U.S. Government Protection Profile

for

Application-level Firewall

In Basic Robustness Environments

Information Assurance Directorate

Version 1.1

July 25, 2007

Forward

This Protection Profile "*US Government Protection Profile for Application-level Firewall in Basic Robustness Environments"* (PP) was updated using Version 3.1 of the Common Criteria (CC).

Editor's note: The purpose of this update was to bring the PP up to the new CC 3.1 standard without changing the authors' original meaning or purpose of the documented requirements. The original PP was developed using version 2.x of the CC. The CC version 2.3 was the final version 2 update that included all international interpretations. CC version 3.1 used the final CC version 2.3 Security Functional Requirements (SFR)s as the new set of SFRs for version 3.1. Some minor changes were made to the SFRs in version 3.1, including moving a few SFRs to Security Assurance Requirements (SAR)s. There may be other minor differences between some SFRs in the version 2.3 PP and the new version 3.1 SFRs. These minor differences were not modified to ensure the author's original intent was preserved.

The version 3.1 SARs were rewritten by the common criteria international community. The NIAP/CCEVS staff developed an assurance equivalence mapping between the version 2.3 and 3.1 SARs. The assurance equivalent version 3.1 SARs replaced the version 2.3 SARs in the PP.

Any issue that may arise when claiming compliance with this PP can be resolved using the observation report (OR) and observation decision (OD) process.

Further information, including the status and updates of this protection profile can be found on the CCEVS website: http://www.niap-ccevs.org/cc-scheme/pp/. Comments on this document should be directed to ppcomments@missi.ncsc.mil. The email should include the title of the document, the page, the section number, the paragraph number, and the detailed comment and recommendation.

Protection Profile Title:

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

Criteria Version:

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

Constraints:

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

Table of contents

Conventions and Terminology

CONVENTIONS

The notation, formatting, and conventions used in this Protection Profile are largely consistent with those used in version 2 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.

Appendices:

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

Acronyms are provided to facilitate comprehension of frequently used terms.

Robustness Environment Characterization, contains a discussion characterizing the level of robustness TOEs compliant with the PP can achieve. The PPRB created a discussion that provides a definition of factors for TOE environments as well as an explanation of how a given level of robustness is categorized.

1 APPLICATION LEVEL FIREWALL PROTECTION PROFILE (PP) INTRODUCTION

1.1 PP IDENTIFICATION

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

Sponsor: National Security Agency (NSA)

CC Version: CC Version 2.1

PP Version: Version 1.1, dated July 25, 2007

Keywords: information flow control, firewall, network security, proxy server, application gateway, protection profile

1.2 PP OVERVIEW

This Application Level Firewall Protection Profile defines the minimum-security requirements for firewalls used by U. S. Government organizations handling unclassified information in a Basic Robustness environment (see appendix A3). 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 is used. It also defines the threats that are 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.

STs that claim conformance to this PP shall meet a minimum standard of demonstrable-PP conformance as defined in section D3 of part 1.

RELATED PROTECTION PROFILES

U.S. Government Traffic-Filter Firewall Protection Profile for Basic Robustness Environments.

2 TARGET OF EVALUATION (TOE) DESCRIPTION

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 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.

The TOE mediates information flows between clients and servers located on internal and external networks governed by the TOE. TOEs must 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.

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.

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 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.

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.

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

Protection Profile-compliant TOEs are intended to be used either in environments in which, at most, sensitive but unclassified information is processed, or the sensitivity level of information in both the internal and external networks is equivalent.

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 140-2 is required. FIPS PUB 140-2 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.

3.1 ASSUMPTIONS

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

A.PHYSEC The TOE is physically secure.

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

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

A.PUBLIC The TOE does not host public data.

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

A.SINGEN Information 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 cannot 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

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

3.2.1 Threats Addressed by the TOE

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

3.2.2 Threat to be Addressed by Operating Environment

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

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

3.3 ORGANIZATIONAL SECURITY POLICIES

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 140-2 (level 1).

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

4 SECURITY OBJECTIVES

4.1 INFORMATION TECHNOLOGY (IT) SECURITY OBJECTIVES

The following are the IT security objectives for the TOE:

O.IDAUTH The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to TOE functions or, for certain specified services, to a connected network.

O.SINUSE The TOE must prevent the reuse of authentication data for users attempting to authenticate to the TOE from a connected network.

O.MEDIAT The TOE must mediate the flow of all information between clients and servers located on internal and external networks governed by the TOE, and must ensure that residual information from a previous information flow is not transmitted in any way.

O.SECSTA Upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE must not compromise its resources or those of any connected network.

O.ENCRYP The TOE must protect the confidentiality of its dialogue with an authorized administrator through encryption, if the TOE allows administration to occur remotely from a connected network.

O.SELPRO The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.

O.AUDREC The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search and sort the audit trail based on relevant attributes.

O.ACCOUN The TOE must provide user accountability for information flows through the TOE and for authorized administrator use of security functions related to audit.

O.SECFUN The TOE must provide functionality that enables an authorized administrator to use the TOE security functions, and must ensure that only authorized administrators are able to access such functionality.

O.LIMEXT The TOE must provide the means for an authorized administrator to control and limit access to TOE security functions by an authorized external IT entity.

O.EAL The TOE must be structurally tested and shown to be resistant to obvious vulnerabilities.

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

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, in addition to those assumptions, are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

O.PHYSEC The TOE is physically secure.

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

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 cannot 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.

For a detailed mapping between threats, assumptions, and the non-IT security objectives listed above see section 6 of the Rationale.

5 IT SECURITY REQUIREMENTS

5.1 TOE SECURITY REQUIREMENTS

23
This section 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

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

	Functional Components
FCS_COP.1	Cryptographic operation
FPT_STM.1	Reliable time stamps
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit review
FAU_SAR.3	Selectable audit review
FAU_STG.1	Protected audit trail storage
FAU_STG.4	Prevention of audit data loss
FMT_MOF.1	Management of security functions behavior (1)
FMT_MOF.1	Management of security functions behavior (2)

Table 5.1 - Functional Requirements

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.

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.

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.

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.

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 140-2 compliant for the reasons stated in Section 3.

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.

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

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

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

FIA_ATD.1 User attribute definition

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

a) [identity;
b) association of a human user with the authorized administrator role;
c) any other user security attributes {to be determined by the Security Target writer(s)}].

FIA_UID.2 User identification before any action

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

FIA_AFL.1 Authentication failure handling

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

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

FIA_UAU.5 Multiple authentication mechanisms

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

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

a) single-use authentication mechanism shall be used for authorized administrators to access the TOE remotely such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that authorized administrator;
b) single-use authentication mechanism shall be used for authorized external IT entities accessing the TOE such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that authorized external IT entity;
c) single-use authentication mechanism shall be used for human users sending or receiving information through the TOE using FTP or Telnet such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that human user;
d) reusable password mechanism shall be used for authorized administrators to access the TOE via a directly connected terminal such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that authorized administrator].

Application 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.

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 to the TOE. 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)

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;

c) operation: pass information].

FDP_IFC.1 Subset information flow control (2)

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;

c) operation: initiate service and pass information].

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

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

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.]

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].

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.

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]

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;
- 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)}].

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.]

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.

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 in FDP_IFF.1.1(b), could be identified,

for example, in the case of the File Transfer Protocol (FTP) service as an FTP STOR or FTP RETR.

FMT_MSA.1 Management of security attributes (1)

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

FMT_MSA.1 Management of security attributes (2)

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

FMT_MSA.1 Management of security attributes (3)

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)

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

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.

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

Application Note: 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)

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)

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

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

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

FDP_RIP.1 Subset residual information protection

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

> *Application Note: 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

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

> *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, AES 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 140-2 Level 1. The intent of this requirement is not for the evaluator to perform a FIPS PUB 140-2 evaluation; rather, the evaluator will check for a certificate, verifying that the module did complete a FIPS PUB 140-2 evaluation.*

FPT_STM.1 Reliable time stamps

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

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

FAU_GEN.1.1 - The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;
b) All auditable events for the *not specified* level of audit**;** and
c) [the events listed in Table 5.2].

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

a) Date and time of the event, type of event, subject identity, outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [information specified in column three of Table 5.2].

Functional Component	Auditable Event	Additional Audit Record Content
FMT_SMR.1	Modifications to the group of users that are part of **the authorized administrator** role.	The identity of the authorized administrator performing the modification and the user identity being associated with the authorized administrator role
FIA_UID.2	All use of the user identification mechanism.	The user identities provided to the TOE
FIA_UAU.5	Any use of the authentication mechanism.	The user identities provided to the TOE
FIA_AFL.1	The reaching of the threshold for unsuccessful authentication attempts and the subsequent **restoration by the authorized administrator of the 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 type of cryptographic operation	The identity of the external IT entity attempting to perform the cryptographic operation
FPT_STM.1	Changes to the time.	The identity of the authorized administrator performing the operation
FMT_MOF.1	Use of the functions listed in this requirement pertaining to audit.	The identity of the authorized administrator performing the operation

Table 5.2 - Auditable Events

FAU_SAR.1 Audit review

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

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

FAU_SAR.3 Selectable audit review

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

a) [user identity;
b) presumed subject address;
c) ranges of dates;
d) ranges of times;
e) ranges of addresses].

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

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

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

FAU_STG.4 Prevention of audit data loss

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

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)

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

a) [operation of the TOE;
b) multiple use authentication functions described in FIA_UAU.5] to [an authorized administrator].

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

FMT_MOF.1 Management of security functions behavior (2)

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

a) [audit trail management;
b) backup and restore for TSF data, information flow rules, and audit trail data; and
c) communication of authorized external IT entities with the TOE] to [an authorized administrator].

Application Note: Determine and modify the 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

The TOE assurance requirements for this PP are EAL2 augmented by ALC_FLR.2 as shown in the table below. All assurance requirements are summarized in the table below.

Assurance Class	Assurance Components	Assurance Components Description
Development	ADV_ARC.1	Architectural Design with domain separation and non-bypassability
	ADV_FSP.2	Security-enforcing Functional Specification
	ADV_TDS.1	Basic design
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative User guidance
Life Cycle Support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.2	**Flaw Reporting Procedures**
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - conformance
Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis

Table 1 – Assurance Requirements: EAL2 Augmented

Class ADV: Development

5.1.2.1 ADV_ARC.1 Security architecture description

Dependencies: ADV_FSP.1 Basic functional specification
ADV_TDS.1 Basic design

Developer action elements:

ADV_ARC.1.1D The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.

ADV_ARC.1.3D The developer shall provide a security architecture description of the TSF.

Content and presentation elements:

ADV_ARC.1.1C The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

ADV_ARC.1.2C The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

ADV_ARC.1.3C The security architecture description shall describe how the TSF initialization process is secure.

ADV_ARC.1.4C The security architecture description shall demonstrate that the TSF protects itself from tampering.

ADV_ARC.1.5C The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

Evaluator action elements:

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

5.1.2.2 **ADV_FSP.2 Security-enforcing functional specification**

Dependencies: ADV_TDS.1 Basic design

Developer action elements:

ADV_FSP.2.1D The developer shall provide a functional specification.

ADV_FSP.2.2D The developer shall provide a tracing from the functional specification to the SFRs.

Content and presentation elements:

ADV_FSP.2.1C The functional specification shall completely represent the TSF.

ADV_FSP.2.2C The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP.2.3C The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.2.4C For each SFR-enforcing TSFI, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.

ADV_FSP.2.5C For SFR-enforcing TSFIs, the functional specification shall describe direct error messages resulting from processing associated with the SFR-enforcing actions.

ADV_FSP.2.6C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

Evaluator action elements:

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

ADV_FSP.2.2E The evaluator *shall determine* that the functional specification is an accurate and complete instantiation of the SFRs.

5.1.2.3 **ADV_TDS.1 Basic design**

Dependencies: ADV_FSP.2 Security-enforcing functional specification

Developer action elements:

ADV_TDS.1.1D The developer shall provide the design of the TOE.

ADV_TDS.1.2D The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

Content and presentation elements:

ADV_TDS.1.1C The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.1.2C The design shall identify all subsystems of the TSF.

ADV_TDS.1.3C The design shall describe the behavior of each SFR-supporting or SFR-non-interfering TSF subsystem in sufficient detail to determine that it is not SFR-enforcing.

ADV_TDS.1.4C The design shall summarize the SFR-enforcing behavior of the SFR-enforcing subsystems.

ADV_TDS.1.5C The design shall provide a description of the interactions among SFR-enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.

ADV_TDS.1.6C The mapping shall demonstrate that all behavior described in the TOE design is mapped to the TSFIs that invoke it.

Evaluator action elements:

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

ADV_TDS.1.2E The evaluator *shall determine* that the design is an accurate and complete instantiation of all security functional requirements.

Class AGD: Guidance documents

5.1.2.4 AGD_OPE.1 Operational user guidance

Dependencies: ADV_FSP.1 Basic functional specification

Developer action elements:

AGD_OPE.1.1D The developer shall provide operational user guidance.

Content and presentation elements:

AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6C The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.

Evaluator action elements:

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

5.1.2.5 AGD_PRE.1 Preparative procedures

Dependencies: No dependencies.

Developer action elements:

AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures.

Content and presentation elements:

AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

Evaluator action elements:

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

AGD_PRE.1.2E The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

Class ALC: Life-cycle support

5.1.2.6 ALC_CMC.2 Use of a CM system

Dependencies: ALC_CMS.1 TOE CM coverage

Developer action elements:

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

ALC_CMC.2.2D The developer shall provide the CM documentation.

ALC_CMC.2.3D The developer shall use a CM system.

Content and presentation elements:

ALC_CMC.2.1C The TOE shall be labeled with its unique reference.

ALC_CMC.2.2C The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.2.3C The CM system shall uniquely identify all configuration items.

Evaluator action elements:

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

5.1.2.7 ALC_CMS.2 Parts of the TOE CM coverage

Dependencies: No dependencies.

Developer action elements:

ALC_CMS.2.1D The developer shall provide a configuration list for the TOE.

Content and presentation elements:

ALC_CMS.2.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; and the parts that comprise the TOE.

ALC_CMS.2.2C The configuration list shall uniquely identify the configuration items.

ALC_CMS.2.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

Evaluator action elements:

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

5.1.2.8 **ALC_DEL.1 Delivery procedures**

Dependencies: No dependencies.

Developer action elements:

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

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

Content and presentation elements:

ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

Evaluator action elements:

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

5.1.2.9 **ALC_FLR.2 Flaw reporting procedures**

Dependencies: No dependencies.

Developer action elements:

ALC_FLR.2.1D The developer shall document flaw remediation procedures addressed to TOE developers.

ALC_FLR.2.2D The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.

ALC_FLR.2.3D The developer shall provide flaw remediation guidance addressed to TOE users.

Content and presentation elements:

ALC_FLR.2.1C The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.2.2C The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

ALC_FLR.2.3C The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

ALC_FLR.2.4C The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

ALC_FLR.2.5C The flaw remediation procedures shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.

ALC_FLR.2.6C The procedures for processing reported security flaws shall ensure that any reported flaws are remediated and the remediation procedures issued to TOE users.

ALC_FLR.2.7C The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.

ALC_FLR.2.8C The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.

Evaluator action elements:

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

Class ATE: Tests

5.1.2.10 ATE_COV.1 Evidence of coverage

Dependencies: ADV_FSP.2 Security-enforcing functional specification
ATE_FUN.1 Functional testing

Developer action elements:

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

Content and presentation elements:

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

Evaluator action elements:

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

5.1.2.11 ATE_FUN.1 Functional testing

Dependencies: ATE_COV.1 Evidence of coverage

Developer action elements:

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

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation elements:

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

ATE_FUN.1.2C The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.3C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.4C The actual test results shall be consistent with the expected test results.

Evaluator action elements:

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

5.1.2.12 ATE_IND.2 Independent testing - sample

Dependencies: ADV_FSP.2 Security-enforcing functional specification
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures
ATE_COV.1 Evidence of coverage
ATE_FUN.1 Functional testing

Developer action elements:

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

Content and presentation elements:

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

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

Evaluator action elements:

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

ATE_IND.2.2E The evaluator *shall execute* a sample of tests in the test documentation to verify the developer test results.

ATE_IND.2.3E The evaluator *shall test* a subset of the TSF interfaces to confirm that the TSF operates as specified.

Class AVA: Vulnerability assessment

5.1.2.13 AVA_VAN.2 Vulnerability analysis

Dependencies: ADV_ARC.1 Security architecture description
ADV_FSP.1 Basic functional specification
ADV_TDS.1 Basic design
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures

Developer action elements:

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

Content and presentation elements:

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

Evaluator action elements:

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

AVA_VAN.2.2E The evaluator *shall perform* a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.2.3E The evaluator *shall perform* an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design and security architecture description to identify potential vulnerabilities in the TOE.

AVA_VAN.2.4E The evaluator *shall conduct* penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

Application Note: The TOE version used as the basis for testing should include a reference to the specific signature set in place when this activity is conducted.

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.AUDFUL and T.NOAUTH because it requires that the TOE protect itself from attempts to bypass, deactivate, or tamper with TOE security functions.

O.AUDREC This security objective is necessary to counter the threat: T.AUDACC by requiring a readable audit trail and a means to search and sort the information contained in the audit trail.

O.ACCOUN This security objective is necessary to counter the threat: T.AUDACC because it requires that users are accountable for information flows through the TOE and that authorized administrators are accountable for the use of security functions related to audit.

O.SECFUN This security objective is necessary to counter the threats: T.NOAUTH, T.REPLAY and T.AUDFUL by requiring that the TOE provide functionality that ensures that only the authorized administrator has access to the TOE security functions.

O.LIMEXT This security objective is necessary to counter the threat: T.NOAUTH because it requires that the TOE provide the means for an authorized administrator to control and limit access to TOE security functions.

O.EAL This security objective is necessary to counter the threat: T.LOWEXP because it requires that the TOE is resistant to penetration attacks performed by an attacker possessing minimal attack potential.

	T.NOAUTH	T.REPEAT	T.REPLAY	T.ASPOOF	T.MEDIAT	T.OLDINF	T.PROCOM	T.AUDACC	T.SELPRO	T.AUDFUL	T.LOWEXP	P.CRYPTPO
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 and IT Security Objectives

6.2 RATIONALE FOR SECURITY OBJECTIVES FOR THE ENVIRONMENT

O.PHYSEC The TOE is physically secure.

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

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.PUBLICThe 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

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

The security requirements are derived according to the general model presented in Part 1 of the Common Criteria. Specifically, Table 6.3 illustrates the mapping between the security requirements and the security objectives and Table 6.1 demonstrates the relationship between the threats, policies and IT security objectives. The functional and assurance requirements presented in this Protection Profile are mutually supportive and their combination meets the stated security objectives.

FMT_SMR.1 Security roles
Each of the CC class FMT components in this Protection Profile depends 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
This component exists to provide users with attributes to distinguish one user from another, for accountability purposes and to associate the role chosen in FMT_SMR.1 with a user. This component traces back to and aids in meeting the following objectives: O.IDAUTH and O.SECFUN.

FIA_UID.2 User identification before any action
This component ensures that before anything occurs on behalf of a user, the user's identity is identified to the TOE. This component traces back to and aids in meeting the following objectives: O.IDAUTH and O.ACCOUN.

FIA_AFL.1 Authentication failure handling
This component ensures that human users who are not authorized administrators 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
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. A 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)
This component identifies the entities involved in the UNAUTHENTICATED information flow control SFP (i.e., users sending information to other users and vice versa). This component traces back to and aids in meeting the following objective: O.MEDIAT.

FDP_IFC.1 Subset information flow control (2)
This component identifies the entities involved in the AUTHENTICATED information flow control SFP (i.e., users of the services 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)
This component identifies the attributes of the users sending and receiving the information in the UNAUTHENTICAED SFP, as well as the attributes for the information itself. Then the policy is defined by saying under what conditions information is permitted to flow. This component traces back to and aids in meeting the following objective: O.MEDIAT.

FDP_IFF.1 Simple security attributes (2)

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

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

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

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

FMT_MSA.1 Management of security attributes (4)
This component ensures the TSF enforces the AUTHENTICATED_SFP to restrict the ability to create or delete rules for security attributes that are listed in FDP_IFF.1(2). This component traces back to and aids in meeting the following objectives: O.MEDIAT, O.SECSTA, and O.SECFUN.

FMT_MSA.3 Static attribute initialization
This component ensures that there is a default deny policy for the information flow control security rules. This component traces back to and aids in meeting the following objectives: O.MEDIAT and O.SECSTA.

FMT_MTD.1 Management of TSF data (1)
This component ensures that the TSF restrict abilities to query, modify, delete and assign certain user attributes as defined in FIA_ATD.1.1 to only the authorized administrator. This component traces back to and aids in meeting the following objective: O.SECFUN.

FMT_MTD.1 Management of TSF data (2)
This component ensures that the TSF restrict abilities to set the time and date used to form timestamps to only the authorized administrator. This component traces back to and aids in meeting the following objective: O.SECFUN.

FMT_MTD.2 Management of limits on TSF data

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

FDP_RIP.1 Subset residual information protection
This component ensures that neither information that had flowed through the TOE nor any TOE internal data are used when padding is used by the TOE for information flows. This component traces back to and aids in meeting the following objective: O.MEDIAT.

FCS_COP.1 Cryptographic operation
This component ensures that if the TOE does support authorized administrators to communicate with the TOE remotely from an internal or external network that AES is used to encrypt such traffic. This component traces back to and aids in meeting the following objective: O.ENCRYP and O.EAL.

ADV_ARC.1 Security architecture description
This component must describe how the architecture ensures that the TSF are always invoked. This component traces back to and aids in meeting the following objective: O.SELPRO and O.SECSTA.

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

FPT_STM.1 Reliable time stamps

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

FAU_GEN.1 Audit data generation
This component outlines what data must be included in audit records and what events must be audited. This component traces back to and aids in meeting the following objectives: O.AUDREC and O.ACCOUN.

FAU_SAR.1 Audit review
This component ensures that the audit trail is understandable. This component traces back to and aids in meeting the following objective: O.AUDREC.

FAU_SAR.3 Selectable audit review
This component ensures that a variety of searches and sorts can be performed on the audit trail. This component traces back to and aids in meeting the following objective: O.AUDREC.

FAU_STG.1 Protected audit trail storage

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

FAU_STG.4 Prevention of audit data loss
This component ensures that the authorized administrator will be able to take care of the audit trail if it should become full. But this component also ensures that no other auditable events as defined in FAU_GEN.1 occur. Thus the authorized administrator is permitted to perform potentially auditable actions though these events will not be recorded until the audit trail is restored to a non-full status. This component traces back to and aids in meeting the following objectives: O.SELPRO, O.SECFUN and O.SECSTA.

FMT_MOF.1 Management of security functions behavior (1)
This component was to ensure the TSF restricts the ability of the TOE start up and shut down operation and multiple authentication function to the authorized administrator. This component traces back to and aids in meeting the following objectives: O.SECFUN, O.LIMEXT, and O.SECSTA.

FMT_MOF.1 Management of security functions behavior (2)
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.SECFUN, O.LIMEXT, and O.SECSTA.

	O.IDAUTH	O.SINUSE	O.MEDIAT	O.SECSTA	O.ENCRYP	O.SELPRO	O.AUDREC	O.ACCOUN	O.SECFUN	O.LIMEXT
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	

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

Table 6.3 – Summary of Mappings between Threats and IT Security Objectives

6.4 RATIONALE FOR ASSURANCE REQUIREMENTS

Basic robustness was chosen to ensure a level of security in the absence of complete vendor documentation. Specifically, the assurance requirements (that is, documentation and testing) were chosen to demonstrate that a low to moderate level of independently assured security exists as defined in Part 3, Section 6.2.2 of the CC. Minimal additional tasks are imposed upon the vendor to the extent that if the vendor applies reasonable standards of care to the development, evaluation may be feasible without vendor involvement other than support for functional testing, strength of function analysis and vulnerability testing verification.

The chosen assurance level is consistent with the postulated threat environment. Specifically, the threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low, and the product will have undergone a search for obvious flaws. This is supported by the inclusion of the AVA_VLA.1 requirement.

6.5 RATIONALE FOR NOT SATISFYING ALL DEPENDENCIES

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

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 must be FIPS PUB 140-2 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 140-2 compliant. For more information, refer to section 4.7 of FIPS PUB 140-2.

7 APPENDICES

A.1 References

Common Criteria for Information Technology Security Evaluation, CCIB-99-031 Version 2.1, August 1999.

Common Criteria for Information Technology Security Evaluation, CCMB-206-09-001,002,003 Version 3.1, Revision 1 September 2006.

U.S. Government Traffic-Filter Firewall Protection Profile for Basic Robustness Environments; Version 1.1, July 25, 2007.

Federal Information Processing Standard Publication FIPS 197, *Advanced Encryption Standard (AES*), November 26, 2001

Federal Information Processing Standard Publication (FIPS-PUB) 140-2, *Security Requirements for Cryptographic Modules, with change notices (12-03-2002).*

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

A.2 Acronyms

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

A.3 Robustness Environment Characterization

General Environmental Characterization

In trying to specify the environments in which TOEs with various levels of robustness are appropriate, it is useful to first discuss the two defining factors that characterize that environment: value of the resources and authorization of the entities to those resources.

In general terms, the environment for a TOE can be characterized by the authorization (or lack of authorization) the least trustworthy entity has with respect to the highest value of TOE resources (i.e. the TOE itself and all of the data processed by the TOE).

Note that there are an infinite number of combinations of entity authorization and value of resources; this conceptually "makes sense" because there are an infinite number of potential environments, depending on how the resources are valued by the organization, and the variety of authorizations the organization defines for the associated entities. In the next section, these two environmental factors will be related to the robustness required for selection of an appropriate TOE.

Value of Resources

Value of the resources associated with the TOE includes the data being processed or used by the TOE, as well as the TOE itself (for example, a real-time control processor). "Value" is assigned by the using organization. For example, in the DoD low-value data might be equivalent to data marked "For Official Use Only", while high-value data may be those classified Top Secret. In a commercial enterprise, low-value data might be the internal organizational structure as captured in the corporate on-line phone book, while high-value data might be corporate research results for the next generation product. Note that when considering the value of the data one must also consider the value of data or resources that are accessible through exploitation of the TOE. For example, a firewall may have "low value" data itself, but it might protect an enclave with high value data. If the firewall was being depended upon to protect the high value data, then it must be treated as a high-value-data TOE.

Authorization of Entities

Authorization that entities (users, administrators, other IT systems) have with respect to the TOE (and thus the resources of that TOE, including the TOE itself) is an abstract concept reflecting a combination of the trustworthiness of an entity and the access and privileges granted to that entity with respect to the resources of the TOE. For instance, entities that have total authorization to all data on the TOE are at one end of this spectrum; these entities may have privileges that allow them to read, write, and modify anything on the TOE, including all TSF data. Entities at the other end of the spectrum are those that are authorized to few or no TOE resources. For example, in the case of a router, non-administrative entities may have their packets routed by the TOE, but that is the extent of their authorization to the TOE's resources. In

the case of an OS, an entity may not be allowed to log on to the TOE at all (that is, they are not valid users listed in the OS's user database).

It is important to note that authorization **does not** refer to the **access** that the entities actually have to the TOE or its data. For example, suppose the owner of the system determines that no one other than employees was authorized to certain data on a TOE, yet they connect the TOE to the Internet. There are millions of entities that are not **authorized** to the data (because they are not employees), but they actually have connectivity to the TOE through the Internet and thus can attempt to access the TOE and its associated resources.

Entities are characterized according to the value of resources to which they are authorized; the extent of their authorization is implicitly a measure of how trustworthy the entity is with respect to compromise of the data (that is, compromise of any of the applicable security policies; e.g., confidentiality, integrity, availability). In other words, in this model the greater the extent of an entity's authorization, the more trustworthy (with respect to applicable policies) that entity is.

Selection of Appropriate Robustness Levels

Robustness is a characteristic of a TOE defining how well it can protect itself and its resources; a more robust TOE is better able to protect itself. This section relates the defining factors of IT environments, authorization, and value of resources to the selection of appropriate robustness levels.

When assessing any environment with respect to Information Assurance the critical point to consider is the likelihood of an attempted security policy compromise, which was characterized in the previous section in terms of entity authorization and resource value. As previously mentioned, robustness is a characteristic of a TOE that reflects the extent to which a TOE can protect itself and its resources. It follows that as the likelihood of an attempted resource compromise increases, the robustness of an appropriate TOE should also increase.
It is critical to note that several combinations of the environmental factors will result in environments in which the likelihood of an attempted security policy compromise is similar. Consider the following two cases:

The first case is a TOE that processes only low-value data. Although the organization has stated that only its employees are authorized to log on to the system and access the data, the system is connected to the Internet to allow authorized employees to access the system from home. In this case, the least trusted entities would be unauthorized entities (e.g. non-employees) exposed to the TOE because of the Internet connectivity. However, since only low-value data are being processed, the likelihood that unauthorized entities would find it worth their while to attempt to compromise the data on the system is low and selection of a basic robustness TOE would be appropriate.

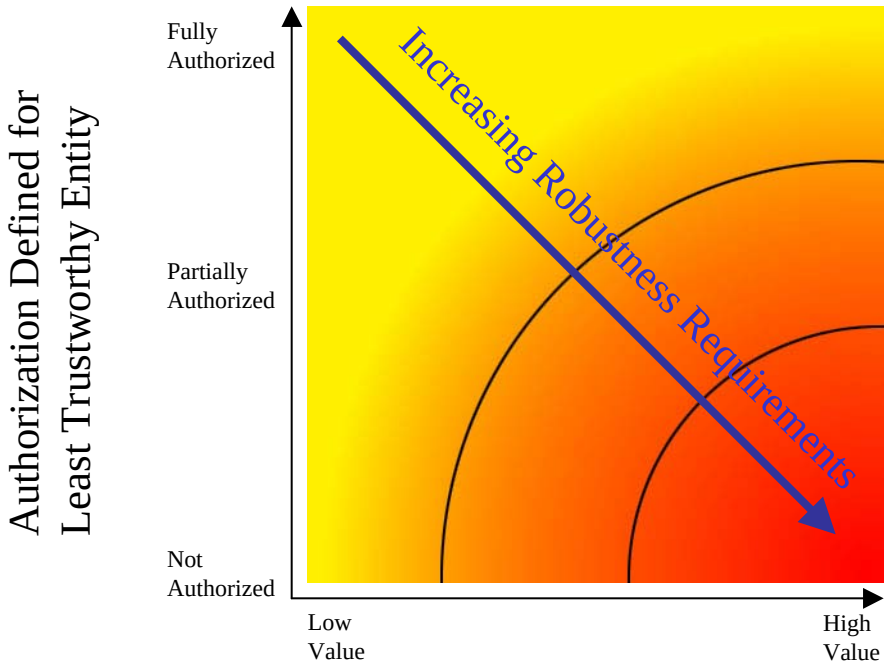
The second case is a TOE that processes high-value (e.g., classified) information. The organization requires that the TOE be stand-alone, and that every user with physical and logical access to the TOE undergo an investigation so that they are authorized to the highest value data on the TOE. Because of the extensive checks done during this investigation, the organization is assured that only highly trusted users are authorized to use the TOE. In this case, even though

high value information is being processed, it is unlikely that a compromise of that data will be attempted because of the authorization and trustworthiness of the users and once again, selection of a basic robustness TOE would be appropriate.

The preceding examples demonstrated that it is possible for radically different combinations of entity authorization/resource values to result in a similar likelihood of an attempted compromise. As mentioned earlier, the robustness of a system is an indication of the protection being provided to counter compromise attempts. Therefore, a basic robustness system should be sufficient to counter compromise attempts where the likelihood of an attempted compromise is low. The following chart depicts the “universe” of environments characterized by the two factors discussed in the previous section: on one axis is the authorization defined for the least trustworthy entity, and on the other axis is the highest value of resources associated with the TOE.

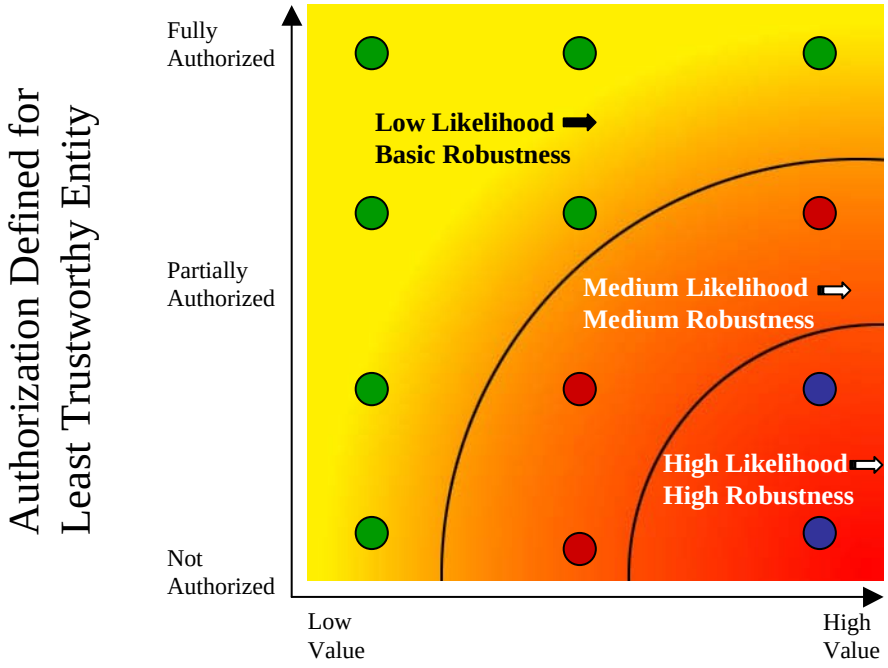
As depicted in the following figure, the robustness of the TOEs required in each environment steadily increases as one goes from the upper left of the chart to the lower right; this corresponds to the need to counter increasingly likely attack attempts by the least trustworthy entities in the environment. Note that the shading of the chart is intended to reflect- the notion that different environments engender similar levels of “likelihood of attempted compromise”, signified by a similar color. Further, the delineations between such environments are not stark, but rather are finely grained and gradual.

While it would be possible to create many different "levels of robustness" at small intervals along the “Increasing Robustness Requirements” line to counter the increasing likelihood of attempted compromise due to those attacks, it would not be practical nor particularly useful. Instead, in order to implement the robustness strategy where there are only three robustness levels: Basic, Medium, and High, the graph is divided into three sections, with each section corresponding to a set of environments where the likelihood of attempted compromise is roughly similar. This is graphically depicted in the following chart.



In this second representation of environments and the robustness plane below, the "dots" represent given instantiations of environments; like-colored dots define environments with a similar likelihood of attempted compromise. Correspondingly, a TOE with a given robustness should provide sufficient protection for environments characterized by like-colored dots. In choosing the appropriateness of a given robustness level TOE PP for an environment, then, the user must first consider the lowest authorization for an entity as well as the highest value of the resources in that environment. This should result in a "point" in the chart above, corresponding to the likelihood that that entity will attempt to compromise the most valuable resource in the environment. The appropriate robustness level for the specified TOE to counter this likelihood can then be chosen.

The difficult part of this activity is differentiating the authorization of various entities, as well as determining the relative values of resources; (e.g., what constitutes "low value" data vs. "medium value" data). Because every organization will be different, a rigorous definition is not possible. In Section 3 of this PP, the targeted threat level for a Basic robustness TOE is characterized. This information is provided to help organizations using this PP -ensure that the functional requirements specified by this Basic robustness PP are appropriate for their intended application of a compliant TOE.


Authorization Defined for Least Trustworthy Entity
Fully Authorized
Partially Authorized
Not Authorized
Low Likelihood
Basic Robustness
Medium Likelihood
Medium Robustness
High Likelihood
High Robustness
Low Value
High Value
Highest Value of Resources Associated with the TOE