUNTABILITY	Basic-Level FW PP
P.ADMINISTRATION	Basic-Level FW PP
P.AUDIT_REVIEW	Basic-Level FW PP
P.CONFIDENTIALITY	Basic-Level FW PP
P.CRYPTO	High-Level MG PP
P.INTEGRITY	Basic-Level FW PP
P.KEY_MANAGEMENT	Basic-Level FW PP
P.MANDATORY_ACCESS_CONTROL	High-Level MG PP

Table 15 – Organizational Security Policies for the High-Level FW PP.

## 4.4 Security Objectives

This section shows the security objectives for the TOE and the TOEs Operating Environment (OE) for the High-Level Firewall Protection Profile.

#### 4.4.1 Security Objectives for the TOE

Security Objectives	Security Objective Source
O.ACCOUNTABILITY	Basic-Level FW PP
O.ADMINISTRATION	Basic-Level FW PP
O.AUDIT	Medium-Level FW PP
O.CONFIDENTIALITY	High-Level MG PP
O.EVALUATION_ ASSURANCE_LEVEL	Updated to EAL4
O.INTEGRITY	Basic-Level FW PP
O.LIMIT_EXTERNAL_ACCESS	Basic-Level FW PP
O.MEDIATE	Medium-Level FW PP
O.SECURITY_INFRASTRUCTURE	Basic-Level FW PP
O.SELF_PROTECT	Basic-Level FW PP
O.SINUSE	Medium-Level FW PP
O.SECSTA	Medium-Level FW PP
O.SECFUN	Medium-Level FW PP
O.AUDIT_PROTECT	High-Level MG PP
O.AUDIT_SELECT	High-Level MG PP
O.AUTHENTICATION	High-Level MG PP
O.COVERT_CHANNEL	High-Level MG PP
O.CRYPTOGRAPHY	High-Level MG PP
O.DOMAIN_SEPARATION	High-Level MG PP
O.IMPERSONATE	High-Level MG PP
O.INFORMATION_FLOW	High-Level MG PP
O.NON-BYPASSABILITY	High-Level MG PP
O.RECOVERY	High-Level MG PP
O.ROLE_SEPARATION	High-Level MG PP
O.SELF_TEST	High-Level MG PP
O.SOF	High-Level MG PP

Table 16 – TOE Security Objectives for the High-Level FW PP.

#### 4.4.2 Security Objectives for the Operating Environment

All of the assumptions stated in section 4.3.1 are considered to be security objectives for the High-Level Firewall environment and will be found in this section as well. The only two exceptions are listed below. The first one appears in the Basic-Level FW PP and the second appears in the Medium-Level FW PP. Both will be included in the High-Level FW PP.

- OE.CONFIGURATION states that the TOE, and any underlying operating system and hardware, must be installed, administered, and maintained in a manner that preserves the integrity and confidentiality of TOE

data and data traversing the TOE.

- O.ADMTRA states that Authorized Administrators are trained as to the establishment and maintenance of security policies and practices.

## **4.5 IT Security Requirements**

This section documents the functional and assurance security requirements that are to be included in the High-Level FW PP.

### **4.5.1 TOE Functional Security Requirements**

The functional requirement for the High-Level FW PP is the union of the set of functional components listed in the Basic-Level FW PP section (2.5.1) and the table below. The table below consists of functional components that are sourced from the Medium-Level FW PP and the High-Level MG PP but do not appear in the Basic-Level FW PP.

<b>Functional Component Class</b>	<b>Functional Component</b>	<b>Component source</b>
Security Audit	FAU_SEL.1	High-Level MG PP
User Data Protection	FDP_ETC.1	High-Level MG PP
	FDP_ETC.2	High-Level MG PP
	FDP_IFF.2	High-Level MG PP
	FDP_IFF.3	High-Level MG PP
	FDP_ITC.1	High-Level MG PP
	FDP_ITC.2	High-Level MG PP
	FDP_RIP.1	Medium-Level FW PP
	FDP_RIP.2	High-Level MG PP
Identification and Authentication	FIA_UAU.5	Medium-Level FW PP
Security Management	FMT_MOF.1 (1)	Medium-Level FW PP
	FMT_MOF.1 (2)	Medium-Level FW PP
	FMT_MSA.1 (2)	Medium-Level FW PP
	FMT_MSA.1 (3)	Medium-Level FW PP
	FMT_MSA.1 (4)	Medium-Level FW PP
	FMT_SMR.2	High-Level MG PP
	FMT_SMR.3	High-Level MG PP
Protection of the TOE Security Functions	FPT_ITT.1	High-Level MG PP
	FPT_RCV.2	High-Level MG PP
	FPT_SEP.2	High-Level MG PP
	FPT_TDC.1	High-Level MG PP

Table 17 – The TOE Security Functional Requirements that will appear in the

High-Level FW PP.

#### **4.5.2 TOE Security Assurance Requirements**

The assurance requirements that will be in the High-Level FW PP are shown grouped together in classes in the table below.

Table 18 – following page – TOE Security Assurance Requirements for the High-Level FW PP.

<b>Assurance Class</b>	<b>Assurance Components</b>	<b>Component Source</b>
Configuration Management	ACM_CAP.2	Basic-Level FW PP
	ACM_AUT.1	High-Level MG PP
	ACM_CAP.4	High-Level MG PP
	ACM_SCP.2	High-Level MG PP
Delivery and Operation	ADO_DEL.1	Basic-Level FW PP
	ADO_DEL.2	High-Level MG PP
	ADO_IGS.1	Basic-Level FW PP
Development	ADV_FSP.1	Basic-Level FW PP
	ADV_HLD.1	Basic-Level FW PP
	ADV_RCR.1	Basic-Level FW PP
	ADV_HLD.2	Medium-Level FW PP
	ADV_IMP.1	Medium-Level FW PP
	ADV_LLD.1	Medium-Level FW PP
	ADV_FSP.3	High-Level MG PP
	ADV_HLD.4	High-Level MG PP
	ADV_IMP.3	High-Level MG PP
	ADV_INT.2	High-Level MG PP
	ADV_LLD.2	High-Level MG PP
	ADV_RCR.2	High-Level MG PP
	ADV_SPM.2	High-Level MG PP
Guidance Documents	AGD_ADM.1	Basic-Level FW PP
	AGD_USR.1	Basic-Level FW PP
Life Cycle Support	ALC_DVS.2	High-Level MG PP
	ALC_FLR.3	High-Level MG PP
	ALC_LCD.1	High-Level MG PP
	ALC_TAT.1	Medium-Level FW PP
Tests	ATE_COV.1	Basic-Level FW PP
	ATE_FUN.1	Basic-Level FW PP
	ATE_IND.2	Basic-Level FW PP
	ATE_COV.3	High-Level MG PP
	ATE_DPT.2	High-Level MG PP
	ATE_FUN.2	High-Level MG PP
Vulnerability Assessment	AVA_SOF.1	Basic-Level FW PP
	AVA_VLA.1	Basic-Level FW PP
	AVA_VLA.3	Medium-Level FW PP
	AVA_CCA.2	High-Level MG PP
	AVA_MSU.3	High-Level MG PP
	AVA_VLA.4	High-Level MG PP

## 4.6 Rationale

This section will be updated to justify what has been placed into the High-Level Firewall PP. As an example of what will be placed in this section an in-depth view into the inclusion of some of the security measures from the High-Level Mail Guard PP is included.

### 4.6.1 Same Level Data Flow Measure

The first security measure that will be explained is one of the Organizational Security Policies from the Security Environment Section. This is the P.MANDATORY\_ACCESS\_CONTROL policy. It is a mandatory access control policy based on hierarchical security levels. Information shall not be allowed to flow from a higher security level to a lower security level or between non-comparable security levels. This policy appears in the High-Level Mail Guard PP but in neither of the High-Level Firewall PP precursors. Information is categorised to its level of sensitivity and is therefore meant to stay at its defined level. With this policy a user cannot transmit this information to a lower security level whether intentionally or by accident. It stops the intentional compromising of information by a threat agent or the accidental compromising by a user who might try and send it to a lower security level.

### 4.6.2 Local AA Access Measure

The second security measure that is to be included is one that involves the remote administration abilities of the Authorized Administrators (AA). The AAs can access the TOE remotely in the Basic-Level and Medium-Level Firewall PPs after certain precautions are taken. These precautions include the identification and authentication of the AA by the TOE using a VPN mechanism before the TOE will allow the information to flow into the network. In the High-Level Mail Guard PP this is not allowed. The AAs must administer the TOE locally via a physically protected direct connection to a console port. The ability to remotely administer the TOE provides another line of attack for a threat agent. The communication could be monitored and the authentication and identification information could be stolen and reused by a threat agent. With the AA having to locally administer the TOE this type of attack is made impossible. It means that whatever sensitive information being protected behind the Firewall cannot be deleted or corrupted by a threat agent pretending to be an AA from a remote location. When AAs are required to administer the TOE locally they also have to pass through additional security measures. These can include multifactor user authentication and the inspection of the person by security personnel.



### 4.6.3 Audit Security Measure

When the audit trail is filled in the Medium-Level Firewall PP, only auditable events made by the AAs are recorded. This same procedure is done in the High-Level PP when the data recorded exceeds 90%. However the extra feature that will be added to the High-Level Firewall PP that appears in the High-Level Mail Guard PP is the notifying of the AA when this happens.

In the section Threats Addressed By The TOE the audit records issue is referred to. In the Basic-Level and Medium-Level Firewall PPs and also the High-Level Mail Guard PP, the threats T.AUDIT\_FULL and T.AUDIT\_UNDETECTED are present. T.AUDIT\_FULL states that an agent may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust storage capacity, thus masking an attackers actions. T.AUDIT\_UNDETECTED deals with the threat that an agent may cause auditable events to go undetected. In the High-Level Mail Guard PP there is an extra measure dealing with the audit, T.EXCESS\_AUDIT. This threat is when a threat agent may cause an Authorized Administrator to be unable to analyze audit data due to an excess volume of data being recorded. In the Security Objectives section of the High-Level Mail Guard PP this threat is answered by the O.Audit objective. The objective states that the TOE must detect and notify the Authorized Administrator and/or the Guard Application Administrator when the audit log becomes full. This means that the audit trail will not lose track of auditable events and that the TOE cannot be tampered with without there being a record of it.

### 4.6.4 Authentication of AAs

A new measure that is found in the High-Level Mail Guard PP and not in the Basic-Level and Medium-Level Firewall PPs is the authentication objective. O.AUTHENTICATION states that the TOE must require that AAs and Guard Application Administrators be authenticated (via a single-use authentication mechanism) before performing any TSF-mediated activities. Authentication of information passing through the TOE must be based on cryptographic mechanisms. The TOE must prevent brute force attacks by limiting the number of authentication attempts allowed in a session. In both the Basic-Level and Medium-Level Firewall there is no mention of ways to combat the possible threat of a threat agent using brute force methods to authenticate itself as an AA. With measures for the limiting of authentication attempts per session the possibility of a threat agent impersonating an AA are drastically reduced.

#### **4.6.5 Strength of Function**

There are three Strength Of Function levels defined in Part 1 of the Common Criteria: SOF-basic, SOF-medium and SOF-high. SOF-high is the strength of function level for the High-Level Firewall PP. SOF-high states, “a level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organized breach of TOE security by attackers possessing a high attack potential”. SOF-high is needed to counteract the threat T.HIGH\_ATTACK\_POTENTIAL.

#### **4.6.6 Acronyms and References**

These sections will appear the same in the High-Level Firewall PP as they do in the appendix of this report.

## **5 Observations and Conclusions**

Firewalls act as a boundary between an internal network and an external network. They either permit or block the flow of information across this boundary. Firewalls used to be categorised as either traffic-filter or application-level (proxy) firewalls. Traffic-filter firewalls provide greater throughput by typically only examining a packets headers to determine whether or not to allow the packet across the firewall. Application-level proxies provide the firewall with greater security granularity by providing policy enforcement not only based on IP address or transport layer protocol, but on specific application.

The Protection Profile Database constructed in the project provides an easily navigated and viewed environment for the security measures of the three PPs studied, their contrasts and the conclusions on what security measures should be included in a High-Level FW PP.

To use the analogy of building a house, the U.S. Department of Defence Firewall Protection Profile For Basic Robustness Environments can be considered as our foundation for Protection Profile research. The U.S. Department of Defence Application-Level Firewall Protection Profile for Medium Robustness Environments builds on this foundation. However to make it strong enough to endure the harshest environment, the Application-Level Firewall Protection Profile for High Robustness Environments will provide the reinforcement. The U.S. Department of Defence Mail Guard For High Robustness Environments provides the insight into what is required to endure the harshest environments.

The Medium-Level FW PP is a step up from the Basic-Level FW PP. Then it is logical to assume that the High-Level FW PP will have roughly the same step up in standards from the Medium-Level FW PP. The Medium-Level FW PP

incorporates most of the security measures from the Basic-Level FW PP and bolsters them with new security measures for its level. This leads to the decision that the High-Level FW PP will consist of most of the security measures from the Medium-Level FW PP with the addition of certain security constraints that will atone for the security level step up.

The U.S. Department of Defence Mail Guard for High Robustness Environments Protection Profile [12] was chosen as the benchmark for a High-Level PP for this project. The High-Level MG PP was chosen because it has a partial author overlap with the other two Firewall PPs, it shares a common sponsor (NSA) and it was produced for the same entity (U.S. Department of Defence). For these reason it shares a similar structure with the Firewall PPs and allows comparisons to be easily made. The Basic-Level and Medium-Level FW PPs provide platforms for the High-Level FW PP and thus a viewpoint from below. The High-Level MG PP gives a different viewpoint and a feel for the standards that the High-Level FW should attain.

The Application-Level Protection Profile for High Robustness Environments will retain a similar structure to that of the Basic-Level and Medium-Level FW PPs. It will contain security measures that are present in both previous firewall PPs. It will contain certain higher-level security functions and objectives that will be able to counteract the higher-level of security threats. These can be sourced from the High-Level MG PP. The security measures that are to be included in the High-Level FW PP are listed in section 4. Such new security measures include no remote administration and the use of multifactor user authentication. For this project a summary of security measures that are to be included in a High-Level FW PP was produced. However this summary did not include all details that are to be included in a PP. Moreover, we also have to review our results with respect to the recent release of a new Medium-Level FW PP [16] that was supersedes the two previously (and also in our project) used profiles [13, 14].

In any case, any firewall PP can be considered useful only once a firewall actually has been evaluated against it. The plans for future work in this project aim at publication of a High-Level FW PP (proposal) in its entirety, and the evaluation of a firewall against it.

## **References**

- [1] **Firewalls and Internet Security: Repelling the Wily Hacker**, Second Edition, William R. Cheswick, Steven M. Bellovin, and Aviel D. Rubin.
- [2] **Common Criteria for Information Technology Security Evaluation**, CCIB-98-031 Version 2.1, August 1999.
- [3] **Department of Defence Chief Information Officer Guidance and Policy Memorandum No. 6-8510, Guidance and Policy for the Department of Defence Global Information Grid Information Assurance (GIG)**, June 2000.
- [4] **U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments**, April 1999.
- [5] **U.S. Department of Defence Application-level Firewall Protection Profile for Basic Robustness Environments**, June 2000.
- [6] **U.S. Department of Defence Virtual Private Network (VPN) Boundary Gateway Protection Profile for Basic Robustness Environments, Draft Version 0.5**, May 2001.
- [7] **Federal Information Processing Standard Publication (FIPS-PUB) 46-3, Data Encryption Standard (DES)**, October 1999.
- [8] **Implementing Virtual Private Networks**, Steven Brown, McGraw Hill, 1999.
- [9] **Internet Engineering Task Force, IP Encapsulating Security Payload (ESP), RFC 2406**, November 1998.
- [10] **Internet Engineering Task Force, Internet Key Exchange (IKE), RFC 2409**, November 1998.
- [11] **Internet Engineering Task Force, ESP CBC-Mode Cipher Algorithms, RFC 2451**, November 1998.
- [12] **Department of Defence Mail Guard for High Robustness Environments Protection Profile, Version 0.1**, September 2001.
- [13] **U.S. Department of Defence Traffic-Filter Firewall Protection Profile for Medium Robustness Environments**, May 2000.
- [14] **U.S. Department of Defence Application-level Firewall Protection Profile for Medium Robustness Environments, Version 1.0**, June 2000.
- [15] **U.S. Department of Defence Application-level Firewall Protection Profile for Basic Robustness Environments, Version 0.6a**, September 2001.
- [16] **U.S. Government Firewall Protection Profile for Medium Robustness Environments, v.1.0**; October 2003.

**Copyright © 2004, Faculty of Informatics, Masaryk University.  
All rights reserved.**

**Reproduction of all or part of this work  
is permitted for educational or research use  
on condition that this copyright notice is  
included in any copy.**

**Publications in the FI MU Report Series are in general accessible  
via WWW and anonymous FTP:**

`http://www.fi.muni.cz/informatics/reports/  
ftp ftp.fi.muni.cz (cd pub/reports)`

**Copies may be also obtained by contacting:**

**Faculty of Informatics  
Masaryk University  
Botanická 68a  
602 00 Brno  
Czech Republic**