FINAL

U.S. Government

Traffic-Filter Firewall

Protection Profile

for

Low-Risk Environments

Version 1.1

April 1999

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	4/1/1999	Report 4/1/1999

4. TITLE AND SUBTITLE
US Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments

5. FUNDING NUMBERS

6. AUTHOR(S)
Wayne Jansen, Jack Walsh, Kathy V. Dolan, Patricia A. Wright

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

Booz Allen & Hamilton
8283 Greensboro Drive
McLean, VA 22102

8. PERFORMING ORGANIZATION REPORT NUMBER

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

NSA and NIST

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

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

12b. DISTRIBUTION CODE
A

13. ABSTRACT *(Maximum 200 Words)*

This traffic-filter firewall Protection Profile defines the minimum security requirements for firewalls used by U.S Government organizations handling unclassified information in a low-risk environment. Firewalls may consist of one or more devices that act as part of an organization’s overall security defense by isolating an organization’s internal network from the Internet or other external networks. Firewalls pass and block information flows based on a set of screening rules defined by an authorized administrator. This Protection Profile applies to firewalls that are capable of screening network traffic at the network and transport protocol levels, authenticating the authorized administrator for actions at the firewall, and auditing security-relevant events that occur. For clarification of terms, see terminology section.

14. SUBJECT TERMS
IATAC Collection, firewall, cryptography, authentication

15. NUMBER OF PAGES
60

16. PRICE CODE

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

Protection Profile Title:

U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments.

Criteria Version:

This Protection Profile (PP) was developed using Version 2.0 of the Common Criteria (CC) [1].

Constraints:

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

Authors:

This Protection Profile was prepared by:

Wayne Jansen, National Institute of Standards and Technology

Jack Walsh, National Security Agency

Kathy V. Dolan, National Security Agency

Patricia A. Wright, National Security Agency

Acknowledgements:

The authors would like to acknowledge Thomas Karygiannis from the National Institute of Standards and Technology, Jandria Alexander and Mario Tinto from The Aerospace Corporation, and Kris Britton from the National Security Agency.

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 security requirements; *refinement*, *selection*, *assignment*, and *iteration* are defined in paragraph 2.1.4 of Part 2 of the CC. Except for the *iteration* operation, 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 FDP_IFC.1 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. Target writer operations are indicated by the words {determined by the security target writers} in braces. For example, see FIA_AFL.1 in this Protection Profile.

As a vehicle for providing a further understanding of and context for security 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 traffic-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 firewalls 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.

Appendix A provides a list of relevant vulnerabilities against which Protection Profile compliant products must be checked.

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

Traffic-Filter Firewall Protection Profile

1 PROTECTION PROFILE (PP) INTRODUCTION

1.1 PP IDENTIFICATION

Title: U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments.

Registration: <to be provided upon registration>.

Keywords: information flow control, firewall, packet filter, network security, protection profile.

1.2 PP OVERVIEW

This traffic-filter firewall Protection Profile defines the minimum security requirements for firewalls used by U.S Government organizations handling unclassified information in a low-risk environment. Firewalls may consist of one or more devices that act as part of an organization's overall security defense by isolating an organization's internal network from the Internet or other external networks. Firewalls pass and block information flows based on a set of screening rules defined by an authorized administrator. This Protection Profile applies to firewalls that are capable of screening network traffic at the network and transport protocol levels, authenticating the authorized administrator for actions at the firewall, and auditing security-relevant events that occur. For clarification of terms, see terminology section.

1.3 RELATED PROTECTION PROFILES:

U.S. Government Application-Level Firewall Protection Profile for Low-Risk Environments [2].

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 basically fall into two major categories: traffic-filter and application-level firewalls. This Protection Profile specifies the minimum security requirements for TOEs composed of a traffic-filter firewall.

The TOE selectively routes information flows among internal and external networks according to a 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. Traffic filtering decisions are typically made on the source address, destination address, transport layer protocol, source port, destination port, and are based on the interface on which the packet arrives or goes out.

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 TOE provides the capability for remote administration, then 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 trusted 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 authenticated. However, authorized external IT entities attempting to send information to the TOE must always be identified and authenticated (using a single-use authentication mechanism). This subset of external IT entities are permitted to perform a limited number of security functions as determined by an authorized administrator. 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, and all information flow control decisions made by the TOE according to the security policy rules. 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 140-1 is required[1]. FIPS PUB 140-1 defines security requirements for cryptographic modules. A cryptographic module is that part of a system or application that provides cryptographic services such as encryption, authentication, or electronic signature generation and verification. Products and systems compliant with this Protection Profile are expected to utilize cryptographic modules for remote administration compliant with this FIPS PUB.

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

3.1 ASSUMPTIONS

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

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

3.2 THREATS

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 may carry out spoofing in which information flow through the TOE into a connected network by using a spoofed source address.

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.

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 a insecure manner by either authorized or unauthorized persons.

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.

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

O.MEDIAT The TOE must mediate the flow of all information from users on a connected network to users on another connected network, 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.

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.

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

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

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 6.2 of the Rationale.

5 IT Security Requirements

5.1 TOE SECURITY REQUIREMENTS

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_UAU.1	Timing of authentication
FIA_AFL.1	Authentication failure handling
FIA_UAU.4	Single-use authentication mechanisms

Functional Components	
FDP_IFC.1	Subset information flow control
FDP_IFF.1	Simple security attributes
FMT_MSA.3	Static attribute initialization
FDP_RIP.1	Subset residual information protection
FCS_COP.1	Cryptographic operation
FPT_RVM.1	Non-bypassability of the TSP
FPT_SEP.1	TSF domain separation
FPT_STM.1	Reliable time stamps
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit review
FAU_SAR.3	Selectable audit review
FAU_STG.1	Protected audit trail storage
FAU_STG.4	Prevention of audit data loss
FMT_MOF.1	Management of security functions behavior

Table 5.1 – Security Requirements

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

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

FIA_UAU.1 – Strength of Function shall be demonstrated such that the probability that authentication data can be guessed is no greater than one in one million (000001).

FIA_UAU.4 – Strength of Function shall be demonstrated for the single-use authentication mechanism(s) by demonstrating compliance with the "Statistical random number generator tests" and the "Continuous random number generator test" found in section 4.11.1 of FIPS PUB 140- [5].

FCS_COP.1 – Strength of Function shall be demonstrated for the cryptographic algorithm and secret generation mechanism by demonstrating compliance with the "Cryptographic algorithm test", the Statistical random number generator tests", the Pair-wise consistency test (for public and private keys)", the Manual key entry test", and the "Continuous number generator test" found in section 4.11.1 of FIPS PUB 140-1 [5].

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. Since authentication must follow successful identification, component FIA_UAU.1 appears after FIA_UID.2. Then, component FIA_AFL.1 describes what results if the user fails to authenticate after some settable number of attempts. Lastly, component FIA_UAU.4 discusses when single-use authentication mechanisms must be used.

There is one information flow control SFP, and it is 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. 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. 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 140-1 compliant for the reasons stated in Section 3.

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

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 **human** 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_UAU.1 Timing of authentication

FIA_UAU.1.1 - The TSF shall allow [identification as stated in FIA_UID.2] on behalf of the authorized administrator or authorized external IT entity accessing the TOE to be performed before the authorized administrator or authorized external IT entity is authenticated.

FIA_UAU.1.2 - The TSF shall require each authorized administrator or authorized external IT entity to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that authorized administrator or authorized IT entity.

FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 - The TSF shall detect when [a settable, non-zero number, {to be determined by the Security Target writer(s),}] **of** unsuccessful authentication attempts occur related to [external IT entities attempting to authenticate from an internal or external network.]

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

FIA_UAU.4 Single-use authentication mechanisms

FIA_UAU.4.1 - The TSF shall prevent reuse of authentication data related

to [authentication attempts from either an internal or external network by:

a) authorized administrators;

b) authorized external IT entities].

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 such capabilities and their associated single-use 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 a single information flow control Security Function Policy (SFP). The information flow control SFP 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 information flowing between subjects in the policy 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.

FDP_IFC.1 Subset information flow control

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_IFF.1 Simple security attributes[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:

---

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

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].

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.1.6 - 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.]

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.

FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1 - The TSF shall enforce the [UNAUTHENTICATED 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 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.

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* the following objects: [resources that are used by the subjects of the TOE to communicate through the TOE to other subjects].

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:

- [Data Encryption Standard (DES) as specified in FIPS PUB 46-2 [3] and implementing any mode of operation specified in FIPS PUB 81 [4]]

and cryptographic key sizes [that are 64 binary digits in length] that meet the following: [FIPS PUB 46-2 [3] and FIPS PUB 81 [4]].

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, DES encryption must protect the communications between the authorized administrator and the TOE, and the associated cryptographic module(s) must comply at a minimum with FIPS PUB 140-1 Level 1.

FPT_RVM.1 Non-bypassability of the TSP

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

FPT_SEP.1 TSF domain separation

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

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

FPT_STM.1 Reliable time stamps

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

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 **relevant** auditable events for the *minimal or basic* level of audit **specified in Table 5.2;** and

c) [the event in Table 5.2 listed at the "extended" level].

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**s** identit**ies**, 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 four of Table 5.2].

Functional Component	**Level**	**Auditable Event**	**Additional Audit Record Contents**
FMT_SMR.1	minimal	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	basic	All use of the user identification mechanism	The user identities provided to the TOE
FIA_UAU.1	basic	Any use of the authentication mechanism.	The user identities provided to the TOE
FIA_AFL.1	minimal	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	basic	All decisions on requests for information flow.	The presumed addresses of the source and destination subject.
FCS_COP.1	minimal	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	minimal	Changes to the time.	The identity of the authorized administrator performing the operation
FMT_MOF.1	extended	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) [presumed subject address;

b) ranges of dates;

c) ranges of times;

d) ranges of addresses].

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

FMT_MOF.1.1 - The TSF shall restrict the ability to ***perform*** the functions:

a) [{start-up and shutdown;

b) create, delete, modify, and view information flow security policy rules that permit or deny information flows;

c) create, delete, modify, and view user attribute values defined in FIA_ATD.1;

d) enable and disable single-use authentication mechanisms in FIA_UAU.4 (if the TOE supports authorized IT entities and/or remote administration from either an internal or external network);

e) modify and set the threshold for the number of permitted authentication attempt failures (if the TOE supports authorized IT entities and/or remote administration from either an internal or external network);

f) restore authentication capabilities for users that have met or exceeded the threshold for permitted authentication attempt failures (if the TOE supports authorized IT entities and/or remote administration from either an internal or external network);

g) enable and disable external IT entities from communicating to the TOE (if the TOE supports authorized external IT entities);

h) modify and set the time and date;

i) archive, create, delet, empty, and review the audit trail;

j) backup of user attribute values, information flow security policy rules, and audit trail data, where the backup capability shall be supported by automated tools;

k) recover to the state following the last backup;

l) additionally, if the TSF supports remote administration from either an internal or external network:

- enable and disable remote administration from internal and external networks;
- restrict addresses from which remote administration can be performed;

m) other security-relevant administrative functions {to be determined by the Security Target writer(s)}].

to [an authorized administrator].

5.1.2 TOE SECURITY ASSURANCE REQUIREMENTS

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

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

Table 5.3 - Assurance Requirements: EAL2

ACM_CAP.2 Configuration items

Developer action elements:

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

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

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

Content and presentation of evidence elements:

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

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

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

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

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

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

Evaluator action elements:

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

ADO_DEL.1 Delivery procedures

Developer action elements:

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

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

Content and presentation of evidence elements:

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

Evaluator action elements:

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

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

Developer action elements:

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

Content and presentation of evidence elements:

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

Evaluator action elements:

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

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

ADV_FSP.1 Informal functional specification

Developer action elements:

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

Content and presentation of evidence elements:

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

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

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

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

Evaluator action elements:

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

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

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

ADV_HLD.1 Descriptive high-level design

Developer action elements:

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

Content and presentation of evidence elements:

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

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

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

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

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

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

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

Evaluator action elements:

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

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

Requirements Overview: ADV_RCR.1 ensures that there is consistency between each level of design decomposition for the TOE. Each higher level of design decomposition (the higher the level of design decomposition, the more abstract) should map to the one below it, until a level of design decomposition maps to the least abstract representation, the implementation itself. Thus, for Security Targets derived from this Protection Profile there are three layers of abstraction (from high to low): the STs "TOE Summary Specification" section, the Functional Specification, and the High-Level Design.[3]

ADV_RCR.1 Informal correspondence demonstration

Developer action elements:

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

Content and presentation of evidence elements:

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

Evaluator action elements:

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

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

meets all requirements for content and presentation of evidence.

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

AGD_ADM.1 Administrator guidance

Developer action elements:

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

Content and presentation of evidence elements:

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

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

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

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

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

AGD_ADM.1.6C - The administrator guidance shall describe each type of

security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

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

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

Evaluator action elements:

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

AGD_USR.1 User guidance

Developer action elements:

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

Content and presentation of evidence elements:

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

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

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

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

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

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

Evaluator action elements:

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

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

ATE_COV.1 Evidence of coverage

Developer action elements:

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

Content and presentation of evidence elements:

ATE_COV.1.1C - The evidence of the test coverage shall show the

correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

Evaluator action elements:

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

ATE_FUN.1 Functional testing

Developer action elements:

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

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

Content and presentation of evidence elements:

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

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

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

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

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

Evaluator action elements:

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

ATE_IND.2 Independent testing - sample

Developer action elements:

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

Content and presentation of evidence elements:

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

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

Evaluator action elements:

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

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

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

AVA_SOF.1 Strength of TOE security function evaluation[4]

Developer action elements:

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

Content and presentation of evidence elements:

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

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

Evaluator action elements:

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

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

Application Note: The security mechanisms defined by the following requirements have a specific strength of function claim: FIA_UAU.1, FIA_UAU.4, and FCS_COP.1. Section 5.1.1 of this PP defines the specific strength of function metric for each of these mechanisms.

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

AVA_VLA.1 Developer vulnerability analysis

Developer action elements:

AVA_VLA.1.1D - The developer shall perform and document an analysis of the TOE deliverables searching for obvious ways in which a user can violate the TSP.

AVA_VLA.1.2D - The developer shall document the disposition of obvious vulnerabilities.

Content and presentation of evidence elements:

AVA_VLA.1.1C - The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

Evaluator action elements:

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

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

Application Note: According to the Common Criteria Part 3, obvious vulnerabilities include those in the public domain. The evaluation body will be provided a current list of such vulnerabilities which should be included as part of vulnerability analysis and penetration testing. The first instantiation of this list is called Vulnerability list for AVA_VLA.1 and is included as Appendix A of this document.

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

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

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

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

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

	T.NOAUTH	T.REPEAT	T.REPLAY	T.ASPOOF	T.MEDIAT	T.OLDINF	T.PROCOM	T.AUDACC	T.SELPRO	T.AUDFUL
O.IDAUTH	X									
O.SINUSE		X	X							
O.MEDIAT				X	X	X				
O.SECSTA	X								X	
O.ENCRYP	X						X			
O.SELPRO									X	X
O.AUDREC								X		
O.ACCOUN								X		
O.SECFUN	X		X							X
O.LIMEXT	X									

Table 6.1a - 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.PUBLIC The TOE does not host public data.

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

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

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

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

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

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

	T.TUSAGE
O.GUIDAN	X
O.ADMTRA	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 rationale for the chosen level of SOF-basic is based on the low attack potential of the threat agents identified in this protection profile. Those security objectives imply probablistic or permutational security mechanism and that the metrics defined are the minimal "industry" accepted (for the passwords) and government required (for the encryption) metrics they should be good enough for SOF-Basic.

FMT_SMR.1 Security roles

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

FIA_ATD.1 User attribute definition

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.SINUSE.

FIA_UID.2 User identification before any action

This component ensures that before anything occurs on behalf of a user, the users identity is identified to the TOE. This component traces back to and aids in

meeting the following objectives: O.IDAUTH and O.ACCOUN.

FIA_UAU.1 Timing of authentication

This component ensures that users are authenticated at the TOE. The TOE is permitted to pass information before users are authenticated. Authentication must occur whether the user is a human user or not and whether or not the user is an authorized administrator. If the authorized administrator was not always required to authenticate, there would be no means by which to audit any of their actions. An additional SOF metric for this requirement is defined in section 5.1.1 to ensure that the authentication mechanism chosen cannot be easily bypassed. This component traces back to and aids in meeting the following objectives: O.IDAUTH and O.SINUSE.

FIA_AFL.1 Authentication failure handling

This component ensures that human users who are not authorized administrators can not endlessly attempt to authenticate. After some number of failures that the ST writer 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.4 Single-use authentication mechanisms

This component was chosen to ensure that some one-time authentication mechanism is used in all attempts to authenticate at the TOE from an internal or external network. An additional SOF metric for this requirement is defined in section 5.1.1 to ensure that the mechanism is of adequate cryptologic strength. This component traces back to and aids in meeting the following objective: O.SINUSE.

FDP_IFC.1 Subset information flow control

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_IFF.1 Simple security attributes

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.

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 , O.SECSTA, and O.SECFUN.

FDP_RIP.1 Subset residual information protection

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

FCS_COP.1 Cryptographic operation

This component ensures that if the TOE does support authorized administrators to communicate with the TOE remotely from an internal or external network that DES is used to encrypt such traffic. An additional SOF metric is defined in section 5.1.1 to ensure that the encryption mechanism chosen is adequate strength to protect the traffic and is implemented correctly. This component traces back to and aids in meeting the following objective: O.ENCRYP.

FPT_RVM.1 Non-bypassability of the TSP

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

FPT_SEP.1 TSF domain separation

This component ensures that the TSF have a domain of execution that is separate and that cannot be violated by unauthorized users. This component traces back to and aids in meeting the following objective: O.SELPRO.

FPT_STM.1 Reliable time stamps

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. Only the authorized administrator is permitted to do anything to the audit trail. This component traces back to and aids in meeting the following objectives: O.SELPRO and O.SECFUN.

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 and O.SECFUN.

FMT_MOF.1 Management of security functions behavior

This component was chosen and modified to some extent via permitted CC operations in an attempt to consolidate all TOE management/administration/security functions. 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_UAU.1	X	X								
FIA_AFL.1						X				
FIA_UAU.4		X								
FDP_IFC.1			X							
FDP_IFF.1			X							
FMT_MSA.3			X	X					X	

	O.IDAUTH	O.SINUSE	O.MEDIAT	O.SECSTA	O.ENCRYP	O.SELPRO	O.AUDREC	O.ACCOUN	O.SECFUN	O.LIMEXT
FDP_RIP.1			X							
FCS_COP.1					X					
FPT_RVM.1						X				
FPT_SEP.1						X				
FPT_STM.1							X			
FAU_GEN.1							X	X		
FAU_SAR.1							X			
FAU_SAR.3							X			
FAU_STG.1						X			X	
FAU_STG.4						X			X	
FMT_MOF.1				X					X	X

Table 6.3 - Summary of Mappings Between TOE Security Functions and IT Security Objectives

6.4 RATIONALE FOR ASSURANCE REQUIREMENTS

EAL2 was chosen to provide a low to moderate level of independently assured security in the absence of ready availability of the complete development record from the vendor. As such, 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 and vulnerability testing verification. The chosen assurance level is consistent with the postulated threat environment. Specifically, that the threat of malicious attacks is not greater than moderate, and the product will have undergone a search for obvious flaws.

6.5 RATIONALE FOR NOT SATISFYING ALL DEPENDENCIES

Functional component FMT_MSA.3 depends on functional component FMT_MSA.1 Management of security attributes. In an effort to place all the management requirements in a central place, FMT_MOF.1 was used. Therefore FMT_MOF.1 more than adequately satisfies the concerns of leaving FMT_MSA.1 out of 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 140-1 compliant. If the cryptographic module is indeed compliant with this FIPS PUB, then the dependencies of key generation, key destruction and secure key values will have been satisfied in becoming FIPS PUB 140-1 compliant. For more information, refer to sections 4.8.1 and 4.8.5 of FIPS PUB 140-1.

Appendix A

Vulnerability List for AVA_VLA.1

This appendix is the first instantiation of the service or application-related vulnerabilities. The most current list can be obtained from the scheme evaluation body. If the service described in one of the following vulnerabilities is not supported by the TOE, then the vulnerability is not applicable. The TOE shall also be subject to a search for obvious operating system and platform vulnerabilities.

FTP daemon vulnerabilities

Description:

In certain versions of the FTP daemon, a vulnerability exists allowing local and remote users to gain root privileges. This is accomplished through different means for distinct version such as through the signal handling routine increasing process privileges or through exploiting the SITE EXEC command.

See the relevant CERT advisory summaries including, CA-97:16, CA-95:16, and CA-94:08.

rlogin with TERM environment variable vulnerability

Description:

If, during a rlogin attempt on certain vulnerable systems, the buffer containing the value of the TERM environment variable is overflowed, arbitrary code can be executed as root.

See the relevant CERT advisory summaries including, CA-97:06.

Sendmail vulnerabilities

Description:

Remote users may be able to execute arbitrary commands with root privileges on systems receiving mail that are running a vulnerable version of sendmail that support MIME.

A second vulnerability to certain versions of sendmail occurs when an attacker gains group permissions of another user. This is possible when mail is sent to a users .forward or :include: file which is located in a directory that is writable by the attacker.

A third vulnerability to certain versions of sendmail occurs when users other than root invoke sendmail in daemon mode, bypassing code intended to prevent this.

A fourth vulnerability to certain versions of sendmail occurs when buffer overflows lead to unauthorized users gaining root access.

A fifth vulnerability to certain versions of sendmail occurs in the case of resource starvation. A user with an account can exploit sendmail when sendmail cannot distinguish between a "resource failure" and "user id not found" error. Starving sendmail will create files owned by the "default user" which can then be used to gain access to other files owned by that user.

See the relevant CERT advisory summaries including, CA-97:05, CA-96:25, CA-96:24, CA-96:20, and CA-95:08.

Telnet Environment Option vulnerability

Description:

If the system to which the Telnet connection attempt is directed is running Telnet daemons that are RFC 1408 or RFC 1572 compliant and the system supports shared object libraries then the system may be vulnerable. Both users with and without accounts on the system could become root by transferring environment variables that influence the login program called by the Telnet daemon.

See the relevant CERT advisory summaries including, CA-95:14.

TFTP daemon attacks

Description:

Remote users on the Internet may access world-readable files on an internal network using an unrestricted TFTP service. Thus sensitive files could be retrieved by an adversary on the external side of the firewall.

See the relevant CERT advisory summaries including, CA-91:19 and CA-91:18.

Syslog Vulnerability

The syslog(3) subroutine uses an internal buffer for building messages that are sent to the syslogd(8) daemon. This subroutine does no range checking on data stored in this buffer. It is possible to overflow the internal buffer and rewrite the subroutine call stack. It is then possible to execute arbitrary programs.

This problem is present in virtually all versions of the UNIX Operating System except the following:

- Sony's NEWS-OS 6.X
- SunOS 5.5 (Solaris 2.5)
- Linux with libc version 4.7.2 released in May, 1995

The sendmail(8) program uses the syslog(3) subroutine, and a script has been written and is being used to exploit the vulnerability.

Impact: Local and remote users can execute commands. Prior access to the system is not needed. Exploitation can lead to root access.

See the relevant CERT advisory summaries including, CA-95:13.

IP Spoofing attacks

Description:
Firewalls are vulnerable to IP spoofing attacks, including TCP SYN Flooding attacks. Firewalls should have a mechanism to handle SYN Flooding attacks. Firewalls should be capable of preventing traffic from entering the protected local network when packets claim to originate from local network, broadcast network, reserved network, or loopback network addresses.

See the relevant CERT advisory summaries including, CA-96:21.

UDP attacks

Description:

Tools exist to flood UDP ports with packets causing degradation in system performance and increased network congestion. Firewalls must be capable of being configured to filter all UDP services.

See the relevant CERT advisory summaries including, CA-96:01.

ICMP (ping) vulnerability

Large ICMP datagrams may cause systems to crash, freeze, or reboot, resulting in a denial of service.

See the relevant CERT advisory summaries for more information including, CA-96.26.

IP loose source route option vulnerability

Description:

Firewalls should be capable of rejecting packets that use the IP loose source route option. A TCP connection where the loose source route option is enabled allows an attacker to explicitly route packets through the network to a destination without following the usual routing process. A malicious attacker can pose as a host that is on the return path for this type of TCP traffic since, according to RFC 1122, the traffic must follow the reverse order of the route which it followed from source to destination.

RIP vulnerability

Description:

As a result of the ease with which bogus RIP packets may be injected into a network, packets can be lead away from their intended destination if the attacking host is closer to the target than the valid sending host. This occurs when routers accept RIP packets and because RIP performs no type of authentication. Firewalls should be configured to disallow routing along certain links such as intermediate links on an external network while the source and destination hosts are both on the internal network.

ARP vulnerability

Description:

Because any host can respond to an ARP request, a malicious host can send false ARP responses back to the sender before the true recipient receives the ARP request and responds back. Thus the sender will now be fooled into sending traffic to the malicious host in the middle rather than the proper destination host. The malicious host can either impersonate the destination host, or

intercept, modify, and resend the traffic to the sending host's intended destination. Firewalls should not allow ARP requests to pass through them and should not perform proxy ARP for requests from an external network.

DNS vulnerabilities

Description:

A flood of DNS responses injected into the network could cause a denial of service since the DNS server may become confused.

A DNS resolver may check several different levels before checking the correct one. If a host, FOO.BAR.COM, attempts to connect to ONE.TWO, the check will be made first to ONE.TWO.BAR.COM and then to ONE.TWO.COM and finally to ONE.TWO. Thus a malicious host can impersonate a domain that the resolver would encounter before encountering the appropriate level.

If an attacker can contaminate a target's DNS responses cache before the call is made, the target can be fooled into believing that the cross-check it performs is legitimate. As a result, the attacker gains access.

References

[1] *Common Criteria for Information Technology Security Evaluation*, CCIB-98-026 Version 2, May 1998.

[2] *U.S. Government Application-Level Firewall Protection Profile for Low-Risk Environments*; Version 2.0, June 1998.

[3] Federal Information Processing Standard Publication (FIPS-PUB) 46-2, *Data Encryption Standard (DES)*, December 1993.

[4] Federal Information Processing Standard Publication (FIPS-PUB) 81, *DES Modes of Operation*, December 1980.

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

[6] Building Internet Firewalls, Chapman & Zwicky, O'Reilly & Associates, Inc., November1995.

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