OULLIM Information Technology, Inc.

Security Target for

SECUREWORKS 3.0

Version 1.41

< Contents >

< List of Table >

1 Security Target Introduction

1 This introductory section presents the security Target (ST) identification information and an overview of the ST.

1.1 ST and TOE Identification

2 This section provides information needed to identify and control this ST and its Target of Evaluation (TOE), the SECUREWORKS 3.0. This ST targets an Evaluation Assurance Level (EAL) 3 level of assurance.

3 Release 4 of SECUREWORKS 3.0 is the release of SECUREWORKS 3.0 that is under evaluation. It is the only release of SECUREWORKS that is publicly released, and so is referred to publicly as "SECUREWORKS 3.0". The terms "SECUREWORKS 3.0" and "SECUREWORKS 3.0 release 4", for these purposes, are equivalent.

ST Title:	Oullim Information Technology SECUREWORKS 3.0 Security Target, September 2003
ST Version:	1.41
Authors	David Eung Soo Kim, Kevin Won Hyung Song
TOE Identification:	SECUREWORKS 3.0
CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999
PP Identification (1):	U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments version 1.1, April 1999
PP Identification (2):	U.S. Department of Defense Application-level Firewall Protection Profile for Basic Robustness Environments version 1.0, June 22, 2000
ST Evaluation:	CMG Australia
Keywords:	Information flow control, firewall, packet filter, application gateway, proxy, network security, traffic filter, security target, network address translation (NAT)

1.2 Conventions, Terminology, and Acronyms

4 This section identifies the formatting conventions used to convey additional information and terminology having specific meaning. It also defines the meanings of abbreviations and acronyms used throughout the remainder of the document.

1.2.1 Conventions

5 This section describes the conventions used to denote CC operations on security requirements and to distinguish text with special meaning. The notation, formatting, and conventions used in this ST are largely consistent with those used in the CC. Selected presentation choices are discussed here to aid the Security Target reader.

6 The CC allows several operations to be performed on functional requirements; assignment, iteration, refinement, and selection are defines in paragraph 2.1.4 of Part 2 of the CC.

- The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment is indicated by showing the value in square brackets [assignment value(s)].
- Iteration of a component is used when a component is repeated more than once with varying operations. Iterated component is indicated by appending an iteration number inside parenthesis to the base requirement identifier from the CC. i.e., FAU_SAR.3 (1) and FAU_SAR.3 (2)
- 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.
- The selection operation is picking one or more items from a list in order to narrow the scope of a component element. Selections are denoted by *underlined italicized* text.

7 Plain *italicized* text is used for both official document titles and text meant to be emphasized more than plain text.

1.2.2 Terminology

8 In the Common Criteria, many terms are defined in Section 2.3 of Part 1. The following terms are a subset of those definitions. They are listed here to aid the reader of the Security Target.

- 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, un-trusted or trusted, outside of the TOE that interacts with the TOE.
- Identity – A representation (e.g., a string) uniquely identifying an authorized user, which can be either the full or abbreviated name of that user or a pseudonym.
- Authentication data – Information used to verify the claimed identify of a user.

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

- End User - Any entity who interacts with the TOE without Authorized Administrator privileges.
- Authorized Administrator – A role which 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 rule enforced by the TOE.
- Audit Record – Audit data that is kept to record TOE security related events.
- OTP – One time password mechanism used to implement a single use authentication mechanism.

1.2.3 Acronyms

10 The following abbreviations from the Common Criteria are used in this Security Target:

CC	Common Criteria for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
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

1.3 Security Target Overview

11 The SECUREWORKS System described in this ST is a security application designed to protect organizational assets in a network environment. In particular, it provides facilities to control the movement of network data between networks. For example, when used to interconnect an organization's network to the Internet it can be used to protect that network from attacks originating from the Internet.

12 SECUREWORKS System uses a hybrid technology of dynamic packet filtering and an application gateway (proxies) to control and monitor the information flow of IP packets through the firewall. The packet filtering functions provide traffic filtering based upon packet attributes available at the transport and network protocol layers. For application gateway filtering, the packet content is examined to determine if it complies with rules that have been established by an Authorized Administrator. SECUREWORKS has a number of application proxies built into its application gateway filtering capability. This allows filtering to be based on application specific features. For example, the FTP proxy can be configured to only allow a subset of FTP commands through to the FTP server.

13 SECUREWORKS consists of two major components:

- Administration Server that manages the security policy rules. This module provides a “http” interface that can be accessed via a web browser. With the web browser interface, the administrator can access the Administration Server either locally or remotely to control and monitor SECUREWORKS System through SSL protocols. Remote Administration is not included within the scope of the evaluation.

- The Firewall Server is responsible for implementing the security policy rules. It is composed of a kernel driver that implements the security policy rules an authentication server that authenticates administrators and users, a log server that manages the audit record, and an application gateway that provides application level filtering.

1.4 Common Criteria Conformance

14 The TOE conforms to:

- The U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments, Version 1.1. [TFFPP]

- The U.S. Department of Defense Application-level Firewall Protection Profile for Basic Robustness Environments, Version 1.0. [ALFPP]

- Part 2 and Part 3 of the Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999

2 TOE DESCRIPTION

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

2.1 Architecture

16 SECUREWORKS 3.0 is comprised of two software modules, the Administration Server and the Firewall Server.

17 The Firewall Server includes the following components

- Authentication Server
- Audit Server
- Kernel Driver
- Application gateways

18 A Web browser is used as the management interface to the administration server. The Administration server performs management functions such as setup, initialization of configuration data, and analysis of disk space.

19 The Authentication Server manages the user authentication request from either the Application Gateway or a user. The Normal (SECUREWORKS) password and One Time Password user authentication methods are included in the scope of this TOE.

20 The Audit Server is responsible for managing the audit functions of the TOE. When an audit event occurs, an audit record is saved in the database. SECUREWORKS also provides the facility to designate alarms against events. When an alarm is triggered SECUREWORKS will either send an email or execute a script.

21 The Kernel Driver performs dynamic packet filtering and network address translation. It either allows or denies the packets based on the Packet Filtering Security Policy rule.

22 The application gateways perform application level filtering. These gateways perform the function of application proxies. These proxies understand the syntax application data and can filter network traffic based upon application specific rules. SECUREWORKS provides built in proxies for applications such as FTP, Telnet, HTTP, SMTP and rlogin.

2.2 Product Type

23 The SECUREWORKS is a firewall employing both application gateway filtering and packet filtering.

- Application Gateway – mediates flows between clients and servers located on internal and external networks governed by the firewall. The Application Gateway may employ proxies to screen information flows based upon rules regarding the packet content. Only valid requests are relayed to the actual server by the proxy server on either an internal or external network. Some proxy servers such as FTP can be configured to require authentication by users before requests for such services are authorized.

- Packet Filter Firewall – selectively routes information flows between an internal and an external network according to a site's security policy rules, the default policy being deny all. Only an authorized administrator has the authority to change the security policy rules. Traffic filtering decisions are made on the source address, destination address, transport layer protocol, source port, user, time, destination port, and are based on the interface on which the packet arrives or goes out.

2.3 Scope and Boundaries of the Evaluated configuration

24 This section provides a general description of the physical and logical scope and boundaries of the TOE.

2.3.1 Physical Scope and Boundaries

25 The TOE is SECUREWORKS 3.0

26 The evaluated configuration consists of the TOE together with the following components installed on a single physical server.

- Two network interfaces with one designated as internal and the other as external.
- UNIX OTP calculator
- The Solaris 5.8 Operating System installed.

27 SECUREWORKS v3.0 provides two types of OTP: (UNIX OTP Calculator & Windows OTP Calculator for client). To use the One Time Password authentication method the user must have installed a Windows OTP calculator on a client host. It should be noted the OTP calculator is publicly available shareware that contains no secret data. The UNIX OTP Calculator may be distributed with the TOE and may be used with the TOE in its evaluated configuration.

28 The physical scope of the evaluation includes the hardware and software elements identified in [Table2-1].

[Table 2-1] Components in the evaluated configuration of the TOE

Components	Items
Software	SECUREWORKS 3.0
	Netscape 6.1
	UNIX OTP calculator
	SunOS 5.8
Hardware	Sun Sparc with 256MB Memory 8GB Hard Disk space 2 Network Interface Cards D.A.T Backup Device

2.3.2 Logical Scope and Boundaries

29 The TOE provides the following security features:

30 Security Audit: SECUREWORKS provides logging for all activities pertaining to the actions to or through the product. It also records events pertaining to accessing Security Management. For example, mail forwarding and violation of the security policy rule are logged. Also the TOE can be configured to send the administrator an alarm when specific events occur. Audit generation can be enabled or disabled for each Packet Filtering Rule.

31 Authorized administrator can view and search the logs at any time. The Audit Records can be searched by keyword, time, source address and destination. These records can be summarized and sorted once a day or as specified by an administrator.

32 Information Flow Control: SECUREWORKS control all packets flow to or through SECUREWORKS by configuring the security policy rule. The Kernel Driver carries out the inspection process itself. SECUREWORKS also provides advanced security features through the provision of application level proxies. With the application proxies, rules specific to the FTP, HTTP, SMTP, Telnet, Rlogin, POP3, IMAP4, H323, and NNTP applications can be implemented.. Application proxies also provide both authentication and protection from malformed service requests. TCP/IP common gateways such as POP3, Telnet, RLOGIN, IMAP4, and H.323 do not provide an authentication method. The Firewall Server ensures that information contained in packets is deleted before the memory object for that packet is reused.

33 Identification and Authentication: The TOE has an Authentication Server that provides both password and single use authentication methods for users and administrators. User authentication can be executed at both the Packet filter and Application Gateway level. The Authentication Server also provides an authentication failure handling mechanism that can locks-out user accounts when a defined number of unsuccessful authentication attempts have been made. Only an administrator can re-enable the locked account.

34 Security Management: The Management Module maintains all security attributes for SECUREWORKS authorized administrators. Security Procedures ensure that only authorized administrators can access the Management Module for action such as viewing logs, defining Security Policy rule, alarm setup.

35 Protection of Security Functions: The Administration Server constantly checks the status of other firewall daemons. If an expected daemon is not running, the server invokes the appropriate daemon. SECUREWORKS ensures non-bypassability, as all network traffic to the TOE host must go through the TOE first. After Installation, Generation, and Startup are completed, SECUREWORKS will always be invoked on subsequent system startups. Integrity checking is provided for a number of critical TOE and system files.

36 SECUREWORKS 3.0 is a comprehensive software suite that provides a wide range of functionality. Only a portion of this product has been included in the TOE and has been subjected to an evaluation. Software and hardware feature outside the scope of the defined TOE Security Functions (TSF) and thus not evaluated are:

- Encrypting Functions of SSL (Socket Security Layer) Protocol
- Remote administration
- Virus filtering(Mail attachment control/removal)
- HA (High Availability)
- SecurID Authentication
- Harmful Site Filtering Setup(HTTP redirection)
- VPN (Virtual Private Network) Module
- REDIRECT NAT, EXCLUDE NAT
- Integration with ASEN product
- Telnet session capture function
- Check Integrity on startup
- Store FTP transfer files
- OTP (One Time Password) calculator for windows
- RADIUS Server
- SNMP trap occurrence.
- SQL NET/NET8 Application Gateway
- CGI security check
- OS password authentication
- SecureDNS
- StreamWorks Application Gateway
- HTTP Proxy Keep-Alive function
- HTTP Allow extended methods (Support WebDAV-MSN expolorer)
- Web Cache
- Webtrends Log Analysis Server Working together function
- Authentication LDAP
- OpenSSL crypto library except for where it provides this bit of OTP.
- Network Interface Card Management
- Routing Table Management
- Routing Protocol RIP Management
- ARP (Adress Request Protocol) Management
- Remote LogServer
- Authentication method for users not registered with SECUREWORKS.
- CA (Certificate Authority) function
- Text Administration
- User: Frame protocol(PPP+SLIP)
- Policy Rules: Confidentiality.
- Telnet and Rlogin Application Gateway’s Authentication function
- H.323 Application Gateway’s max session and timeout function
- SMTP Application Gateway’s max mail size limit function
- IPSec Fragment option

2.4 Application Context

37 The evaluated TOE has a Management Module consists of UI Client (Web Browser), an Administration Server and a Firewall Server installed on the same computer platform. The evaluated configuration requires that SECUREWORKS be installed on a dual-homed host. The firewall itself must be configured for static IP routing.

3 TOE SECURITY ENVIRONMENTS

38 The TOE is a dual-homed device mediating information flows between two networks such as an internal, protected network, and an external, hostile network. To clarify and define the security environment, assumptions about the security environment and/or the manner in which the TOE will be used are provided.

39 The assumptions and threat identification combined with any organization security policy statement or rules requiring TOE compliance completes the definition of the security environment. It is necessary that a comprehensive system security policy be established for the site in which the product is operated and that it is enforced and adhered to by all users of the product.

40 The system security policy is expected to include measures for:

- Physical security - to restrict physical access to areas containing the product, computer system and associated equipment and protect physical resources, including media and hardcopy material, from unauthorized access, theft or deliberate damage.
- Procedural security - to control the use of the computer system, associated equipment, the product and information stored and processed by the product and the computer system, including use of the product's security features and physical handling of information.
- Personnel security - to limit a user's access to the product and to the computer system to those resources and information for which the user has a need-to-know and, as far as possible, to distribute security related responsibilities among different users.

3.1 ASSUMPTIONS

41 This section lists the assumptions about the environment within which the TOE will operate.

42 [Table 3-1] contains those assumptions taken, without modification, from the ALFPP.

[Table 3-1] Assumptions from the ALFPP

Name	Description
A.PHYSEC	The TOE is physically secure..
A.LOWEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
A.PUBLIC	The TOE does not host public data.
A.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.
A.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.

43 The following assumptions from the ALFPP have been modified to reflect the specific architecture of the TOE.

[Table 3-2] Modified Assumptions

Name	Description
A.GENPUR	TOE only executes security relevant applications and only stores data required for its secure operation. The operating system upon which the TOE executes has been hardened to restrict general-purpose computing capabilities and storage.
A.DIRECT	Human users(End Users) within the physically secure boundary protecting the TOE may only attempt to access the TOE directly, via its console.
A.NOREMO	Human Users(Administrators) cannot access the TOE remotely from the internal or external networks .

44 The following assumptions have been added to reflect the specific architecture of the TOE

[Table 3-3] Added Assumptions

Name	Description
A.NOACC	Only the Authorized Administrators may have an account on the TOE host system.

45 The ALFPP specified that some functional requirements are optional. Since remote access control of administrator is optional functional requirement in the ALFPP and out of scope, the following assumption from ALFPP is not included in the ST.

[Table 3-4] Omitted Assumptions

Name	Description
A. REMACC	Authorized Administrators may access the TOE remotely from the internal and external networks.

3.2 THREATS

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

3.2.1 Threats addressed by the TOE

47 This section lists the threats faced by the TOE. The threats are countered either by the TOE or by its environment.

48 [Table 3-5] contains those threats taken, without modification, from the ALFPP.

[Table 3-5] Threats from the ALFPP

Name	Description
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 bypass 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.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.

49 Additional threats not described in the ALFPP have been addressed by the SECUREWORKS ST. These threats are described in [Table 3-6] below.

[Table 3-6] Additional Threats

T.PRIVACY	With knowledge of the real IP addresses of external IT entities on the internal network, an unauthorized person may determine enough information about the internal network to affect the internal network in an undesirable observation
T.UNDETECTED	A treat agent may cause auditable events to go undetected.

50 The ALFPP states that remote access administration is an optional function. This functionality is not included as part of the TOE. As a consequence the following threat from ALFPP is not included in the ST.

[Table 3-7] Omitted Threat

Name	Description
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.

3.2.2 Threats Addressed by the Operating Environment

51 [Table 3-8] contains the threat addressed by the operating environment rather than the TOE itself. This threat is taken, without modification, from the ALFPP.

[Table 3-8] Threat Addressed by the Operating Environment

Name	Description
T.USAGE	The TOE may be inadvertently configured, used, and administered in an insecure manner by a human user.

3.3 Organization Security Policies

52 ALFPP states one Organization Security Policy relating to the use of cryptographic modules. Since SECUREWORKS doesn't provide remote administration, this OSP does not apply. Therefore, the SECUREWORKS ST does not identify any organizational security policy statements or rules with which the TOE must comply.

4 SECURITY OBJECTIVES

53 Threats can be directed against the TOE or the security environment or both, therefore, the CC identified two categories of security objectives:

- Security objectives for the TOE
- Security objectives for the Operating Environment.

4.1 Security Objectives for the TOE

54 This section lists the security objectives for the TOE.

55 [Table 4.1] contains those objectives taken, without modification, from the ALFPP.

[Table 4-1] Security Objectives for the TOE from ALFPP

Name	Description
O.IDAUTH	The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to TOE functions or, for certain specified services, to a connected network.
O.SINUSE	The TOE must prevent the reuse of authentication data for users attempting to authenticate to the TOE from a connected network.
O.MEDIAT	The TOE must mediate the flow of all information between clients and servers located on internal and external networks governed by the TOE, disallowing passage of non-conformant protocols and ensuring that residual information from a previous information flow is not transmitted in any way.
O.SECSTA	Upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE must not compromise its resources or those of any connected network.
O.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.

56 Additional Security Objectives for the TOE, not described in ALFPP have been included in SECUREWORKS ST. [Table 4-2] states these additional objectives.

[Table 4-2] Additional Security Objectives for the TOE

Name	Description
O.PRIVACY	The TOE must ensure that an Authorized Administrator can prevent users on the external network determining the IP address of the users on the internal network.
O.ALARM	The TOE must provide detecting violations and alerting potential violations as configured by an Authorized Administrator.

57 The ALFPP states that remote access administration is an optional function. This functionality is not included as part of the TOE. As a consequence the following objective from ALFPP is not included in the ST.

[Table 4-3] Omitted Objectives for the TOE

Name	Description
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.

4.2 Security Objectives for the Environment

58 The following are the IT security objectives for the environment. The following objectives in [Table 4-3] are taken, without modification, from the ALFPP.

[Table 4-4] Security Objectives for the Environment

Name	Description	Assumption(s) /Threats
OE.PHYSEC	The TOE is physically secure.	A.PHYSEC
OE.LOWEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.	A.LOWEXP
OE.PUBLIC	The TOE does not host public data.	A.PUBLIC
OE.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.	A.NOEVIL
OE.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.	A.SINGEN
OE.GUIDAN	The TOE must be delivered, installed, administered, and operated in a manner that maintains security.	T.USAGE T.AUDACC
OE.ADMTRA	Authorized administrators are trained as to establishment and maintenance of security policy rules and practices	T.USAGE T.AUDACC

59 The PP security Objectives have been modified and added to in this ST to reflect the security environment and TOE architecture. [Table 4-4] states these modified objectives for the environment.

[Table 4-5] Modified and added Security Objectives for the Environment

Name	Description	Assumption(s) /Threats
OE.GENPUR	TOE only executes security relevant applications and only stores data required for its secure operation. The operating system upon which the TOE executes has been hardened to restrict general-purpose computing capabilities and storage.	A.GENPUR

OE.DIRECT	Human users(End Users) within the physically secure boundary protecting the TOE may only access the TOE directly, via its console.	A.DIRECT
OE.NOREMO	Human Users(Administrator) cannot access the TOE remotely from the internal or external networks.	A.NOREMO

60 The following objectives have been added to reflect the specific architecture of the TOE

[Table 4-6] Added Security Objectives for the environment

Name	Description	Name
OE.NOACC	Only the Authorized Administrators may have an account on the TOE host system.	A.NOACC

61 The ALFPP states that remote access administration is an optional function. This functionality is not included as part of the TOE. As a consequence the following objective for the environment, from the ALFPP, is not included in the ST.

[Table 4-7] Omitted Security Objectives for the Environment

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

5 TOE SECURITY REQUIREMENTS

62 IT security requirement include:

- TOE security requirements and (optionally)
- Security requirements for the TOE's IT environment (that is, for hardware, software, or firmware external to the TOE and upon which satisfaction of the TOE's security objectives depends).

63 These requirements are discussed separately below.

5.1 TOE Security Requirements

64 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.

65 The CC divides security requirements into two categories:

- Security functional requirements (SFRs): that is, requirements for security functions such a information flow control, audit, and identification.
- Security assurance requirements (SARs): provide grounds for confidence that the TOE meets its security objectives.

5.1.1 TOE Security Functional Requirements

66 This section presents the SFRs for the TOE. This section has the following four subsections:

- Restated PP SFRs: those PP security functional requirements with which the ST claims compliance and for which no additional operations are to be performed. These PP SFRs are included in the ST verbatim.
- Tailored PP SFRs: those PP security functional requirements with which the ST claims compliance but for which additional operations are to be performed.

- Additions to PP SFRs (optional): any security functional requirements additional to those of the PP.

- SFRs with Strength of Function (SOF) Declarations: any security functional requirement that requires a SOF declaration.

5.1.1.1 Restated PP SFRs

67 The TOE shall satisfy the SFRs stated in [Table 5-1] that lists the CC names of the SFR components contained in the ALFPP and TFFPP. Following the table, the individual functional requirements are restated from the ALFPP and TFFPP.

[Table 5-1] Restated Security Functional Requirements

Functional Component ID	Functional Component Name
FAU_SAR.1	Audit review
FDP_RIP.1	Subset residual information protections
FIA_UID.2	User identification before any action
FPT_SEP.1	TSF domain separation
FPT_RVM.1	Non-bypassability of the TSP
FAU_STG.1	Protected audit trail storage
FMT_SMR.1	Security roles
FMT_MSA.1 (1)	Management of security attribute (1)
FDP_IFC.1 (1)	Subset information flow control (1)
FIA_UAU.4	Single use authentication
FPT_STM.1	Reliable time stamp
FAU_STG..4	Prevention of audit data loss
FAU_SAR.3	Select audit review
FMT_MTD.1 (2)	Management of TSF data (2)
FMT_MTD.2	Management limits on TSF data

68 **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.

69 **FDP_RIP.1 Subset residual information protections**

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: [all object].

Application Note: If, for example, the TOE pads information with bits in order to properly prepare the information before sending it out on interface, these bits would be considered a "resource". The intent of the requirement is 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**.**

70 **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.

Application Note: 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). (See ALFPP paragraph 10 and O.IDAUTH)

71 **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.

72 **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.

73 **FAU_STG.1 Protected audit trail storage**

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

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

74 **FMT_SMR.1 Security roles**

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

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

75 **FMT_MSA.1 (1) Management of security attribute (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) and FDP_IFF.1.1 (2)] to [the authorized administrator].

76 **FDP_IFC.1 (1) Subset information flow control (1)**

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

[Subjects: unauthenticated external IT entities that send and receive information through the TOE to one another

Information: packet sent through the TOE from one subject to another;

Operations: pass information].

77 **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.

78 **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.

79 **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

80 **FAU_SAR.3 Select 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

81 **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 [an authorized administrator].

82 **FMT_MTD.2 Management limits on TSF data**

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

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

5.1.1.2 Omitted PP SFRs

83 The TFFPP and ALFPP specify that some functional requirements are optional and may be omitted from compliant TOEs. [Table 5-2] identifies the SFRs that have been omitted from this ST.

[Table 5-2] Functional Components Omitted from the TOE

Reference	Description	Rational
FCS_COP.1	Cryptographic operation	The TOE does not include support for remote administration of the TOE. However, due to the hashing algorithm, a modified FCS_COP value is restated in 5.1.1.3 as a tailored SFR.

5.1.1.3 Tailored PP SFRs

84 The TFFPP and ALFPP identified several SFRs that contain operations to be completed in PP –compliant security targets. This section identifies those TFFPP and ALFPP requirements and performs the required operations. (In addition, this section contains PP SFRs that were refined to specifically capture TOE functionality.) The TOE shall satisfy the resultant requirements.

85 [Table 5-3] names the SFRs for which the ST is required to perform operations. The table also identifies the operations (assignment, iteration, refinement, and selection) performed on them in this ST. Following the table, the individual functional requirements are restated from the ALFPP and TFFPP, and the operations completed.

86 The ALFPP iterated FDP_IFC.1, FDP_IFF.1 components twice. However, this ST iterates the each component three times by adding one which is UNAUTHENTICATED_PROXY SFP. The subjects under control of this policy do not require TOE authentication for End Users on an internal or external network.

[Table 5-3] Tailored SFRs

Functional Component ID	Functional Component Name	Operation
FAU_GEN.1	Audit data generation	Assignment
FDP_IFC.1 (2)	Subset information flow control(2)	Assignment
FDP_IFC.1(3)	Subset information flow control(3)	Assignment
FDP_IFC.1(4)	Subset information flow control(4)	Assignment
FDP_IFF.1 (1)	Simple security attributes(1)	Assignment
FDP_IFF.1 (2)	Simple security attributes(2)	Assignment
FDP_IFF. 1(3)	Simple security attributes(3)	Assignment
FDP_IFF. 1(4)	Simple security attributes(4)	Assignment
FIA_AFL.1	Authentication failure handling	Assignment
FIA_ATD.1	User attribute definition(1)	Assignment Refinement
FMT_MSA.1 (2)	Management of security attribute(2)	Iteration
FMT_MSA.1 (3)	Management of security attribute(3)	Iteration
FMT_MSA.1 (4)	Management of security attribute(4)	Iteration
FMT_MSA.1 (5)	Management of security attribute(5)	Iteration
FMT_MSA.1 (6)	Management of security attribute(6)	Iteration
FMT_MTD.1 (1)	Management of TSF data(1)	Assignment
FMT_MOF.1 (1)	Management security function behavior (1)	Assignment
FMT_MOF.1 (2)	Management security function behavior (2)	Assignment

FIA_UAU.5	Multiple authentication mechanisms	Assignment
FIA_UAU.1	Time of authentication	Assignment Refinement
FMT_MSA.3	Static attribute initialization	Assignment
FCS_COP.1	Cryptographic operation	Assignment

87 **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 *minimal or basic* level of audit specified in Table 5-4
c) [the event in Table 5-4 listed at the "extended" level].
d)

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 ST, [information specified in column three of Table 5-4]

[Table 5-4] Auditable Events

Functional Component	Level	Auditable Event	Additional Audit Record Contents
FMT_SMR.1	Minimal	Modification 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_UAU.5	Not specified	Any use of the authentication mechanism	User identities provided to the TOE
FIA_AFL.1	Minimal	The reaching of the threshold for unsuccessful authentication attempts and	The identity of the offending user and the authorized administrator.

		the subsequent restoration by the authorized administrator of the users capability to authenticate.	
FDP_IFF.1 (1)	Basic	All decisions on requests for information flow.	The presumed addresses of the source, destination subject, service, interface, protocol, user, time, data size, status (indicates packet's status; allow, deny, closed), and its reason.
FDP_IFF.1 (2)	Basic	All decisions on requests for information flow.	The presumed addresses of the source, destination subject, service, interface, protocol, user, time, data size, status (indicates packet's status; allow, deny, closed), and its reason.
FDP_IFF.1 (3)	Basic	All decisions on requests for information flow.	The presumed addresses of the source, destination subject, service, interface, protocol, user, time, data size, status (indicates packet's status; allow, deny, closed), and its reason.
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.

88 **FDP_IFC.1 (2) Subset information flow control (2)**

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

a) [Subjects: End Users that sends and receive information through the TOE to one another

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

c) Operation: authentication and pass information].

89 **FDP_IFC.1 (3) Subset information flow control (3)**

FDP_IFC.1.1 (3)The TSF shall enforce the [UNAUTHENTICATED_PROXY SFP] on:

a) [Subjects: End Users that sends and receive information through the TOE to one another

b) Information: Telnet, RLOGIN, POP3, IMAP4, and H.323 traffic sent through the TOE from one subject to another; and

c) Operation: initiate service and pass information].

90 **FDP_IFC.1 (4) Subset information flow control(4)**

FDP_IFC.1.1 (4)The TSF shall enforce the [AUTHENTICATED SFP] on:

a) [Subjects: End Users that sends and receives FTP, HTTP, SMTP, and NNTP information through the TOE to one another, only after the End Users initiating the information flow has authenticated at the TOE per FIA_UAU.5

b) Information: FTP, HTTP, SMTP, and NNTP traffic sent through the TOE from one subject to another; and

c) Operation: initiate service and pass information].

91 **FDP_IFF.1 (1) Simple security attributes (1)**

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

a) [Subject security attributes:
- Presumed address;

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
- Services
- Time]

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

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

- All the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values

of the Information flow security attributes, created by the authorized administrator;
- The presumed address of the source subject, in the information, translates to an internal network address
- And the presumed address of the destination subject, in the information, translates to an address on the other connected network.

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

- All the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;
- The presumed address of the source subject, in the information, translates to an external network address;
- And the presumed address of the destination subject, in the information, translates to an address on the other connected network.]

FDP_IFF.1.3 (1) The TSF shall enforce the [initailization].

FDP_IFF.1.4 (1) The TSF shall provide the following [for each rule in the UNAUTHENTICATED SFP:

a) On/off switch
b) On/off log switch
c) Rule applying order can be rearranged.
d) initialization]

FDP_IFF.1.5 (1) The TSF shall explicitly authorize an information flow based on the following rules: [none].

FDP_IFF.1.6 (1) The TSF shall explicitly deny an information flow based on the following rules:

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

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

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

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

e) IP source route - 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.

g) Land attack –The TOE shall detect and deny requests if the source IP address is same as the destination IP address.

h) Finger print scan – The TOE shall detect and deny packets if an unused flag value is in the TCP header flag.

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_IFF1.1 (b), could be identified, for example, by a source port number and/or destination port number.

92 **FDP_IFF.1 (2) Simple security attributes (2)**

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

a) [Subject security attributes:
- Presumed address;

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
- User identity (must belong to the User Group defined by the rule)
- Services
- Time

FDP_IFF.1.2 (2) The TSF shall permit an information flow between a controlled subject and **another** controlled **subject** via 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(End 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(End 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.1.3 (2) The TSF shall enforce the [initialization].

FDP_IFF.1.4 (2) The TSF shall provide the following [for each rule in the UNAUTHENTICATED SFP:

a) On/off switch
b) On/off log switch
c) Rule applying order can be rearranged.

FDP_IFF.1.5 (2) The TSF shall explicitly authorize an information flow based on the following rules: [none].

FDP_IFF.1.6 (2) The TSF shall explicitly deny an information flow based on the following rules:[none]

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_IFF1.1 (b), could be identified, for example, by

a source port number and/or destination port number.

93 **FDP_IFF.1 (3) Simple security attributes (3)**

FDP_IFF.1.1 (3) The TSF shall enforce the [UNAUTHETICATED_PROXYSFP] base on **at least** the following types of subject and information security attributes:

a) [Subject security attributes:
- Presumed address;

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
- Services (Telnet, RLOGIN, POP3, IMAP4 and H.323)
- Timeout value (except for H.323)
- Maximum connect (that is, maximum number of users not exceeded) (except for H.323)

FDP_IFF.1.2 (3) The TSF shall permit an information flow between a controlled **subject** and **another** controlled subject via 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
- 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
- And the presumed address of the destination subject, in the information, translates to an address on the other connected network.]

FDP_IFF.1.3 (3) The TSF shall enforce the [none].

FDP_IFF.1.4 (3) The TSF shall provide the following [on/off switch each rule in the UNAUTHENTICATED_PROXY SFP and Upload/Down load control of UNAUTHENTICATED SFP for telnet].

FDP_IFF.1.5 (3) The TSF shall explicitly authorize an information flow based on the following rules: [none].

FDP_IFF.1.6 (3) The TSF shall explicitly deny an information flow based on the [following rules:

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

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

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

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

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

f) For the Telnet, RLOGIN, POP3, IMAP4 and H.323 application protocols the TOE shall deny any access or service requests that do not conform to their associated published protocol specification. This shall be accomplished through protocol filtering proxies that are designed for that purpose.]

94 **FDP_IFF.1 (4) Simple security attributes (3)**

FDP_IFF.1.1 (4) The TSF shall enforce the [AUTHENTICATED SFP] base on **at least** the following types of subject and information security attributes:

a) [Subject security attributes:
- Presumed address;

b) Information security attributes;
- User identity; (must belong to the User Group defined by the rule)
- Presumed address of source subject;
- Presumed address of destination subject;
- Transport layer protocol;
- TOE interface on which traffic arrives and departs;

- Services (FTP, HTTP, SMTP, and NNTP);
- security-relevant service command; and
- Timeout value
- Maximum connect (that is, maximum number of users not exceeded)]

FDP_IFF.1.2 (4) The TSF shall permit an information flow between a controlled **subject** and **another** controlled subject via 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(End 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
- 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(End 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.1.3 (4) The TSF shall enforce the [none].

FDP_IFF.1.4 (4) The TSF shall provide the following [following list:

a) Enable/disable switch for each rule in the AUTHENTICATED SFP

b) Allow FTP data port automatically option, allow only when FTP-DATA source port is 20 that AUTHENTICATE SFP for FTP

c) Contents blocking and content and method filtering AUTHENTICATED SFP for HTTP

d) [maximum recipient, sender domain check, reverse DNS check, Mail relay prevention, create local copy, forward e-mails to PostMaster, queue retry interval, daily permitted maximum count per sender of AUTHENTICATED SFP for SMTP

FDP_IFF.1.5 (4) The TSF shall explicitly authorize an information flow based on the following rules: [none]

FDP_IFF.1.6 (4) 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.]

95 **FIA_AFL.1 Authentication failure handling**

FIA_AFL.1.1 The TSF shall detect when [a settalbe, a non-zero number determined by the authorized administrator and when the ID is not existing] of unsuccessful authentication attempts occur related to [authorized TOE administrator access or authorized TOE IT entity access 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 or delay the offending user from successfully authenticating until an authorized administrator takes some action to make authentication possible for the user in question.]

96 **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) Dates and Times they are permitted to authenticate

d) Authentication data

e) Account Status

f) Password method and password change time

g) administrator's accessibility – Log, User, Policy]

97 **FMT_MSA.1 (2) Management of security attribute (2)**

FMT_MSA.1.1 (2) The TSF shall enforce the [UNAUTHENTICATED_PROXY SFP] to restrict the ability to [delete attributes from a rule, modify attributes in a rule, add attributes to a rule] the security attributes [listed in section FDP_IFF1.1 (3)] to [the authorized administrator].

98 **FMT_MSA.1 (3) Management of security attribute (3)**

FMT_MSA.1.1 (3) 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 (4)] to [the authorized administrator].

99 **FMT_MSA.1 (4) Management of security attribute (4)**

FMT_MSA.1.1 (4) The TSF shall enforce the [UNAUTHENTICATED SFP and AUTHENTICATED_FILTER SFP] to restrict the ability to *delete* and [create and apply] the security attributes [information flow rules described in FDP_IFF.1 (1) and FDP_IFF.1 (2)] to [the authorized administrator].

100 **FMT_MSA.1 (5) Management of security attribute (5)**

FMT_MSA.1.1 (5) The TSF shall enforce the [UNAUTHENTICATED_PROXY SFP] to restrict the ability to *delete,* [create and apply] the security attributes [information flow rules described in FDP_IFF.1 (3)] to [the authorized administrator].

101 **FMT_MSA.1 (6) Management of security attribute (6)**

FMT_MSA.1.1 (6) The TSF shall enforce the [AUTHENTICATED SFP] to restrict the ability to *delete,* [create and apply] the security attributes [information flow rules described in FDP_IFF.1 (4)] to [the authorized administrator].

102 **FMT_MTD.1 (1) Management of TSF data (1)**

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

103 **FMT_MOF.1 (1) Management security function behavior (1)**

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

a) Enable and disable start-up and shutdown;
b) 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);
c) Multiple use authentication as described in FIA_UAU.5]
d) 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);
e) 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); to [an authorized administrator].

104 **FMT_MOF.1 (2) Management security function 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) Object attributes used for all Security Functions
c) Backup and restore for TSF data, information flow rules, audit trail data; and the Administrator assigned file or directory.
d) Alarm rules of security events
e) Integrity system file check rule and time
f) Communication of authorized external IT entities with the TOE
g) TOE system applied TCP session timeout and UDP reply timeout
h) NTP server IP and System Time
i) NAT Policy Rule
j) Consecutive authentication failure option
k) Configure the administrator's accessibility – Log, User, Policy] to [the authorized administrator].

105 **FIA_UAU.1 Time of authentication**

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

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

106 **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 End Users to access the TOE for authentication remotely such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that authorized human users.

b) Single-use authentication mechanism shall be used for authorized End Users sending or receiving information through the TOE using FTP or SMTP or NNTP or HTTP that is capable of authentication such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that End User.

c) 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].

d) Reusable password mechanism shall be used for authorized End Users to access the TOE for authentication remotely such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that authorized End Users.- password method for End User authentication.

e) Reusable password mechanism shall be used for authorized End Users sending or receiving information through the TOE using FTP or SMTP or HTTP or NNTP that is capable of authentication such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that End User.

f) No End User authentication method shall be used for users sending or receiving information through the TOE remotely through Packet Filtering level, if the Packet Filtering Security Policy rule being used does not specify a End User authentication method.

Application note: No End User authentication method is used for users sending or receiving information through the TOE, if no users are allocated to a security policy rule.

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. The SECUREWORKS 3.0's remote administration is an out of scope feature. However, the End Users' remote authentication is a target of evaluation feature because the End Users access the TOE to get authentication. Those above authentication mechanisms are used.

107 **FMT_MSA.3 Static attribute initialization**

FMT_MSA.3.1 The TSF shall enforce the [UNAUTHENTICATED SFP, AUTHENTICATED_FILTER SFP, UNAUTHENTICATED_PROXY 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 on object or information is created.

Application Notes: The default value is intended to be restrictive in the sense that both inbound and outbound information is denied after the SECUREWORKS is installed. Also, only user object has a function to change the default value. To obtain more information about User Object, please refer the Security Management in section 6.1.1.

108 **FCS_COP.1 Cryptographic operation**

FCS_COP.1.1 The TSF shall perform [hashing] in accordance with a specified cryptographic algorithm [SHA-1 and MD5] and cryptographic key sizes [160 bit] that meet the following: [FIPS PUB 180-1 and ISO].

Application Notes: This component FCS_COP.1 does not comply exactly as the claimed PP is stated originally. According to the claimed PP, it chose this component for remote administration. However, this ST chose this component as a part of SFR for both SHA-1 and MD5 as hashing algorithms.

5.1.1.4 Additions to PP SFRs

109 An additional SFR from CC Part 2 is identified for the TOE. [Table 5-5] identifies the SFR added to the ST.

[Table 5-5] Additional CC part 2 Functional Component for TOE

Reference	Description
FAU_GEN.2	User identity association
FAU_SAA.1	Potential violation analysis
FAU_ARP.1	Security alarm
FPR_PSE.1 (1)	Pseudonym (Dynamic)(1)
FPR_PSE.1 (2)	Pseudonym (Static)(2)
FPT_TST.1	TSF Testing
FAU_SEL.1	Selective audit
FMT_SMF.1	Specification of Management Functions
FPT_AMT.1	Abstract machine testing

110 **FAU_GEN.2 User identity association**

FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

111 **FAU_SAA.1 Potential violation analysis**

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [port scanning audit events] known to indicate a potential security violation

b) [None]

112 **FAU_ARP.1 Security alarm**

FAU_ARP.1.1 The TSF shall take [one or more of the following activities as specified by an authorized administrator:

a) Optionally produce an alarm for the following types of intrusion attempts:
   A. Source Route
   B. IP Spoof
   C. Land
   D. UDP Echo Loop
   E. Finger Print Scan
   F. Port Scan

b) Produce an alarm for other events based on type, service, destination address, source address and user ID as selected by an Authorized Administrator.]

upon detection of a potential security violation

113 **FPR_PSE.1 (1) Pseudonym (Dynamic)(1)**

FPR_PSE.1.1 (1) (Dynamic) The TSF shall ensure that [external IT entities on the external network] are unable to determine the real **IP address** bound to [external IT entities on the internal network that generate connections to external IT entities on the external network].

FPR_PSE.1.2 (1) The TSF shall be able to provide [50000] aliases of the **real IP address** to [external IT entities on the internal network].

FPR_PSE.1.3 (1) The TSF shall *determine an alias for an external IT entity on the internal network* and verify that it conforms to the [Normal NAT port randomness algorithm].

114 **FPR_PSE.1 (2) Pseudonym (Static)(2)**

FPR_PSE.1.1 (2) The TSF shall ensure that [external IT entities on the external network] are unable to determine the real **IP address** bound to [external IT entities on the internal network].

FPR_PSE.1.2 (2) The TSF shall be able to provide [255] aliases of the real **IP address** to [external IT entities on the internal network].

FPR_PSE.1.3 (2) The TSF shall *determine an alias for an external IT entity on the internal network* and verify that it conforms to the [Reverse NAT rule specified by the authorized administrator].

115 **FPT_TST.1 TSF Testing**

FPT_TST.1.1 The TSF shall run a suite of self tests [*during initial start-up, periodically during normal operation*] to demonstrate the correct operation of the TSF.

FPT_TST.1.2 The TSF shall provide **the authorized administrator** with the capability to verify the integrity of TSF data.

FPT_TST.1.3 The TSF shall provide **the authorized administrator** with the capability to verify the integrity of stored TSF executable code.

116 **FAU_SEL.1 Selective audit**

FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

a) *Event type*
b) [Service and protocol].

117 **FMT_SMF.1 Specification of Management Functions**

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [

a) Operation of the TOE;
b) Multiple use authentication as described in FIA_UAU.5]
c) Each Information flow rule]
d) Audit trail management;
e) Object attributes used for all Security Functions
f) Backup and restore for TSF data, information flow rules, audit trail data; and the Administrator assigned file or directory.
g) Alarm rules of security events
h) Integrity system file check rule and time
i) Communication of authorized external IT entities with the TOE
j) TOE system applied TCP session timeout and UDP reply timeout
k) NTP server IP and System Time
l) NAT Policy Rule
m) Consecutive authentication failure option]
n) Request kill current session
o) Configure the administrator's accessibility – Log, User, Policy

118 **FPT_AMT.1 Abstract machine testing**

FPT_AMT.1.1 The TSF shall run a suite of tests [selection: during initial start-up, periodically during normal operation, at the request of an authorised user] to demonstrate the correct operation of the security assumptions provided by the abstract

machine that underlies the TSF.

5.1.1.5 SFRs With SOF Declarations

119 The FIA_UAU.1 SFR requires that the TOE have an authentication mechanism that has a probability of authentication data being guessed will be less than on in a million.

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

121 The overall Strength of function claim for the TOE is SOF-basic.

5.1.2 TOE Security Assurance Requirements

122 [Table 5-6] identifies the security assurance components drawn from CC part 3: Security Assurance Requirements, EAL.3.

[Table 5-6] EAL3 Assurance Requirements

Assurance Class	Assurance Component ID	Assurance Component Name
Configuration Management	ACM_CAP.3	Authorization controls
	ACM_SCP.1	TOE CM coverage
Delivery and operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation, and start-up procedures
Development	ADV_FSP.1	Information functional specification
	ADV_HLD.2	Security enforcing high-level design
	ADV_RCR.1	Informal correspondence demonstration
Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Life-cycle support activity	ALC_DVS.1	Identification of security measures
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: high-level design

	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability assessment	AVA_MSU.1	Examination of guidance
	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

123 **ACM_CAP.3 Authorizations controls**

Developer action elements:
ACM_CAP.3.1D The developer shall provide a reference for the TOE.
ACM_CAP.3.2D The developer shall use a CM system.
ACM_CAP.3.3D The developer shall provide CM documentation.

Content and presentation of evidence elements:
ACM_CAP.3.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.3.2C The TOE shall be labeled with its reference.

ACM_CAP.3.3C The CM documentation shall include a configuration list and a CM plan.

ACM_CAP.3.4C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.3.5C The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.3.6C The CM system shall uniquely identify all configuration items.

ACM_CAP.3.7C The CM plan shall describe how the CM system is used.

ACM_CAP.3.8C The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.

ACM_CAP.3.9C The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

ACM_CAP.3.10C The CM system shall provide measures such that only authorized changes are made to the configuration items.

Evaluator action elements:
ACM_CAP.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

124 **ACM_SCP.1 TOE CM coverage**

Developer action elements:
ACM_SCP.1.1D The developer shall provide CM documentation.

Content and presentation of evidence elements:
ACM_SCP.1.1C The CM documentation shall show that the CM system, as a minimum, tracks the following: the TOE implementation representation, design documentation, test documentation, user documentation, administrator documentation, and CM documentation.

ACM_SCP.1.2C The CM documentation shall describe how configuration items are tracked by the CM system.

Evaluator action elements:
ACM_SCP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

125 **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.

126 **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 functional requirements.

127 **ADV_HLD.2 Security enforcing high-level design**

Developer action elements:
ADV_HLD.2.1D The developer shall provide the high-level design of the TSF.

Content and presentation of evidence elements:
ADV_HLD.2.1C The presentation of the high-level design shall be informal.

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

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

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

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

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

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

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

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

Evaluator action elements:
ADV_HLD.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

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

128 **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 meets all requirements for content and presentation of evidence.

129 **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:
ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C T he 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.

130 **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.

131 **ALC_DVS.1 Identification of security measures**

Developer action elements:
ALC_DVS.1.1D The developer shall produce development security documentation.

Content and presentation of evidence elements:
ALC_DVS.1.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

ALC_DVS.1.2C The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

Evaluator action elements:
ALC_DVS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DVS.1.2E The evaluator shall confirm that the security measures are being applied.

132 **ATE_COV.2 Analysis of coverage**

Developer action elements:
ATE_COV.2.1D The developer shall provide an analysis of the test coverage.

Content and presentation of evidence elements:
ATE_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

ATE_COV.2.2C The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.

Evaluator action elements:
ATE_COV.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

133 **ATE_DPT.1 Testing: high-level design**

Developer action elements:
ATE_DPT.1.1D The developer shall provide the analysis of the depth of testing.

Content and presentation of evidence elements:
ATE_DPT.1.1C The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.

Evaluator action elements:
ATE_DPT.1.2E T he evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

134 **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.

135 **ATE_IND.2 Independent testing - sample**

Developer action elements:
ATE_IND.2.1D The developer shall provide the TOE for testing.

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.

136 **AVA_MSU.1 Examination of guidance**

Developer action elements:
AVA_MSU.1.1D The developer shall provide guidance documentation.

Content and presentation of evidence elements:
AVA_MSU.1.1C The guidance documentation 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.

AVA_MSU.1.2C The guidance documentation shall be complete, clear, consistent and reasonable.

AVA_MSU.1.3C The guidance documentation shall list all assumptions about the intended environment.

AVA_MSU.1.4C The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

Evaluator action elements:
AVA_MSU.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_MSU.1.2E The evaluator shall repeat all configuration and installation procedures to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.

AVA_MSU.1.3E The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

137 **AVA_SOF.1 Strength of TOE security function evaluation**

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.

138 **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.1.1E 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.

5.2 Security Requirements for the IT Environment

139 The TOE has no security requirements allocated to its IT environment

6. TOE Summary Specification

140 This Chapter presents a functional overview of the TOE; the security functions implemented by the TOE; and the Assurance Measures applied to ensure their correct implementation.

6.1 TOE Security Functions

141 This section presents the security functions performed by the TOE.

6.1.1 Security Management (SW_ADMIN)

142 The TOE authorized administrator uses a web browser to access the TOE. Remote administration is not permitted for the TOE and the browser must be running on the same host as the TOE.

143 Each authorized administrator has an individual ID. After the successful login to the Administration Server, the administrator has the authority to manage only given aspects of the TOE.

144 The following administrative functions can be performed once an authorized administrator has been successfully authenticated by the TOE:

- Create, delete, view and modify the information flow security policy rule (Packet Filtering Policy Rule, NAT Policy Rule and Application Gateway Policy Rule) of the TOE.
- Enable and disable the information flow security policy rule (Packet Filtering Policy Rule, NAT Policy Rule and Application Gateway Policy Rule) of the TOE
- Create, delete, view and modify Object (User, Network Group, Service-Port, Time range).
- Query, modify and delete a user's attributes- can query by user ID.
- Setup the authentication method for End Users and the Administrator– One Time Password (OTP) method, Normal password method, none.
- Create, delete, view and modify the Backup Policy Rule for Audit Record and Backup Audit Record.
- Backup and restore the TOE configuration data.
- Create, delete, view, and modify Alarm Rule for security related event
- Create, delete and view integrity verification file or directory.
- Set auto-check schedule, daily integrity check, and file permission(SETUID, SETGID, all write, group write) options for system integrity.

- Change user account status
- Adjust TOE's system time to a NTP server's time.
- Set TOE's system time by the administrator without using a NTP server's time information.
- Startup & shut down of the TOE through the TOE console by running command.

145 Default values for the TOE are such that all information flow (inbound and outbound) is denied. SECUREWORKS provide a method to setup a default value of End User profile attribute to override an initial default value.

146 To simplify management of large system the Administrator can define objects for User Groups, Network Group, Services, and Time. Once an object is defined, it can be used to create and manage information flow security policy rules.

147 Objects available for use within the TOE consist of:

- User Group is used for an authentication and it is composed of a number of users.
- Network Group object is composed of source or destination address and can be grouped by a host unit or IP class unit.
- Service object is composed of protocol and port number, and can be grouped by multiple ports.
- Time Object is used to apply Security Policy Rule by time, day in week and date.

Functional Requirements Satisfied: FMT_MOF.1 (1), FMT_MOF.1 (2), FMT_MSA.1 (1), FMT_MSA.1 (2), FMT_MSA.1 (3), FMT_MSA.1 (4), FMT_MSA.1 (5), FMT_MSA.1 (6), FMT_MSA.3, FMT_MTD.2, FMT_SMR.1, FMT_MTD.1 (1), FMT_MTD.1 (2), FMT_SMF.1, FDP_IFF.1.4 (1), FIA_SEL.1, FIA_ATD.1, FDP_IFF.1.4(1), FAU_SEL.1 and FIA_ATD.1

6.1.2 Audit (SW_AUDIT)

148 The Audit Security functional requirements are composed of Audit Record generation, audit review, selectable audit review, protected audit trail storage, and prevention of Audit Record loss.

6.1.2.1 Audit data generation

149 Audit generation can be enabled or disabled by each information flow security policy rule (UNAUTHENTICATED SFP and ATHENTCATED_SFP). Audit Record is generated for any connection of the corresponding rule.

150 The following items are recorded in the Audit Record. See, [Table 5-4]

- sequence number
- The date and time of the event;
- Subject identity (source and destination IP);
- Type of event (ERROR, WARNING, NOTICE, ACCOUNT);
- Outcome (success or failure) of the event;
- Human user ID and protocol;
- Details about corresponding information flow (allow or deny, packet data size and error messages, etc);
- Enabling an d disabling of any of the analysis mechanisms
- Actions taken due to imminent security violations
- Reading of information from the audit record
- All modification to the audit configuration that occur while the audit collection function are operating
- Actions taken due to the audit storage failure
- All decision to permit requested information flow
- The reaching of the threshold for the unsuccessful authentication attempts and actions(e.g. disabling of a terminal) taken and the subsequent, of appropriate, restoration to the normal state(e.g. re-enabling of a terminal)
- All use of the authentication mechanism
- Attempts to reuse authentication data
- The result of each activated mechanism together with the final decision.
- All use of the user identification mechanism, including the user identity provided.
- All modifications in the behavior of the functions in the TSF.
- All modifications of the values of security attributes
- All modifications of the initial values of security attributes
- All modifications to the values of TSF data.
- All modifications in the actions to be taken in case of violation of the limits
- Modification to the group of users that are part of a role
- The subject/user that requested resolution of the user identity should be audited.
- Execution of the tests of the underlying machine and the results of the tests
- Change to the time
- Execution of the TSF self tests and the result of the tests

151 When an End User is authenticated or uses an Application Gateway through SECUREWORKS, the SECUREWORKS logs corresponding Audit Record with user ID. Therefore, the logged Audit Record enables SECUREWORKS to trace back who conducted this particular action.

152 The following events all generate Audit Records:

- Startup and Shutdown of the TOE
- Starting and stopping all daemon process (i.e. Log Server, Administration Server)

- Create, delete, and modify information flow security policy rules that permit or deny information flows
- Create, delete, and modify user attributes
- Event occurring against pre-defined alarm rule.
- Setup or check an integrity verification file.
- Action against End User authentication success or failure.
- Action against Administrator authentication success of failure.

153 When there exists the violation of the alarm rule that the administrator preset the TOE can inform the administrator by E-mail, scripts.

154 The TOE can generate and log the Audit Record based on the administrator selected options. The options are log type, service and protocols.

155 Functional Requirements Satisfied: FAU_GEN.1, FAU_GEN.2, FAU_ARP.1, FAU_SAA.1, FAU_SEL.1,FPT_STM.1, FAU_SAR.3

6.1.2.2 Audit review

156 The TOE permits an authorized administrator to view, search and monitor the audit record on all required parameters for all records.

157 The view function enables the display of audit data by event type, specific date or time.

158 Authorized administrators can search the saved Audit Record from the TOE with following conditions.

- Date and time
- Event type
- User
- Service
- Source
- Destination
- System
- Keyword

159 Authorized administrator can review the statistic report by sorting saved Audit Record from the TOE with following conditions.

- Packet information by date and time (Last 1 week and last 1 month summary) as follows:
  - Total number of packets, allowed packets and denied packets
  - Data size
- And its ratio

- Number of sessions, packets, and data size for each services (Application Gateway)
- Source and destination address sorted by:
  - Number of sessions
  - Number of packets
  - Size of data
- Number of sessions and data size by Users
- Event type, audit generated service and corresponding log's actual example by its occurring frequency

160 Search result can be saved in a file.

161 Authorized administrator can view the Audit Record in real time. To view the real time Audit Record, the following conditions must be defined. When there exist Audit Records that meet the conditions, the result will be displayed on the administrator GUI.

- Event Type
- User ID
- Service
- Source and Destination IP Address
- System Name: TOE name
- Keyword

162 Functional Requirements Satisfied: FAU_SAR.1, FAU_SAR.3

6.1.2.3 Audit Record Storage

163 Only authorized administrators are permitted to login to the firewall host and, subsequently, access the Audit Record files.

164 Audit data loss when the audit trail is full is prevented through the following mechanism. When the available space of the system is below 5%(default), an administrator will receive the alarm. Furthermore, when the available space of the system is below 3%(default), all services that go through the TOE will stop all service.

165 Unauthorized users can not delete or modify a TOE's audit record files, because only 'swadmin' account can execute security functions of the TOE. The 'swadmin' account is created when the TOE is installed initially. As an example, it is a relevant case when the TOE stores an audit record or backups audit records. Since the 'swadmin' is only owner of the audit records and TOE's security function, unauthorized users can not compromise the audit records or execute any security functions in any ways. The Audit Record file' file system permission is following: (owner 'swadmin' has read/write permission, group 'swadmin' has read only permission, and other has no permission.) Moreover when a TOE is installed for the first time, the TOE prohibits any access from external network by running

'inetd' daemon. The 'inetd' daemon kills and disables all remote connection services such as FTP, TELNET, and etc... Therefore, only authorized administrator can view, delete or modify audit records. Management of audit records is a TSF because only authorized administrators can access the security management screen to set the options for 'Obsolete Data Management' (ie. clean logs, clean statistics, and clean sessions by deletion/compression).).

166 Functional Requirements Satisfied: FAU_STG..1, FAU_STG.4, FAU_ARP.1

6.1.3 Information Flow Control (SW_IFC)

167 TOE provides security through the following mechanisms: Packet filtering, application proxies, and network address translation (NAT). TOE ensures that previous packet data is unavailable for the next packet being processed. For each packet received by the Kernel Driver, the information flow policy rules are always applied and enforced.

168 Information flow control within the TOE is conducted in two distinct stages. All packets entering the TOE are first subjected to the Packet Filtering Security Policy rule. Packets that are permitted by this policy are passed to the Application Gateway proxy filters for further filtering.

6.1.3.1 Packet Filtering

169 Packet filtering Information flow control uses attributes associated with packets received by the TOE to determine if that packet should be allowed or denied passage through the TOE. Information used to determine access includes the source of the packet, the destination, the protocol used, the port number, and other similar information.

170 The default rule for all data flow is deny all. Authorized administrators can create rules in the Packet Filter Security Policy Rule to define what packet may and may not pass through the TOE. Packets that pass the rules in this policy are passed to the Application Gateway security policy rules for further filtering.

171 The TOE Packet Filter determines whether to allow or deny the packet based on the following attributes defined in the Packet Filter Security Policy rules.

- Source IP Address;
- Destination IP Address;
- Service: Protocol and port;
- Network Interface Card where the request came from.
- Time Object
- User object when an authentication is used.
- Action (deny, allow)

172 The packet filtering security policy rule includes an implicit rule permitting response packets as part of an existing TCP session that has been established in accordance with the policy.

173 The packet filter includes rules to explicitly deny access under the following circumstances:

174 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.

175 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.

176 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;

177 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 loop-back network;

178 IP source route - The TOE shall reject requests in which the subject specifies the route in which information shall flow en route to the receiving subject; and

179 For application protocols supported by the TOE 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.

180 Land attack –The TOE shall detect and deny requests if the source IP address is same as the destination IP address.

181 Finger print scan – The TOE shall detect and deny packets if any unused flag values are set in the TCP header flag.

182 In order to block the packets with source IP option that goes through a firewall, administration server creates the rule to deny the packet and transfer it to the Kernel Driver.

183 The data storage used for all packets that pass through Kernel Driver is erased before that storage is reused.

184 Functional Requirements Satisfied: FDP_IFC.1 (1) FDP_IFF.1 (1), FDP_RIP.1, FMT_MSA.1 (4), FMT_MOF.1 (2), FDP_IFF.1.4(1), FDP_IFF.1.2(1), FDP_IFF.1.6(1) FAU_ARP.1, FAU_SAA.1, FPT_RMV.1, FPT_SEP.1, FAU_APR.1, FAU_SAA.1

6.1.3.2 Application Gateway

185 The Application Gateway employs proxies to screen information flows based upon rules regarding the packet content. Only valid requests are relayed to the actual server by the proxy server on either an internal or external network. End User can use the functions of the application gateway without any specific setup.

186 The SECUREWORKS proxies, HTTP, SMTP, FTP, and NNTP Application Gateway can be setup to require End User authentication. Also, the number of users to access the gateway concurrently can be limited. After completion of the detailed setup for Application Gateway, user group, source/destination, and network group information is used to configure the Application Gateway Security Policy rule.

187 The HTTP gateway can allow or deny the access by the destination address (URL) or keyword in the address. Also, when a specific address is accessed, it can be redirected to a predefined site.

188 The SMTP gateway can filter all mails through the gateway and make a copy of each mail. Integrity can be provided for the copied mail. The SMTP gateway also can filter specific keywords in the filename, content, subject or all.

189 The FTP gateway can control the exploitable FTP commands. Optionally all transferred file can be saved. Integrity can be provided for the saved file.

190 For authenticated services the TOE Application Gateway Filter determines whether to allow or deny the packet based upon the following attributes defined in the Application Gateway Security Policy rules.

- User identity
- Presumed address of source subject;
- Presumed address of destination subject;
- Transport layer protocol;
- TOE interface on which traffic arrives and departs;
- Services (FTP, HTTP, SMTP, and NNTP);
- Security-relevant service command; and
- Timeout value
- Maximum connect

191 For unauthenticated services the TOE Application Gateway Filter determines whether to allow or deny the packet based upon the following attributes defined in the Application Gateway Security Policy rules.

- Presumed address of source subject;
- Presumed address of destination subject;
- Transport layer protocol;
- TOE interface on which traffic arrives and departs
- Services (POP3, Telnet, RLOGIN, IMAP4 and H.323)
- Timeout value(except for H.323)
- Maximum connect (except for H.323)

192 Functional Requirements Satisfied: FDP_RIP.1, FDP_IFC.1 (2), FDP_IFC.1 (3), FDP_IFF.1 (2), FDP_IFF.1 (3), FMT_MSA.1(3), FMT_MSA.1(5), FMT_MOF.1 (2)

6.1.3.3 Network Address Translation (NAT)

193 In order to conceal details of the internal network, the internal IP address can be aliased. When NAT is used, only the TOE's external address is exposed to the public. The TSF implements two types of NAT:

194 Normal NAT is used when internal hosts access the external network (Dynamic).

195 Reverse NAT is used when the public hosts access the hidden internal network (Static).

196 In Normal NAT, the TOE translates the source address of the internal host into the external address of TOE. When receiving the response, TOE look up the NAT table and forward the packets to the corresponding internal host.

197 In Reverse NAT, when the external host accesses a hidden internal host (resources), TOE responds instead and forwards the requests to the corresponding internal host.

198 When there is no action during a time period that the administrator assigned (system time-out value), TOE will terminate all NAT sessions.

199 Functional Requirements Satisfied: FPR_PSE.1 (1), FPR_PSE.1 (2)

6.1.4 Identification and Authentication (SW_I&A)

200 TOE has two authentication methods for both End User Users and authorized administrators. They are SECUREWORKS password method that uses ID/Password and single-use authentication method (OTP). 35,000 users can be registered and managed. Also, accessible time (day in week and date) of each normal user can be controlled.

201 End User authentication can be executed at either the Packet Filter level (AUTHENTICATED_FILTER SPF) or at the Application Gateway (AUTHENTICATED_SFP) for each user.

202 End User authentication function (AUTHENTICATED_FILTER SFP) enables End User authentication method for all services. Telnet or a web interface is used to perform this End User authentication.

203 SECUREWORKS One Time Password (S/KEY) method works as follows. To use the OTP method a user enters their user id in the same way as for normal password. In the case of OTP the TOE responds with a challenge value that consists of an algorithm ID, sequence number and seed value. None of these factors is confidential, only the sequence number changes between successive, successful log in attempts (it decrements by one each time). The user enters these values into the OTP generator that then produces a response value. This response value is then entered instead of the password. The OTP generator is a shareware product and is not required to retain any information between login attempts.

204 The authentication failure handling mechanism can be configured to lock out the individual users that have been installed within the user database. The users are locked or delayed individually when a specified number of unsuccessful authentication attempts have been reached. Default value is 5 times. If an individual user's account is locked due to the exceed of unsuccessful authentication attempts, the user's account will be locked until an administrator unlocks it.

205 The Authentication module allows the administrator to set an authentication policy, which is enforced for the administration accounts on the TOE. Neither all numbered password nor all alphabetic charactered password is allowed for administrator's password. The authentication policy required to meet the assurance requirements of AVA_SOF.1 is described below:

206 The Normal (SECUREWORKS) Password Authentication mechanism used by the TOE to authenticate general users has the following characteristics. Neither all numbered password nor all alphabetic charactered password is allowed for user's password.

a) The pass space must be at least seven and no greater than eight digits long;
b) The possible characters are a-z(26), A-Z(26), 0–9(10) and Special characters ~ ! @ # $ % ^ * ( ) _ + | ` - = \ { } : ” < > ? [ ] ; ’ , . / (31) except for & - Total: 93

207 The One Time Password Authentication (S/KEY) mechanism used by the TOE to authenticate general users has the following characteristics,

a) The password must be at least seven and no greater than eight digits long;
b) The password can consist of the characters a-z(26), A-Z(26), 0–9(10) and Special characters ~ ! @ # $ % ^ * ( ) _ + | ` - = \ { } : ” < > ? [ ] ; ’ , . / (31) except for & - Total: 93

c) Hash algorithm used is MD5 which is provided by openSSL.

208 Note that the OTP seed values are developed by the random number generator which complies with the “Continuous random number tests” and “Statistical random number generator tests” found in section 4.11.1 of FIPS PUB 140-1.

209 User cannot initiate their own change of passwords. However users can change their passwords only if password changes are forced either at the expiry of the password change cycle or when the OTP sequence number reaches 1. When an administrator successfully log into the security management screen, the administrator can change his/her own password.

210 Functional Requirements Satisfied: FIA_UID.2, FIA_AFL.1, FIA_ATD.1, FIA_UAU.5, FIA_UAU.1, FIA_UAU.4, FCS_COP.1, FMT_MTD.2, FMT_MOF.1(2)

6.1.5 Protection of Security Function (SW_PSF)

211 Protection of Security Functions requirements are composed of non-bypassability of the TSP, TSF domain separation, TSF Testing.

212 The TOE undertakes TSF testing in two ways. Firstly, the Administration Server constantly checks the status of other firewall daemons. If an expected daemon is not running, the server invokes the appropriate daemon. After Installation, Generation, and Startup are completed, SECUREWORKS will always be invoked on subsequent system startups. Secondly, Integrity checking is undertaken for a number of critical TOE and system files. The administrator can add additional files to the integrity checking list.

213 By default, the TOE performs integrity verification process to check integrity of TOE related configuration files, library file, and exe files. Integrity verification process can be performed in two different ways: ① When initiated by the administrator . ②On the day at the time that is scheduled by an administrator.

214 And also the administrator can add/remove a target file or directory to/from the list of integrity verification. By doing so, the administrator can verify more file or directory’s integrity whether it is violated or not.

215 In order to perform integrity verification process, TOE creates a hash value from a target file or directory and then saves it. When TOE creates a hash value, it uses the openSSL’s library SHA-1 algorithm. The created hash value is stored in the TOE’s configuration file. This saved hash value will be used to verify the file’s integrity by comparing it with target’s newly generated hash value. If they are matched together, then it is considered as a integrity kept file therefore it continues its TSF. If they are not matched together, then it is considered as a integrity violated file therefore it alarms this error to the administrator.

216 Domain separation is achieved by ensuring that all network access to the TOE host goes through the TOE. This means that all network traffic is subject to the Information flow policies as described in this Security Target. This function is enforced through the TOE intercepting at the Network layer in the protocol stack, all data entering the TOE host via a Network Interface Card (NIC). This ensures no data can bypass the TOE and the TOE information flow policies can be used to protect its own execution domain.

217 After Installation, Generation, and Startup are completed, the configuration is saved to non-volatile memory and will be invoked on subsequent system startup

218 When the TOE audits an event, it records its audit information with its occurrence time. Since the TOE adjusts its system time to the trustable NTP server's time(U.S. Naval Observatory 192.5.41.209 & Korea KRISS 203.254.163.74), TOE will always keep its system time correct.

219 Functional Requirements Satisfied: FPT_TST.1, FTP_AMT.1, FPT_SEP.1, FPT_RVM.1, FPT_STM.1,FCS_COP.1

6.2 Assurance Measures

220 The TOE claims to satisfy the CC EAL 3 assurance requirements. TOE has assurance measures for the TOE to satisfy the stated SARs. [Table 6-1] shows which assurance measures are traced to the assurance requirements identified in Section 5.1.2:

[Table 6-1] Traced Assurance Measures

Assurance Component ID	Assurance Component Name	Assurance Measure
ACM_CAP.3	Authorization controls	Configuration Management Plan For SECUREWORKS V3.0 Version 1.26, and CI LIST for CC Version 1.1
ACM_SCP.1	TOE CM coverage	Configuration Management Plan, Configuration List Verion 1.26
ADO_DEL.1	Delivery procedures	Delivery Documentation for SECUREWORKS V3.0 Version 1.9
ADO_IGS.1	Installation, generation, and start-up	Installation guidance

	procedures	Revision 4, Dec 2002
ADV_FSP.1	Information functional specification	Function Specification for SECUREWORKS V3.0 Version 1.18
ADV_HLD.2	Security enforcing high-level design	High-level Design for SECUREWORKS V3.0 Version 1.18
ADV_RCR.1	Informal correspondence demonstration	Analysis of Correspondence (FS, HLD)
AGD_ADM.1	Administrator guidance	Administrator guidance Revision 4, DEC 2002
AGD_USR.1	User guidance	User guidance Revision 4, Dec 2002
ALC_DVS.1	Identification of security measures	Development Security for SECUREWORKS V3.0 Version 1.11
ATE_COV.2	Analysis of coverage	Test Documentation for SECUREWORKS v3.0 Version 1.7
ATE_DPT.1	Testing: high-level design	Test Documentation for SECUREWORKS v3.0 Version 1.7
ATE_FUN.1	Functional testing	Test Documentation for SECUREWORKS v3.0 Version 1.7
ATE_IND.2	Independent testing – sample	N/A (Evaluator action)
AVA_MSU.1	Examination of guidance	Administrator guidance Revision 4, DEC 2002
AVA_SOF.1	Strength of TOE security function evaluation	Strength of Function Analysis for SECUREWORKS V3.0 Version 1.11
AVA_VLA.1	Developer vulnerability analysis	Vulnerability Analysis for SECUREWORKS V3.0 Version 1.9

7 PP CLAIMS

221 This section provides the PP conformance claim statements.

7.1 PP Claim – Application Level Firewall

7.1.1 PP Reference

222 The TOE conforms to the following PP

- The U.S. Department of Defense Application-level Firewall Protection Profile for Basic Robustness Environments, Version 1.0., June 22,2000 [ALFPP]

7.1.2 PP Refinements and Additions

7.1.2.1 PP Security Function Requirements

223 The following PP SFRs were further refined for this Security Target.

[Table 7-1] Security Functional Requirements

Functional Component	Functional Component Name	Status/Operation
FAU_GEN.1	Audit data generation	Refinement
FDP_IFC.1(2)	Subset information flow control(2)	Assignment
FDP_IFC.1(3)	Subset information flow control(3)	Assignment
FDP_IFC.1(4)	Subset information flow control(4)	Assignment
FDP_IFF.1(1)	Simple security attributes(1)	Assignment
FDP_IFF.1(2)	Simple security attributes(2)	Assignment
FDP_IFF.1(3)	Simple security attributes(3)	Assignment
FDP_IFF.1(4)	Simple security attributes(4)	Assignment
FIA_AFL.1	Authentication failure handling	Assignment
FIA_ATD.1	User attribute definition(1)	Assignment Select

FMT_MSA.1(1)	Management of security attribute(1)	Iteration
FMT_MSA.1(2)	Management of security attribute(2)	Iteration
FMT_MSA.1(3)	Management of security attribute(3)	Iteration
FMT_MSA.1(4)	Management of security attribute(4)	Iteration
FMT_MSA.1(5)	Management of security attribute(5)	Iteration
FMT_MSA.1(6)	Management of security attribute(6)	Iteration
FMT_MTD.1(1)	Management of TSF data(1)	Assignment Select
FMT_MOF.1 (1)	Management security function behavior (1)	Assignment
FMT_MOF.1 (2)	Management security function behavior (2)	Assignment
FIA_UAU.5	Multiple authentication mechanisms	Assignment
FMT_MSA.3	Static attribute initialization	Refinement
FCS_COP.1	Cryptographic operation	Assignment

224 In the case of FDP_IFC.1 and FDP_IFF.1, three (3) iterations were required to adequately address the enhanced features of the TOE. The three iterations were chosen on the following basis:

225 UNAUTHENTICATED SFP (1), this SFP states the behavior of the Packet Filter functionality of the TOE.

226 UNAUTHENTICATED_PROXY SFP (2), this SPF states the behavior of the Application Gateway for those proxies for which user authentication is not required.

227 AUTHENTICATED SFP (3), this SPF states the behavior of the Application Gateway for those proxies for which user authentication is required.

228 Six (6) iterations of FMT_MSA.1 are needed to manage the security attributes identified in the three iterations of IFF and IFC.

FMT_MSA.1 (1) manages FDP_IFF.1 (1) attributes.

FMT_MSA.1 (2) manages FDP_IFF.1 (2) attributes.

FMT_MSA.1 (3) manages FDP_IFF.1 (3) attributes.

FMT_MSA.1 (4) manages FDP_IFC.1 (4) attributes.

FMT_MSA.1 (5) manages FDP_IFC.1 (5) attributes.

FMT_MSA.1 (6) manages FDP_IFC.1 (6) attributes.

The follow component is omitted from ALFPP.

FCS_COP.1	Cryptographic operation	The TOE does not include support for remote administration of the

		TOE

229 In the case of FCS_COP.1, the main purpose of this component from the claimed PP is not same as this ST's. Though the claimed PP chose this component for remote administration, this ST chose this component for hashing algorithms. However, this FCS_COP is also stated in the out of scope functions, because this ST omitted this component because the remote administration is an out of scope function

7.1.2.2 PP Security Assurance Requirements

230 The following PP SARs describe additional EAL3 requirements of the ST to the EAL2 requirements of PP.

[Table 7-2] Security Assurance Requirements

Assurance Component	Assurance Component Name
ACM_CAP.3	Authorization controls
ACM_SCP.1	TOE CM coverage
ADV_HLD.2	Security enforcing high-level design
ALC_DVS.1	Identification of security measures
ATE_COV.2	Analysis of coverage
ATE_DPT.1	Testing: high-level design
AVA_MSU.1	Examination of guidance

7.1.2.3 PP Assumptions

231 The following PP Assumptions were further modified or added for this Security Target.

[Table 7-3] Modified and added Assumptions

Assumption Name	Status
A.GENPUR	Modified Assumption
A.DIRECT	Modified Assumption
A.NOREMO	Modified Assumption
A.NOACC	Added assumption

7.1.2.4 PP Objectives

232 The following security objectives for the TOE were added in this ST:

[Table 7-4] Added Objectives for the TOE

Objectives Name	Status
O.PRIVACY	Added objectives
O.ALARM	Added objectives

233 The following security objectives for the environment were added in this ST:

[Table 7-5] Modified and added Objectives for environment

Objectives Name	Status
OE.GENPUR	Modified Objectives
OE.DIRECT	Modified Objectives
OE.NOREMOTE	Modified Objectives
OE.NOCAA	Added Objectives

7.1.3 Rationale for not implementing all PP security objectives

234 The ST does not include the following TOE and environment security objectives: O.ENCRYP, and OE.REMACC. These security objectives are relevant to secure remote administration of the TOE. As remote administration is optional in the PP and is not part of TOE. These objectives are beyond the scope of this evaluation.

7.2 PP Claim – Traffic Filter Firewall

7.2.1 PP Reference

235 The TOE conforms to the following PP:

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

7.2.2 PP Refinements and Additions

236 The ALFPP contains a superset of SFRs identified in the TFFPP. However, the refinements of similar SFRs differ between the profiles. Where the refinement is different, the SFR refinement was taken from the ALFPP. The ALFPP refinements are such that they permit both traffic filter and application level functionality. The iteration convention has been utilized for several SFRs to ensure compliance with both PPs.

237 PP claimed SFRs both ensure the compliance with ALFPP and TFFPP. However, FDP_RIP.1 claimed a functional requirement that was refined in ALFPP. The ALFPP version has been used.

238 FAU_GEN.1 and FMT_MOF.1 are significantly different in the ALFPP from the TFFPP. Although the FAU_GEN.1 was taken from the ALFPP, the requirement captures the intent of the TFFPP requirement because the same set of security functions are audited. The TFFPP FMT_MOF.1 requirement is captured in the following ALFPP requirements: FMT_MOF.1 (1) and FMT_MOF.1 (2); FMT_MSA.1 (1), (2), (3), and (4); FMT_MTD.1 (1) and (2); FMT_MTD.2. Because the ST includes these ALFPP requirements, it satisfies the TFFPP FMT_MOF.1 requirement.

8 RATIONALE

239 This section demonstrates the completeness and consistency of this ST.

8.1 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 T.SELPRO.

O.SELPRO This security objective is necessary to counter the threats: T.SELPRO, T.NOAUTH, and T.AUDFUL because it requires that the TOE protect itself from attempts to bypass, deactivate, or tamper with TOE security functions.

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

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

security functions related to audit.

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

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

O.PRIVACY This security objective is necessary to counter the threats: T.PRIVACY because the TOE denies the direct access from the external network to the internal system by translating the address of internal system.

O.ALARM This security objective is necessary to counter the threats: T.UNDETECTED because the TOE can take appropriate measures against the serious security related event by alarming administrator.

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.

[Table 8-1] Mapping of threats to security objectives

	T.NOAUTH	T. REPEAT	T.REPLAY	T.ASPOOF	T.MEDIAT	T. OLDINF	T.AUDACC	T.SELPRO	T.AUDFUL	T.PRIVACY	T.UNDETECT	T.LOWEXP
O.IDAUTH	X											
O.SINUSE		X	X									
O.MEDIAT				X	X	X						
O.SECSTA	X							X				
O.SELPRO	X							X	X			
O.AUDREC							X					
O.ACCOUN							X					
O.SECFUN	X		X						X			

O.LIMEXT	X											
O.PRIVACY										X		
O.ALARM									X		X	
O.EAL												X

8.2 Rationale For Security Objectives For The Environments

OE.PUBLIC The TOE does not host public data.

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

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

OE.PHYSEC The TOE is physically secure.

OE.GENPUR TOE only executes security relevant applications and only stores data required for its secure operation. The operating system upon which the TOE executes has been hardened to restrict general-purpose computing capabilities and storage.

OE.DIRECT Human users(End Users) within the physically secure boundary protecting the TOE may only access the TOE directly, via its console.

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

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

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

OE.NOREMO Human users(End Users) cannot access the TOE remotely from the internal or external networks

OE.NOACC Only authorized administrators may have an account on the TOE host system.

[Table 8-2] Mapping of threats to security objectives for the Environment

	T.USAGE	A.LOWEXP	A.PUBLIC	A.SINGEN	A.NOEVIL	A.PHYSEC	A.GENPUR	A.DIRECT	A.NOREMO	A.NOACC	T.AUDACC
OE.LOWEXP		X									
OE.PUBLIC			X								
OE.NOEVIL					X						
OE.SINGEN				X							
OE.NOREMO									X		
OE.PHYSEC						X					
OE.GENPUR							X				
OE.DIRECT								X			
OE.GUIDAN	X										X
OE.ADMTRA	X										X
OE.NOACC										X	

8.3 Rationale For Security Requirements

240 The security requirements are derived according to the general model presented in Part 1 of the Common Criteria. Specifically, Table [8-3] illustrates the mapping between the security requirements and the security objectives and Table [8-1] 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.

241 The rationale for the SOF is based on the minimal attack potential identified in the claimed Protection Profile. The security objectives imply the need for probabilistic or permutational security mechanisms. The metrics defined in this Security Target are acceptable (i.e., passwords) metrics to protect information in environments which process, at most, sensitive but unclassified information, or the sensitivity level of information in both the internal and external networks is equivalent.

242 **FMT_SMR.1 Security roles**

Each of the CC class FMT components in this Security Target 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.

243 **FIA_ATD.1 User attribute definition**

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

244 **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.

245 **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 were 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(TOE Security Requirements) 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.

246 **FIA_AFL.1 Authentication failure handling**

This component ensures that human users(End Users) who are not authorized administrators cannot endlessly attempt to authenticate. After some number of failures that the authorized administrator decides, that must not be zero, the user becomes unable or delay 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.

247 **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 crypto logic strength. This component traces back to and aids in meeting the following objective: O.SINUSE.

248 **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. An additional SOF metric for this requirement is defined in section 5.1.1(TOE Security Requirements) 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.

249 **FDP_IFC.1 (1) Subset information flow control (1)**

This component identifies the entities involved in the UNAUTHENTICATED SFP 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.

250 **FDP_IFC.1 (2) Subset information flow control (2)**

This component identifies the entities involved in the AUTHENTICATED_FILTER SFP information flow control SFP (i.e., Users can send/receive information only after successful authentication). This component traces back to and aids in meeting the following objective: O.MEDIAT, O.IDAUTH

251 **FDP_IFC.1 (3) Subset information flow control (3)**

This component identifies the entities involved in the UNAUTHENTICATION_PROXY SFP information flow control SFP (i.e., users of the services POP3, Telnet, RLOGIN, IMAP4, H.323 traffic sending information to other users and vice versa). This component traces back to and aids in meeting the following objective: O.MEDIAT.

252 **FDP_IFC.1 (4) Subset information flow control (4)**

This component identifies the entities involved in the AUTHENTICATION SFP information flow control SFP (i.e., users of the services FTP, HTTP, SMTP, or NNTP traffic sending information to servers and vice versa). This component traces back to and aids in meeting the following objective: O.MEDIAT.

253 **FDP_IFF.1 (1) Simple security attributes (1)**

This component identifies the attributes of the users sending and receiving the information in the UNAUTHENTICATED_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.

254 **FDP_IFF.1 (2) Simple security attributes (2)**

This component identifies the attributes of the users sending and receiving the information after successful authentication in the AUTHENTICATED_FILTER 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, O.IDAUTH

255 **FDP_IFF.1 (3) Simple security attributes (3)**

This component identifies the attributes of the users sending and receiving the information in the UNAUTHENTICATION_PROXY_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.

256 **FDP_IFF.1 (4) Simple security attributes (4)**

This component identifies the attributes of the users sending and receiving the

information in the AUTHENTICATION 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.

257 **FMT_MSA.1 (1) Management of security attributes (1)**

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

258 **FMT_MSA.1 (2) Management of security attributes (2)**

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

259 **FMT_MSA.1 (3) Management of security attributes (3)**

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

260 **FMT_MSA.1 (4) Management of security attributes (4)**

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

261 **FMT_MSA.1 (5) Management of security attributes (5)**

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

262 **FMT_MSA.1 (6) Management of security attributes (6)**

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

263 **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.

264 **FMT_MTD.1 (1) Management of TSF data (1)**

This component ensures that the TSF restrict abilities to query, modify, delete and assign certain human user(End 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

265 **FMT_MTD.1 (2) Management of TSF data (2)**

This component ensures that the TSF restrict abilities to modify and assign the administrator 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

266 **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.

267 **FDP_RIP.1 Subset residual information protection**

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

268 **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 and O.SECSTA.

269 **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.

270 **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.

271 **FAU_GEN.2 User identity association**

This component is able to associate each auditable event with the identity of the user that caused the event. This component traces back to and aids in meeting the following objectives: O.AUDREC and O.ACCOUN.

272 **FAU_SAA.1 Potential violation analysis**

This component is able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP. This component traces back to and aids in meeting the following objectives: O.ALARM.

273 **FAU_ARP.1 Security Alarm**

This component ensures that the TOE can alert in the case that a potential security violation is detected. This component traces back to and aids in meeting the following objectives: O.ALARM.

274 **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.

275 **FPR_PSE.1 (1) Pseudonym (1) – Static**

This component ensures that provide the functionality to provide network address translation such that the identity of internal IP addresses cannot be determined. This component traces back to and aids in meeting the following objectives: O.PRIVACY

276 **FPR_PSE.1 (2) Pseudonym (2) – Dynamic**

This component ensures that provide the functionality to provide network address translation such that the identity of internal IP addresses cannot be determined. This component traces back to and aids in meeting the following objectives: O.PRIVACY

277 **FPT_TST.1 TSF Testing**

This component ensures that provide the ability to test the TSF's correction operation and verify the integrity of TSF data and executing code. This component traces back to and aids in meeting the following objectives: O.SELPRO and O.SECSTRA

278 **FPT_AMT.1 Abstract machine testing**

This component ensures that provide the ability to perform testing to demonstrate the security assumptions made about the underlying abstract machine upon which the TSF relies. This component traces back to and aids in meeting the following objectives: O.SELPRO and O.SECSTRA.

279 **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.

280 **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.

281 **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 and O.SECFUN.

282 **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 may 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.

283 **FMT_SMF.1 Specification of management functions**

This component ensures that an appropriate set of management functions are available for the management of the TOE. This component traces back to and aids in meeting the following objectives: O.SECSTA and O.SECFUN.

284 **FMT_MOF.1 (1) Management of security functions behavior (1)**

This component ensures that the TSF restricts the ability to enable and disable the function that operation of the TOE and multiple use authentication to the authorized administrator. This component traces back to and aids in meeting the following objectives: O.SECSTA, O.SECFUN and O.LIMEXT.

285 **FMT_MOF.1 (2) 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 up and restore for TSF data, and communication of authorized external IT entities with the TOE to an authorized administrator. This component traces back to and aids in meeting the following objectives: O.SECSTA, O.SECFUN, O.LIMEXT.

286 **FAU_SEL.1 Selective audit**

This component was chosen to ensure that audit record is generated for the each log type, service and protocol. This component traces back to and aids in meeting the following objective: O.AUDREC

287 **FCS_COP.1 Cryptographic operation**

This component was chosen to ensure the usage of secure cryptographic algorithm while generating hash values for one time password or integrity verification. This

component traces back to and aids in meeting the following objective: O.IDAUTH, O.EAL

[Table 8-3] Mappings between TOE Security Functions and IT Security Objectives

	O.IDAUTH	O.SINUSE	O.MEDIAT	O.SECSTA	O.SELPRO	O.AUDREC	O.ACCOUN	O.SECFUN	O.PRIVACY	O.ALARM	O.LIMEXT	O.EAL
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										
FIA_UAU.5	X	X										
FDP_IFC.1 (1)			X									
FDP_IFC.1 (2)	X		X									
FDP_IFC.1 (3)			X									
FDP_IFC.1 (4)			X									
FDP_IFF.1 (1)			X									
FDP_IFF.1 (2)	X		X									
FDP_IFF.1 (3)			X									
FDP_IFF.1 (4)			X									
FMT_MSA.1 (1)			X	X				X				
FMT_MSA.1 (2)			X	X				X				
FMT_MSA.1 (3)			X	X				X				
FMT_MSA.1 (4)			X	X				X				
FMT_MSA.1 (5)			X	X				X				
FMT_MSA.1 (6)			X	X				X				
FMT_MSA.3			X	X								
FMT_MTD.1 (1)								X				
FMT_MTD.1 (2)								X				
FMT_MTD.2								X				
FDP_RIP.1			X									

FPT_RVM.1				X	X							
FPT_SEP.1					X							
FAU_GEN.1						X	X					
FAU_GEN.2						X	X					
FAU_SAA.1										X		
FAU_ARP.1										X		
FPR_PSE.1 (1)									X			
FPR_PSE.1 (2)									X			
FPT_TST.1				X	X							
FPT_AMT.1				X	X							
FAU.SAR1						X						
FAU_SAR.3						X						
FAU_STG.1					X			X				
FAU_STG.4				X	X			X				
FMT_SMF.1				X				X				
FMT_MOF.1 (1)				X				X				
FMT_MOF.1 (2)				X				X			X	
FAU_SEL.1						X					X	
FPT_STM.1							X					
FCS_COP.1	X											X

8.4 Rationale For Assurance Requirement

288 EAL3 was chosen to provide a moderate level of independently assured security. The chosen assurance level is consistent with the postulated threat environment. Specifically, that the threat of malicious attacks is not greater than low, and the product will have undergone a search for obvious flaws. The assurance level has been increased over the PP due to ready availability of the majority of the development record.

8.5 Rationale for TOE Summary Specification

289 This section demonstrates that the TOE security functions and assurance measures are suitable to meet the TOE security requirements.

8.5.1 TOE Security Functions

290 The specified TOE security functions work together so as to satisfy the TOE security functional requirements. [Table 8-4] provides a mapping of SFRs to the security functional requirements to show that all SFRs are captured within a security function.

[Table 8-4] Mapping for SFRs to Security Functions

Security Function	Security Functional Requirement
Security Management	FMT_SMF.1
	FMT_MOF.1 (1)
	FMT_MOF.1 (2)
	FMT_MSA.1 (1)
	FMT_MSA.1 (2)
	FMT_MSA.1 (3)
	FMT_MSA.1 (4)
	FMT_MSA.1 (5)
	FMT_MSA.1 (6)
	FMT_MSA.3
	FMT_MTD.2
	FMT_SMR.1
	FMT_MTD.1 (1)
	FMT_MTD.1 (2)
	FIA_ATD.1
Audit	FAU_GEN.1
	FAU_GEN.2
	FAU_SAR.1
	FAU_SAR.3
	FAU_ARP.1
	FAU_STG.1
	FAU_STG.4
	FAU_SAA.1
	FAU_SEL.1
	FPT_STM.1
Information Flow Control	FDP_IFC.1 (1)
	FDP_IFC.1 (2)
	FDP_IFC.1 (3)
	FDP_IFC.1 (4)
	FDP_IFF.1 (1)
	FDP_IFF.1 (2)
	FDP_IFF.1 (3)

	FDP_IFF.1 (4)
	FDP_RIP.1
	FPR_PSE.1 (1)
	FPR_PSE.1 (2)
	FPT_RMV.1
	FPT_SEP.1
	FAU_APR.1
	FAU_SAA.1
	FMT_MTD.2
Identification & Authentication	FIA_UID.2
	FIA_AFL.1
	FIA_ATD.1
	FIA_UAU.4
	FIA_UAU.5
	FIA_UAU.1
	FMT_MTD.2
	FMT_MOF.1(2)
	FCS_COP.1
Protection of Security Function	FPT_TST.1
	FPT_SEP.1
	FPT_RVM.1
	FPT_AMT.1
	FCS_COP.1

291 The following paragraphs briefly summarize which security functions implement specific function requirements specified in Section 5.1.1, TOE Security Functional Requirements:

292 Component FMT_MOF.1 (1), management of security functions behavior has a security function associated with this SFR. Administration Server only provides this function to administrator who successfully login the Administration Server. Administrator can change or set the TOE configuration data that are defined under this SFR.. (SW_ADMIN)

293 Component FMT_MOF.1 (2), management of security functions behavior has a security function associated with this SFR. Administration Server only provides this function to administrator who successfully login the Administration Server. Administrator can change or set the TOE configuration data that are defined under this SFR. (SW_ADMIN)

294 Component FMT_SMF.1, specification of management functions behavior has several security functions associated with this SFR. Administration Server only provides this function to administrator who successfully login the Administration Server.(SW_ADMIN)

295 Component FMT_MSA.1 (1), management of security attributes allows administrator to add, delete, and modify attributes of a rule that are needed to enforce Packet Filtering Policy(UNAUTHENTCATED SFP and AUTHENTICATED FILTER SFP). Administration Server only provides this function to the administrator who successfully login the Administration Server. (SW_ADMIN)

296 Component FMT_MSA.1 (2), management of security attributes allows administrator to add, delete, and modify attributes of a rule that are needed to enforce Application Gateway Policy(UNAUTHENTICATED_PROXY SFP). Administration Server only provides this function to the administrator who successfully login the Administration Server. (SW_ADMIN)

297 Component FMT_MSA.1 (3) management of security attributes allows administrator to add, delete, and modify attributes of a rule that are needed to enforce Application Gateway Policy(AUTHENTICATED SFP). Administration Server only provides this function to the administrator who successfully login the Administration Server. (SW_ADMIN)

298 Component FMT_MSA.1 (4) management of security attributes allows administrator to add, delete, and apply a Packet Filtering Policy Rule. Administration Server only provides this function to the administrator who successfully login the Administration Server. (SW_ADMIN)

299 Component FMT_MSA.1 (5) management of security attributes allows administrator to add, delete, and apply an Unauthenticated Application Gateway Policy Rule. Administration Server only provides this function to the administrator who successfully login the Administration Server. (SW_ADMIN)

300 Component FMT_MSA.1 (6) management of security attributes allows administrator to add, delete, and apply an Authenticated Application Gateway Policy Rule. Administration Server only provides this function to the administrator who successfully login the Administration Server. (SW_ADMIN)

301 Component FMT_MSA.3 static attribute initialization function provides default value for End User attributes and Information Flow Control SFP. (SW_ADMIN)

302 Component FMT_MTD.2 management limit on TSF data allows administrator to set attributes for User Authentication Failure. Administration Server only provides this function to the administrator who successfully login the Administration Server. (SW_ADMIN)

303 Component FMT_SMR.1 security role allows administrator to delegate TOE administration role to a suitable user. Administration Server only provides this function to the administrator who successfully login the Administration Server. (SW_ADMIN)

304 Component FMT_MTD.1 (1) management of TSF data allows administrator to query, modify and delete user attributes. Administration Server only provides this function to the administrator who successfully login the Administration Server. (SW_ADMIN)

305 Component FMT_MTD.1 (2) management of TSF data allows administrator to set time and date of the timestamp that is provided by the TOE. Administration Server only provides this function to the administrator who successfully login the Administration Server. (SW_ADMIN)

306 Component FAU_GEN.1 audit generation provides a function of audit generation. This is implemented by SECUREWORKS Log Server and the audit record contains security related information.(SW_AUDIT)

307 Component FAU_GEN.2, User identify association is implemented by SECUREWORKS Log Server and Authentication Server. After user authentication is executed, the log is recorded for each user. (SW_AUDIT)

308 Component FAU_SAR.1, audit review is accomplished via the graphic user interface (GUI) of the Administration server. The SECUREWORKS Administration Server allows administrator to view, search the audit record and review the generated statistics through web browser. Also, it provides the interface to configure the security policy rule of SECUREWORKS. (SW_AUDIT)

309 Component FAU_SAR.3, selectable audit review is accomplished via the graphic user interface(GUI) of the Administration server. The SECUREWORKS Administration Server allows administrator to search and sort the audit record based on the various conditions. (SW_AUDIT)

310 Component FAU_ARP.1, security alarm is implemented by Log Server to alarm administrator based on the administrator-predefined rule. (SW_AUDIT)

311 Component FAU_STG.1, protected audit trail storage, is implemented by the Solaris UNIX system identification and authentication mechanism. Only administrator can login to the SECUREWORKS system. (SW_AUDIT)

312 Component FAU_STG.4, prevention of audit data loss, is implemented by SECUREWORKS stopping the flow of packets when the allocated disk space has been reached and the firewall is unable to continue storing audit records. (SW_AUDIT)

313 Component FAU_SAA.1, potential violation analysis is implemented by Log Server to detect the potential violation and protect the TOE. (SW_AUDIT)

314 Component FAU_SEL.1, Selective audit, is implemented by Log server to generate the audit record for each event type, event protocol, and event service.

(SW_AUDIT)

315 Component FDP_IFC.1 (1), The Packet Filtering subset information flow control, is implemented by Firewall Module that form part of the Firewall system. Management Module will support this functionality by allowing administrator to configure the associated rule set. (SW_IFC)

316 Component FDP_IFC.1 (2), The Unauthenticated Application Gateway subset information flow control, is implemented by Firewall Module that form part of the Firewall system. The POP3, H.323, IMAP4, Telnet and RLOGIN application gateway (proxy) also a role in enforcing this requirement. Management Module will support this functionality by allowing administrator to configure the associated rule set. (SW_IFC)

317 Component FDP_IFC.1 (3), The Authentication Application Gateway subset information flow control, is implemented by Firewall Module that form part of the Firewall system. The HTTP, FTP, NNTP, SMTP application gateway (proxy) also a role in enforcing this requirement. Management Module will support this functionality by allowing administrator to configure the associated rule set. (SW_IFC)

318 Component FDP_IFF.1 (1) simple security attribute provides numerous security attributes so the SECUREWORKS can enforce information flow control based on them. This is implemented by Firewall Module as Packet Filtering.(SW_IFC)

319 Component FDP_IFF.1 (2) simple security attribute provides numerous security attributes so the SECUREWORKS can enforce information flow control based on them only after successful End User authentication. This is implemented by Firewall Module as Packet Filtering. (SW_IFC)

320 Component FDP_IFF.1 (3) provides numerous security attributes so the SECUREWORKS can enforce information flow control based on them if TCP/IP application is being used which does not support authentication. This is implemented by Firewall Module as Unauthenticated Application Server. (SW_IFC)

321 Component FDP_IFF.1 (4) provides numerous security attributes so the SECUREWORKS can enforce information flow control based on them if TCP/IP application is being used which supports authentication. This is implemented by Firewall Module as Authenticated Application Server. (SW_IFC)

322 Component FPR_RIP.1, full residual information protection, is implemented by the Firewall Module. Firewall Module Kernel Driver doesn't allow the packet, which was already passed firewall, to be used again. (FW_IFC)

323 Component FPR_PSE.1 (1), Pseudonym (Dynamic)(1), is implemented by Firewall Module's NAT services. The Normal NAT services also a role in enforcing this requirement. This is satisfied by port mapping. Management Module will support this functionality by allowing administrator to configure the associated rule set. (SW_IFC)

324 Component FPR_PSE.1 (2), Pseudonym (Static)(2), is implemented by Firewall Module's NAT services. The SECUREWORKS' Reverse NAT, services also a role in enforcing this requirement. This is satisfied by port mapping. Management Module will support this functionality by allowing administrator to configure the associated rule set. (SW_IFC)

325 Component FIA_UID.2, user identification before any action is provided by Authentication Server. This is satisfied when administrator defines authentication attribute in UNAUTHENTICATED_FILTER SFP and AUTHENTICATED SFP.

326 Component FIA_AFL.1, authentication failure handling functionality is implemented by Authentication Server. When user consecutively fails the authentication for the number of times that administrator set, user account is locked.

327 Component FIA_ATD.1, user attribution definition, administrator can update, delete and add user profile and change its own password and password authentication scheme.

.

328 Component FIA_UAU.4, single use authentication mechanism is used to authenticate administrator or user by using One Time Password (SKEY) method

329 Component FIA_UAU.5, multiple authentication mechanism is used to authenticate administrator or user by using One Time Password (SKEY) method and SECUREWORKS Password (Normal Password). In order to use OTP, there must be preset password information.

330 Component FIA_UAU.1, timing of authentication administrator is provided by Administration Server. This is satisfied when administrator defines authentication attribute in UNAUTHENTICATED_FILTER SFP and AUTHENTCIATED SFP.

331 Component FPT_SEP.1, TSF domain separation is implemented by the TOE and network environment. All network traffic to the TOE host goes via the TOE. This allows the TOE information control policies to be used to provide separation of the TSF code and data structures from potential network based threat agents. Threat agents local to the TOE host are countered by environmental assumptions.

332 Component FPT_RVM.1 non-bypassability ensures that security TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed. This is implemented by Firewall Server and network environment. (SW_IFC)

333 Component FPT_TST.1, TSF self test, is implemented by Administration Server. It verifies the integrity of TSF data during operation.

334 Component FPT_AMT.1, Abstract machine test, is implemented by Administration Server. TOE performs testing to demonstrate the security assumptions made about the underlying abstract machine upon which the TSF relies.

335 Component FCS_COP.1, Cryptographic operation, is used to authenticate an administrator or a user by using One Time Password (SKEY) method and integrity verification check. OTP generates hash values by using encryption algorithm that is supported by this component.

336 Component FPT_STM.1, Reliable time stamps is implemented by the NTP Server. The TOE has an interface which synchronies the TOE's system time with a NTP server providing time so its system time can be synchronized to the NTP server's time. Also the TOE's system time can be freely set by the administrator.

8.5.2 TOE SOF Claims

337 The Strength of TOE function claims for the normal password and OTP authentication method are both valid. The ALFPP and the TFFPP both require an overall SOF claim of SOF-basic. This is a requirement set by the authors of the PP. This ST is claiming conformance to both of these PPs and is therefore claiming the same SOF.

338 Additionally, the PP authors have provided specific metrics for both mechanisms that require a SOF claim. The identified metrics and SOF claim is commensurate with the EAL3 level of assurance.

339 The following security functions are realized by probabilistic or permutational mechanisms:

- SW_I&A (one cryptographic mechanism and one mechanism requiring an SOF claim)
- SW_PSF (cryptographic mechanism only)

340 The assessment of the strength of cryptographic algorithms is outside the scope of the CC.

8.5.3 TOE Assurance Requirements

341 The TOE satisfies the SARs specified in the ALFPP. Because Section 5.1.2 of this documentation's assurance measures applied by SECUREWORKS to satisfy the CC EAL3 assurance requirements. The following [Table 8-5] illustrates the assurance measures compliance with the assurance requirements as Section 5.1.2

[Table 8-5] Assurance Measure Compliance Table

Assurance Component ID	Configuration Management	Delivery and Operation	Development	Lifecycle Support	Guidance	Test	Vulnerability Assessment
ACM_CAP.3	X						
ACM_SCP.1	X						
ADO_DEL.1		X					
ADO_IGS.1		X					
ADV_FSP.1			X				
ADV_HLD.2			X				
ADV_RCR.1			X				
AGD_ADM.1					X		
AGD_USR.1					X		
ALC_DVS.1				X			
ATE_COV.2						X	
ATE_DPT.1						X	
ATE_FUN.1						X	
ATE_IND.2						X	
AVA_MSU.1							X
AVA_SOF.1							X
AVA_VLA.1							X

342 ACM_CAP.3, Authorization controls, Assurance measure for ACM_CAP(Authorization Controls) is the Configuration Management Documents. It contains configuration item lists and configuration management document. This describes the method used to uniquely identify the configuration items. The CM plan documentation describes how the CM system is used. This evidence shall demonstrate that the CM system is operating in accordance with the CM plan.

343 ACM_SCP.1, TOE CM coverage, Assurance measure for this is the Configuration Management. It describes how the CM system tracks configuration items.

344 ADO_DEL.1, Delivery procedures, Assurance measure addresses delivery procedures for the TOE and documentations how SECUREWORKS is securely delivered to a customer.

345 ADO_IGS.1, Installation, generation, and start-up procedures, Assurance measure addresses Installation, Generation and Startup procedures for the evaluated TOE.

346 ADV_FSP.1, Information functional specification, describes assurance measure TOE's functions. This includes identifying and describing the external TOE security function interfaces.

347 ADV_HLD.2, Security enforcing high-level design, describe the structure of the TSF in terms of subsystems and security functionality of each subsystem and supporting protection mechanisms implementation. And this assurance measure describes the purpose and method of use of all interfaces to the subsystems of TSF, providing details of effects, exceptions and error messages.

348 ADV_RCR.1, Informal correspondence demonstration, assurance measure was specifically written to address the EAL.3 requirement for correspondence evidence. This includes showing a correspondence analysis between the security target and the functional specification; and between the functional specification and high-level design.

349 AGD_ADM.1, Administrator guidance, assurance measure addresses administrator guidance. It describes how to securely administrate the TOE.

350 AGD_USR.1, User guidance, assurance measure address user guidance. It describes the instructions and guidance for secure use of the TOE.

351 ALC_DVS.1, Identification of security measures, assurance measure describes all the physical, procedural, personnel, an other security measures. So It protects the confidentiality and integrity of the TOE design and implementation in its development environment.

352 ATE_COV.2, Analysis of coverage, assurance measure includes showing which security functions were tested and demonstrate the correspondence between functional specification and the tests identified in the test documentation is complete.

353 ATE_DPT.1, Testing: high-level design, assurance measure address analysis of the depth of testing.

354 ATE_FUN.1, Functional testing, assurance measure provides the test documentation used by the vendor to test TOE functionality

355 ATE_IND.2, No justification for this.

356 AVA_MSU.1, Examination of guidance, assurance measure provides the guidance documentation which identifies all possible modes of operation of the TOE.

357 AVA_SOF.1, Strength of TOE security function evaluation, assurance measure includes a chapter that discusses strength of function of the authentication mechanism.

358 AVA_VLA.1, Developer vulnerability analysis, assurance measure addresses the intended environment for the TOE. This includes that there are no exploitable obvious vulnerabilities.

8.6 Rationale For SFR dependencies

[Table 8-6] SFR Dependency Satisfaction Table

Functional Component ID	Functional Component Name	Dependency (ies)	Satisfied
FMT_MOF.1 (1)	Management security function behavior (1)	FMT_SMR.1	YES
FMT_MOF.1 (2)	Management security function behavior (2)	FMT_SMR.1	YES
FMT_MSA.1 (1)	Management of security attributes (1)	FDP_IFC.1 FMT_SMR.1	YES
FMT_MSA.1 (2)	Management of security attributes (2)	FDP_IFC.1 FMT_SMR.1	YES
FMT_MSA.1 (3)	Management of security attributes (3)	FDP_IFC.1 FMT_SMR.1	YES
FMT_MSA.1 (4)	Management of security attributes (4)	FDP_IFC.1 FMT_SMR.1	YES
FMT_MSA.1 (5)	Management of security attributes (5)	FDP_IFC.1 FMT_SMR.1	YES
FMT_MSA.1 (6)	Management of security attributes (6)	FDP_IFC.1 FMT_SMR.1	YES
FMT_MSA.3	Static attribute initialization	FMT_SMR.1 FMT_MSA.1	YES
FMT_MTD.2	Management of limits on TSF data	FMT_SMR.1 FMT_MTD.1	YES
FMT_SMR.1	Security roles	FIA_UID.1	YES
FMT_MTD.1 (1)	Management of TSF data (1)	FMT_SMR.1	YES
FMT_MTD.1 (2)	Management of TSF data (2)	FMT_SMR.1	YES
FAU_GEN.1	Audit data generation	FPT_STM.1	YES
FAU_GEN.2	User identity association	FAU_GEN.1 FIA_UID.1	YES
FAU_SAR.1	Audit review	FAU_GEN.1	YES
FAU_SAR.3	Security audit review	FAU_SAR.1	YES
FAU_ARP.1	Security alarm	FAU_SAA.1	YES
FAU_STG.1	Protected audit trail storage	FAU_GEN.1	YES

FAU_STG.4	Prevention of audit data loss	FAU_STG.1	YES
FAU_SAA.1	Potential violation analysis	FAU_GEN.1	YES
FAU_SEL.1	Selective audit	FAU_GEN.1 FMT_MTD.1	YES
FDP_IFC.1 (1)	Subset information flow control (1)	FDP_IFF.1	YES
FDP_IFC.1 (2)	Subset information flow control (2)	FDP_IFF.1	YES
FDP_IFC.1 (3)	Subset information flow control (3)	FDP_IFF.1	YES
FDP_IFC.1 (4)	Subset information flow control (3)	FDP_IFF.1	YES
FDP_IFF.1 (1)	Simple security attributes (1)	FDP_IFC.1 FMT_MSA.3	YES
FDP_IFF.1 (2)	Simple security attributes (1)	FDP_IFC.1 FMT_MSA.3	YES
FDP_IFF.1 (3)	Simple security attributes (1)	FDP_IFC.1 FMT_MSA.3	YES
FDP_IFF.1 (3)	Simple security attributes (1)	FDP_IFC.1 FMT_MSA.3	YES
FDP_RIP.1	Subset residual information protection	NONE	NONE
FPR_PSE.1 (1)	Pseudonym (Dynamic) (1)	NONE	NONE
FPR_PSE.1 (2)	Pseudonym (Static) (2)	NONE	NONE
FIA_UID.2	User authentication before any action	NONE	NONE
FIA_AFL.1	Authentication failure handling	FIA_UAU.1	YES
FIA_ATD.1	User attribute definition	NONE	NONE
FIA_UAU.4	Single use authentication mechanism	NONE	NONE
FIA_UAU.5	Multiple authentication mechanism	NONE	NONE
FIA_UAU.1	Timing of authentication	FIA_UID.1	YES
FPT_TST.1	TSF self test	FPT_AMT.1	YES
FPT_AMT.1	Abstract machine test	NONE	NONE
FPT_SEP.1	TSF domain separation	NONE	NONE
FPT_RVM.1	Non-bypassability the TSP	NONE	NONE
FPT_STM	Reliable time stamp	NONE	NONE
FCS_COP.1	Cryptographic operation	FDP_ITC.1 or FCS_CKM.1 FCS_CKM.4 FMT_MSA.2	PP (see below)

359 DEPTH: FIA_UID.1 is satisfied by selecting FIA_UID.2.

360 PP: With the exception of the functional component FCS_COP.1, all dependencies are contained in the claimed Protection Profile.

361 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. However, none of these dependencies apply, or are required, because FCS_COP.1 is only being used for hashing in this TOE.