Network

Intrusion Prevention System Protection Profile V1.1

December 21, 2005

(This page left blank on purpose for double-side printing)

Protection Profile Title

Network Intrusion Prevention System Protection Profile

Evaluation Criteria Version

This Protection Profile has been prepared in conformance to the Common Criteria for Information Technology Security Evaluation (Ministry of Information & Communication Public Notice No. 2005-25).

Developer

This Protection Profile has been developed by the following developers:

Wan s. Yi, Philyong Kang, Yungi Seong, Eunjoo La

Korea Information Security Agency (KISA)

Revision History

Version	Date	Details
1.0	2005. 5. 24	- Network Intrusion Prevention System protection profile 1.0
1.1	2005. 12. 21	- Reflected the CC V2.3 - Deleted assumption of A.Attacker level and listed the related contents in threat, modified attack level from medium to low in order to handle AVA_VLA.2 - Modified note at application so that reliable time stamp component of FPT_STM.1 can be implemented in IT environment of TOE - FRU_FLT.1 Fault Tolerance: Deleted description of error types in partial application component and operation not completed in order to enable developers to implement - Others: Modified editing error and supplemented contents, etc.

Table of Contents

List of Tables

List of Figure

1. Protection Profile(PP) Introduction

1 This Protection Profile has been developed by the Korea Information Security Agency (KISA) and intended to define security functional requirements to be equipped by network intrusion prevention system and security assurance requirements to safely guarantee the security functional requirements. Network intrusion prevention system developed in accordance with this protection profile defines basic requirements of intrusion prevention system. System administrator shall be able to use this protection profile as reference in order to propose requirements for safely maintaining IT system.

1.1 PP Identification

2 Title : Network Intrusion Prevention System Protection Profile

3 Sponsor : ITSCC, MIC

4 Developer : IT Security Evaluation Division, Evaluation Planning Team, KISA

5 Contributor : Firewall Protection Profile Development Expert Group

6 Common Criteria Version : CC V2.3

7 Evaluation Assurance Level : EAL4

8 Protection Profile Version : V1.2, Dec. 21. 2005

9 Registration Number : PP-009

10 Evaluation Result : Pass

11 Keywords : Network Intrusion Prevention System, Information Flow Control, Firewall

1.2 PP Overview

12 This protection profile defines security requirements of network intrusion prevention system used as a means to protect internal information and communications network of an organization from external Internet tampering attacks.

13 Developer or author of Security Target(ST) may add security requirements of higher level than protection profile requirements when implementing network intrusion prevention system. Protection profile defines threats, assumptions and Organizational security policies to be dealt with in network intrusion prevention system and describes security objectives, security functional requirements and security assurance requirements independent to implementation environment. Lastly, protection profile provides rationale for security objectives and security requirements.

14 The strength of function(SOF) of this PP is “SOF-medium”.

1.3 Conventions

15 The notation, formatting and conventions used in this Protection Profile are consistent with the Common Criteria for Information Technology Security Evaluation (hereafter referred to as “CC”).

16 The CC allows several operations to be performed on functional requirements; refinement, selection, assignment, and iteration. Each of these operations is used in this Protection Profile.

Assignment

It is used to assign specific values to unspecified parameters (e.g. : password length). The result of assignment is indicated in square brackets, i.e., [assignment_Value].

Iteration

It is used when a component is repeated with varying operations. The result of iteration is marked by iteration number in parenthesis following the component identifier, i.e., (Iteration No.).

Refinement

It is used to add detail to a requirement, and thus further restricts a requirement. The result of refinement is shown in **bold text**.

Security target(ST) author Operation

It is used to denote points in which final determination of attributes is left to the ST author. ST author operation is indicated by the words { determined by ST author } in braces. In addition, operations of the security functional requirements that are not completely performed in the Protection Profile shall be performed fully by ST author.

Selection

It is used to select one or more options provided by the CC in stating a requirement. The result of selection is shown as *<u>underlined and italicized.</u>*

17 Application Notes are provided to help to clarify the intent of a requirement, identify implementation choices or to define "Pass/Fail" criteria for a requirement. Application Notes will follow relevant requirements where appropriate.

1.4 Terms and Definitions

18 Terms that are used herein and defined in the CC as well are to have the same meaning as in the CC.

Audit Trail

A set of records showing who has accessed a system and what operations he or she has performed

Object

An entity within the TSC(TSF Scope of Control) that contains or receives information and upon which subjects perform operations.

Attack Potential

The perceived potential for success of an attack, should an attack be launched, expressed in terms of an attacker's expertise, resources and motivation.

Strength Of Function (SOF)

A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms.

SOF-medium

A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.

Iteration

The use of a component more than once with varying operations.

Security Target (ST)

A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

Protection profile (PP)

An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

Human User

Any person who interacts with the TOE.

User

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

Selection

The specification of one or more items from a list in a component.

Identity

A representation (e.g. a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.

Element

An indivisible security requirement.

Role

A predefined set of rules establishing the allowed interactions between a user and the TOE.

Operation

Modifying or repeating that component. Allowed operations on components are assignment, iteration, refinement and selection.

Threat Agent

An unauthorized user or external IT entity that brings assets under such threats as illegal access, modification or deletion.

External IT Entity

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

Authorized Administrator

A authorized user, in accordance with the TSP, operation and manage firewall protection system.

Authentication Data

Information used to verify the claimed identity of a user.

Assets

Information or resources to be protected by the countermeasures of a TOE.

Refinement

The addition of details to a component.

Organizational security policies

One or more security rules, procedures, practices, or guidelines imposed by an organization upon its operations.

Dependency

A relationship between requirements such that the requirement that is depended upon shall normally be satisfied for the other requirements to be able to meet their objectives.

Subject

An entity within the TSC that causes operations to be performed.

Augmentation

The addition of one or more assurance component(s) from CC Part 3 to an EAL or assurance package.

Component

The smallest selectable set of elements that may be included in a PP, an ST, or a package.

Class

A grouping of families that share a common focus.

Target of Evaluation (TOE)

An IT product or system and its associated guidance documentation that is the subject of an evaluation.

Evaluation Assurance Level (EAL)

A package consisting of assurance components from CC Part 3 that represents a point on the CC predefined assurance scale.

Family

A grouping of components that share security objectives but may differ in emphasis or rigour.

Packet

Packet refers to a group of data used for data transmission in Internet network. For packet transmission, data between two points are not continuously transmitted. After dividing data to be transmitted into appropriate size to form separate packets, each of the packets is individually transmitted. Each packet contains not only data of the prescribed size, but also control information, such as data destination, address or control code, etc.

Assignment

The specification of an identified parameter in a component.

TOE Security Functions (TSF)

A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy (TSP)

A set of rules that regulate how assets are managed, protected and distributed within a TOE.

TSF Data

Data created by and for the TOE, that might affect the operation of the TOE.

TSF Scope of Control (TSC)

The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

1.5 Protection Profile Organization

19 Section 1 provides the introductory material for the Protection Profile.

20 Section 2 defines TOE and describes the IT environment on which the TOE depends.

21 Section 3 describes the TOE security environment and includes security problems of the TOE and its IT environment from such as assumptions, threats and organizational security policies.

22 Section 4 defines the security objectives for the TOE and its IT environment to respond to identified threats and support the assumptions and organizational security policies.

23 Section 5 contains the IT security requirements including the functional and assurance requirements intended to satisfy security objectives.

24 Section 6 describes Application Notes which deserve notice in applying the PP herein.

25 Section 7 provides a rationale to demonstrate that the security objectives for the TOE and its IT environment cope with the defined security problems appropriately and the IT security requirements are adequate and complete to satisfy the security objectives.

26 References contain references to noteworthy background and/or supporting materials for prospective users of the PP who may be interested in knowing more than what is specified herein.

27 Acronym is an acronym list that defines frequently used acronyms.

2. TOE Description

28 TOE refers to network intrusion prevention system implemented in the form of hardware, firmware or software that holds the function to safely protect internal network assets and to detect and block out intrusion. TOE is connected in In-line type to the point where internal network is connected to external network through Internet and executes the function to detect and block out intrusion and attack of network traffic that flows from outside to the inside on a real-time basis.

External Internet Environment

29 In the earlier phase of Internet use, many of the attacks through Internet were illegal service accesses and attacks to server that provided services to internal network by using network layers. However, viruses and attacks of the recent times are occurring on personal computers by using mainly the application layer. Frequency of attacks using virus and hacking has also astronomically increased in comparison to the earlier phase in which Internet use was expanded.

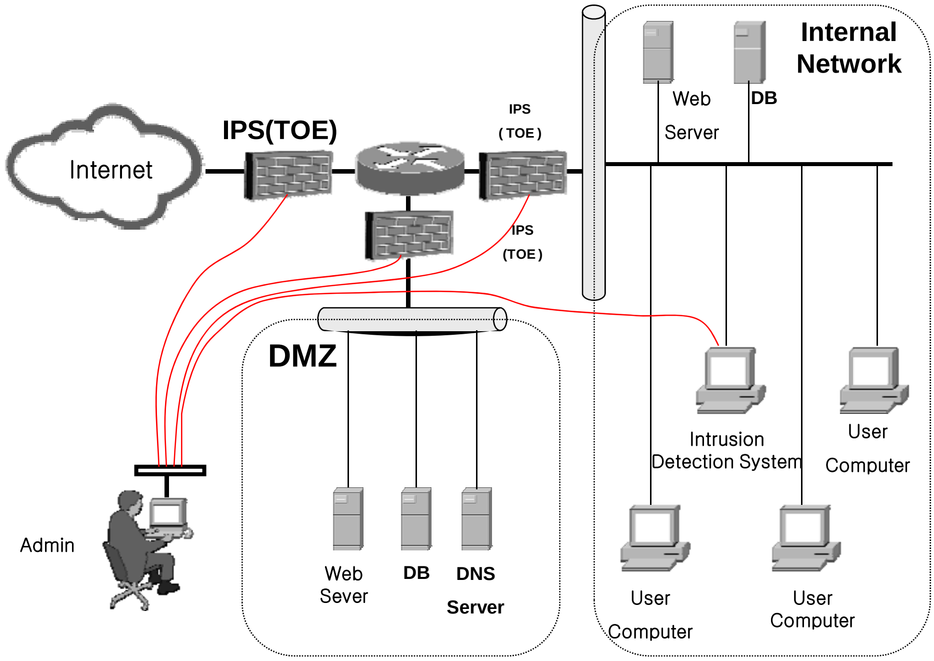
30 This is because, due to rapid development of Internet and increase of Internet users, many computers are connected to Internet network and environment was created for a single damage to be easily expanded into similar types of damages. Also, computer system and service vulnerability is easily detected. Therefore, violation accidents using such vulnerability, such as by hacking, attack through e-mail, virus and worm have rapidly increased. Recently, due to characteristics of computer viruses in the recent times, a single damage is reproduced, therefore is expanded into other computers. Accordingly, when a single computer is affected, the damage instantly spreads to all other computers in internal network. This phenomenon resulted in significant increase in threats of an organization through Internet compared to the past.

Environment of TOE Use

31 In order to block out inflow of harmful Internet traffic from external network into internal network, TOE administers monitoring and control on network traffic according to its security policy.

32 As shown in (Figure 1), TOE is installed and operated in inline type at the point of connection between Internet and internal network or where network is branched off into external and internal networks. Also, administration console executes regional or remote control on the TOE.

33 TOE users are divided into 2 types, IT entities, such as user and computer. User refers to administrator that conducts administration by connecting to a TOE. Administrator connects to a TOE after authentication by identifier and authentication data. IT entity includes host that provides services to internal network through the TOE and external computer that interacts with personal computer. TOE mainly controls connection of IT entity to host of internal network to be protected.



(Figure 1) Network installed with network intrusion prevention system

TOE Security Function

34 TOE provides the following security functions according to the previously described environment.

35 TOE detects and blocks off harmful traffic flown from Internet network into internal network, therefore securely protects information assets and resources of internal network. Harmful traffic includes unauthorized service access, all network packets that do not hold normal packet structure, packet containing computer worm and virus and packet that makes the attack of service denial to damage the availability of internal computer resources, etc.

36 TOE shall be equipped with procedures of renewing vulnerability information into vulnerability database and be able to block off attacks as much as possible by detecting vulnerability of computer system. Therefore, TOE can promptly handle new viruses, worms or transformed attacks.

37 TOE monitors and processes all traffics flown from the outside to the inside. Therefore, TOE shall be ensured of high-performance processing and availability to withstand fault occurrence.

3. TOE Security Environment

38 The TOE security environment consists of assumptions that describe the security of the TOE environment, the security threats that may possibly be posed by threat agents against the TOE assets or environment and the organizational security policies that provide for rules, procedures, practices and guidelines requiring compliance by the TOE.

3.1 Assumptions

39 The following assumptions shall be applied to the TOE operational environment to conform to this PP.

A.Physical Security

40 The TOE shall be located in the physically secure environment that can be accessed only by the authorized users.

A.Security Maintenance

41 When internal network environment changes due to change in the network configuration, host increase/decrease and service increase/decrease, etc., the changed environment and security policy shall immediately be reflected in TOE operation policy so that security level can be maintained to be the same as before.

A.Trusted Administrator

42 Authorized administrator of TOE shall be non-malicious users, have completed appropriate training on TOE administration functions and fulfill obligations according to administrator guidelines.

A. Operating System Reinforcement

43 Reliability and security of an operating system shall be ensured by administering operations to remove services or means in operating system not required by TOE and reinforcement on vulnerabilities in the operating system.

A.Sole Connection Point

44 TOE, when installed and operated in network, branches off network into external and internal networks and all communications between external and internal networks are carried out only through the TOE.

3.2 Threats

45 This protection profile(PP) defines security threats exerted by external threat agents to protection assets of TOE by categorizing them into threats to TOE and threats to TOE operational environment.

46 Major assets to be protected by TOE are computer resources and network services of DMZ or the internal network operated by organization. External threat agent attacks computer resources by illegal access or to exhaust its availability.

47 Threat agents are generally computer users or IT entity that accesses computer of the inside from the outside. Threat agents hold low level of professional knowledge, resources and motives. It is presumed that possibility for the threat agents to detect vulnerability that can be made of malicious use is low. In other words, using distinct vulnerability information, attacker can illegally obtain information or damage the targeted computer resources by easily acquiring vulnerability information that can be made of malicious use in relation to operating system and application program. The TOE protects assets from threats on such distinct vulnerability.

3.2.1 Threats on the TOE

T.Masquerade

48 Threat agents may access TOE by masquerading as authorized administrator.

T.Breakdown

49 TOE may not provide normal services to user as it is in use or breakdown occurred due to external attacks, etc.

T.Recording Failure

50 As storage capacity is insufficient, security-related incidents of TOE may not be recorded.

T.Illegal Information Inflow

51 Computer of internal network may be violated due to inflow of packet that contains unapproved information from external network.

T.Illegal Service Access

52 Threat agent may interrupt normal service provision of host by accessing services not approved to the host of internal network.

T.Abnormal Packet Transmission

53 Threat agent may cause erroneous operation in system of internal network by transmitting network packet that holds abnormal structure.

T.New Vulnerability Attack

54 Threat agents may make attack by using new vulnerability in computer system of internal network located in the TOE or TOE operational environment.

T.Denial of Service Attack

55 Threat agents may interrupt normal use through abnormally excessive using of computer service resources in internal network located in TOE operational environment.

T.Continuous Authentication Attempt

56 Threat agents may access TOE by continuously attempting authentication.

T.Bypass Access

57 Threat agents may access TOE through bypassing security function of TOE.

T.Address Spoofing

58 Threat agents may illegally access internal network by spoofing source address as internal address.

T.Unauthorized TSF Data Change

59 TSF data may be changed without authentication as threat agent makes buffer overflow attack to TOE.

3.2.2 Threats to the TOE Operational environment

TE.Administration Deficiency

60 The TOE may be configured, managed and used in insecure method by authorized administrator.

TE.Distribution and Installation

61 The TOE may be impaired of security in the process of distribution or installation.

3.3 Security Policy of Organization

62 Security policy of organization described in this section shall be observed by TOE to conform to this PP.

P.Audit

63 To trace responsibilities on all security-related activities, security-related events shall be recorded and maintained. Also, the recorded data shall be reviewed.

P.Secure Management

64 The Authorized administrator shall manage the TOE in a secure way.

4. Security Objectives

65 The PP divides the security objectives into the ones for the TOE and the others for the TOE environment. The security objectives for the TOE are addressed directly by the TOE and the security objectives for the TOE environment by the IT domain or non-technical or procedural means.

4.1 Security Objectives for the TOE

66 The followings are the security objectives to be addressed directly by the TOE.

O. Availability

67 The TOE shall provide normal service by maintaining the minimum security function at occurrence of breakdown by incidental attack or external attack.

O. Audit

68 The TOE shall record and maintain security-related incidents in order to enable tracing of responsibilities for security-related acts and must provide means to review the recorded data.

O.Management

69 The TOE shall provide means for authorized administrator of TOE to efficiently manage TOE in secure method.

O.Abnormal Packet Cut-off

70 The TOE shall cut off the packet to hold abnormal structure among packets that pass through the TOE.

Application Note: Abnormal packet refers to those other than TCP/IP packets defined at Internet standard protocol, such as RFC 791 (Internet protocol), RFC 792 (Internet control message protocol) and RFC 793 (transmission control protocol), etc., or packets or which IP address is spoofed, broadcasting packets and roofing packets, etc.

O.Denial Of Service Attack Cut-off

71 In order to enable network service of the protected computer to be used by normal users, the TOE shall cut off using of abnormal computer service resources by attackers.

O.Identification

72 The TOE shall identify users intending to access TOE and all external IT entities that are subject to information flow control by the TOE.

O.Authentication

73 The TOE shall authorize identity of administrator before permitting TOE access after administrator identification.

Application Note: There is possibility for threat agents to obtain authorized data through continuous attempting of authentication by using identity of administrator. To avoid the attack of continuous attempt at authentication, TOE must implement authentication mechanism suitable to security function strength level.

O Information Flow Control

74 The TOE shall control unauthorized flow of information from external network to internal network according to the security policy.

Application Note: This purpose of security implements deny-all policy and allow-all policy executed by TSF. Deny-all policy refers to cutting off all packets with the exception of the explicitly allowed packets. Allow-all policy refers to allowing all packets with the exception of the explicitly denied packets.

O.TSF Data Protection

75 The TOE shall protect TSF data from unauthorized exposure, change and deletion.

4.2 Security Objectives for the Environment

76 The TOE's operational environment shall satisfy the following objectives. These objectives do not levy any IT requirements but are satisfied by procedural or non-technical measures

OE.Physical Security

77 The TOE shall be located in physically secure environment to which access is possible only by authorized administrator.

OE.Security Maintenance

78 When internal network environment changes due to change in network configuration, increase/decrease of host and increase/decrease of service, etc., the changed environment and security policy must be immediately reflected to TOE operation policy in order to maintain security in the same level as before.

OE.Trusted Administrator

79 Authorized administrator of TOE shall be non-malicious users, have completed appropriate training on TOE administration functions and accurately fulfill obligations according to administrator guidelines

OE.Secure Management

80 The TOE shall be distributed and installed in secure method and be configured, managed and used in secure method by authorized administrator.

OE.Operating system Reinforcement

81 Reliability and security of operating system must be assured by administering operations to remove services or means in operating system not required by the TOE and reinforcement on vulnerabilities in the system.

OE.Sole Connection

82 The TOE, when installed and operated in network, branches off network into external and internal networks and all communications between external and internal networks are carried out only through the TOE.

OE.Vulnerability List Renewal

83 In order for protection against the external attacks using new vulnerability of internal computer, administrator must renew and manage database on vulnerabilities managed by the TOE.

5. IT Security Requirements

84 This section provides functional and assurance requirements that must be satisfied by a Protection Profile-compliant TOE.

5.1 TOE Security Functional Requirements

85 The functional security requirements for this Protection Profile consist of the following components from Part 2 of the CC, summarized in the following [Table 1].

86 The strength of function(SOF) of this PP is “SOF-medium”

[Table 1] Security functional requirements

Functional Class	Functional Component	
Security Audit	FAU_ARP.1	Security Alarms
	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User Identity Association
	FAU_SAA.1	Potential Violation Analysis
	FAU_SAR.1	Audit Review
	FAU_SAR.3	Selectable Audit Review
	FAU_SEL.1	Selective Audit
	FAU_STG.1	Protected Audit Trail Storage
	FAU_STG.3	Action in case of possible audit data loss
	FAU_STG.4	Prevention of audit data loss
User Data Protection	FDP_IFC.1(1)	Subset information flow control(1)
	FDP_IFC.1(2)	Subset information flow control(2)
	FDP_IFF.1	Simple security attributes
Identification And Authentication	FIA_AFL.1	Authentication failure handling
	FIA_ATD.1(1)	User attribute definition (1)
	FIA_ATD.1(2)	User attribute definition (2)
	FIA_UAU.1	Timing of authentication
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2(1)	User identification before any action(1)
	FIA_UID.2(2)	User identification before any action(2)
Security Management	FMT_MOF.1	Management Of Security Functions Behaviour
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_MTD.1	Management of TSF data

	FMT_MTD.2	Management of limits on TSF data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles
Protection Of The TSF	FPT_AMT.1	Abstract machine testing
	FPT_FLS.1	Failure with preservation of secure state
	FPT_RVM.1	Non-bypassability of the TSP
	FPT_SEP.1	TSF domain separation
	FPT_STM.1	Reliable time stamps
	FPT_TST.1	TSF testing
Resource Utilisation	FRU_FLT.1	Degraded fault tolerance
	FRU_RSA.1	Maximum quotas
TOE Access	FTA_SSL.1	TSF-initiated session locking
	FTA_SSL.3	TSF-initiated termination
Trusted Path/Channel	FTP_ITC.1	Inter-TSF trusted channel

5.1.1 Security Audit

FAU_ARP.1 Security alarms

Hierarchical to : No other components.

87 FAU_ARP.1.1 The TSF shall take [{list of actions determined by ST author}] upon detection of a potential security violation.

Dependencies : FAU_SAA.1 Potential violation analysis

FAU_GEN.1 Audit data generation

Hierarchical to : No other components.

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

a) Start-up and shutdown of the audit functions;

b) All auditable events for the ***minimum*** level of audit; and

c) [assignment : *other specifically defined auditable events*].

89 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, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment : other audit relevant information].

Dependencies : FPT_STM.1 Reliable time stamps

FAU_GEN.2 User Identity Relevance

Hierarchical to : No other components.

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

Dependencies : FAU_GEN.1 Audit data generation

FIA_UID.1 Timing of identification

Application Note: User refers to authorized administrator and identifier (administrator ID or network IP address) in relation to audit records of activities on network packet.

FAU_SAA.1 Potential violation analysis

Hierarchical to : No other components.

91 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.

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

a) Accumulation or combination of [assignment : subset of defined auditable events] known to indicate a potential security violation;

b) [assignment : any other rules].

Dependencies : FAU_GEN.1 Audit data generation

FAU_SAR.1 Audit review

Hierarchical to : No other components.

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

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

Dependencies : FAU_GEN.1 Audit data generation

FAU_SAR.3 Selectable audit review

Hierarchical to : No other components.

95 FAU_SAR.3.1 The TSF shall provide the ability to perform [selection: *searches, sorting, ordering*] of audit data based on [assignment : *criteria with logical relations*].

Dependencies : FAU_SAR.1 Audit review

FAU_SEL.1 Selective audit

Hierarchical to : No other components.

FMT_MTD.1 Management of TSF data

96 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) [selection: object identity, user identity, subject identity, host identity, event type]

b) [assignment : list of additional attributes that audit selectivity is based upon

Dependencies : FAU_GEN.1 Audit data generation

FAU_STG.1 Protected audit trail storage

Hierarchical to : No other components.

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

98 FAU_STG.1.2 The TSF shall be able to [selection : *prevent, detect*] unauthorized modifications to the stored audit records in the audit trail.

Dependencies : FAU_GEN.1 Audit data generation

FAU_STG.3 Action in case of possible audit data loss

Hierarchical to : No other components.

99 FAU_STG.3.1 The TSF shall [assignment : *actions to be taken in case of possible audit storage failure*] if the audit trail exceeds [assignment : *pre-defined limit*].

Dependencies : FAU_STG.1 Protected audit trail storage

FAU_STG.4 Prevention of audit data loss

Hierarchical to : FAU_STG.3 Action in case of possible audit data loss

100 FAU_STG.4.1 The TSF shall [selection, *choose one of: "ignore auditable events", "prevent auditable events, except those taken by the authorized user with special rights", "overwrite the oldest stored audit records"*] and [assignment : other actions to be taken in case of audit storage failure] if the audit trail is full.

Dependencies : FAU_STG.1 Protected audit trail storage

Application Note : The ST author shall define the maximum capacity of audit data storage and prepare for the attacks such as external attack or the exhaustion of audit trail storage.

5.1.2 User Data Protection

FDP_IFC.1(1) Subset Information Flow Control (1)

Hierarchical to : No other components.

101 FDP_IFC.1.1 The TSF shall enforce the [deny-all policy] on the following list of subjects and information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP.

a) [Entity : Unauthorized external IT entity on the side of information sender

b) Information : Traffic sent from entity to another place through the TOE

c) Operation : Pass when allowing rules exist}

Dependencies : FDP_IFF.1 Simple security attributes

Application Note : This security policy is to cut off all connections with the exception of rules for distinctive allowing. In other words, the TOE is network traffic access control policy that allows access by defining rules on services to be allowed and blocks off the others.

FDP_IFC.1(2) Subset Information Flow Control (2)

Hierarchical to : No other components.

102 FDP_IFC.1.1 The TSF shall enforce the [permission-all policy] on following list of subjects and information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP.

a) [Entity : Unauthorized external IT entity on the side of information sender

b) Information : Traffic sent from entity to another place through the TOE

c) Operation : Block when blocking rules exist}

Dependencies : FDP_IFF.1 Simple security attributes

Application Note : This security policy is to cut off harmful traffic based on signature included in vulnerability list data and is the policy to allow all connections with the exception of rules for explicit blocking.

FDP_IFF.1 Simple security attributes

Hierarchical to : No other components.

103 FDP_IFF.1.1 The TSF shall enforce the [assignment : *information flow control SFP*] based on the following types of subject and information security attributes: [assignment : *list of subjects and information controlled under the indicated SFP, and for each, the security attributes*].

104 FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment : *for each operation, the security attribute-based relationship that must hold between subject and information security attributes*].

105 FDP_IFF.1.3 The TSF shall enforce the [assignment : *additional information flow control SFP rules*].

106 FDP_IFF.1.4 The TSF shall provide the following [assignment : *list of additional SFP capabilities*].

107 FDP_IFF.1.5 The TSF shall explicitly authorise an information flow based on the following rules: [assignment : *rules, based on security attributes, that explicitly authorise information flows*].

108 FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules.

a) [The TOE shall block off request for connection on information to arrive from IT entity of external network that holds IP address of the entity of internal network.

b) The TOE shall block off request for connection on information to arrive from IT entity of internal network that holds IP address of the entity of external network.

c) The TOE shall block off request for connection on information to arrive from IT entity of external network that holds IP address of broadcasting entity.

d) The TOE shall block off request for connection on information to arrive from IT entity of external network that holds IP address of looping entity.

e) The TOE shall block off request for connection on information to arrive from IT entity of external network that holds abnormal packet structure.

f) [Other rules {determined by author of ST}]

Dependencies : FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialisation

Application Note : ST author shall specify functions to control information flow according to the corresponding entity and information in accordance with FDP_IFC.1(1) and FDP_IFC.1(2) policies.

5.1.3 Identification and Authentication

FIA_AFL.1 Authentication failure handling

Hierarchical to : No other components.

109 FIA_AFL.1.1 The TSF shall detect when [selection: [assignment : positive integer number], an administrator configurable positive integer within[assignment : range of acceptable values]] unsuccessful authentication attempts occur related to [assignment : list of authentication events].

110 FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment : list of actions].

Dependencies : FIA_UAU.1 Timing of authentication

FIA_ATD.1(1) User Attribute Definition (1)

Hierarchical to : No other components.

111 FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to IT entity : [the following list of security attributes] .

a) IP Address

b) { determined by ST author } user security attributes

Dependencies : No dependencies.

Application Note : Security functional requirements have the function to identify unauthorized external user that communicates with internal computer passed through and protected by the TOE. Using this, the TOE can identify external IT entity, audit and record security events of external IT entity and trace responsibilities afterwards.

FIA_ATD.1(2) User Attribute Definition (2)

Hierarchical to : No other components.

112 FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to administrator : [the following list of security attributes].

a) IP Address

b) { determined by ST author } user security attributes

Dependencies : No dependencies.

Application Note : Security functional requirements have the function to identify administrator that accesses, interacts with and manages the TOE. Using this, TOE identifies valid administrator and requests authentication after identification.

FIA_UAU.1 Timing of Authentication

Hierarchical to : No other components.

113 FIA_UAU.1.1 The TSF shall allow [assignment : list of TSF mediated actions] on behalf of the user to be performed before the user is authenticated.

114 FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies : FIA_UID.1 Timing of identification

Application Note : This security functional component is applied when authorizing the identified administrator and does not require authentication of the identified IT entity.

FIA_UAU.7 Protected authentication feedback

Hierarchical to : No other components.

115 FIA_UAU.7.1 The TSF shall provide only [assignment : list of feedback] to the **administrator** while the authentication is in progress.

FIA_UID.2(1) User Identification before Any Action (1)

Hierarchical to : FIA_UID.1 Timing of identification

116 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.

Dependencies : No dependencies.

Application Note : TOE users are classified into administrator and IT entity. This component requires identification of IT entity.

FIA_UID.2(2) User Identification before Any Action (2)

Hierarchical to : FIA_UID.1 Timing of identification

117 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.

Dependencies : No dependencies.

Application Note : The TOE users are classified into administrator and IT entity. This component requires identification of administrator.

5.1.4 Security Management

FMT_MTD.1 Management of TSF Data

Hierarchical to : No other components.

118 FMT_MTD.1.1 The TSF shall restrict the ability to [selection: change_default, query, modify, delete, clear,[assignment : other operations]] the [assignment : list of TSF data] to [assignment : the authorized identified roles].

Dependencies : FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MSA.1 Management of security attributes

Hierarchical to : No other components.

119 FMT_MSA.1.1 The TSF shall enforce the [assignment : access control SFP, information flow control SFP] to restrict the ability to [selection: change_default, query, modify, delete,[assignment : other operations]] the security attributes [assignment : list of security attributes] to [assignment : the authorized identified roles].

Dependencies : [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MSA.3 Static attribute initialisation

Hierarchical to : No other components.

120 FMT_MSA.3.1 The TSF shall enforce the [assignment : access control SFP, information flow control SFP] to provide [selection, choose one of: restrictive, permissive,[assignment : other property]] default values for security attributes that are used to enforce the SFP.

121 FMT_MSA.3.2 The TSF shall allow the [assignment : the authorized identified roles] to specify alternative initial values to override the default values when an object or information is created.

Dependencies : FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MTD.1 Management of TSF data

Hierarchical to : No other components.

122 FMT_MTD.1.1 The TSF shall restrict the ability to [selection: change_default, query, modify, delete, clear,[assignment : other operations]] the [assignment : list of TSF data] to [assignment : the authorized identified roles].

Dependencies : FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

Application Note : When new vulnerability is detected, administrator shall renew vulnerability list data and be able to avoid new network attack.

FMT_MTD.2 Management of limits on TSF data

Hierarchical to : No other components.

123 FMT_MTD.2.1 The TSF shall restrict the specification of the limits for [assignment : list of TSF data] to [assignment : the authorized identified roles].

124 FMT_MTD.2.2 The TSF shall take the following actions, if the TSF data are at, or exceed, the indicated limits: [assignment : actions to be taken].

Dependencies : FMT_MTD.1 Management of TSF data

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

Hierarchical to : No other components.

Dependencies : No dependencies.

125 FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [assignment : list of security management functions to be provided by the TSF].

FMT_SMR.1 Security roles

Hierarchical to : No other components.

126 FMT_SMR.1.1 The TSF shall maintain the roles [assignment : the authorized identified roles].

127 FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Dependencies : FIA_UID.1 Timing of identification

5.1.5 Protection of the TSF

FPT_AMT.1 Abstract machine testing

Hierarchical to : No other components.

128 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 authorized user,[assignment : other conditions]] to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

Dependencies : No dependencies.

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to : No other components.

129 FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [assignment : list of types of failures in the TSF].

Dependencies : ADV_SPM.1 Informal TOE security policy model

FPT_RVM.1 Non-bypassability of the TSP

Hierarchical to : No other components.

130 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.

Dependencies : No dependencies.

FPT_SEP.1 TSF domain separation

Hierarchical to : No other components.

131 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.

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

Dependencies : No dependencies.

FPT_STM.1 Reliable time stamps

Hierarchical to : No other components.

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

Dependencies : No dependencies.

Application Note : This requirement is provided a time stamps that the order of the occurrence of auditable events is preserved. Then, this requirement is satisfied that TOE can be used a time provided by TOE operational environment.

FPT_TST.1 TSF testing

Hierarchical to : No other components.

134 FPT_TST.1.1 The TSF shall run a suite of self tests [selection: during initial start-up, periodically during normal operation, at the request of the authorized user, at the conditions[assignment : conditions under which self test should occur]] to demonstrate the correct operation of the TSF. operation of [selection: [assignment : parts of TSF], the TSF].

135 FPT_TST.1.2 The TSF shall provide authorized users with the capability to verify the integrity of [selection: [assignment : parts of TSF], TSF data].

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

Dependencies : FPT_AMT.1 Abstract machine testing

5.1.6 Resource Utilisation

FRU_FLT.1 Degraded fault tolerance

Hierarchical to : No other components.

137 FRU_FLT.1.1 The TSF shall ensure the operation of [assignment : list of TOE capabilities] when the following failures occur: [assignment : list of type of failures].

Dependencies : FPT_FLS.1 Failure with preservation of secure state

Application Note: This function shall aim to ensure the use of network service by users even in the event of failure within the TOE. Therefore, developers shall implement types of failures and handling functions of TOE and specify them in the ST so that users can make the use of minimum network service even in the event of failure within the TOE.

FRU_RSA.1 Maximum quotas

Hierarchical to : No other components.

138 FRU_RSA.1.1 The TSF shall enforce maximum quotas of the following resources: [assignment : controlled resources] that [selection: individual user, defined group of users, subjects] can use [selection: simultaneously, over a specified period of time].

Dependencies : No dependencies.

Application Note : Transmission layer expression refers to SYN packet connection of TCP. SYN packet connection is capable of SYN attack by making half-connection state and this attack obstructs normal connection service of user by exhausting connected table resources. Subject of attack is IT entity and, through this function, service denial attack by protocol stack of TCP is avoided according to the identifier of IT entity.

5.1.7 TOE Access

FTA_SSL.1 TSF-initiated session locking

Hierarchical to : No other components.

139 FTA_SSL.1.1 The TSF shall lock an interactive session after [assignment : time interval of user inactivity] by:

a) clearing or overwriting display devices, making the current contents unreadable;

b) disabling any activity of the user's data access/display devices other than unlocking the session.

140 FTA_SSL.1.2 The TSF shall require the following events to occur prior to unlocking the session: [assignment : events to occur]

Dependencies : FIA_UAU.1 Timing of authentication

FTA_SSL.3 Session Ending by TSF

Hierarchical to : No other components.

Dependencies : No dependencies.

141 FTA_SSL.3.1 The TSF shall terminate an interactive session after a [assignment : time interval of user inactivity].

Application Note : The TSF has the role of mediating connection between internal and external networks. Therefore, as for mutual connection among IT entities that pass through the TOE and interact with each other, the TSF terminates the session in the event of the inactivity for a prescribed period of time.

5.1.8 Trusted Path/Channels

FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to : No other components.

142 FTP_ITC.1.1 The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

143 FTP_ITC.1.2 The TSF shall permit [selection: the TSF, the remote trusted IT product] to initiate communication via the trusted channel.

144 FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [assignment : list of functions for which a trusted channel is required].

Dependencies : No dependencies

Application Note : This component is requirements to implement trusted channel in the event of communication among trusted IT products outside the TOE. The Trusted channel shall be formed in the event that the administrator undergoes remote access to TOE rather than local access or at communication between the TOE and external vulnerability data server.

5.2 TOE Security Assurance Requirement

145 The security assurance requirements for this Protection Profile consist of the following components from Part 3 of the CC v2.3, summarized in the following [table 2] and evaluation assurance level is EAL4.

[Table 2] Security assurance requirement

Assurance Class	Assurance Component	
Configuration management	ACM_AUT.1	Partial CM automation
	ACM_CAP.4	Generation support and acceptance procedures
	ACM_SCP.2	Problem tracking CM coverage
Delivery and Operation	ADO_DEL.2	Detection of modification
	ADO_IGS.1	Installation, generation, and start-up procedures
Development	ADV_FSP.2	Fully defined external interfaces
	ADV_HLD.2	Security enforcing high-level design
	ADV_IMP.1	Subset of the implementation of the TSF
	ADV_LLD.1	Descriptive low-level design
	ADV_RCR.1	Informal correspondence demonstration
	ADV_SPM.1	Informal TOE security policy model
Guidance Documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Life Cycle Supports	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: low-level design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability assessment	AVA_MSU.2	Validation of analysis
	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.2	Independent vulnerability analysis

5.2.1 Configuration management

ACM_AUT.1 Partial CM automation

Dependencies :

ACM_CAP.3 Authorisation controls

Developer action elements :

146 ACM_AUT.1.1D The developer shall use a CM system.

147 ACM_AUT.1.2D The developer shall provide a CM plan.

Content and presentation of evidence elements :

148 ACM_AUT.1.1C The CM system shall provide an automated means by which only authorized changes are made to the TOE implementation representation.

149 ACM_AUT.1.2C The CM system shall provide an automated means to support the generation of the TOE.

150 ACM_AUT.1.3C The CM plan shall describe the automated tools used in the CM system.

151 ACM_AUT.1.4C The CM plan shall describe how the automated tools are used in the CM system.

Evaluator action elements :

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

ACM_CAP.4 Generation support and acceptance procedures

Dependencies :

ALC_DVS.1 Identification of security measures

Developer action elements :

153 ACM_CAP.4.1D The developer shall provide a reference for the TOE.

154 ACM_CAP.4.2D The developer shall use a CM system.

155 ACM_CAP.4.3D The developer shall provide CM documentation.

Content and presentation of evidence elements :

156 ACM_CAP.4.1C The reference for the TOE shall be unique to each version of the TOE.

157 ACM_CAP.4.2C The TOE shall be labelled with its reference.

158 ACM_CAP.4.3C The CM documentation shall include a configuration list, a CM plan, and an acceptance plan.

159 ACM_CAP.4.4C The configuration list shall uniquely identify all configuration items that comprise the TOE.

160 ACM_CAP.4.5C The configuration list shall describe the configuration items that comprise the TOE.

161 ACM_CAP.4.6C The CM documentation shall describe the method used to uniquely identify the configuration items that comprise the TOE.

162 ACM_CAP.4.7C The CM system shall uniquely identify all configuration items that comprise the TOE.

163 ACM_CAP.4.8C The CM plan shall describe how the CM system is used.

164 ACM_CAP.4.9C The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.

165 ACM_CAP.4.10C The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

166 ACM_CAP.4.11C The CM system shall provide measures such that only authorized changes are made to the configuration items.

167 ACM_CAP.4.12C The CM system shall support the generation of the TOE.

168 ACM_CAP.4.13C The acceptance plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

Evaluator action elements :

169 ACM_CAP.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ACM_SCP.2 Problem tracking CM coverage

Dependencies :

ACM_CAP.3 Authorisation controls

Developer action elements :

170 ACM_SCP.2.1D The developer shall provide a list of configuration items for the TOE.

Content and presentation of evidence elements :

171 ACM_SCP.2.1C The list of configuration items shall include the following: implementation representation; security flaws; and the evaluation evidence required by the assurance components in the ST.

Evaluator action elements :

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

5.2.2 Delivery and operation

ADO_DEL.2 Detection of modification

Dependencies :

ACM_CAP.3 Authorisation controls

Developer action elements:

173 ADO_DEL.2.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.

174 ADO_DEL.2.2D The developer shall use the delivery procedures.

Content and presentation of evidence elements :

175 ADO_DEL.2.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

176 ADO_DEL.2.2C The delivery documentation shall describe how the various procedures and technical measures provide for the detection of modifications, or any discrepancy between the developer's master copy and the version received at the user site.

177 ADO_DEL.2.3C The delivery documentation shall describe how the various procedures allow detection of attempts to masquerade as the developer, even in cases in which the developer has sent nothing to the user's site.

Evaluator action elements :

178 ADO_DEL.2.1E 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

Dependencies :

AGD_ADM.1 Administrator guidance

Developer action elements :

179 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 :

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

Evaluator action elements :

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

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

5.2.3 Development

ADV_FSP.2 Fully defined external interfaces

Dependencies :

ADV_RCR.1 Informal correspondence demonstration

Developer action elements :

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

Content and presentation of evidence elements :

184 ADV_FSP.2.1C The functional specification shall describe the TSF and its external interfaces using an informal style.

185 ADV_FSP.2.2C The functional specification shall be internally consistent.

186 ADV_FSP.2.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing complete details of all effects, exceptions and error messages.

187 ADV_FSP.2.4C The functional specification shall completely represent the TSF.

188 ADV_FSP.2.5C The functional specification shall include rationale that the TSF is completely represented.

Evaluator action elements :

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

190 ADV_FSP.2.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

ADV_HLD.2 Security enforcing high-level design

Dependencies :

ADV_FSP.1 Informal functional specification

ADV_RCR.1 Informal correspondence demonstration

Developer action elements :

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

Content and presentation of evidence elements :

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

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

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

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

196 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.

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

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

199 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.

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

Evaluator action elements :

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

202 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.

ADV_IMP.1 Subset of the implementation of the TSF

Dependencies :

ADV_LLD.1 Descriptive low-level design

ADV_RCR.1 Informal correspondence demonstration

ALC_TAT.1 Well-defined development tools

Developer action elements :

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

Content and presentation of evidence elements :

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

205 ADV_IMP.1.2C The implementation representation shall be internally consistent.

Evaluator action elements :

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

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

ADV_LLD.1 Descriptive low-level design

Dependencies :

ADV_HLD.2 Security enforcing high-level design

ADV_RCR.1 Informal correspondence demonstration

Developer action elements :

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

Content and presentation of evidence elements :

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

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

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

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

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

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

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

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

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

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

Evaluator action elements :

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

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

ADV_RCR.1 Informal correspondence demonstration

Dependencies :

No dependencies.

Developer action elements :

221 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 :

222 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 :

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

ADV_SPM.1 Informal TOE security policy model

Dependencies :

ADV_FSP.1 Informal functional specification

Developer action elements :

224 ADV_SPM.1.1D The developer shall provide a TSP model.

225 ADV_SPM.1.2D The developer shall demonstrate correspondence between the functional specification and the TSP model.

Content and presentation of evidence elements :

226 ADV_SPM.1.1C The TSP model shall be informal.

227 ADV_SPM.1.2C The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled.

228 ADV_SPM.1.3C The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled.

229 ADV_SPM.1.4C The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model.

Evaluator action elements :

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

5.2.4 Guidance documents

AGD_ADM.1 Administrator guidance

Dependencies :

ADV_FSP.1 Informal functional specification

Developer action elements :

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

Content and presentation of evidence elements :

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

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

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

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

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

237 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.

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

239 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 :

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

AGD_USR.1 User guidance

Dependencies :

ADV_FSP.1 Informal functional specification

Developer action elements :

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

Content and presentation of evidence elements :

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

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

244 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.

245 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 behaviour found in the statement of TOE security environment.

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

247 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 :

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

5.2.5 Life cycle support

ALC_DVS.1 Identification of security measures

Dependencies :

No dependencies.

Developer action elements :

249 ALC_DVS.1.1D The developer shall produce development security documentation.

Content and presentation of evidence elements :

250 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.

251 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 :

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

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

ALC_LCD.1 Developer defined life-cycle model

Dependencies :

No dependencies.

Developer action elements :

254 ALC_LCD.1.1D The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

255 ALC_LCD.1.2D The developer shall provide life-cycle definition documentation.

Content and presentation of evidence elements :

256 ALC_LCD.1.1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

257 ALC_LCD.1.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

Evaluator action elements :

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

ALC_TAT.1 Well-defined development tools

Dependencies :

ADV_IMP.1 Subset of the implementation of the TSF

Developer action elements :

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

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

Content and presentation of evidence elements :

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

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

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

Evaluator action elements :

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

5.2.6 Tests

ATE_COV.2 Analysis of coverage

Dependencies :

ADV_FSP.1 Informal functional specification

ATE_FUN.1 Functional testing

Developer action elements :

265 ATE_COV.2.1D The developer shall provide an analysis of the test coverage.

Content and presentation of evidence elements :

266 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.

267 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 :

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

ATE_DPT.1 Testing: high-level design

Dependencies :

ADV_HLD.1 Descriptive high-level design

ATE_FUN.1 Functional testing

Developer action elements :

269 ATE_DPT.1.1D The developer shall provide the analysis of the depth of testing.

Content and presentation of evidence elements :

270 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 :

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

ATE_FUN.1 Functional testing

Dependencies :

No dependencies.

Developer action elements :

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

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

Content and presentation of evidence elements :

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

275 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.

276 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.

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

278 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 :

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

ATE_IND.2 Independent testing - sample

Dependencies :

ADV_FSP.1 Informal functional specification

AGD_ADM.1 Administrator guidance

AGD_USR.1 User guidance

ATE_FUN.1 Functional testing

Developer action elements :

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

Content and presentation of evidence elements :

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

282 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 :

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

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

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

5.2.7 Vulnerability assessment

AVA_MSU.2 Validation of analysis

Dependencies :

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

ADV_FSP.1 Informal functional specification

AGD_ADM.1 Administrator guidance

AGD_USR.1 User guidance

Developer action elements :

286 AVA_MSU.2.1D The developer shall provide guidance documentation.

287 AVA_MSU.2.2D The developer shall document an analysis of the guidance documentation.

Content and presentation of evidence elements :

288 AVA_MSU.2.1C 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.

289 AVA_MSU.2.2C The guidance documentation shall be complete, clear, consistent and reasonable.

290 AVA_MSU.2.3C The guidance documentation shall list all assumptions about the intended environment.

291 AVA_MSU.2.4C The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

292 AVA_MSU.2.5C The analysis documentation shall demonstrate that the guidance documentation is complete.

Evaluator action elements :

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

294 AVA_MSU.2.2E The evaluator shall repeat all configuration and installation procedures, and other procedures selectively, to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.

295 AVA_MSU.2.3E The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

296 AVA_MSU.2.4E The evaluator shall confirm that the analysis documentation shows that guidance is provided for secure operation in all modes of operation of the TOE.

AVA_SOF.1 Strength of TOE security function evaluation

Dependencies :

ADV_FSP.1 Informal functional specification

ADV_HLD.1 Descriptive high-level design

Developer action elements :

297 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 :

298 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.

299 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 :

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

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

AVA_VLA.2 Independent vulnerability analysis

Dependencies :

ADV_FSP.1 Informal functional specification

ADV_HLD.2 Security enforcing high-level design

ADV_IMP.1 Subset of the implementation of the TSF

ADV_LLD.1 Descriptive low-level design

AGD_ADM.1 Administrator guidance

AGD_USR.1 User guidance

Developer action elements :

302 AVA_VLA.2.1D The developer shall perform a vulnerability analysis.

303 AVA_VLA.2.2D The developer shall provide vulnerability analysis documentation.

Content and presentation of evidence elements :

304 AVA_VLA.2.1C The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for ways in which a user can violate the TSP.

305 AVA_VLA.2.2C The vulnerability analysis documentation shall describe the disposition of identified vulnerabilities.

306 AVA_VLA.2.3C The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

307 AVA_VLA.2.4C The vulnerability analysis documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.

Evaluator action elements :

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

309 AVA_VLA.2.2E The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure the identified vulnerabilities have been addressed.

310 AVA_VLA.2.3E The evaluator shall perform an independent vulnerability analysis.

311 AVA_VLA.2.4E The evaluator shall perform independent penetration testing, based on the independent vulnerability analysis, to determine the exploitability of additional identified vulnerabilities in the intended environment.

312 AVA_VLA.2.5E The evaluator shall determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low attack potential.

Application Note : The obvious vulnerabilities are considered to be those that are open to the public on the Internet or those that are IPS, firewall or IDS. The developer shall perform the testing for getting the defensive measures. The evaluator shall examine the analysis on the vulnerability that is performed by the developer, and then, based on that evaluator shall perform the penetration testing and determine that the TOE is resistant to penetration attacks.

6. Protection Profile Application Notes:

313 This protection profile is ‘network intrusion prevention system protection profile’ and defines security requirements on the network intrusion prevention system to protect computer resources and internal network of organization.

314 This protection profile can be utilized as of the following. The product developers or the marketers may develop intrusion prevention system by observing all contents defined in this protection profile and the users may utilize the system for selection, operation and management of the product intended for use.

315 This protection profile includes the minimum security requirements and does not make definition on implementation model of the TOE. In relation to security problems possible to occur according to TOE implementation model, the developer shall define additional security environments, security objectives and security requirements. If the TOE is implemented by being dispersed on the network, the developer shall define additional security environments, security objectives and security requirements in the ST in order to protect the data transmitted among each component from external threats.

7. Rationale

316 This chapter describes security objectives defined on the basis of security environments (threats, assumptions and security policy of organization) and rationale of security requirements to satisfy the security objectives. Rationale demonstrates that TOE provides efficient IT security measures in TOE security environments.

7.1 Rationale of Security Objectives

317 Rationale of security objectives demonstrates that the specified security objectives are appropriate, sufficient to handle security problems and are essential, rather than excessive.

318 Rationale of security objectives demonstrates the following.

- Each assumption, threat and security policy of organization is handled by at least one security objective.
- Each security objective handles at least one assumption, threat and security policy of organization.

[Table 3] Security Environments and Security Objective Handling

Security Purpose Security Environment	TOE Security Objective									Security Objective for Environment						
	O.Availability	O.Audit	O.Management	O.TSF Data Protection	O.Abnormal Packet Cut-off	O.Avoiding Denial Of Service Attack	O.Identification	O.Authentication	O.Information Flow Control	OE.Physical Security	OE.Security Maintenance	OE.Trusted Administrator	OE.Safe Management	OE.Operating system Reinforcement	OE.Sole Connection	OE.Vulnerability List Renewal
A.Physical Security										X			X			
A.Security Maintenance											X					
A.Trusted Administrator												X				
A.Operating system Reinforcement														X		
A.Sole Connection															X	
T.Masquerade		X					X	X								
T.Breakdown	X			X									X	X		
T.Record Failure	X	X														
T.Illegal Information Inflow			X						X							
T.Illegal Service Access			X						X							
T.Abnormal Packet Transmission		X			X		X									
T.New Vulnerability Attack			X								X		X	X		X
T.Denial Of Service Attack		X				X	X									
T.Continuous Authentication Attempt		X					X	X								
T.Bypass Access	X								X	X					X	
T.Address Spoofing		X			X	X	X									
T.Unauthorized TSF Data Change	X	X		X			X									
TE.Administration Deficiency			X									X	X			
TE.Distribution and Installation												X	X			
P.Audit		X					X									
P.Safe Management			X									X	X			

7.1.1 Rationale of TOE Security Objective

O.Availability

319 This TOE security objective is to provide TOE availability in order for the minimum network service provision when TOE is in overload state due to attack by attacker or at occurrence of breakdown in TOE.

Therefore, this security objective assures TOE availability in response to T.Breakdown, T.TSF unauthorized data change, T.Threat to bypass access and T.Record failure, the threat to saturation in audit record storage capacity of TOE.

O.Audit

320 As for this TOE security objective, TOE records audit event per user according to audit record policy when user is using security function. Also, the TOE assures to provide the means of safely maintaining and reviewing the recorded audit events. In other words, the TOE provides handling function when audit data reaches saturation state. Audit record creation assures to detect identity of attacker through audit record in case continuous attempts for authentication are made. Spoofing attack, service denial attack and attack to produce and transmit abnormal packet can also be traced through audit record.

Therefore, this security objective handles T.Masquerade, T.Record failure, T. Abnormal packet transmission, T.Service denial attack, T.Continuous authentication attempt, T.Address spoofing and T.Unauthorized TSF data change through audit record and supports P.Audit on security policy of organization.

O.Management

321 In order to execute security policy, TOE sets rules of information flow control, therefore controls illegal access to internal network. For this, the TOE shall provide means to safely manage TOE and TSF data, such as on TOE configuration data creation and management as well as the newest vulnerability signature management, etc.

Therefore, this TOE security objective supports P. Safe management on security policy of organization as it handles T.Illegal information inflow, T.Illegal service access, T. New vulnerability attack, TE.Management deficiency and provides means for the authorized administrator to safely manage TOE.

O.TSF Data Protection

322 Due to unexpected attack from the outside or occurrence of breakdown in TOE, TSF data can be changed beyond recognition by administrator. Therefore it may be impossible to appropriately execute security policy. For this, normal functioning of

TSF shall be assured by ensuring integrity of TSF data after inspecting whether TOE, TSF data changes occurred intentionally or unintentionally.

Therefore, this security objective handles the threats of T.Breakdown and T. Unauthorized TSF data change.

O.Abnormal Packet Cut-off

323 This security objective guarantees for packets not suitable for TCP/IP standard among numerous packets flown from external network into internal network, packets holding address of internal network among packet flown from external network, broadcasting packets and looping packets, etc., to be flown into internal network.

Therefore, this TOE security objective handles threats of T.Abnormal packet transmission and T.Address spoofing.

O.Avoiding Denial Of Service Attack

324 Attacker can execute network service denial attack to internal network computer by passing through the TOE. The representative network service denial attack is for a remote user to exhaust computer resources by making abnormally large service requests to internal computer. In this case, internal computer allocates a large amount of resources to attacker, therefore interrupts normal user from using computer. In preparation to this case, TOE prevents specific user from holding exclusive ownership of specific computer resources, therefore assures computer use by normal user.

Therefore, this security objective handles threats of T.Service denial attack and T. Address spoofing.

O.Identification

325 Users to use TOE are divided into administrator who manages TOE by connecting to TOE with authentication and external user (IT entity) passing through the TOE without authentication simply to use computer of internal network. Two of the above cases require the function of identification to process security-related events. Administrator identification function is required because responsibilities are given to all acts used by administrator. External IT identification is necessary for abnormal packet transmission, avoiding service denial attack, avoiding address spoofing attack and creating audit record on attempts of connection to external IT.

Therefore, this TOE security objective handles threats of T. Masquerade, T.Service denial attack, T.Address spoofing, T.Abnormal packet transmission, T.Continuous authentication attempt and T.Unauthorized TSF data change and supports P.Audit.

O.Authentication

326 User intending to access TOE shall obtain authentication. However, authentication required at access to TOE can be vulnerable to the attack of continuous authentication attempt by outside attacker. Therefore, TOE shall assure authentication mechanism to endure the attack of continuous authentication attempt to suit the level of external attacker. So, this security objective handles the attack of T.Masquerade and T. Continuous authentication attempt.

O.Information Flow Control

327 TOE controls information flow according to security policy by being installed at the point where internal and external networks are separated. This security objective assures identifying and avoiding diverse attacks possible to occur in network according to deny and allow policies. Diverse attacks in network refer to virus attack, e-mail or web service including illegal information and access to service that is not allowed.

The TOE ensures security of internal network by controlling these attacks and preventing them from being flown into internal network according to the set rules.

Therefore, security objective handles threats of T.Illegal information inflow, T.Illegal service access and T.Bypass access.

7.1.2 Rationale of Security Objective for the Environments

OE.Physical Security

328 This security objective for environments guarantees for TOE to be located and operated in physically safe place. Therefore, since defense is made against physical violation attack and TOE change attempt, this security objective supports assumption of A.Physical security and handles threat of T.Bypass access.

OE.Security Maintenance

329 When internal network environment changes due to change in internal network configuration, increase/decrease of host and increase/decrease of service, etc., this security objective for environments guarantees to immediately reflect the changed environment and security policy to operation policy, therefore to maintain security in the same level as before. Therefore, this security objective is required to support assumption of A.Security Maintenance and to handle threat of T.New vulnerability attack.

OE.Trusted Administrator

330 This security objective for environments guarantees that the authorized administrator of TOE can be trusted. Therefore, this is required to support assumption of A.Trusted

administrator and P. Safe management and to handle threats of TE.Management deficiency and TE.Distribution and installation.

OE.Safe Management

331 This security objective for environments guarantees for TOE to be distributed and installed in the safe method and to be configured, managed and used in the safe method by authorized administrator. Therefore, this security objective handles threats of T.Breakdown, T.New vulnerability attack, TE.Management deficiency and TE. Distribution and installation and supports assumption of A.Physical security, security policy of organization and P.Safe management.

OE.Operating system Reinforcement

332 This security objective for environments guarantees for operating system to be safe and trusted by executing operation to eliminate services or means in operating system not required by TOE and reinforcement on vulnerabilities of operating system. Therefore, this security objective is required to support assumption of A. Operating system reinforcement and to handle threats of T.Breakdown and T.New vulnerability attack.

OE.Sole Connection

333 This security objective for environments guarantees for all communications between external and internal networks to take place through the TOE. Therefore, this security objective handles threat of T.Bypass access and supports assumption of A.Sole connection.

OE.Vulnerability List Renewal

334 This security objective for environments guarantees renewal and management of database in relation to vulnerabilities managed by TOE in order for protection against external attack using new vulnerability of TOE and internal network resources protected by the TOE. Therefore, this security objective handles threat of T.New vulnerability attack.

7.2 Rationale of Security Requirements

335 Rational of security requirements demonstrate that the described IT security requirements are suitable to satisfy security objectives and, as a result, appropriate to handle security problems.

7.2.1 Rationale of TOE Security Functional Requirements

336 Rationale of TOE security functional requirements demonstrates the followings.

- Each TOE security objective is handled by at least one TOE security functional requirements.
- Each TOE security functional requirements handle at least one TOE security objective.

[Table 4] Security Objective and Security Functional Requirements Handling

Security Purpose Security Functional Requirements	O. Availability	O. Audit	O. Management	O.TSF Data Protection	O.Abnormal Packet Cutoff	O.Avoiding Denial Of Service Attack	O. Identification	O.Authentication	O.Information Flow Control
FAU_ARP.1		X							
FAU_GEN.1		X							
FAU_GEN.2		X							
FAU_SAA.1		X							
FAU_SAR.1		X							
FAU_SAR.3		X							
FAU_SEL.1		X							
FAU_STG.1		X							
FAU_STG.3		X							
FAU_STG.4		X							
FDP_IFC.1(1)									X
FDP_IFC.1(2)									X
FDP_IFF.1					X				X
FIA_AFL.1								X	
FIA_ATD.1(1)		X			X	X	X		X
FIA_ATD.1(2)		X					X		
FIA_UAU.1			X	X				X	
FIA_UAU.7								X	
FIA_UID.2(1)		X			X	X	X		X
FIA_UID.2(2)		X	X	X			X		
FMT_MOF.1	X		X						
FMT_MSA.1			X	X					X
FMT_MSA.3			X	X					X
FMT_MTD.1			X	X					
FMT_MTD.2	X		X						
FMT_SMF.1			X						
FMT_SMR.1			X				X	X	
FPT_AMT.1	X			X					
FPT_FLS.1	X								X
FPT_RVM.1									X
FPT_SEP.1				X					X
FPT_STM.1		X							

FPT_TST.1	X			X					
FRU_FLT.1	X								X
FRU_RSA.1						X			
FTA_SSL.1				X					
FTA_SSL.3						X			
FTP_ITC.1			X	X					

FAU_ARP.1 Security Alarms

337 This component ensures handling ability in the event of detecting security violation, therefore satisfies TOE security objective of O.Audit.

FAU_GEN.1 Audit Data Generation

338 This component ensures the ability to define event for audit and to generate audit record, therefore satisfies TOE security objective of O.Audit.

FAU-GEN.2 User Identity Association

339 This component requires user identification in order to define incident for audit and to trace association of audit record to user, therefore satisfies TOE security objective of O. Audit.

FAU_SAA.1 Potential Violation Analysis

340 This component ensures the ability to point out security violation by inspecting the audited incident, therefore satisfies TOE security objective of O.Audit.

FAU_SAR.1 Audit Review

341 This component ensures the ability of authorized administrator to review audit record, therefore satisfies TOE security objective of O.Audit.

FAU_SAR.3 Selectable Audit Review

342 This component ensures the ability to search and sort audit records by bases to hold logical relations, therefore satisfies TOE security objective of O.Audit.

FAU_SEL.1 Selective Audit

343 This component ensures the ability to include or exclude incidents for audit on the basis of attributes, therefore satisfies TOE security objective of O.Audit.

FAU_STG.1 Protected Audit Trail Storage

344 This component ensures the ability to protect audit record from unauthorized modification and deletion, therefore satisfies TOE security objective of O.Audit.

FAU_STG.3 Action In Case Of Possible Audit Data Loss

345 This component ensures handling ability in the event audit trail exceeds the pre-defined limit, therefore satisfies TOE security objective of O.Audit.

FAU_STG.4 Prevention of Audit Data Loss

346 This component ensures handling ability in the event audit storage is full, therefore satisfies TOE security objective of O.Audit.

FDP_IFC.1(1) Subset Information Flow Control (1)

347 This component ensures that security policy for TOE information flow control is defined and that scope of security policy is defined, therefore satisfies TOE security objective of O.Information flow control.

FDP_IFC.1(2) Subset Information Flow Control (2)

348 This component ensures that security policy for TOE information flow control is defined and that scope of security policy is defined, therefore satisfies TOE security objective of O.Information flow control.

FDP_IFF.1 Simple Security Attributes

349 This component describes the function to handle explicit attacks, therefore satisfies security objective of O.Abnormal packet cut-off.

FIA_AFL.1 Authentication Failure Handling

350 This component ensures the ability to define the count of authentication attempt failure by user and to take handling actions when the defined count is reached or exceeded, therefore satisfies TOE security objective of O.Authentication.

FIA_ATD.1(1) User Attribute Definition (1)

351 This component requires identifying the identifier for external IT entity with computer IP address. IP address generates audit records by identifying external IT entity. Also, it serves as the basis to assess whether the address has been spoofed and as the basis when determining denial of service attack and information flow control. Therefore, it

satisfies O.Audit, O.Abnormal packet cut-off, O.Avoiding denial of service attack, O. Identification and O.Information flow control.

FIA_ATD.1(2) User Attribute Definition (2)

352 This component requires identification on administrator, therefore satisfies O.Audit and O.Identification.

FIA_UAU.1 Timing Of Authentication

353 This component ensures the ability to successfully authorize administrator, therefore satisfies TOE security objectives of O.Management, O.TSF data protection (Add: Because TOE management and TSF data protection functions are possible when administrator is authorized) and O.Authentication.

AFIA_UAU.7 Protected authentication Feedback

354 This component ensures that only the designated authentication feedback is provided to administrator while authentication is in progress, therefore satisfies TOE security objective of O.Authentication.

FIA_UID.2(1) User Identification before any action (1)

355 This component requires identifying identifier for external IT entity with computer IP address. IP address generates audit records by identifying external IT entity. Also, it serves as the basis to assess whether the address has been spoofed and as the basis when determining denial of service attack and information flow control. Therefore, it satisfies O.Audit, O.Abnormal packet cut-off, O.Avoiding denial of service attack, O. Identification and O.Information flow control.

FIA_UID.2(2) User Identification before any action (2)

356 This component requires identification on administrator, therefore satisfies O. Audit, O. Management, O.TSF data protection and O.Identification.

FMT_MOF.1 Security Function Management

357 This component ensures the ability for authorized administrator to manage security function and availability in the event of TOE breakdown, therefore satisfies TOE security objectives of O.Availability and O.Management.

FMT_MSA.1 Management of Security Attributes

358 This component ensures that security attribute data, the TSF data necessary in executing TOE security function, can be accessed only by authorized administrator, therefore satisfies TOE security objectives of O.Management, O.TSF data protection and O.Information flow control.

FMT_MSA.3 Static Attribute Initialization

359 This component ensures that security attribute data, the TSF data necessary in executing TOE security function, can be accessed only by authorized administrator at security attribute initialization, therefore satisfies TOE security objectives of O. Management, O.TSF data protection and O.Information flow control.

FMT_MTD.1 Management of TSF Data

360 This component requires the function for authorized administrator to manage TSF data, therefore satisfies TOE security objectives of O.Management and O.TSF data protection.

FMT_MTD.2 TSF Data Limit Management

361 This component ensures important availability of TOE by guaranteeing for authorized administrator to manage limits of TSF data and to take handling actions when the designed limits are reached or exceeded, therefore satisfies TOE security objectives of O.Availability and O.Management.

FMT_SMF.1 Specification of Management Function

362 This component requires to specify management functions, such as security attributes, TSF data and security functions, etc., to be provided by TSF, therefore satisfies O.Management.

FMT_SMR.1 Role of Security

363 This component requires the role of TOE security administrator to be limited to the role of administrator, therefore satisfies TOE security objectives of O.Management, O.Identification and O.Authentication.

FPT_AMT.1 Abstract Machine Test

364 This component is to execute a series of tests to show accurate operation of abstract machine at the lower level of TSF, therefore satisfies TOE security objectives of O. Availability and O.TSF data protection.

FPT_FLS.1 Fail Secure when It Needs Troubleshooting

365 This component ensures for TOE to maintain safe status for core security function operation and to execute information flow control function even during breakdown, therefore satisfies TOE security objectives of O.Availability and O.Information flow control.

FPT_RVM.1 TSP Bypass Impossibility

366 This component prevents bypass of information flow control by guaranteeing that the function to execute TSP is invoked and succeeded, therefore satisfies TOE security objective of O.Information flow control.

FPT_SEP.1 TSF domain separation

367 This component ensures for TSF to maintain security fields for self-execution from unauthorized entity, therefore satisfies TOE security objectives of O. TSF data protection and O.Information flow control.

FPT_STM.1 Reliable Time Stamp

368 This component provides reliable time stamp used by TSF. The created time ensures to record sequential security audit events at creation of audit record, therefore satisfies TOE security objective of O.Audit.

FPT_TST.1 Self-test of TSF

369 This component requires the function to assure self-test of TSF for accurate operation and to prevent or promptly detect breakdown of TOE as authorized administrator verifies integrity of TSF data and TSF execution code, therefore satisfies TOE security objectives of O.Availability and O.TSF data protection.

FRU_FLT.1 Fault Tolerance: Partial application

370 This component requires operation of core security function and ensures execution of information flow control function even during breakdown of TOE, therefore satisfies TOE security objectives of O.Availability and O.Information flow control.

FRU_RSA.1 Maximum Assignment

371 This component avoids service denial attack by requiring the function to limit resource use assignment in relation to TOE protection assets per user, therefore satisfies TOE security objective of O.Avoiding service denial attack.

FTA_SSL.1 Session Locking by TSF

372 This component requires the function for TOE to lock the authorized session after non-active period of authorized administrator, therefore satisfies security objective of O. TSF data protection.

FTA_SSL.3 Session Ending by TSF

373 This component requires for external IT entity to end session with internal computer after the prescribed time, therefore satisfies the purpose of O.Avoiding service denial attack as it functions to secure network service availability.

FTP_ITC.1 Trusted Channel between TSF

374 This component requires to form trusted channel in the event administrator manages TOE locally or remotely, or at communication between TOE external vulnerability data servers, therefore satisfies O.Management and O.Authentication to require prohibition of TOE access by unauthorized user and O.TSF data protection as TSF data are protected.

7.2.2 Rationale of TOE Security Assurance Requirements

375 EAL4 security assurance requirements are guarantee package to require systematic design, test and review. Also, EAL4 level, as the highest guarantee level required in commercial development stages, provides methodology capable to most certainly realize the requirements. In most cases, intrusion prevention system is being commercially developed and sold. From the perspective of defending network of organization or environment of use, EAL4 level is appropriate to require partial, but automated configuration management system and safe distribution, etc.

7.3 Rationale of Dependency

7.3.1 Dependency of TOE Security Functional Requirements

376 [Table 5] shows dependency of functional components.

377 FAU_GEN.2, FIA_UAU.1 and FMT_SMR.1 hold dependency to FIA_UID.1. However, this is satisfied by FIA_UID.2, which is in hierarchical relationship with FIA_UID.1.

[Table 5] Dependencies of Functional Components for the TOE

No.	Functional Components	Dependencies	Ref. No.
1	FAU_ARP.1	FAU_SAA.1	4
2	FAU_GEN.1	FPT_STM.1	29
3	FAU_GEN.2	FAU_GEN.1 FIA_UID.1	2 17
4	FAU_SAA.1	FAU_GEN.1	2
5	FAU_SAR.1	FAU_GEN.1	2
6	FAU_SAR.3	FAU_SAR.1	5
7	FAU_SEL.1	FAU_GEN.1 FMT_MTD.1	2 21
8	FAU_STG.1	FAU_GEN.1	2
9	FAU_STG.3	FAU_STG.1	8
10	FAU_STG.4	FAU_STG.1	8
11	FDP_IFC.1	FDP_IFF.1	12
12	FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	11 20
13	FIA_AFL.1	FIA_UAU.1	15
14	FIA_ATD.1	-	-
15	FIA_UAU.1	FIA_UID.1	17
16	FIA_UAU.7	FIA_UAU.1	15
17	FIA_UID.2	-	-
18	FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	23 24
19	FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMF.1 FMT_SMR.1	11 23 24
20	FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	19 24
21	FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	23 24

22	FMT_MTD.2	FMT_MTD.1 FMT_SMR.1	21 24
23	FMT_SMF.1	-	-
24	FMT_SMR.1	FIA_UID.1	17
25	FPT_AMT.1	-	-
26	FPT_FLS.1	ADV_SPM.1	Security Assurance Requirements
27	FPT_RVM.1	-	-
28	FPT_SEP.1	-	-
29	FPT_STM.1	-	-
30	FPT_TST.1	FPT_AMT.1	25
31	FRU_FLT.1	FPT_FLS.1	26
32	FRU_RSA.1	-	-
33	FTA_SSL.1	FIA_UAU.1	15
34	FTA_SSL.3	-	-
35	FTP_ITC.1	-	-

7.3.2 Dependency of TOE Security Assurance Requirements

378 Dependency of each guarantee package provided in information protection system CC is being satisfied.

7.4 Rationale of Strength of Function(SOF)

379 Assets to be provided by TOE of this protection profile are computer resources and services of organization as well as information stored in computer. Threat agents is considered to have low level of expertise, resources and motivation. In common evaluation methodology[1], security function strength for attack success possibility is recommended to be low or higher. In case of administrator accessing TOE installed and operated in internal network, outside access for administrator authentication is possible. Therefore, strength of function was selected as medium.

[1] Appendix A.8 of Common Methodology for Information Technology Security Evaluation 2.3 defines the method to calculate attack success possibility by attacker and the minimum strength of function recommended on the basis of attack success possibility.

(This page left blank on purpose for double-side printing)

REFERENCES

[1] Common Methodology for Information Technology Security Evaluation 2.3, August 2005, CCMB

[2] ISO/IEC TR 15446:2004, Guide for the production of Protection Profiles and Security Targets

[3] U.S. Department of Defense Firewall Protection Profile for Basic Robustness Environments Version 0.6a, September 2001

[4] U.S. Department of Defense Application-level Firewall Protection Profile for Medium Robustness Environments Version 1.0, June 28, 2000

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

[6] U.S. Department of Defense Traffic-Filter Firewall Protection Profile for Medium Robustness Environments Version 1.4, May 1, 2000

[7] U.S. Government Application-level Firewall Protection Profile for Low-Risk Robustness Environments Version 1.d, July 20, 1999

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

[9] Information Assurance Technical Framework Release 3.0, National Security Agency, September 1999

ACRONYMS

CC	Common Criteria
EAL	Evaluation Assurance Level
IT	Information Technology
PP	Protection Profile
RFC	Request for Comments
SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSC	TOE Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy