Final

U. S. Department of Defense

Application-level Firewall

Protection Profile

for

Medium Robustness Environments

Version 1.0

June 28, 2000

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	6/28/2000	Report 6/28/2000

4. TITLE AND SUBTITLE
US Department of Defense Application-Level Firewall Protection Profile for Medium Robustness Environments

5. FUNDING NUMBERS

6. AUTHOR(S)
Kathy V. Dolan, Patricia A. Wright, Rita R. Montequin

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Booz Allen & Hamilton
8283 Greensboro Drive
McLean, VA 22102

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Department of Defense

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; Distribution is unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT ***(Maximum 200 Words)***

8 This Application Level Firewall Protection Profile defines the minimum security requirements for firewalls used by U. S. Government organizations, specifically the Department of Defense, handling unclassified or sensitive but unclassified information for Mission-Critical Categories in a moderate-risk environment. Firewalls may consist of one or more devices that act as part of an organization’s overall security defense by isolating an organization’s internal network from the Internet or other external networks. The Protection Profile defines the assumptions about the security aspects of the environment in which the firewall will be used, defines the threats that are to be addressed by the firewall, defines implementation-independent security objectives of the firewall and its environment, defines the functional and assurance requirements to meet those objectives, and provides a rationale demonstrating how the requirements meet the security objectives

14. SUBJECT TERMS
IATAC Collection, firewall, authentication

15. NUMBER OF PAGES
64

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	abstract_limitation

Protection Profile Title:

U.S. Department of Defense Application-Level Firewall Protection Profile for Medium Robustness Environments.

Criteria Version:

This Protection Profile (PP) was developed using Version 2.1 of the Common Criteria (CC) [1].

Constraints:

Targets of Evaluation (TOEs) developed to satisfy this Protection Profile shall conform to CC Part 2 and CC Part 3.

Authors:

This Protection Profile was prepared by:

Kathy V. Dolan, National Security Agency

Patricia A. Wright, National Security Agency

Rita R. Montequin, National Security Agency

Acknowledgement:

The authors would like to acknowledge Kris Britton from the National Security Agency.

Table of Contents

List of Tables

Conventions and Terminology

Conventions

The notation, formatting and conventions used in this Protection Profile are largely consistent with those used in version 2.1 of the Common Criteria (CC). Selected presentation choices are discussed here to aid the Protection Profile user.

The CC allows several operations to be performed on functional requirements; *refinement*, *selection*, *assignment*, and *iteration* are defined in paragraph 2.1.4 of Part 2 of the CC. Each of these operations is used in this Protection Profile.

The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**. For an example, see FMT_SMR.1 in this Protection Profile.

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by *underlined italicized text*. For an example, see FDP_RIP.1 in this Protection Profile.

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignment is indicated by showing the value in square brackets, [assignment_value]. For an example, see FIA_AFL.1 in this Protection Profile.

The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing the iteration number in parenthesis following the component identifier, (iteration_number). For example, see FDP_IFC in this Protection Profile.

The **security target writer** operation is used to denote points in which the final determination of attributes is left to the security target writer. Security target writer operations are indicated by the words {determined by the security target writers} in braces. For example, see FIA_ATD.1 in this Protection Profile.

As a vehicle for providing a further understanding of and context for functional requirements, “Requirements Overview” sections have been selectively added to this Protection Profile. When they appear in the text, these overviews precede either a component or set of components. They provide a discussion of the relationship between security requirements so that the Protection Profile user can see why a component or group of components was chosen and what effect it is

expected to have as a group of related functions. As an example, see the Requirements Overview which precedes the ADV_RCR.1 assurance component.

Application Notes are provided to help the developer, either to clarify the intent of a requirement, identify implementation choices, or to define “pass-fail” criteria for a requirement. For those components where Application Notes are appropriate, the Application Notes will follow the requirement component. For an example, see the Application Note which follows FMT_MSA.3 in this Protection Profile.

Terminology

In the Common Criteria, many terms are defined in Section 2.3 of Part 1. The following are a subset of those definitions. They are listed here to aid the user of the Protection Profile.

User -- Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

Human user -- Any person who interacts with the TOE.

External IT entity -- Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.

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.

From the above definitions given by the CC, the following terms can be derived:

Authorized external IT entity – Any IT product or system, outside the scope of the TOE that may administer the security parameters of the TOE. Such entities are not subject to any access control requirements once authenticated to the TOE and are therefore trusted to not compromise the security policy enforced by the TOE.

Authorized Administrator – A role which human users may be associated with to administer the security parameters of the TOE. Such users are not subject to any access control requirements once authenticated to the TOE and are therefore trusted to not compromise the security policy enforced by the TOE.

Document Organization

Section 1 is the introductory material for the Protection Profile.

Section 2 provides a general definition for application-filter firewalls.

Section 3 is a discussion of the expected environment for the firewall, in particular the assumptions that must be true about aspects such as physical, personnel, and connectivity conditions. This section then defines the set of threats that are to be addressed by either the technical countermeasures implemented in the firewall's hardware and software, or through the environmental controls.

Section 4 defines the security objectives for both the firewall and the environment in which the firewall resides.

Section 5 contains the functional and assurance requirements derived from the Common Criteria, Part 2 and Part 3, respectively, that must be satisfied by the firewall.

Section 6 provides a rationale to explicitly demonstrate that the IT security objectives satisfy the threats. The section then explains how the set of requirements are complete relative to the objectives; that each security objective is addressed by one or more relevant component requirements.

References are provided as background material for further investigation by interested users of the Protection Profile.

Acronyms are provided to facilitate comprehension of frequently used terms.

Application-Level Firewall Protection Profile

1 PROTECTION PROFILE (PP) INTRODUCTION

1.1 PP IDENTIFICATION

1 Title: U. S. Department of Defense Application-Level Firewall Protection Profile for Medium Robustness Environments

2 Sponsor: National Security Agency (NSA)

3 Authors: Kathy V. Dolan, NSA; Patricia A. Wright, NSA; Rita R. Montequin, NSA; Chuck Hall, NSA

4 CC Version: CC Version 2.1

5 Registration: <to be provided upon registration>

6 PP Version: Version 1.0, dated June 2000

7 Keywords: information flow control, firewall, proxy server, protection profile

1.2 PP OVERVIEW

8 This Application Level Firewall Protection Profile defines the minimum security requirements for firewalls used by U. S. Government organizations, specifically the Department of Defense, handling unclassified or sensitive but unclassified information for Mission-Critical Categories in a moderate-risk environment. Firewalls may consist of one or more devices that act as part of an organization's overall security defense by isolating an organization's internal network from the Internet or other external networks. The Protection Profile defines the assumptions about the security aspects of the environment in which the firewall will be used, defines the threats that are to be addressed by the firewall, defines implementation-independent security objectives of the firewall and its environment, defines the functional and assurance requirements to meet those objectives, and provides a rationale demonstrating how the requirements meet the security objectives.

1.3 RELATED PROTECTION PROFILES

9 U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments [2].

10 U.S. Department of Defense Traffic-Filter Firewall Protection Profile for Medium Robustness Environments [7].

11 U.S. Department of Defense Application-level Firewall Protection Profile for Basic Robustness Environments [6].

2 TARGET OF EVALUATION (TOE) DESCRIPTION

12 The purpose of a firewall is to provide controlled and audited access to services, both from inside and outside an organization's network, by allowing, denying, and/or redirecting the flow of data through the firewall. Although there are a number of firewall architectures and technologies, firewalls basically fall into two major categories: traffic-filter and application-level firewalls. This Protection Profile specifies the minimum security requirements for TOEs composed of an application-level firewall.

13 **The TOE mediates information flows between clients and servers located on internal and external networks governed by the TOE.** TOEs may employ proxies to screen information flows. Proxy servers on the TOE, for services such as FTP and Telnet, require authentication at the TOE by client users before requests for such services can be authorized. Thus, only valid requests are relayed by the proxy server to the actual server on either an internal or external network.

14 TOEs meeting this Protection Profile additionally impose traffic-filtering controls on information flows mediated by the TOE. Information flows between clients and servers according to the site's security policy rules. By default, these security policy rules deny all inbound and outbound information flows. Only an authorized administrator has the authority to change the security policy rules.

15 Users of the TOE consist of human users and host-like entities, called external IT entities. Human users may or may not be associated with the single role on the TOE for authorized administrators. If the information flow security policy rules permit human users (who are not authorized administrators) on an internal or external network to send and receive information to FTP or Telnet servers on an external or internal network, respectively, such users will have to be identified and authenticated (using a single-use authentication mechanism) by the TOE before information is relayed by the proxy server on the TOE to the FTP or Telnet server. Of the human users, only authorized administrators may access the TOE through remote means from an internal or external network. If an authorized administrator accesses the TOE remotely, and after successful identification and authentication (using a single-use authentication mechanism), a channel using Triple DES encryption with securely generated and distributed key values must be used. In addition to remote access, and after successful identification and authentication, authorized administrators may access the TOE through local means without encryption, such as through a console (that may be included as part of the TOE). Though not recommended, the human users who are not authorized administrators may identify and authenticate from a local console to use non-security functions on the TOE. The only security functions available to human

users who are not authorized administrators are the controlled usage of the identification and authentication functions.

16 External IT entities sending information through the TOE do not have to be identified and authenticated, unless those functions are supported by the underlying service (e.g., FTP). However, external IT entities attempting to send information to the TOE must always be identified and authenticated. Those external IT entities that are successfully identified and authenticated (using a single-use authentication mechanism) are authorized external IT entities. This subset of the external IT entities are permitted to perform a limited number of security functions. They are "authorized" to violate the TSP in a well understood and permitted manner. A router sending routing table updates to the TOE, serves as an example of an authorized external IT entity. This router would identify itself to the TOE and then use a single-use authentication mechanism to authenticate. The TOE would then accept routing table updates from the authorized external IT entity. There are no requirements mandating authorized external IT entities.

17 Audit trail data is stamped with a dependable date and time when recorded. Audit events include modifications to the group of users associated with the authorized administrator role, all use of the identification and authentication mechanisms (including any attempted reuse of authentication data), all information flow control decisions made by the TOE according to the security policy rules, and the use of all security functions. If the audit trail becomes filled, then the only auditable events that may be performed are those performed by the authorized administrator. The TOE includes tools to perform searching and sorting on the collected audit trail data according to attributes of the data recorded and ranges of some of those attributes.

3 TOE SECURITY ENVIRONMENT

18 Protection Profile-compliant TOEs, for the Department of Defense, must provide appropriate security to process unclassified or sensitive but unclassified information in the Mission-Critical Categories. Mission-Critical Categories refer to DoD systems that handle information vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. It is assumed that the threat to information designated as Mission-Critical, by nature, is greater and subject to greater risk for disclosure and/or corruption by unauthorized parties as indicated in the Protection Profile by the assumption A.MODEXP. Information and information systems in the Mission-Critical Categories must maintain the appropriate level of confidentiality, integrity, availability, authentication, and non-repudiation based on the sensitivity of the information handled. To ensure the security of Mission-Critical Categories of information, not only must vulnerability analysis by the developer be performed, but the evaluator of the TOE must perform independent penetration testing to determine that the TOE is resistant to penetration attacks performed by attackers possessing a moderate attack potential. This level of testing is required in this Protection Profile by AVA_VLA.3. Additionally, in order to ensure protection of Mission-Critical information, more detailed product information is required from the vendor to facilitate more thorough analysis. This requirement is indicated by ADV_HLD.2, ADV_IMP.1, and ADV_LLD.1 in this Protection Profile.

19 For all Federal agencies, including Department of Defense agencies, for the use of cryptographic modules in the protection of sensitive but unclassified information, compliance with FIPS PUB 140-1 is required[1]. FIPS PUB 140-1 defines security requirements for cryptographic modules. A cryptographic module is that part of a system or application that provides cryptographic services such as encryption, authentication, or electronic signature generation and verification. Products and systems compliant with this Protection Profile are expected to utilize cryptographic modules for remote administration compliant with this FIPS PUB.

[1]. *See FIPS-PUB 140-1 for the schedule by which all cryptographic modules used by Federal agencies must meet the provisions of this standard.*

3.1 ASSUMPTIONS

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

A.PHYSEC The TOE is physically secure.

A.MODEXP The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered moderate.

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 can not 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 can not access the TOE remotely from the internal or external networks.

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

3.2 THREATS

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

3.2.1 THREATS ADDRESSED BY THE TOE

22 The threats discussed below are addressed by Protection Profile-compliant TOEs. 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.

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.MODEXP A skilled attacker with moderate attack potential may attempt to bypass the TSF to gain access to the TOE or the assets it protects.

3.2.2 THREAT TO BE ADDRESSED BY OPERATING ENVIRONMENT

23 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 ORGANIZATIONAL SECURITY POLICIES

24 Federal agencies are required to protect sensitive but unclassified information with cryptography. Products and systems compliant with this Protection Profile are expected to utilize cryptographic modules for remote administration compliant with FIPS PUB 140-1 (level 1).

P.CRYPTO Triple DES encryption (as specified in FIPS 46-3 [3]) must be used to protect remote administration functions, and the associated cryptographic module must comply, at a minimum, with FIPS 140-1 (level 1).

4 SECURITY OBJECTIVES

4.1 INFORMATION TECHNOLOGY (IT) SECURITY OBJECTIVES

25 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, disallowing passage of non-conformant protocols and ensuring 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.

26 For a detailed mapping between threats and the IT security objectives listed above, see section 6.1 of the Rationale.

4.2 SECURITY OBJECTIVES FOR THE ENVIRONMENT

27 All of the assumptions stated in section 3.1 are considered to be security objectives for the environment. The following are the Protection Profile non-IT security objectives which 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.

O.PHYSEC The TOE is physically secure.

O.MODEXP The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered moderate.

O.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.

O.PUBLIC The TOE does not host public data.

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

O.SINGEN Information can not flow among the internal and external networks unless it passes through the TOE.

O.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.

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

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

O.GUIDAN The TOE must be delivered, installed, administered, and operated in a manner that maintains security.

O.ADMTRA Authorized administrators are trained as to establishment and maintenance of security policies and practices.

28 For a detailed mapping between threats, assumptions, and the non-IT security objectives listed above see section 6.2 of the Rationale.

5 IT SECURITY REQUIREMENTS

5.1 TOE SECURITY REQUIREMENTS

29 This Protection Profile provides functional and assurance requirements that must be satisfied by a Protection Profile-compliant TOE. These requirements consist of functional components from Part 2 of the CC and an Evaluation Assurance Level (EAL) containing assurance components from Part 3 of the CC.

5.1.1 TOE SECURITY REQUIREMENTS

30 The functional security requirements for this Protection Profile consist of the following components from Part 2 of the CC, summarized in the following table.

Functional Components	
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
FDP_IFC.1	Subset information flow control (1)
FDP_IFC.1	Subset information flow control (2)
FDP_IFF.1	Simple security attributes (1)
FDP_IFF.1	Simple security attributes (2)
FMT_MSA.1	Management of security attributes (1)
FMT_MSA.1	Management of security attributes (2)
FMT_MSA.1	Management of security attributes (3)
FMT_MSA.1	Management of security attributes (4)
FMT_MSA.3	Static attribute initialization
FMT_MTD.1	Management of TSF data (1)
FMT_MTD.1	Management of TSF data (2)
FMT_MTD.2	Management of limits on TSF data
FDP_RIP.1	Subset residual information protection
FCS_COP.1	Cryptographic operation
FPT_RVM.1	Non-bypassability of the TSP
FPT_SEP.1	TSF domain separation
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

Functional Components	
FAU_STG.4	Prevention of audit data loss
FMT_MOF.1	Management of security functions behavior (1)
FMT_MOF.1	Management of security functions behavior (2)

Table 5.1 - Functional Requirements

31 The statement of the TOE security requirements must include a minimum strength level for the TOE security functions realized by a probablistic or permutational mechanism. In the case of this protection profile, this minimum level shall be SOF-medium. For a rationale for this selected level, see section 6.3 of the rationale.

32 Specific strength of function metrics are defined for the following requirements:

33 FIA_UAU.5 - Strength of Function shall be demonstrated for the single-use authentication mechanism by demonstrating compliance with the "Statistical random number generator tests" found in section 4.11.1 of FIPS PUB 140-1 [4] and the "Continuous random number generator test" found in section 4.11.2 of FIPS PUB 140-1 [4]. Strength of function shall be demonstrated for the password authentication mechanism such that the probability that authentication data can be guessed is no greater than one in two to the fortieth (2^40). The single-use and password authentication mechanisms must demonstrate SOF-medium, as defined in Part 1 of the CC.

34 The following paragraphs are intended to clarify why the functional components in this Protection Profile are presented in the order outlined in Table 5.1. FMT_SMR.1 is the first component because it defines the authorized administrator role, which appears in a number of the components that follow.

35 The class FIA components are listed after FMT_SMR.1. They describe the identification and authentication policy that all users, both human users and external IT entities, must abide by before being able to use other TOE functions.

36 The order of the class FIA components was chosen on the following basis. Since users are already defined in the Terminology section on page vi, the Protection Profile reader is introduced in component FIA_ATD.1 to their security attributes. The next component, FIA_UID.2, forces users to identify themselves to the TOE using the user security attributes of component FIA_ATD.1 before further actions take place. Then, component FIA_AFL.1 describes what results if the user fails to authenticate after some settable number of attempts. Lastly, component FIA_UAU.5 discusses when authentication mechanisms must be used.

37 There are two information flow control SFPs, and they are defined after the class FIA components in FDP_IFC.1. Then the policy rules which must be enforced as well as the attributes of the entities defined in FDP_IFC.1 are written in FDP_IFF.1. Next, the management of the attributes in FDP_IFF.1 are specified in FMT_MSA.1(1), FMT_MSA.1(2), FMT_MSA.1(3) and FMT_MSA.1(4). Component FMT_MSA.3, which FDP_IFF.1 depends on, follows. As part of the installation and start-up of the TOE, FMT_MSA.3 mandates a default deny policy which permits no information to flow through the TOE. FMT_MTD.1(1), FMT_MTD.1(2), and FMT_MTD.2 define the management of TSF data. FDP_RIP.1 is listed next, ensuring that resources are cleared before being allocated to hold packets of information at the TOE.

38 Component FCS_COP.1 is a conditional requirement. If the developer allows administration from a remote location outside the physically protected TOE, then evaluation against this Protection Profile shall require the TOE to meet this component. FCS_COP.1 defines a cryptographic algorithm as well as the key size that must be used. The cryptographic module must be FIPS PUB 140-1 compliant for the reasons stated in Section 3.

39 Components dealing with the protection of trusted security functions come next. These include components FPT_RVM.1 and FPT_SEP.1.

40 Since FAU_GEN.1 requires recording the time and date when audit events occur, it follows the FPT_STM.1 component that alerts developers that an accurate time and date must be maintained on the TOE. The class FAU requirements follow to define the audit security functions which must be supported by the TOE. FAU_GEN.1 is the first audit component listed because it depicts all the events that must be audited, including all the information which must be recorded in audit records. The remainder of the class FAU components ensure that the audit records can be read (component FAU_SAR.1), searched and sorted (component FAU_SAR.3), and protected from modification (FAU_STG.1). Lastly, FAU_STG.4 ensures that the TOE is capable of preventing auditable actions, not taken by an authorized administrator, from occurring in the event that the audit trail becomes full.

41 The last component in the profile is FMT_MOF.1. It appears last because it lists all the functions to be provided by the TOE for use only by the authorized administrator. Almost all of these functions are based on components which precede it. Thus it is listed last.

FMT_SMR.1 Security roles

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

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

FIA_ATD.1 User attribute definition

44 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) any other user security attributes {to be determined by the Security Target writer(s)}].

FIA_UID.2 User identification before any action

45 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.

FIA_AFL.1 Authentication failure handling

46 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].

47 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.]

FIA_UAU.5 Multiple authentication mechanisms

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

49 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 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].

50 Application Note: TOEs that do not provide capabilities for authorized administrators to access the TOE remotely from either an internal or external network (i.e., for remote administration), or for authorized external IT entities do not have to make such functionality available in order to satisfy this requirement. The intent of this requirement is not to require developers to provide all such capabilities and their associated authentication mechanisms. The requirement applies to those developers that do incorporate such functionality and intend for it to be evaluated.

51 Requirements Overview: This Protection Profile consists of 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 two 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. The information flowing between subjects in both 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 twice to correspond to each of the two iterations of FDP_IFC.1.

FDP_IFC.1 Subset information flow control (1)

52 FDP_IFC.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; and

c) operation: pass information].

FDP_IFC.1 Subset information flow control (2)

53 FDP_IFC.1.1 - The TSF shall enforce the [AUTHENTICATED SFP] on:

a) [subjects: a human user or external IT entity that sends and receives FTP 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;

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

c) operation: initiate service and pass information].

FDP_IFF.1 Simple security attributes (1)[2]

54 FDP_IFF.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; and
- other subject security attributes {to be determined by the Security Target writer(s)};

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; and
- other information security attributes {to be determined by the Security Target writer(s)}].

[2]. *The complete set of functional elements of a component must be selected for inclusion in a PP. However, since the following functional elements from the FDP_IFF.1 (1) component do not add anything significant to the PP, they have been moved here to allow for a clearer, smoother flowing presentation of FDP_IFF.1(1).*

FDP_IFF.1.3 - The TSF shall enforce the [none].

FDP_IFF.1.4 - The TSF shall provide the following [none].

FDP_IFF.1.5 - The TSF shall explicitly authorize an information flow based on the following rules: [none].

55 FDP_IFF.1.2 - 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;
- 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;
- 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.]

56 FDP_IFF.1.6 - 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 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.

57 Application Note: Rule f) applies when an application-level proxy is provided for the following protocols: DNS, HTTP, SMTP, and POP3.

FDP_IFF.1 Simple security attributes (2)[3]

58 FDP_IFF.1.1 - 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; and
- other subject security attributes {to be determined by the Security Target writer(s)};

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 and Telnet);
- security-relevant service command; and
- other information security attributes {to be determined by the Security Target writer(s)}]

[3]. *The complete set of functional elements of a component must be selected for inclusion in a PP. However, since the following functional elements from the FDP_IFF.1 (2) component do not add anything significant to the PP, they have been moved here to allow for a clearer, smoother flowing presentation of FDP_IFF.1 (2).*

FDP_IFF.1.3 - The TSF shall enforce the [none].

FDP_IFF.1.4 - The TSF shall provide the following [none].

FDP_IFF.1.5 - The TSF shall explicitly authorize an information flow based on the following rules: [none].

59 FDP_IFF.1.2 - 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:

- 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.]

60 FDP_IFF.1.6 - 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 or FTP 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.

61 Application Note: The TOE can make no claim as to the real address of any source or destination subject, therefore the TOE can only suppose that these addresses are accurate. Therefore, a “presumed address” is used to identify source and destination addresses. A “service”, listed in FDP_IFF.1.1(b), could be identified, for example, by a source port number and/or destination port number. A “service command”, also mentioned FDP_IFF.1.1(b), could be identified, for example, in the case of the File Transport Protocol (FTP) service as an FTP STOR or FTP RETR.

FMT_MSA.1 Management of security attributes (1)

62 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].

FMT_MSA.1 Management of security attributes (2)

63 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].

FMT_MSA.1 Management of security attributes (3)

64 FMT_MSA.1.1(3) - 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].

FMT_MSA.1 Management of security attributes (4)

65 FMT_MSA.1.1(4) - 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].

FMT_MSA.3 Static attribute initialization

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

67 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.

68 Application Note: The default values for the information flow control security attributes appearing in FDP_IFF.1 (1) and FDP_IFF.1 (2) 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.

FMT_MTD.1 Management of TSF data (1)

69 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].

FMT_MTD.1 Management of TSF data (2)

70 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].

FMT_MTD.2 Management of limits on TSF data

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

72 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].

FDP_RIP.1 Subset residual information protection

73 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].

74 Application Note: If, for example, the TOE pads information with bits in order to properly prepare the information before sending it out an interface, these bits would be considered a "resource". The intent of the requirement is that these bits shall not contain the remains of information that had previously passed through the TOE. The requirement is met by overwriting or clearing resources (e.g. packets) before making them available for use.

FCS_COP.1 Cryptographic operation

75 FCS_COP.1.1 - The TSF shall perform [encryption of remote authorized administrator sessions] in accordance with a specified cryptographic algorithm: [Triple Data Encryption Standard (DES) as specified in FIPS PUB 46-3 and implementing any mode of operation specified in FIPS PUB 46-3 with Keying Option 1 (K1, K2, K3 are independent keys)] and cryptographic key sizes [that are 192 binary digits in length] that meet the following: [FIPS PUB 46-3 with Keying Option 1 and FIPS PUB 140-1 (Level 1)].

76 Application Note: This requirement is applicable only if the TOE includes the capability for the authorized administrator to perform security functions remotely from a connected network. In this case, Triple DES encryption must protect the

communications between the authorized administrator and the TOE, and the associated cryptographic module(s) must comply at a minimum with FIPS PUB 140-1 Level 1. The intent of this requirement is not for the evaluator to perform a FIPS PUB 140-1 evaluation; rather, the evaluator will check for a certificate, verifying that the module did complete a FIPS PUB 140-1 evaluation.

FPT_RVM.1 Non-bypassability of the TSP

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

FPT_SEP.1 TSF domain separation

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

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

FPT_STM.1 Reliable time stamps

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

81 Application Note: The word "reliable" in the above requirement means that the order of the occurrence of auditable events is preserved. Reliable time stamps, which include both date and time, are especially important for TOEs comprised of greater than one component.

FAU_GEN.1 Audit data generation

82 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 in Table 5.2].

83 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 Contents
FMT_SMR.1	Modifications to the group of users that are part of **the authorized administrator** role. Unsuccessful attempts to authenticate the authorized administrator role.	The identity of the authorized administrator performing the modification and the user identity being associated with the authorized administrator role. The user identity and the role.
FIA_UID.2	All use of the user identification mechanism.	The user identities provided to the TOE.
FIA_UAU.1	Any use of the authentication mechanism.	The user identities provided to the TOE.
FIA_UAU.5	The final decision on authentication.	The user identity and the success or failure of the authentication.
FIA_AFL.1	The reaching of the threshold for unsuccessful authentication attempts and the subsequent **restoration by the authorized administrator of the users 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 identity of the external IT

Functional Component	Auditable Event	Additional Audit Record Contents
	the type of cryptographic operation.	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 - Auditable Events

FAU_SAR.1 Audit review

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

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

FAU_SAR.3 Selectable audit review

86 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; and

e) ranges of addresses].

87 Application Note: The Security Target writer(s) is expected to describe, as part of their "TOE Summary Specification" section, the capabilities of the tool(s) used by the TOE to perform these searches and sorts.

FAU_STG.1 Protected audit trail storage

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

89 FAU_STG.1.2 - The TSF shall be able to *prevent* modifications to the audit records.

FAU_STG.4 Prevention of audit data loss

90 FAU_STG.4. - 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.

91 Application Note: The Security Target writer(s) is expected to provide, as part of their "Security requirements rationale" section, 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.

FMT_MOF.1 Management of security functions behavior (1)

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

a) [operation of the TOE; and

b) multiple use authentication as described in FIA_UAU.5] to [an authorized administrator].

93 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" in b) above, we mean the management of password and single-use authentication mechanisms.

FMT_MOF.1 Management of security functions behavior (2)

94 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].

95 Application Note: Determine and modify the behavior 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.

5.1.2 TOE SECURITY ASSURANCE REQUIREMENTS

96 The assurance security requirements for this Protection Profile, taken from Part 3 of the CC, compose EAL2 Augmented. These assurance components are summarized in the following table.

Assurance Class	Assurance Components	
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.2	Security enforcing high-level design
	ADV_IMP.1	Implementation representation
	ADV_LLD.1	Low-level design
	ADV_RCR.1	Informal correspondence demonstration
Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
	ALC_TAT.1	Tools and techniques
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.3	Moderately resistant

Table 5.3 - Assurance Requirements: EAL2 Augmented

ACM_CAP.2 Configuration items

Developer action elements:

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

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

99 ACM_CAP.2.3D - The developer shall provide CM documentation.

Content and presentation of evidence elements:

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

101 ACM_CAP.2.2C - The TOE shall be labeled with its reference.

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

103 ACM_CAP.2.4C - The configuration list shall describe the configuration items that comprise the TOE.

104 ACM_CAP.2.5C - The CM documentation shall describe the method used to uniquely identify the configuration items.

105 ACM_CAP.2.6C - The CM system shall uniquely identify all configuration items.

Evaluator action elements:

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

ADO_DEL.1 Delivery procedures

Developer action elements:

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

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

Content and presentation of evidence elements:

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

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

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

Developer action elements:

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

Content and presentation of evidence elements:

113 ADO_IGS.1.1C - The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE. Evaluator action elements:

Evaluator action elements:

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

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

ADV_FSP.1 Informal functional specification

Developer action elements:

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

Content and presentation of evidence elements:

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

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

119 ADV_FSP.1.3C - The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects,

exceptions and error messages, as appropriate.

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

Evaluator action elements:

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

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

123 Application Note: This requirement can potentially be met by a combination of documents provided by the developer, including the Security Target and external interface specification.

ADV_HLD.2 Security enforcing high-level design

Developer action elements:

124 ADV_HLD.2.1D - The developer shall provide the high-level design of the TSF.

Content and presentation of evidence elements:

125 ADV_HLD.2.1C - The presentation of the high-level design shall be informal.

126 ADV_HLD.2.2C - The high-level design shall be internally consistent.

127 ADV_HLD.2.3C - The high-level design shall describe the structure of the TSF in terms of subsystems.

128 ADV_HLD.2.4C - The high-level design shall describe the security functionality provided by each subsystem of the TSF.

129 ADV_HLD.2.5C - The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

130 ADV_HLD.2.6C - The high-level design shall identify all interfaces to the subsystems of the TSF.

131 ADV_HLD.2.7C - The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

132 ADV_HLD.2.8C - The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.

133 ADV_HLD.2.9C - The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.

Evaluator action elements:

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

135 ADV_HLD.2.2E - The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

136 Application Note: The elements within this family define a requirement that the evaluator determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements. This provides a direct correspondence between the TOE security functional requirements and the high-level design, in addition to the pairwise correspondences required by the ADV_RCR family. It is expected that the evaluator will use the evidence provided in ADV_RCR as an input to making this determination, and the requirement for completeness is intended to be relative to the level of abstraction of the high-level design.

ADV_IMP.1 Subset of the implementation of the TSF

Developer action elements:

137 ADV_IMP.1.1D - The developer shall provide the implementation representation for a selected subset of the TSF.

Content and presentation of evidence elements:

138 ADV_IMP.1.1C - The implementation representation shall unambiguously define the TSF to a level of detail such that the TSF can be generated without further design decisions.

139 ADV_IMP.1.2C – The implementation representation shall be internally consistent.

Evaluator action elements:

140 ADV_IMP.2.1E - The evaluator shall confirm that the information provided

meets all requirements for content and presentation of evidence.

141 ADV_IMP.1.2E - The evaluator shall determine that the least abstract TSF representation provided is an accurate and complete instantiation of the TOE security functional requirements.

ADV_LLD.1 Descriptive low-level design

Developer action elements:

142 ADV_LLD.1.1D - The developer shall provide the low-level design of the TSF.

Content and presentation of evidence elements:

143 ADV_LLD.1.1C - The presentation of the low-level design shall be informal.

144 ADV_LLD.1.2C - The low-level design shall be internally consistent.

145 ADV_LLD.1.3C - The low-level design shall describe the TSF in terms of modules.

146 ADV_LLD.1.4C - The low-level design shall describe the purpose of each module.

147 ADV_LLD.1.5C - The low-level design shall define the interrelationships between the modules in terms of provided security functionality and dependencies on other modules.

148 ADV_LLD.1.6C - The low-level design shall describe how each TSP-enforcing function is provided.

149 ADV_LLD.1.7C - The low-level design shall identify all interfaces to the modules of the TSF.

150 ADV_LLD.1.8C - The low-level design shall identify which of the interfaces to the modules of the TSF are externally visible.

151 ADV_LLD.1.9C - The low-level design shall describe the purpose and method of use of all interfaces to the modules of the TSF, providing details of effects, exceptions and error messages, as appropriate.

152 ADV_LLD.1.10C - The low-level design shall describe the separation of the TOE into TSP-enforcing and other modules.

Evaluator action elements:

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

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

155 Requirements Overview: ADV_RCR.1 ensures that there is consistency between each level of design decomposition for the TOE. Each higher level of design decomposition (the higher the level of design decomposition, the more abstract) should map to the one below it, until a level of design decomposition maps to the least abstract representation, the implementation itself. Thus, for Security Targets derived from this Protection Profile there are four layers of abstraction (from high to low): the STs "TOE summary specification" section, the Functional Specification, the high-level design, and the TOE itself.[4]

ADV_RCR.1 Informal correspondence demonstration

Developer action elements:

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

Content and presentation of evidence elements:

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

Evaluator action elements:

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

159 Application Note: The intent of this requirement is for the vendor to provide, and the evaluator to confirm, that there exists accurate, consistent, and clear mappings between each level of design decomposition. Thus there can be no TOE security functions defined at a lower layer of abstraction absent from a higher level of abstraction and vice versa.

[4]. *For related information, see section 4.2.1 in Part 1 of the CC.*

AGD_ADM.1 Administrator guidance

Developer action elements:

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

161 Content and presentation of evidence elements:

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

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

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

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

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

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

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

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

Evaluator action elements:

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

AGD_USR.1 User guidance

Developer action elements:

171 AGD_USR.1.1D - The developer shall provide user guidance.

Content and presentation of evidence elements:

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

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

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

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

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

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

Evaluator action elements:

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

179 Application Note: This assurance component is trivially met if neither authorized external IT entities nor human users who are not authorized administrators are permitted on the TOE. If authorized external IT entities and/or human users who are not authorized administrators are permitted on the TOE, it is intended that functions and interfaces for these users be described. If the developer permits human users who are not authorized administrators on the TOE, AGD_USR.1.2C is not intended to permit security functions or interfaces to exist for such users beyond those security functions described in the CC class FIA functional components in section 5.1.1. If the developer does not permit human users who are not authorized administrators on the TOE, AGD_USR.1.2C only applies if authorized external IT entities are permitted.

ALC_TAT.1 Well-defined development tools

Developer action elements:

180 ALC_TAT.1.1D - The developer shall identify the development tools being used for the TOE.

181 ALC_TAT.1.2D - The developer shall document the selected implementation-dependent options of the development tools.

Content and presentation of evidence elements:

182 ALC_TAT.1.1C - All development tools used for implementation shall be well-defined.

183 ALC_TAT.1.2C - The documentation of the development tools shall unambiguously define the meaning of all statements used in the implementation.

184 ALC_TAT.1.3C - The documentation of the development tools shall unambiguously define the meaning of all implementation-dependent options.

Evaluator action elements:

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

186 Application Note: There is a requirement for well-defined development tools. These are tools that have been shown to be applicable without the need for intensive further clarification. For example, programming languages and computer aided design (CAD) systems that are based on a standard published by standards bodies are considered to be well-defined. The requirement in ALC_TAT.1.2C is especially applicable to programming languages so as to ensure that all statements in the source code have an unambiguous meaning.

ATE_COV.1 Evidence of coverage

Developer action elements:

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

Content and presentation of evidence elements:

188 ATE_COV.1.1C - The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the TSF

as described in the functional specification.

Evaluator action elements:

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

ATE_FUN.1 Functional testing

Developer action elements:

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

191 ATE_FUN.1.2D - The developer shall provide test documentation.

Content and presentation of evidence elements:

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

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

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

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

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

Evaluator action elements:

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

ATE_IND.2 Independent testing - sample

Developer action elements:

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

Content and presentation of evidence elements:

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

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

Evaluator action elements:

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

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

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

AVA_SOF.1 Strength of TOE security function evaluation[5]

Developer action elements:

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

Content and presentation of evidence elements:

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

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

Evaluator action elements:

207 AVA_SOF.1.1E - The evaluator shall confirm that the information provided

[5]. *This component is intended to apply strictly to those security functions that are vulnerable to an attack involving a quantitative or statistical analysis (e.g., password guessing). A short discussion of how a security mechanism may be vulnerable is provided under the "Objectives" heading for AVA_SOF, in Part 3 of the CC.*

meets all requirements for content and presentation of evidence.

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

209 Application Note: The security mechanisms defined by the following requirements have a specific strength of function claim: FIA_UAU.5. Section 5.1.1 of this PP defines the specific strength of function metric for each of these mechanisms.

AVA_VLA.3 Moderately resistant

Developer action elements:

210 AVA_VLA.3.1D - The developer shall perform and document an analysis of the TOE deliverables searching for ways in which a user can violate the TSP.

211 AVA_VLA.3.2D - The developer shall document the disposition of identified vulnerabilities.

Content and presentation of evidence elements:

212 AVA_VLA.3.1C - The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

213 AVA_VLA.3.2C - The documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.

214 AVA_VLA.3.3C - The evidence shall show that the search for vulnerabilities is systematic.

Evaluator action elements:

215 AVA_VLA.3.1E - The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

216 AVA_VLA.3.2E - The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure identified vulnerabilities have been addressed.

217 AVA_VLA.3.3E - The evaluator shall perform an independent vulnerability analysis

218 AVA_VLA.3.4E - The evaluator shall perform independent penetration testing, based on the independent vulnerability analysis, to determine the exploitability of

additional identified vulnerabilities in the intended environment.

219 AVA_VLA.3.5E - The evaluator shall determine that the TOE is resistant to penetration attacks performed by an attacker possessing a moderate attack potential.

6 RATIONALE

6.1 RATIONALE FOR IT 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.NOAUTH and T.AUDFUL 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.MODEXP because it requires that the TOE is resistant to penetration attacks performed by an attacker possessing moderate attack potential.

	T.NOAUTH	T.REPEAT	T.REPLAY	T.ASPOOF	T.MEDIAT	T.OLDINF	T.PROCOM	T.AUDACC	T.SELPRO	T.AUDFUL	T.MODEXP	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	

Table 6.1 – Summary of Mappings Between Threats, Policies and IT Security Objectives

6.2 RATIONALE FOR SECURITY OBJECTIVES FOR THE ENVIRONMENT

O.PHYSEC The TOE is physically secure.

O.MODEXP The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered moderate.

O.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.

O.PUBLIC The TOE does not host public data.

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

O.SINGEN Information can not flow among the internal and external networks unless it passes through the TOE.

O.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.

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

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

O.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.

O.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.

	T.TUSAGE	**T.AUDACC**
O.GUIDAN	X	X
O.ADMTRA	X	X

Table 6.2 - Summary of Mappings Between Threats and Security Objectives for the Environment

220 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.

6.3 RATIONALE FOR SECURITY REQUIREMENTS

221 The functional and assurance requirements presented in this Protection Profile are mutually supportive and their combination meet the stated security objectives. The security requirements were derived according to the general model presented in Part 1 of the Common Criteria. Table 6.3 illustrates the mapping between the security requirements and the security objectives. Table 6.1 demonstrates the relationship between the threats, policies and IT security objectives. Together these tables demonstrate the completeness and sufficiency of the requirements.

222 The rationale for the SOF is based on the moderate attack potential identified in this Protection Profile. The security objectives imply the need for probablistic or permutational security mechanisms. The metrics defined in this Protection Profile are acceptable (i.e., passwords) metrics to protect information in DoD Mission-Critical Categories.

FMT_SMR.1 Security roles

223 Each of the CC class FMT components in this Protection Profile depend on this component. It requires the PP/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

224 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

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

FIA_UAU.1 Timing of authentication

226 This component ensures that users are authenticated at the TOE. The TOE is permitted to pass information (aside from FTP and Telnet information) before users are authenticated. Authentication must occur whether the user is a human user or not and whether or not the user is an authorized administrator. If the authorized administrator was not always required to authenticate, there would be no means by which to audit any of their actions. An additional SOF metric for this

requirement is defined in section 5.1.1 to ensure that the authentication mechanism chosen cannot be easily bypassed. This component traces back to and aids in meeting the following objectives: O.IDAUTH and O.SINUSE.

FIA_AFL.1 Authentication failure handling

227 This component ensures that human users who are not authorized administrators can not 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

228 This component was chosen to ensure that multiple authentication mechanism are used appropriately in all attempts to authenticate at the TOE from an internal or external network. An additional SOF metric for this requirement is defined in section 5.1.1 to ensure that the mechanisms are of adequate probabilistic strength to protect against authentication data compromise. This component traces back to and aids in meeting the following objective: O.SINUSE and O.IDAUTH.

FDP_IFC.1 Subset information flow control (1)

229 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)

230 This component identifies the entities involved in the AUTHENTICATED information flow control SFP (i.e., users of the services 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_IFF.1 Simple security attributes (1)

231 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)

232 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.

FMT_MSA.1 Management of security attributes (1)

233 This component ensures the TSF enforces the UNAUTHENTICATED_SFP to restrict the ability to add, delete, and modify within a rule those security attributes that are listed in section 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 (2)

234 This component ensures the TSF enforces the AUTHENTICATED_SFP to restrict the ability to add, delete, and modify within a rule those security attributes that are listed in section 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 (3)

235 This component ensures the TSF enforces the UNAUTHENTICATED_SFP to restrict the ability to create and 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 (4)

236 This component ensures the TSF enforces the AUTHENTICATED_SFP to restrict the ability to create and 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 and O.SECSTA.

FMT_MSA.3 Static attribute initialization

237 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)

238 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)

239 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

240 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

241 This component ensures that neither information that had flown 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

242 This component ensures that if the TOE does support authorized administrators to communicate with the TOE remotely from an internal or external network that Triple DES is used to encrypt such traffic. This component is necessitated by the postulated threat environment. This component traces back to and aids in meeting the following objective: O.ENCRYP and O.EAL.

FPT_RVM.1 Non-bypassability of the TSP

243 This component ensures that the TSF are always invoked. This component traces back to and aids in meeting the following objective: O.SELPRO and O.SECSTA.

FPT_SEP.1 TSF domain separation

244 This component 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.

FPT_STM.1 Reliable time stamps

245 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

246 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

247 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

248 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

249 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.SECSTA and O.SECFUN.

FAU_STG.4 Prevention of audit data loss

250 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.SECSTA and O.SECFUN.

FMT_MOF.1 Management of security functions behavior (1)

251 This component ensures that 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.SECSTA, O.SECFUN, and O.LIMEXT.

FMT_MOF.1 Management of security functions behavior (2)

252 This component was to ensure the TSF restricts the ability to modify the behavior 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.SECSTA, O.SECFUN, and O.LIMEXT.

	O.IDAUTH	**O.SINUSE**	**O.MEDIAT**	**O.SECSTA**	**O.ENCRYP**	**O.SELPRO**	**O.AUDREC**	**O.ACCOUN**	**O.SECFUN**	**O.LIMEXT**	**O.EAL**
FMT_SMR.1									X		
FIA_ATD.1	X								X		
FIA_UID.2	X							X			
FIA_AFL.1						X					
FIA_UAU.5	X	X									
FDP_IFC.1 (1)			X								
FDP_IFC.1 (2)			X								
FDP_IFF.1 (1)			X								
FDP_IFF.1 (2)			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.3			X	X							
FMT_MTD.1 (1)									X		
FMT_MTD.1 (2)									X		
FMT_MTD.2									X		
FDP_RIP.1			X								
FCS_COP.1					X						
FPT_RVM.1				X		X					
FPT_SEP.1						X					
FPT_STM.1							X				

	O.IDAUTH	O.SINUSE	O.MEDIAT	O.SECSTA	O.ENCRYP	O.SELPRO	O.AUDREC	O.ACCOUN	O.SECFUN	O.LIMEXT	O.EAL
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 6.3 – Summary of Mappings Between Functional Requirements and IT Security Objectives

6.4 RATIONALE FOR ASSURANCE REQUIREMENTS

253 EAL2 Augmented was chosen to ensure a moderate level of security for protecting information in DoD Mission-Critical Categories. Mission-Critical Categories of information is assumed, by nature, to have a greater threat for disclosure and/or corruption by unauthorized parties as indicated in the Protection Profile by the assumption A.MODEXP. To ensure the security of Mission-Critical Categories of information, not only must vulnerability analysis by the developer be performed, but an evaluator must perform independent penetration testing to determine that the TOE is resistant to penetration attacks performed by attackers possessing a moderate attack potential. This level of testing is required in this Protection Profile by AVA_VLA.3. As an indirect dependency of vulnerability analysis, tools and techniques used to develop, analyze and implement the TOE must be identified and documented. This is supported by the requirement ALC_TAT.1.

254 Since the threat to Mission-Critical Categories of information is greater, more detailed product information is required as indicated by requirements ADV_HLD.2, ADV_IMP.1, and ADV_LLD.1 in this Protection Profile. The chosen assurance level as supported by O.EAL is consistent with the postulated threat environment. Specifically, that the threat of malicious attacks is not greater than moderate, and the product will have undergone vulnerability analysis by the developer and independent penetration testing by the evaluator.

6.5 RATIONALE FOR NOT SATISFYING ALL DEPENDENCIES

255 With the exception of the functional component FCS_COP.1, all dependencies are contained in this Protection Profile.

256 Functional component FCS_COP.1 depends on the following functional components: FCS_CKM.1 Cryptographic key generation, FCS_CKM.4 Cryptographic key destruction and FMT_MSA.2 Secure Security Attributes. Cryptographic modules used in support of this PP must be FIPS PUB 140-1 compliant. If the cryptographic module is indeed compliant with this FIPS PUB, then the dependencies of key generation, key destruction and secure key values will have been satisfied in becoming FIPS PUB 140-1 compliant. For more information, refer to sections 4.8.1 and 4.8.5 of FIPS PUB 140-1.

REFERENCES

[1] *Common Criteria for Information Technology Security Evaluation*, CCIB-98-031 Version 2.1, August 1999.

[2] *U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments*; Version 1.1, April 1999.

[3] Federal Information Processing Standard Publication (FIPS-PUB) 46-3, *Data Encryption Standard (DES)*, October 1999.

[4] Federal Information Processing Standard Publication (FIPS-PUB) 140-1, *Security Requirements for Cryptographic Modules*, dated January 11, 1994.

[5] Building Internet Firewalls, Chapman & Zwicky, O'Reilly & Associates, Inc., November 1995.

[6] *U.S. Department of Defense Application-level Firewall Protection Profile for Basic Robustness Environments*; Version 1.0, June 2000.

[7] *U.S. Department of Defense Traffic-Filter Firewall Protection Profile for Medium Robustness Environments*, Version 1.0, April 2000.

Acronyms

257 The following abbreviations from the Common Criteria are used in this Protection Profile:

CC	Common Criteria for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
FIPS PUB	Federal Information Processing Standard Publication
IT	Information Technology
PP	Protection Profile
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy