EXSHIELD V1.0.1.R

Security Target

Version 1.10

SECUI

Revision History

ST_eXshield V1.0.1.R_V1.10.doc		
Revision	**Date**	**Description**
V1.10	2008.05.09	✓ "1.2. ST overview" corrected ✓ "2.1. Product type and configuration" corrected ✓ "2.2. TOE scope" corrected ✓ "4.1. Security objectives for the TOE" corrected ✓ "4.2. Security objectives for the environment" corrected ✓ "5.1.1. TOE security functional requirements" corrected ✓ "5.1.2. TOE security assurance requirements" corrected ✓ "6. TOE summary specification" corrected ✓ "7.2. PP tailoring" corrected ✓ "8.1. Security objectives rationale" corrected ✓ "8.2. Security requirements rationale" corrected ✓ "8. Rationale" corrected → All are detailed in the ST V1.10
V1.9	2008.04.07	✓ "1.2. ST overview" corrected ✓ "6.1.1.1. Audit generation and protection" → Action in case of the log server file system exhaustion corrected
V1.8	2008.03.25	✓ "Report" function deleted ✓ "VPN" function deleted ✓ "V1.7 Non-official modification" reflected
V1.7	2008.02.25	✓ "Report" function that processes statistics of audit data deleted - "5.1.1.4.3 FMT_MTD Management of TSF data" → Processing statistics of audit data deleted - "6.1.1.2 Audit review (Audit_Review)" → Content related to Report function deleted - "6.1.4.3.1 Restriction of TSF data management to an authorized administrator" → Processing statistics of audit data deleted ✓ "5.1.1.5.1 FPT_AMT Underlying abstract machine test" → "periodically during normal operation" deleted from the selection options in FPT_AMT.1.1 ✓ "6.1.5.2 Security function stability self test (Secui_Self_Test)" →

		"periodically during normal operation" deleted in accordance with FPT_AMT.1.1
V1.6	2008.02.20	✓ Correction according to EOR-06 (Refer to EOR-06_ST for details)
V1.5	2008.01.07	✓ Correction according to EOR-03 (Refer to EOR-03_Corrections for details) ✓ Correction according to ST_V1.4(Unofficial corrections) (Refer to ST_V1.4(Unofficial corrections) for details)
V1.4	2007.11.26	✓ "1.5. Terminology → "Administrator console" deleted, "authorized administrator" and "authorized user" are united to "authorized administrator" ✓ "2.2.1. Physical boundaries and scope" → Identification of TOE_Gateway and TOE_LServer clarified ✓ "3.2.2. Threats to the operational environment → TE.Data added; TE.TOEtime and TE.TSFdata corrected according to the threat ✓ "FAU_SAR.3 Selectable audit review" → Rules for an assignment operation corrected for clarity ✓ "FAU_STG.3 Action in case of possible audit data loss" → Content modified to "a value from 1 through 100% (by default 99%) that may changed by the authorized administrator" ✓ "FCS_CKM.1 Cryptographic key generation" → Standard cryptographic algorithm specified: 3DES, AES ✓ "FDP_ACC.2 Complete access control" → "TSF data" corrected to "all TSF data" in b) ✓ "FDP_ACF.1 Security attribute based access control" → Forbidding a double connection with an authorized administrator's ID clarified further in FDP_ACF.1.4 ✓ "FDP_IFF.1 Simple security attributes" → Rules separated into allow-all policy, deny-all policy, and VPN rules ✓ "FIA_ATD.1(1) User attribute definition(1)" → "Security level" added ✓ "FMT_MOF.1 Management of security functions behavior" → Overlap with FMT_MTD.1 deleted ✓ "FMT_MSA.1 Management of security attributes → TSF data and TSF executable file deleted from administrator access control policy ✓ "FPT_TST.1 TSF testing" → "TSF data" corrected to "TSF data

		except for the audit records”
V1.3	2007.11.21	✓ Correction according to EOR-1 (Refer to EOR-01_Corrections for detail)
V1.2	2007.10.12	✓ “2.2. TOE scope” → Descriptions about the physical boundaries and scope, logical boundaries and scope, and non-TOE scope added. ✓ “6.1.5. TSF stability” → Separate the inter-TSF trusted path and the protected objects by the TSF.
V1.1	2007.10.08	✓ Changed functions updated
V1.0	2007.01.30	✓ Register a draft

Table of Contents

List of Figures

List of Tables

1. ST Introduction

This document describes the functionality and scope of eXshield V1.0.1.R provided by SECUI.com Corp. and presents the environment, security objectives, and security requirements of the TOE, the TOE summary specification, protection profile claim, and rationale.

The TOE described in this ST refers to an intrusion prevention system that protects the network and DMZ from illicit intrusion or attack launched from outside.

1.1. ST identification

File name	ST_eXshield V1.0.1.R_V1.10.doc
Title	eXshield V1.0.1.R Security Target Version 1.10
Document history	Refer to Revision History
Author	Nanyoung Kim, Mihyun Chang / Technical planning team, Technology department, SECUI.com Corp.
Date	19 May 2008
Evaluation Criteria	Common Criteria for Information Technology Security Evaluation (CC, Notification no.2005-25 by the MIC)
CC identification	Common Criteria V2.3
Protection profile	Network intrusion prevention system protection profile V1.1
EAL	EAL4
TOE name	eXshield V1.0.1.R
Product name	eXshield Security Switch V1.0
Product type	Intrusion prevention system
Keyword	Intrusion prevention system, IPS, security target, ST
Evaluation facility	Korea System Assurance, Inc.
Certification body	IT Security Certification Center, National Intelligence Service

1.2. ST overview

This ST gives a specification of the security functions of eXshield V1.0.1.R, which is an intrusion prevention system that detects and blocks possible intrusion so that it protects the assets within the network.

eXshield V1.0.1.R locates on the point that connects the Internet and the internal network or the point that separates the internal network and external network in a router or in-line type. It performs, for all packets sent from the Internet to the internal network, detection of, protection from, and blocking(F/W) of the inflow of malicious traffic and protection of the assets and resources of the internal network from DDoS attack, Flooding attack, and Smurf attack.

1.2.1. eXshield V1.0.1.R specifications

Security audit

Being located on the network contacts, eXshield V1.0.1.R records every log on the passing packets and the start-up and termination of all processes. It gives an alarm in the case of exceeded audit storage. It can make audit records selectively by the administrator and refer to the records easily with user-friendly GUI.

Identification and authentication

Only an authorized administrator can access the TOE by establishing an administrator account. The TOE identifies the administrator by the ID and authenticates using password or OTP. It locks administrator session after a specific interval of inactivity and requires re-authentication.

User data protection

This is the main part of the TOE security functions, as it performs administrator access control, packet filtering, intrusion prevention, network address translation, network traffic control, etc. Administrator access control is that the TOE controls access of the administrator (the access subject) to the TSF data or TSF executable file (the object) based on the administrator's security attributes – administrator authentication data, IP address, or access level. After identifying a user (access subject), the TOE enforces packet filtering discretionary information flow control based on the IP address, Port, protocol, and Flag information of the user (source) and information (destination). Intrusion prevention is to detect illicit access to or attack on the network or assets that are protected by the TOE. Network

address translation allows the customers, when they want to hide the internal IP address, to set up the internal IPs as private and use public IP to access the external network using the NAT function provided by the TOE. Network traffic control defines the maximum quotas for resource utilization by network traffic so that the traffic is limited to the defined bandwidth in accordance with the policy of packet filtering.

Security management

This provides function to determine, disable, enable, and modify the behavior of security function and supports providing the ability to change default of, query, delete, and generate the security attributes used in access control and information flow control only for the authorized administrator. The TSF data can be the subject of query, modification, deletion, generation, and backup to a semi-permanent auxiliary memory. The TSF maintains the role of authorized administrator.

TSF stability

This supports the operation of the TOE as it performs HA function, self-testing of the stability of the security functions, TSF protection, and process monitoring. HA function ensures high availability by sending traffic to the Slave TOE when the Master TOE is not able to operate. Self-testing of the stability of the security functions performs integrity check on the TSF data and executable code and supports an action to be taken on impairment. TSF protection ensures that all traffic inside and outside must pass the TOE first to communicate with the external network. Process monitoring checks the operation of the application-level process acting in the TOE and re-starts the abnormally terminate process; this makes the management functions set by the administrator not to be stopped due to errors but to provide constant service.

1.3. ST contents

This document comprises the following contents:

Chapter 1 ST introduction identifies this document and the TOE, summarizes the whole contents of this document, and identifies the CC to which this ST claims conformance.
Chapter 2 TOE description describes the scope, boundaries, and functions of the TOE.
Chapter 3 TOE security environment identifies and describes the intended usage of the TOE, the assumptions about the environment, the threats to the assets that shall be protected by the TOE or its environment, and the organizational security policies with which the TOE must comply.
Chapter 4 Security objectives describes the security objectives for the TOE and its environment that shall counter the identified threats and cover the identified organizational security policies (OSPs) and assumptions.
Chapter 5 IT security requirements describes the security functional requirements and the security assurance requirements that need to be satisfied in order to meet the security objectives.
Chapter 6 TOE summary specification describes the IT security functions and assurance measures of the TOE.
Chapter 7 PP claims describes the protection profile to which this ST claims conformance with.
Chapter 8 Rationale demonstrates that the security objectives are suitable to cover the assumptions, threats, and OSPs; that the IT security requirements are suitable to meet the security objectives; and that the TOE IT security functions are suitable to satisfy the TOE security functional requirements.

1.4. CC conformance

The TOE addressed in this ST conforms to the following standards:

- Common Criteria for Information Technology Security Evaluation (CC, Notification no.2005-25 by the MIC)
- CC V2.3
- CC Part 2 conformant
- CC Part 3 comformant
- Assurance level: EAL4
- PP claimed: Network intrusion prevention system protection profile V1.1

1.5. Terminology

A

Access Control

Monitoring and controlling access to the assets of information system. Protects against unallowed or inappropriate access and monitors an access policy.

Administrator console

Administers the TOE; the GUI administrator console that is accessible using Java and the CLI administrator console that can directly be connected to the TOE using the serial port of eXshield Security Switch V1.0.

Assets

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

Assignment

One of the CC operations; the specification of an identified parameter in a component.

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.

Augmentation

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

Authorized Administrator

An authorized user that operates and administers TOE_Gateway and TOE_LServer in accordance with the TOE security policy.

Authentication Data

Information used to verify the claimed identity of a user.

C

Class

A grouping of families that share a common focus.

Component

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

Common Criteria for Information Technolocy Security Evaluation (CC)

The common criteria (CC) is meant to be used as the basis for evaluation of security properties of IT products and systems. It comprises existing criteria from different countries

to develop criteria that can be accepted and applied everywhere with a common language and understanding. The CC was translated into Korean and announced by the Minister of Information and Communication.

D

Dependency

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

E

Element

An indivisible security requirement.

Evaluation Assurance Level (EAL)

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

External IT Entity

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

F

Family

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

H

Hash

Transformation of a variable-length data block or message into a unique fixed-length one, which is the hash value.

HA (High Availability)

A property that protects applications from any error of CPU, hard disk, and network components and secures continuous services of the applications and the operational environment. This also means a service stop will be recovered as soon as possible.

Host

Host means, in the Internet, a computer that provides interactive communication with another through the Internet; In IBM or other main frame computer environment, a main frame computer.

Human User

Any person who interacts with the TOE.

I

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.

Identification and authentication

A security procedures to confirm a terminal log-on information in a Multi-user computer system or network operating system.

IETF (Internet Engineering Task Force)

An open organization under the Internet Architecture Board (IAB) of network designers, operators, researchers, and vendors that aims to solve issues regarding the operation, management, and technology of the Internet.

Information Flow Control

Applying security policies on the TSF data based on the security attributes of information and subject that caused an information flow.

Integrity

A property that intends to protect information or assets from illicit modification.

Internal IT entity

Any IT product or system, untrusted or trusted, within the internal networked environment of the TOE that interacts with the TOE.

Internet

The world's biggest computer communication network; network of networks; began with a local area network (LAN) that connects small networks, now it is a collection of huge networks all over the world.

Intrusion Detection

A function to detect an intrusion that threatens the security of information system.

Iteration

One of the CC operations; the use of a component more than once with varying operations.

J

Java

An object-oriented programming language developed by Sun Microsystems, US.

K

Kernel

The central part of operating systems, which is in the main memory. It comprises special processes for handling the initialization and interrupt of the system, the process monitors, the exchange of environment between processes, and the modules that create a new process.

KLSM

A security subsystem that is implemented into the IP Layer among network stacks and processes input/output of packets. Performs validity check, access control, and intrusion detection of the packets imported through the Physical Layer or Application Layer.

L

LINUX

An operating system made by Linus Tovalds in 1991 such that Unix, which used to be operating on bigger machines, has been made operatable on 386 PC.

M

Malicious traffic

Accesses without authority, any network packet whose structure is not in a normal state, a packet that exploits using a computer worm or virus, and a packet that compromises the availability of the internal resources of a computer.

Message Authentication Code (MAC)

A certain value or part that is sent with a message to authenticate the validity of attributes of the message such as the content, author, source, etc.

N

NAT (Network Address Translation)

A technique of exchanging a specific address of a company and a public IP address, which makes it possible to access the Internet from a node to which a specific address is not assigned.

O

Object

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

Operation

Specifying a component of the CC to counter a specific threat or satisfy a specific security policy; iteration, assignment, selection, and refinement.

Operating System (OS)

A software or global control program that works and operates a computer so that a user's application can be executed effectively. The OS is a program that will be loaded first into a computer upon its start-up, the kernel of which will be in the main storage area.

Organizational Security Policies (OSP)

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

P

Packet

A block of data used for data transmission.

Protected systems

Assets protected by the security policies of an intrusion prevention system (IPS). In the case of a network-based IPS the protected system is the network services or resources; in the case of a host-based IPS it's the resources or information stored in the host.

Protection Profile (PP)

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

R

Refinement

One of the CC operations; the addition of details to a requirement.

Role

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

S

SECUI Update Server

This server under the in-house management of SECUI does update of IPS Signature list and ICEC list.

Security Target (ST)

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

Selection

One of the CC operations; the specification of one or more items from a list in a component.

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.

SSL (Secure Socket Layer)

A standard protocol that provides secure transmission of data between www browser and www server.

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.

Subject

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

T

Target of Evaluation (TOE)

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

TCP/IP

Combination of TCP and IP; Communication protocol among computers developed by the DoD; TCP/IP is currently being used on the Internet. After the unification of the communication protocol, information may be sent to or received from any kind of computer in any place in the world.

Treat Agent

An unauthorized user or external IT entity that causes threats to assets such as illicit access, modification, or deletion.

TOE Security Function (TSF)

A set consisting of all hardware, software, and installation images 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 distributes 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.

U

UNIX

An operation system for multi users developed by Bell Laboratories in order to make environment for research and development of programming.

URI

Abbreviation of Uniform Resource Identifier; a unified identifier of information and resources on the Internet, which is used to identify text, video, sound, still or animation image. The most common form of URI is a web page address that tells, for example, all resources access mechanisms, computer that possesses resource, or resource name.

URL

A standardized logical address to show resources, such as files or news group, on the Internet; Comprises a protocol to be used (e.g. http, ftp, etc.), name and address of the main computer, the location of directory that stores a file, and the file name.

User

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

V

Virtual IP address

An address that, though not existing on a computer, is assumed to be on a program.

1.6. Conventions

This document uses both Korean and English for some abbreviations or to communicate a clear meaning. Notations, forms, and conventions used conform to the Common Criteria for Information Technology Security Evaluation.

Permitted operation on the security functional requirements in the CC are iteration, assignment, selection, and iteration. All of them are used in this ST.

Iteration

The use of a component more than once with varying operations. The result of iteration operation is marked by adding a figure in a parenthesis, (the number of iteration), next to the component identified.

Selection

The specification of one or more items from a list in a component. The result is marked by *underlined italics*.

Refinement

The addition of details to a requirement, thus further limiting it. The result is marked by **bold letters**.

Assignment

The specification of a parameter, for example a password length. The result is marked with the value in a square bracket.

ST author

The operations written as { Decided by the ST author } in the PP is performed by the ST author to be specified as { assignment_value } in the ST.

Additions by the ST author

The ST author can add items other than what is included in the PP, the security environment of the TOE, security objectives, and IT security requirements. The added detail may be recognized by (*) marked by the end of it.

Application notes

Application notes may be provided to make the meaning of requirements clear, give information about the options for implementation, and define the standard of “conformant/non-conformant” requirement. Application notes will be presented with the requirement they concern as appropriate.

2. TOE Description

This chapter describes the environment in which the TOE will be used and the scope and boundaries of the TOE.

2.1. Product type and configuration

eXshield Security Switch V1.0 is an Intrusion Prevention System that detects and blocks intrusion beforehand so that it protects the assets within the network. Being located on the contact point of the internal network and external network that are connected through the Internet in a router or in-line type, it detects and blocks intrusion and attack of the network traffic that goes from outside to inside of the network in real time.

As the figure below shows, installation of eXshield Security Switch V1.0 on the contact of external untrusted network ensures the intrusion prevention function for the illicit intrusion and attack from outside.

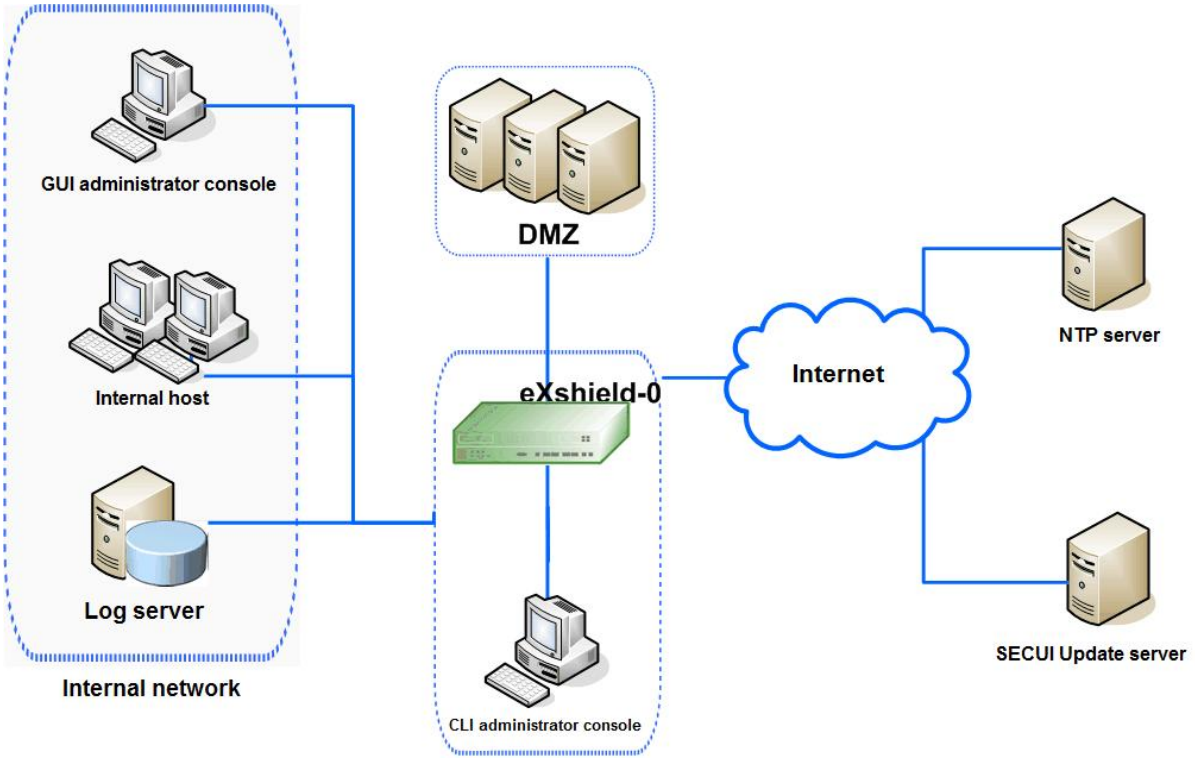

Figure 2-1 Configuration of eXshield Security Switch V1.0

eXshield Security Switch V1.0 uses its intrusion prevention function to prevent, detect, and block illicit access or hacking attack that makes resources of host and network exhausted or causes problem in the accessibility by exploiting vulnerabilities.

The authorized administrator is able to perform the security management of eXshield Security Switch V1.0 by using GUI administrator console, which accesses through the Internet explorer or eXshield Manager, and CLI administrator console, which connects directly to the serial port. The administrator can also manage the log server of eXshield Security Switch V1.0 by establishing an IP for connection to the log server through the CLI administrator console. The log server manager can perform the security management functions after accessing the log server that stores audit data of eXshield Security Switch V1.0.

eXshield Security Switch V1.0 is a distributed product, comprising one to perform network intrusion prevention and a log server to store audit data. Since the former does not have a hard disk in it, a log server accessible from an authorized administrator should be provided in the internal network to store all audit data created.

Intranet servers, DNS server, SMTP server, Web server, or FTP server will be in the DMZ, the

network of which will be separated to protect the internal network.

For the protection against external attacks exploiting new vulnerabilities of the internal network, the administrator of eXshield Security Switch V1.0 updates and manages the Signature list on the vulnerabilities of the product using the update server.

The administrator ensures a sequential generation of audit data using time source provided by the NTP server or OS, which helps regular Signature update.

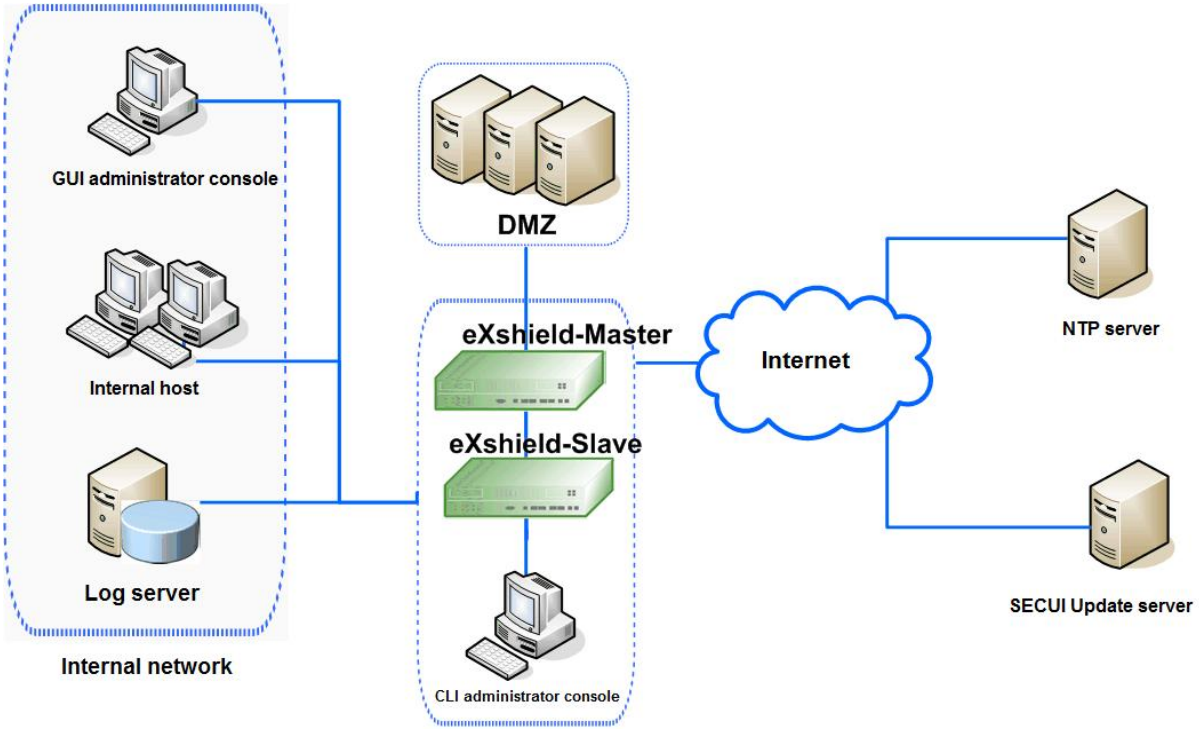

Figure 2-2 Configuration of eXshield Security Switch V1.0: 2

eXshield Security Switch V1.0 is an intrusion prevention system that performs an access control and information flow control.

eXshield Security Switch V1.0 performs the access control function based on the packet filtering rule, which checks whether there is any policy that allows a subject to access information and whether a subject has the security level necessary to access information.

eXshield Security Switch V1.0 comprises of Master and Slave in HA mode, where kernels synchronize the session information and check operational state and roles to realize distributed load

and HA. Master and Slave regularly check each other in operation through HA link. Slave synchronizes with Master every 1 minute and works on behalf of Master if necessary.

eXshield Security Switch V1.0 is comprised of hardware, OS, image(software). The OS is SecuiOS V1.2 developed by Secui.

2.2. TOE scope

This clause describes the physical and logical scope of the TOE.

2.2.1. Physical boundaries and scope

The TOE comprises TOE_Gateway that performs network intrusion prevention and TOE_LServer that stores audit data. TOE_Gateway needs TOE_LServer for storing audit data because it does not have a hard disk.

The TOE includes TOE_Gateway(Master) and TOE_Gateway(Slave), which synchronize the session information and check the operational state and roles of the other part. Slave plays the role of Master if required to support continuous network services.

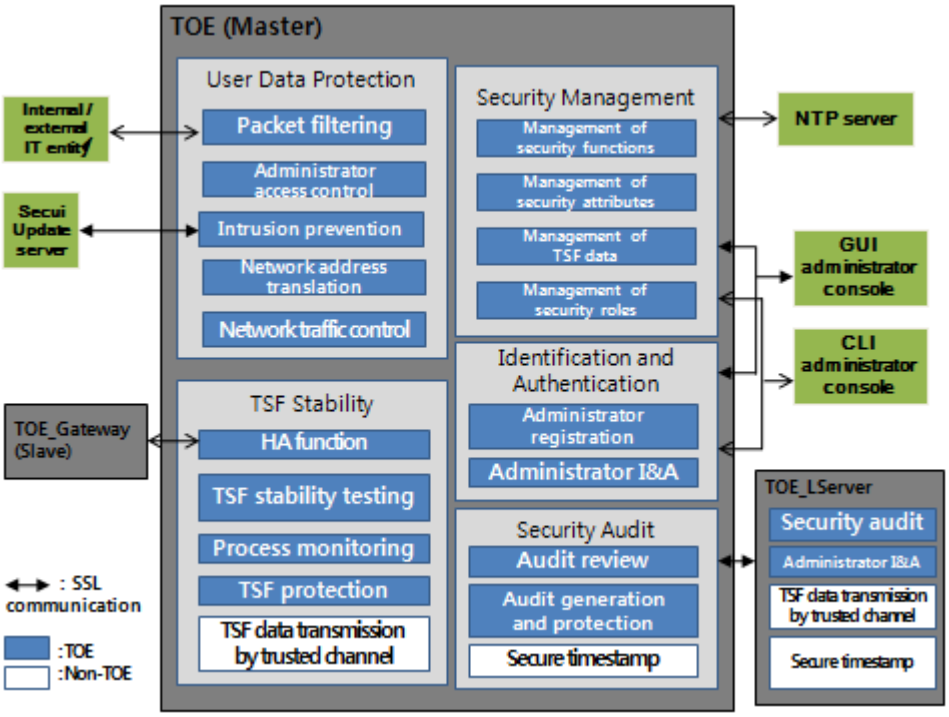

Figure 2-3 Physical boundaries and scope of the TOE

TOE_Gateway updates database on new vulnerabilities from Secui Update server to control information flow of external IT entity and protect the internal network from attacks from outside

exploiting those vulnerabilities. TOE_Gateway receives trusted time source from the NTP server and OS.

TOE_LServer stores the records on the security relevant events occurred in TOE_Gateway; the audit records generated in TOE_Gateway will be sent to TOE_LServer through SSL cryptographic communication.

NTP server, administrator consoles, internal/external IT entity, and Secui Update server in Figure 2-3 are excluded from the physical boundaries and scope.

The hardware and OS for the installation and operation of eXshield V1.0.1.R are not considered in the evaluation. Secui recommends the following physical specification of hardware for the installation and operation of eXshield V1.0.1.R and is not responsible for what might happen due to the customer's using any other hardware without discussion with Secui.

- Images of eXshield V1.0.1.R:
  - TOE_Gateway : eXshield Gateway V1.0.1.R
  - TOE_LServer : ext_log-V1.0.1

- Installation and operation of eXshield V1.0.1.R:

TOE_Gateway	Specification	Notes
CPU	XLR 732 1.2GHz XLR 532 1.2Ghz	
Main Memory	8GB	
CF Card	2GB	
HDD	None	Log server
NIC	26 Ports (1 Gbps * 24, 10/100/1000 Mbps * 2)	
Console	1 Ports	RJ 45 Type
OS	SecuiOS V1.2	
TOE_LServer	**Minimum specification**	**Recommended specification**
CPU	Intel Pentium III 1GHz and above	Intel Xeon 2.8GHz
Main Memory	256MB and above	2GB
HDD	20GB and above	400GB

NIC	2 Ports (1000BaseT, 100BaseT)	2 Ports (1000BaseT, 100BaseT)
OS	RedHat Enterprise Linux 4 Update 4	

Secui recommends for the installation and operation of the administrator console of eXshield V1.0.1.R, which manages access, as below:

- Installation and operation of the administrator console of eXshield V1.0.1.R:

Administrator console	**Minimum specification**
CPU	Intel Pentium III 133MHz and abov
Main Memory	256MB and above
HDD	20 GB and above
NIC	1 or more
Software	Internet Explorer 6.0, JRE V1.5.0_14
OS	Windows XP SP2

2.2.2. Logical boundaries and scope

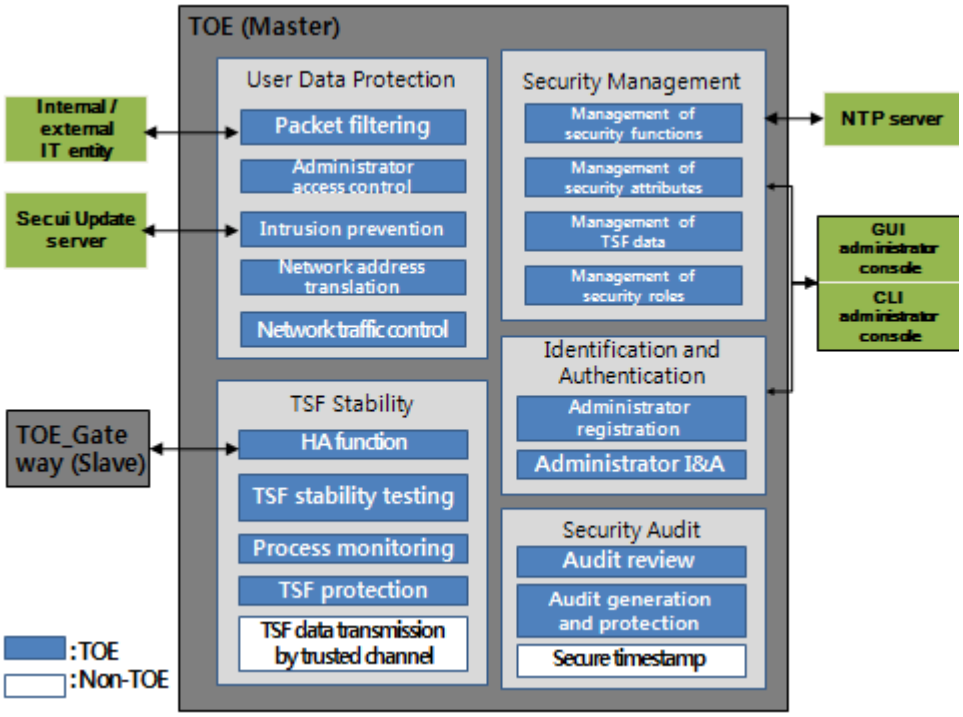

Figure 2-4 Logical boundaries and scope of the TOE

The TOE has 5 major functions – User data protection, TSF stability, Security audit, Security management, and Identification and authentication. The trusted timestamp to show the records of Audit generation and protection (Security audit) are made in the order it is generated, Identification and authentication of a log manager through the OS, and TSF data transmission by trusted channel (TSF stability) are provided by the IT environment.

The following clauses will describe about each function.

2.2.2.1. Security audit

Audit generation and protection

Generates audit records on the initiation and termination of the TOE and of all behavior and processes via the TOE. Alarms the administrator when the occupied capacity excesses the predefined limit so the storage will not be exhausted. Protects the audit data from illegal modification or deletion.

Audit review

Audit data can be reviewed through the monitor of the administrator console.

2.2.2.2. Identification and authentication

Administrator registration

An authorized administrator registers an admin account to make it accessible to the TOE. TOE users are the authorized administrators to manage the TOE. An administrator is registered after the first administrator's registration of the IP address at the initial access to the system.

Administrator identification and authentication

Identifies and authenticates the registered TOE administrator using an ID and password. After a specific period of the administrator's inactivity, locks the session and requires re-authentication.

The SOF of a password used in authentication of an administrator is "SOF-medium" and conforms to the authentication measures metric.

2.2.2.3. User data protection

Administrator access control

The TOE performs an access control of an access subject (the administrator) to an object (the TSF data or TSF executable files) using the security attributes of the subject (identification data, IP address, or access level).

Packet filtering

After a user (access subject) is identified, the TOE applies packet filtering information flow control based on the IP addresses, Port, protocols, and Flag information of the user (source) and information (destination). A user will pass through the information flow control based on the security label, which

compares the security levels of an object and a user, after the discretionary information flow control. When the security level check shows a user's security level is not high enough to access the information, terminate the connection of the user to stop information flow.

Intrusion prevention

The TOE detects illegal access or attack to the network or assets it is intended to protect and takes actions on the detected attacks as defined in the security policy.

Network address translation

TOE users can translate the internal IP address when they want to hide the address using NAT function of the TOE; they can set the internal IPs as private and access the external network to communicate from a public IP. This ensures the internal IP addresses are kept confidential from outside and that a chance for the internal IP address to be exposed and exploited by an attack is minimized.

Network traffic control

Defines the maximum quotas for resource utilization by network traffic so that the traffic is limited to the defined bandwidth in accordance with the policy of packet filtering.

2.2.2.4. Security management

Management of security functions

Provide the ability to determine, disable, enable, and modify the behavior of the security functions only for the authorized administrator.

Management of security attributes

Only the authorized administrator can change default of, query, delete, and generate the security attributes used in access control and information flow control. Default values provided are restrictive and, at the modification, the authorized administrator specifies selective initial values.

Management of TSF data

Only the authorized administrator can perform backup and recovery, the function to query, modify, generate, and delete the access control rules and information flow control rules, and function to modify, generate, delete, and change the time of the identification and authentication data. If the TSF data are at the indicated limits, the TOE takes actions.

Management of security roles

The TSF maintains authorized administrator's role.

2.2.2.5. TSF stability

HA function

The TOE realizes high availability by ensuring that traffics are transferred to Slave in the case that Master cannot perform its function.

TSF stability testing

Performs integrity check of the TSF data, except for the audit records, and TSF executable code and supports action to be taken when it is impaired. Performs self-testing to demonstrate the correct operation of the underlying abstract machine..

TSF protection

All traffics that flow between the inside and outside the TOE should pass through the TOE to communicate, because it locates on the network contact point. Once network traffic arrives at an internal/external network port of the TOE, it passes through the kernel module; and the TSF enforces TSP based on the contents of a packet, which will be transferred to the external/internal network through the external/internal network port. Therefore, it is impossible for traffic to bypass the TOE.

Process monitoring

Monitors operation of the application-level processes on the TOE and re-enables abnormally terminated process. This ensures the security functions set by the administrator are not stopped by any error but providing services continuously.

2.2.2.6. Security function provided by the IT environment

Identification and authentication through the OS

The log server manager shall be identified and authenticated by the underlying OS before allowed to do any actions.

Secure timestamp

TOE_Gateway receives time information from the NTP server or underlying OS. TOE_Gateway shows that audit events are recorded in the order they are performed using received timestamp.

TSF data transmission by trusted channel

Supports cryptographic communication that uses encryption algorithm to ensure a trusted channel between TSFs. This protects data sent received between TSFs.

2.3. Non-TOE scope

This evaluation rules out the following:

2.3.1. Physical non-TOE scope

- SECUI Update Server for URL update and Signature update
- TOE environment hardware
- TOE operating system (SecuiOS)
- Environment hardware of GUI administrator console and CLI administrator console used to manage the TOE
- Internal/external IT entity that sends and receives packet through the TOE

2.3.2. Logical non-TOE scope

- SSL protocol for secure communication between the TOE and administrator console, TOE_Gateway and TOE_LServer, and the TOE and Secui Update server
- Timestamp provided by the external NTP server
- Timestamp provided by the OS for sequential generation of audit data
- Identification and authentication provided by the OS that underlies the TOE

3. TOE Security Environment

The TOE security environment comprises the assumptions, threats, and organizational security policies.

3.1. Assumptions

The description of assumptions of the TOE describes the environment in which the TOE will be used. It includes information about the intended usage of the TOE, including the intended application, potential asset value, and possible limitations of use and information about the environment of use of the TOE, including physical, personnel, and connectivity aspects.

The following assumptions apply to the operational environment of the TOE that conforms to this ST:

A.Locate
The TOE is located in a physically secure environment that only authorized personnel can access.
A.Security
When the internal network environment changes due to a network configuration change, increase or decrease of host or services, the changed environment and security policies are reflected to the TOE operational policy to maintain the same security as before.
A.Administrator
The authorized TOE administrator is not malicious, well trained of the TOE management functions, and performs duties as specified in the administrator's guideline.
A.OSpatch
Eliminates services or measures not required by the TOE and patches the vulnerabilities to ensure confidence and stability of the OS.
A.Connection
The TOE on a network divides it into internal and external, such that all communications between which are mediated by the TOE.
A.Server(*)
The NTP server and SECUI Update server that locate outside the TOE for the secure operation

of the TOE functions are secure.

3.2. Threats

The threats can be explained in terms of a threat agent, assets, and an attack method.

A threat agent may be a computer user, an external IT entity that accesses a computer inside the network, or a user that intends to flow information out to the external.

A threat agent is assumed to have a low-level expertise, resources, and motivation, which means that the possibility of the threat agent to find exploitable vulnerabilities is low. The threat agent is an attacker using the obvious vulnerability information that is able to obtain the exploitable vulnerability information about the OS or application and attack tools from the Internet to impair the resources of the targeted computer or get information illegally. The TOE protects assets from a threat using obvious vulneratbilities like this.

The assets to be protected by the TOE are the computer resources and network services of the internal network or DMZ operated by the organization. The external threat agent accesses the resources illegally and launches an attack to exhaust the availability of the resources.

Threats are categorized into either to the TOE or to the TOE operational environment.

3.2.1. Threats to the TOE

The following threats are the ones to be countered by the TOE.

T.Masquerade
A threat agent may masquerade as an authorized administrator to access the TOE.
T.Failure
The TOE in use may not be able to provide regular services as it is supposed to due to a failure happened by external attack.
T.Record
The TOE may fail to record a security-relevant event due to the storage exhaustion.
T.Import
A packet of information that is not permitted may be imported from the external network to

tamper with the computer in the internal network.
T.Service
A threat agent may access the services of the hosts in the internal network without permission to interfere with the host in providing regular services.
T.Packet
A threat agent may send a network packet of abnormal structure to cause malfunction of the system of the internal network.
T.Vulnerability
A threat agent may make use of new vulnerability of the TOE or the computer system of the internal network in the operational environment to attack.
T.DoS
A threat agent may interfere with other users' using the service resources of the internal network in the operational environment of the TOE by overusing them.
T.Authentication
A threat agent may attempt to be authenticated consecutively to access the TOE.
T.Bypass
A threat agent may bypass the TOE security functions to access the TOE.
T.Spoofing
A threat agent may fake the source IP as an internal address to access the internal network illegally.
T.ModifyTSFdata
A threat agent may launch a buffer overflow attack against the TOE, which results in unintended modification of the TSF data.
T.Export(*)
A threat agent may export information to outside illegally through the network.
T.AttackTSFdata(*)
A threat agent may expose or change the TSF data without permission during communication between TOE_Gateway and TOE_LServer, which are the components of the distributed TOE, the TOE and Secui Update server, or the TOE and GUI administrator console.

3.2.2. Threats to the operational environment

Threats to the TOE operational environment are related to the misconfiguration of the TOE. The following are the threats to be countered by the TOE.

TE.Administration
The TOE may be configured, administered, and used in an insecure way by the authorized administrator.
TE.Delivery
The security of the TOE may be damaged during delivery and installation.
TE.Time(*)
The TOE may receive a wrong time source and make an incorrect audit record.

3.3. Organizational security policies

The TOE shall conform to the following OSPs.

P.Audit
To ensure the accountability of all security-relevant actions, the security-relevant events shall be recorded and maintained, and the data be reviewed.
P.Administration
The authorized administrator shall manage the TOE in a secure manner.

4. Security objectives

This ST describes the security objectives that the TOE or environment should achieve to deal with the security environment: the security objectives for the TOE and for the environment. The former is to be directly addressed by the TOE and the latter is by the IT domain or non-technical/procedural means.

4.1. Security objectives for the TOE

This section describes the security objectives that shall be directly addressed by the TOE as the following:

O.Availability
The TOE shall provide regular services even in the case of failure due to incidental or external attack by maintaining the minimum security functions.
O.Audit
To ensure that all security-relevant actions are accountable, the TOE shall make and maintain the records on the security-relevant events and provide a means to review the recorded data.
O.Administration
The TOE shall provide in a secure manner the authorized administrator with a means to administer the TOE effectively.
O.Packet
The TOE shall block a packet of abnormal structure that passes through the TOE. Application notes: Abnormal packets can be a spoofing packet, broadcasting packet, looping packet, or those that are not TCP/IP packets defined in the internet standard protocol, such as RFC 791 Internal Protocol, RFC 792 Internet Control Message Protocol, or RFC 793 Transmission Control Protocol.
O.DoS
The TOE shall block attackers when they try to use the service resources of the computer it protects in an abnormal way so that users can use the network services.
O.Identification
The TOE shall identify all external IT entities under the information flow control of the TOE and users who intend to access.

O.Authentication
After identification, the TOE shall authenticate the administrator before allowing access to the TOE. Application notes: A threat agent may obtain the authentication data after consecutive attempts using the administrator's identity. The TOE shall implement authentication mechanism that satisfies the SOF level enough to block such authentication attempts.
O.Information
The TOE shall control all unauthorized import or export of information between the internal and external.
O.TSFdata
The TOE shall protect the TSF data from unauthorized disclosure, modification, and deletion.
O.Access(*)
The TOE shall control access according to the security policy rules.
O.Vulnerability
The TOE shall provide a means to update and manage the database on the vulnerabilities managed by the TOE to protect it from external attack exploiting new vulnerabilities of the internal computer.

4.2. Security objectives for the environment

This section describes the security objectives that shall be addressed by the IT domain or non-technical/procedural means as the following:

OE.Locate
The TOE shall be located in a physically secure environment that only an authorized administrator can access.
OE.Security
When the internal network environment changes due to a network configuration change, increase or decrease of host or services, the changed environment and security policies shall be reflected to the TOE operational policy to maintain the same security as before.
OE.Administrator
The authorized TOE administrator shall be not malicious, well trained of the TOE management functions, and perform duties as specified in the administrator's guideline.
OE.Administration

The TOE shall be delivered and installed in a secure manner and be configured, administered, and used in a secure way by the authorized administrator.
OE.OSpatch
Services or measures not required by the TOE shall be eliminated and patches for the vulnerabilities shall be performed to ensure confidence and stability of the OS.
OE.Connection
The TOE on a network shall divide it into internal and external, such that all communications between which shall be mediated by the TOE.
OE.IA(*)
The log server manager shall be identified and authenticated by the underlying OS before allowed to access TOE_LServer.
OE.Timestamp(*)
The TOE shall receive time source from the NTP server or underlying OS securely.
OE.Channel(*)
The TOE shall be provided with a trusted channel using SSL for secure communication between TOE_Gateway and TOE_LServer, TOE and SECUI Update server, or the TOE and GUI administrator console.
OE.Server(*)
The NTP server and SECUI Update server that locate outside the TOE for the secure operation of the TOE functions shall be secure.

5. IT security requirements

This chapter describes the security functional and assurance requirements that shall be satisfied in the TOE. The requirements are composed of the functional components from the CC Part 2 and assurance components from the CC Part 3.

5.1. TOE security requirements

5.1.1. TOE security functional requirements

The TOE security functional requirements (SFR) in this ST are composed of the functional components from the CC Part 2.

This ST claims SOF-medium.

Table 5-1 TOE SFRs that reflect SOF claim

Functional component		Securitiy function
FIA_UAU.2	User authentication before any action	Identification and authentication of administrator (Admin_InA)
FIA_UAU.4	Single-use authentication mechanism	

Table 5-2 SFRs

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

Functional class	Functional component	
	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_ACC.2	Complete access control(*)
	FDP_ACF.1	Security attribute based access control(*)
	FDP_IFC.1(1)	Subset information flow control(1)
	FDP_IFC.1(2)	Subset information flow control(2)
	FDP_IFF.1(1)	Simple security attributes(1)
	FDP_IFF.1(2)	Simple security attributes(2)
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_SOS.1	Verification of secrets(*)
	FIA_UAU.2	User authentication before any action
	FIA_UAU.4	Single-use authentication mechanism(*)
	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
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialization
	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_RCV.4	Function recovery(*)
	FPT_RVM.1	Non-bypassability of the TSP
	FPT_SEP.1	TSF domain separation
	FPT_TST.1	TSF testing
Resource utilization	FRU_FLT.1	Degraded fault tolerance
	FRU_RSA.1(1)	Maximum quotas(1)

Functional class	Functional component	
	FRU_RSA.1(2)	Maximum quotas(2)
TOE access	FTA_SSL.1	TSF-initiated session locking
	FTA_SSL.3	TSF-initiated termination

5.1.1.1. Security audit

5.1.1.1.1. FAU_ARP Security audit automatic response

FAU_ARP.1 Security alarms

Hierarchical to: No other components

Dependencies: FAU_SAA.1 Potential violation analysis

FAU_ARP.1.1 The TSF shall take [the least disruptive actions { to inform the authorized administrator using an alarm popup through the GUI administrator console, send an email to the address registered by the authorized administrator }] upon detection of a potential security violation.

5.1.1.1.2. FAU_GEN Security audit data generation

FAU_GEN.1 Audit data generation

Hierarchical to: No other components

Dependencies: FPT_STM.1 Reliable time stamps

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) [the “auditable events” specified in Table 5-3 Auditable events except for the minimum level of audit]

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 ST, [the “additional audit records” in Table 5-3 Auditable events]

Table 5-3 Auditable events

Functional component	Auditable events	Additional audit records
FAU_ARP.1	Actions taken due to imminent security violations	Identity of recipient of the action
FAU_SAA.1	Enabling and disabling of any of the analysis mechanisms; Automated responses performed by the tool	-
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating	-
FDP_ACF.1	Successful requests to perform an operation on an object covered by the SFP	Identification information of object
FDP_IFF.1	Decisions to permit requested information flows	Identification information of object Decision to deny
FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the actions taken and the subsequent, if appropriate, restoration to the normal state	-
FIA_SOS.1	Rejection by the TSF of any tested secret	-
FIA_UAU.2	Unsuccessful use of the authentication mechanism	
FIA_UAU.4	Attempts to reuse authentication data	
FIA_UID.2	Unsuccessful use of the user identification mechanism, including the user identity provided	-
FMT_SMF.1	Use of the management functions	-
FMT_SMR.1	Modifications to the group of users that are part of a role	-
FPT_STM.1	Changes to the time	-
FPT_TST.1	Integrity errors	-
FPT_RCV.4	If possible, the impossibility to return to a secure state after failure of a security function	
FRU_FLT.1	Any failure detected by the TSF	
FRU_RSA.1	Rejection of allocation operation due to resource limits	-
FTA_SSL.1	Locking of an interactive session by the session locking mechanism; Successful unlocking of an	-

Functional component	Auditable events	Additional audit records
	interactive session	
FTA_SSL.3	Termination of an interactive session by the session locking mechanism	-
FTP_ITC.1	Failure of the trusted channel functions; Identification of the initiator and target of failed trusted channel functions	

FAU_GEN.2 User identity association

Hierarchical to: No other components

Dependencies: FAU_GEN.1 Audit data generation

FIA_UID.1 Timing of identification

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

Application notes: “User” means the identifier of an authorized administrator or audit record of network packets, for example, an administrator ID or network IP address

5.1.1.1.3. FAU_SAA Security audit analysis

FAU_SAA.1 Potential violation analysis

Hierarchical to: No other components

Dependencies: FAU_GEN.1 Audit data generation

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

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

a) Accumulation or combination of [Unsuccessful use of the authentication mechanism (FIA_UAU.2), Access control rule violation (FDP_ACF.1), Information flow control rule violation (FDP_IFF.1), Integrity errors (FPT_TST.1)] known to indicate a potential security violation;

b) [

- Excessive rejection of packet
- Too little traffic from the external network
- Too much traffic from the external network
- Interface down
- Excessive session use
- Excessive CPU use
- Excessive memory use

- Errors in HA mode
- Virtual IP Address error

]

5.1.1.1.4. FAU_SAR Security audit review

FAU_SAR.1 Audit review

Hierarchical to: No other components

Dependencies: FAU_GEN.1 Audit data generation

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

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

FAU_SAR.3 Selectable audit review

Hierarchical to: No other components

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the ability to perform *searches, sorting* of audit data based on [the following rules:

Type of event	Audit review item	Rule
Counter Log	Time, Rule ID	Search by key word for each item For more than one audit review item, use 'AND' search
Counter Log for each server	Time	
Activity Log	Time, Protocol, Interface, Rule ID, Src IP, Src Port, Dest IP, Dest Port	
IPS - Activity Log	Time, Protocol, Interface, Policy Code, Src IP, Src Port, Dest IP, Dest Port, Action	
IPS - Counter Log	Time	
IPS - Signature	Time, Protocol, Interface, Policy Code, Src IP, Src Port, Dest IP, Dest Port	

IPS - Flooding packet	Time, Protocol, Interface, Rule ID, Src IP, Src Port, Dest IP, Dest Port	
IPS - TOP attack information	Time	

].

5.1.1.1.5. FAU_SEL Security audit event selection

FAU_SEL.1 Selective audit

Hierarchical to: No other components

Dependencies: FAU_GEN.1 Audit data generation

FMT_MTD.1 Management of TSF data

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

a) Event type

b) [eXshield information flow control policy]

5.1.1.1.6. FAU_STG Security audit event storage

FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components

Dependencies: FAU_GEN.1 Audit data generation

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

FAU_STG.1.2 The TSF shall be able to *prevent* unauthorized modifications to the stored audit records in the audit trail.

FAU_STG.3 Action in case of possible audit data loss

Hierarchical to: No other components

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.3.1 The TSF shall take [inform the authorized administrator using an alarm popup through the GUI administrator console, send an email to the address registered by the authorized administrator] if the audit trail exceeds [a value from 1 through 100% (by default 99%) that may be changed by the authorized administrator].

FAU_STG.4 Prevention of audit data loss

Hierarchical to: FAU_STG.3

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4.1 The TSF shall *prevent auditable events, except those taken by the authorized administrator with special rights* and [none] if the audit trail is full.

Application notes: In the actual case that the audit storage is full, the TOE shall allow only the access of the authorized administrator to back up or compress the audit data with which can generate audit records after recovery.

5.1.1.2. User data protection (FDP)

5.1.1.2.1. FDP_ACC Access control policy

FDP_ACC.2 Complete access control

Hierarchical to: FDP_ACC.1

Dependencies : FDP_ACF.1 Security attribute based access control

FDP_ACC.2.1 The TSF shall enforce the [administrator access control policy] on [the following list of subjects, objects] and all operations among subjects and objects covered by the SFP.

[

a) List of subjects: Administrator

b) List of objects: All TSF data, TSF executable files

]

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.

5.1.1.2.2. FDP_ACF Access control functions

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 The TSF shall enforce the [administrator access control policy] to objects based on the following:

[

a) List of subjects: Administrator

b) Subject security attributes: Administrator ID, IP address, access level (either 1, 2, or 3), login options (READ only)

c) List of objects: All TSF data, TSF executable files

d) Object security attributes: READ, WRITE, EXECUTE, HALT

]

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

[

a) When an administrator accesses to the GUI administrator console, allow if the IP address matches the registered one, and deny otherwise

b) Allow READ but not WRITE on an object when “READ only” option is selected from the login options of the GUI administrator console

c) Allow READ but not WRITE on an object when the access level of an administrator authorized through the administrator console is 1

d) Allow READ and WRITE on an object when the access level of an administrator authorized through the administrator console is 2

e) Allow READ, WRITE, and HALT on an object when the access level of an administrator authorized through the administrator console is 3

f) Allow EXECUTE on an object when the access level of an administrator authorized through the CLI administrator console is more than 2

]

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [None]

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [rule that denies connection with the same ID as the connected one].

5.1.1.2.3. FDP_IFC Information flow control policy

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

Hierarchical to: No other components

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the [**eXshield information flow control policy**] on [the following list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP:

a) Subject: Unauthorized external IT entity at the information sender’s site

b) Information: Traffic sent from a subject through the TOE

c) Operation: Allow if an allow-rule exists].

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

Hierarchical to: No other components

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the [**exshield IPS information flow control policy**] on [the following list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP:

a) Subject: Unauthorized external IT entity at the information sender's site

b) Information: Traffic sent from a subject through the TOE

c) Operation: Block if a block-rule exists].

Application notes: eXshield information flow control policy in FDP_IFC.1(1) is the deny-all policy and eXshield IPS information flow control policy in FDP_IFC.1(2) is the allow-all policy. Both are the same policies included in the Network Intrusion Prevention System Protection Profile V1.1 (hereinafter IPS-PP), only the names are changed.

5.1.1.2.4. FDP_IFF Information flow control functions

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

Hierarchical to: No other components

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialization

FDP_IFF.1.1 The TSF shall enforce the [eXshield information flow control policy] based on the following types of subject and information security attributes:

[

a) List of subjects: Unauthorized external IT entity at the information sender's site

Subject security attributes: IP address, Security level (1~20), Port number, Subject group

b) List of information: Traffic sent from a subject through the TOE

Information security attributes: Destination URI(uniform resource identifier), Time, Source IP, Destination IP, Port, Protocol, Flag information, Data information, Security level(1~20)

]

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:

[

a) Block packets according to the information flow control policy the authorized administrator established based on the Source IP, Destination IP, Port, Protocol, and Flag information.

b) Allow traffic to the Destination URI, Destination IP, Port, Protocol, and Flag information, and Data information if it is caused by a subject explicitly allowed by the authorized administrator on allowed time and the security level of the subject is the same as or higher than that established for the Destination URI and Protocol information.

c) Block traffic to the Destination URI, Source IP, Destination IP, Port, Protocol, Flag information, and Data information if it is caused by a subject explicitly denied by the authorized administrator on denied time and the security level of the subject is lower than that established for the Destination URI and Protocol Information.

d) If the attributes match the default policy rule but not the one established by the administrator, deny all of them.

]

FDP_IFF.1.3 The TSF shall enforce the [None].

FDP_IFF.1.4 The TSF shall provide the following:

[

a) If the attributes correspond to the NAT rule set by the authorized administrator, change the IP address and port number into the established values.

b) If the attributes correspond to the ICMP rule set by the authorized administrator, send “ICMP Unreachable Code” to the subject who sent the packet.

c) If the attributes correspond to the Reset rule set by the authorized administrator, send “Reset” to the subject who sent the packet.

]

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

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

[None].

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

Hierarchical to: No other components

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialization

FDP_IFF.1.1 The TSF shall enforce the [eXshield IPS information flow control policy] based on the following types of subject and information security attributes:

[

a) List of subjects: Unauthorized external IT entity at the information sender's site
Subject security attributes: IP address

b) List of information: Traffic sent from a subject through the TOE
Information security attributes: Destination URI(uniform resource identifier), Header and Data information of the packet

]

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:

[

a) Permit access unless the traffic includes the Destination URI, header and data information that are defined to be blocked explicitly by the authorized administrator.

]

FDP_IFF.1.3 The TSF shall enforce the [None].

FDP_IFF.1.4 The TSF shall provide the following [None].

FDP_IFF.1.5 The TSF shall explicitly authorize an information flow based on the following rules:

[

a) The TOE shall allow information flow if the Destination URI and header of a packet (IP address) are included on the exception list made by an authorized administrator for the functions like URL blocker, Whitelist check, SYN Flooding, UDP Flooding, Ping Flooding, and Scanning attack.

]

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

[

a) The TOE shall block a request for connection if the information from an external

IT entity has an internal subject IP address.

b) The TOE shall block a request for connection if the information from an internal IT entity has an external subject IP address.

c) The TOE shall block a request for connection if the information from an external IT entity has a subject IP address for broadcasting.

d) The TOE shall block a request for connection if the information from an external IT entity has a subject IP address for looping.

e) The TOE shall block a request for connection if the information from an external IT entity has an abnormal packet structure.

f) { The TOE shall block a request for connection if the information from an external/internal IT entity is one of the items on a list made by the authorized administrator such as Table 5-4 Additional block-information-flow list below. }

]

Table 5-4 Additional block-information-flow list

Additional block-information-flow list
Block Destination URI if it matches the defined block-list.
Block a packet if the Source IP and Destination IP or the Source Port and Destination Port of its header are the same.
Block ICMP packet if it is bigger than 65535byte.
Block ICMP packet if its header has a packet of Destination Unreachable Type.
Block a packet if its IP header includes a Source Route option as an IP option.
Block a packet if its header has the same pattern with the predefined Signature.
Store the information of the SYN packet that is input first for the TCP 3-way handshaking and compare it with that of the second incoming SYN packet; pass when they match, otherwise block it.
Block UDP packet when generated more than the predefined limit of number during a specific time.
Block ICMP packet when generated more than the predefined limit of number during a specific time.
Block a TCP, UDP, or ICMP packet when generated more than the predefined limit of number during a specific time from a Source IP with varying Destination IP.
Block a TCP or UDP packet when generated more than the predefined limit of number during a specific time from a Source IP with varying Destination Port.
Block an ICMP ECHOREPLY type packet among ICMP protocols when it comes from the external network to the TOE.
Block a packet requiring a DNS address if its Request domain and Response domain do not correspond.
Compare the Source IP and MAC Address of a packet with those predefined; block it if they do not

Additional block-information-flow list
correspond.
Compare the Payload of all packets with the defined Signature, and block if the patterns match.

5.1.1.3. Identification and authentication (FIA)

5.1.1.3.1. FIA_AFL Authentication failures

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when *an administrator configurable positive integer within [1 through 10] (default 3)* unsuccessful authentication attempts occur related to [authentication attempts].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [prevent authentication of a disabled administrator before an authorized administrator unlocks the state, generate an audit record on the surpassed limit of unsuccessful authentication attempts].

Application notes: Only an administrator with level 3 authority registered at the initialization is able to unlock the state.

5.1.1.3.2. FIA_ATD User attribute definition

FIA_ATD.1(1) User attribute definition(1)

Hierarchical to: No other components

Dependencies: No dependencies

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual **IT entities**:

[

a) IP address

b) { Security level (1~20) }

]

Application notes: This SFR intends to identify an unauthorized external user that communicates via the TOE with the internal computer to be protected by the TOE.

FIA_ATD.1(2) User attribute definition(2)

Hierarchical to: No other components

Dependencies: No dependencies

FIA_ATD.1.1 The TSF shall mainitain the following list of security attributes belonging to individual **administrators**:

[

a) Identifier

b) { IP address, access level (Level 1, Level 2, or Level 3) }

]

5.1.1.3.3. FIA_SOS Specification of secrets

FIA_SOS.1 Verification of secrets

Hierarchical to: No other components

Dependencies: No dependencies

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [the following metric on password:

- From 6 through 32 letters
- Combination rule:
  - More than one numeric number, alphabet (uppercase and lowercase), and special letter
  - More than 3 repeated characters or digits are disallowed
  - More than 3 consecutive numerical or alphabetical sequences are disallowed
  - ID and Password cannot have more than 3 consecutive letters in common
  - NAME and Password cannot have more than 3 consecutive letters in common
  - Well-Known Word(admin, admimistrator, test, qwe, user) is disallowed
- Cycle of change
  - Administrator's password: Change every 20 access

]

Application notes: The defined metric may include, for a passwork authentication mechanism, a minimum length, combination rule, and cycle of change.

5.1.1.3.4. FIA_UAU User authentication

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2.1 The TSF shall require each **administrator** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that **administrator**.

FIA_UAU.4 Single-use authentication mechanisms

Hierarchical to: No other components

Dependencies: No dependencies

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to [administrator authentication mechanism].

FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.7.1 The TSF shall provide only [an input character presented as a dot] to the **administrator** while the authentication is in progress.

5.1.1.3.5. FIA_UID User identification

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

Hierarchical to: FIA_UID.1

Dependencies: No dependencies

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

Application notes: A TOE user can be an administrator or an IT entity. This component requires the IT entity to be identified.

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

Hierarchical to: FIA_UID.1

Dependencies: No dependencies

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

Application notes: A TOE user can be an administrator or an IT entity. This component requires the administrator to be identified.

5.1.1.4. Security management (FMT)

5.1.1.4.1. FMT_MOF Management of functions in TSF

FMT_MOF.1 Management of security functions behavior

Hierarchical to: No other components

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

FMT_MOF.1.1 The TSF shall restrict the ability to *determine the behavior of, disable, enable, modify the behavior of* the functions [the following list of functions] to [the authorized administrator].

[

Table 5-5 Management of security functions

Function	Capability
Action in case of possible audit storage failure	Determine the behavior, disable, and modify the behavior
Action in case of audit storage failure	Determine the behavior, disable, enable, and modify the behavior
Maintain rules for potential violation analysis	
Specify maximum quota of the number of session	
eXshield IPS information flow control	
Audit data backup	Determine the behavior and modify the behavior
Establish the cycle of audit data compression	
eXshield information flow control	
Manage user group with authority to read security audit review	
Terminate the GUI administrator console after a specified time of the authorized administrator's inactivity	
Selective audit data generation	Disable and enable
Receive reliable timestamps from the NTP server	
SNMP function	
Activate the function of NAT rule	
Action in case of security alarms	Disable, enable, and modify the

	behavior
Disable and reactivate system	Determine the behavior and enable
Manage the group of authorized administrators that are part of a role	Determine the behavior, enable, and modify the behavior
Determine emailing an administrator in case of authentication failure	Determine the behavior
Unlock a disabled administrator by an authorized administrator	
Manual testing of an abstract machine	Enable
Check the TOE state and network information	
System backup and recovery	
Specify maximum quota of network traffic	Determine the behavior, disable, and enable

]

5.1.1.4.2. FMT_MSA Management of security attributes

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components

Dependencies: [FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.1.1 The TSF shall enforce the [following SFPs in Table 5-6] to restrict the ability to *change_default, modify, delete, query, [generate]* to [the authorized administrator].

[

Table 5-6 Management of security attributes

SFP	Security attribute	Operation
Administrator access control policy	Administrator IP address	Change_default, modify, delete, and generate
	Administrator ID	Modify, delete, and generate

	Access level	Change_default, modify, delete, and generate
	Login options, execution	Change_default and modify
eXshield information flow control policy	Security level (1~20)	Change_default and modify
	Subject group	Query, modify, and delete
	IP address	Modify, delete, and generate
	Service (Port number)	Modify and generate
	Destination URI	Modify, delete, and generate
	Time	Modify
	Data information	Modify, delete, and generate
eXshield IPS information flow control policy	Destination URI	Modify, delete, and generate
	Time	Modify
	Data information	Modify, delete, and generate

]

FMT_MSA.3 Static attribute initialization

Hierarchical to: No other components

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [administrator access control policy, eXshield information flow control policy] to provide *restrictive* default values for security attributes that are used to enforce the SFP.

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

5.1.1.4.3. FMT_MTD Management of TSF data

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

FMT_MTD.1.1 The TSF shall restrict the ability to *query, modify, delete, [generate, back up to a*

semi-permanent auxiliary memory, recover] the [following TSF data in Table 5-7] to [the authorized administrator].

[

Table 5-7 Management of TSF data

TSF data	Operation
Important files that form the TOE	Back up to a semi-permanent auxiliary memory and recover
Identification data	Delete and generate
Authentication data	Modify, delete, and generate
Time	Query and modify
System	
The number of administrator's login failure	
Time of the authorized administrator inactivity	
Bandwidth control rule	
Session control rule	
Limits on the file system	
Administrator access control policy eXshield information flow control policy eXshield IPS information flow control policy	Query, modify, delete, and generate
Administrator information	
TOE_LServer configuration information	
High Availability configuration information	
SNMP configuration information	
URL block rule	
Network interface information	
Ethernet bridging information	
Interface trunking information	
Routing information	
DNS information necessary to email an authorized administrator	
IPS Signature	Modify
The number of unsuccessful authentication attempts	
IPS signature update information	Query
CPU use of each Zone of DashBoard; memory use; current session, BPS, PPS, IPS signature check state	

Current server state	
Current session, NAT change table, IPS block list, current access administrator	

]

Application notes: The administrator shall be able to update the vulnerability data when a new vulnerability is detected to block a new attack against the network.

FMT_MTD.2 Management of limits on TSF data

Hierarchical to: No other components

Dependencies: FMT_MTD.1 Management of TSF data

FMT_SMR.1 Security roles

FMT_MTD.2.1 The TSF shall restrict the specification of the limits for [audit storage capacity, the number of unsuccessful authentication attempts, limits on controlling bandwidth] to [the authorized administrator].

FMT_MTD.2.2 The TSF shall take the following actions, if the TSF data are at, or exceed, the indicated limits:

[

Table 5-8 Management of limits on TSF data

TSF data	Action when the limits are reached or exceeded
Audit storage capacity	Record audit. Send an alarm mail to the authorized administrator. Use an alarm popup if the administrator is logged on to the GUI administrator console.
The number of unsuccessful authentication attempts	Prevent re-authentication of the inactive user before any action by the authorized administrator, Record audit. Inform the authorized administrator using an alarm popup through the GUI administrator console. Send an email to the address registered by the

	authorized administrator.
Limit on the bandwidth control	Record audit

]

5.1.1.4.4. FMT_SMF Specification of management functions

FMT_SMF.1 Specification of management functions

Hierarchical to: No other components

Dependencies: No dependencies

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

[

a) Functions specified in FMT_MOF.1 Management of security functions behavior

b) Functions specified in FMT_MSA.1 Management of security attributes

c) Functions specified in FMT_MSA.3 Static attribute initialization

d) Functions specified in FMT_MTD.1 Management of TSF data

e) Functions specified in FMT_MTD.2 Management of limits on TSF data

]

5.1.1.4.5. FMT_SMR Security management roles

FMT_SMR.1 Security roles

Hierarchical to: No other components

Dependencies: FIA_UID.1 Timing of identification

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

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

5.1.1.5. Protection of the TSF (FPT)

5.1.1.5.1. FPT_AMT Underlying abstract machine test

FPT_AMT.1 Abstract machine testing

Hierarchical to: No other components

Dependencies: No dependencies

FPT_AMT.1.1 The TSF shall run a suite of tests *during initial start-up, at the request of an authorized* ***administrator*** to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

5.1.1.5.2. FPT_FLS Fail secure

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components

Dependencies: ADV_SPM.1 Informal TOE security policy model

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur:
[Abnormal termination of the application processes that form the TOE, network circuit error of Master devices]

5.1.1.5.3. FPT_RCV Trusted recovery

FPT_RCV.4 Function recovery

Hierarchical to: No other components

Dependencies: ADV_SPM.1 Informal TOE security policy model

FPT_RCV.4.1 The TSF shall ensure that [Reactivation of process, abnormal termination of the application processes that form the TOE] have the property that the SF either completes successfully, or for the indicated failure scenarios, recovers to a

consistent and secure state.

5.1.1.5.4. FPT_RVM Reference mediation

FPT_RVM.1 Non-bypassability of the TSP

Hierarchical to: No other components

Dependencies: No dependencies

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.

5.1.1.5.5. FPT_SEP Domain separation

FPT_SEP.1 TSF domain separation

Hierarchical to: No other components

Dependencies: No dependencies

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

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

5.1.1.5.6. FPT_TST TSF self test

FPT_TST.1 TSF testing

Hierarchical to: No other components

Dependencies: FPT_AMT.1 Abstract machine testing

FPT_TST.1.1 The TSF shall run a suite of self tests *during initial start-up, periodically during normal operation, at the request of the authorized* ***administrator*** to demonstrate the correct operation of *[TSF data except for the audit records]*.

FPT_TST.1.2 The TSF shall provide authorized **administrators** with the capability to verify the integrity of *[TSF data except for the audit records]*.

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

5.1.1.6. Resource utilization (FRU)

5.1.1.6.1. FRU_FLT Fault tolerance

FRU_FLT.1 Degraded fault tolerance

Hierarchical to: No other components

Dependencies: FPT_FLS.1 Failure with preservation of secure state

FRU_FLT.1.1 The TSF shall ensure the operation of [Slave performing all of the TOE activities in place of Master] when the following failures occur: [Network circuit error of Master devices].

Application notes: This SFR intends to ensure that users can use network services under the failure of the TOE.

5.1.1.6.2. FRU_RSA Resource allocation

FRU_RSA.1(1) Maximum quotas(1)

Hierarchical to: No other components

Dependencies: No dependencies

FRU_RSA.1.1 The TSF shall enforce maximum quotas of the following resources: [TCP packets having SYN Flag from multi sources to a specific destination or from a specific source to multi destinations, suh as in a DDoS attack] that *individual **IT entity*** can use *over a specified period of time*.

FRU_RSA.1(2) Maximum quotas(2)

Hierarchical to: No other components

Dependencies: No dependencies

FRU_RSA.1.1 The TSF shall enforce maximum quotas of the following resources: [Network traffic, the number of session] that *individual **IT entity**, defined group of users* can use *over*

a specified period of time.

5.1.1.7. TOE access (FTA)

5.1.1.7.1. FTA_SSL Session locking

FTA_SSL.1 TSF-initiated session locking

Hierarchical to: No other components

Dependencies: FIA_UAU.1 Timing of authentication

FTA_SSL.1.1 The TSF shall lock an **authorized administrator's** session after [1~120 (default 10) minute(s) of the authorized administrator inactivity] by:

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

b) Disabling any activity of the **authorized administrator**'s data access/display devices other than unlocking the session

FTA_SSL.1.2 The TSF shall require the following events to occur prior to unlocking the session: [Re-authentication].

FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components

Dependencies: No dependencies

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [30 minutes of an IT entity inactivity].

Application notes: Playing a role to mediate the connection between the internal and external networks, the TSF terminates the session between IT entities that interact via the TOE after the specified period of time of inactivity.

5.1.2. TOE security assurance requirements

The TOE security assurance requirements (SAR) in this ST are composed of the assurance components from the CC Part 3. The targeted assurance level in this ST is EAL4. The following table summarizes the assurance components.

Table 5-9 SARs: EAL4

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 support	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: high-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

5.1.2.1. Configuration management (ACM)

5.1.2.1.1. ACM_AUT.1 Partial CM automation

Dependencies: ACM_CAP.3 Authorization controls

Developer action elements

ACM_AUT.1.1D	The developer shall use a CM system.
ACM_AUT.1.2D	The developer shall provide a CM plan.

Content and presentation of evidence elements

ACM_AUT.1.1C	The CM system shall provide an automated means by which only authorized changes are made to the TOE implementation representation.
ACM_AUT.1.2C	The CM system shall provide an automated means to support the generation of the TOE.
ACM_AUT.1.3C	The CM plan shall describe the automated tools used in the CM system.
ACM_AUT.1.4C	The CM plan shall describe how the automated tools are used in the CM system.

Evaluator action elements

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

5.1.2.1.2. ACM_CAP.4 Generation support and acceptance procedures

Dependencies: ALC_DVS.1 Identification of security measures

Developer action elements

ACM_CAP.4.1D	The developer shall provide a reference for the TOE.
ACM_CAP.4.2D	The developer shall user a CM system.
ACM_CAP.4.3D	The developer shall provide CM documentation.

Content and presentation of evidence elements

ACM_CAP.4.1C	The reference for the TOE shall be unique to each version of the TOE.
ACM_CAP.4.2C	The TOE shall be labelled with its reference.
ACM_CAP.4.3C	The CM documentation shall include a configuration list, a CM plan, and an acceptance plan.
ACM_CAP.4.4C	The configuration list shall uniquely identify all configuration items that comprise the TOE.
ACM_CAP.4.5C	The configuration list shall describe the configuration items that comprise the TOE.
ACM_CAP.4.6C	The CM documentation shall describe the method used to uniquely identify the configuration items that comprise the TOE.
ACM_CAP.4.7C	The CM system shall uniquely identify all configuration items that comprise the TOE.
ACM_CAP.4.8C	The CM plan shall describe how the CM system is used.
ACM_CAP.4.9C	The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.
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.
ACM_CAP.4.11C	The CM system shall provide measures such that only authorized changes are made to the configuration items.
ACM_CAP.4.12C	The CM system shall support the generation of the TOE.
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

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

5.1.2.1.3. ACM_SCP.2 Problem tracking CM coverage

Dependencies: ACM_CAP.3 Authorization controls

Developer action elements

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

Content and presentation of evidence elements

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

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

5.1.2.2. Delivery and operation (ADO)

5.1.2.2.1. ADO_DEL.2 Detection of modification

Dependencies: ACM_CAP.3 Authorization controls

Developer action elements

ADO_DEL.2.1D	The developer shall document procedures for delivery of the TOE or parts of it to the user.
ADO_DEL.2.2D	The developer shall use the delivery procedures.

Content and presentation of evidence elements

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.
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.
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

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

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

Dependencies: AGD_ADM.1 Administrator guidance

Developer action elements

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

Content and presentation of evidence elements

ADO_IGS.1.1C The 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

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

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

5.1.2.3. Development (ADV)

5.1.2.3.1. ADV_FSP.2 Fully defined external interfaces

Dependencies: ADV_RCR.1 Informal correspondence demonstration

Developer action elements

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

Content and presentation of evidence elements

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

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

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.

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

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

Evaluator action elements

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

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

5.1.2.3.2. ADV_HLD.2 Security enforcing high-level design

Dependencies: ADV_FSP.1 Informal functional specification
ADV_RCR.1 Informal correspondence demonstration

Developer action elements

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

Content and presentation of evidence elements

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

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

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

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

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

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

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

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

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

Evaluator action elements

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

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

5.1.2.3.3. 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

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

Content and presentation of evidence elements

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.

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

Evaluator action elements

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

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.

5.1.2.3.4. 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

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

Content and presentation of evidence elements

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

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

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

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

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.
ADV_LLD.1.6C	The low-level design shall describe how each TSP-enforcing function is provided.
ADV_LLD.1.7C	The low-level design shall identify all interfaces to the modules of the TSF.
ADV_LLD.1.8C	The low-level design shall identify which of the interfaces to the modules of the TSF are externally visible.
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.
ADV_LLD.1.10C	The low-level design shall describe the separation of the TOE into TSP-enforcing and other modules.

Evaluator action elements

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

5.1.2.3.5. ADV_RCR.1 Informal correspondence demonstration

Dependencies: No dependencies

Developer action elements

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

Content and presentation of evidence elements

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

Evaluator action elements

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

5.1.2.3.6. ADV_SPM.1 Informal TOE security policy model

Dependencies: ADV_FSP.1 Informal functional specification

Developer action elements

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

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

Content and presentation of evidence elements

ADV_SPM.1.1C The TSP model shall be formal.

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

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.

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

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

5.1.2.4. Guidance documents (AGD)

5.1.2.4.1. AGD_ADM.1 Administrator guidance

Dependencies: ADV_FSP.1 Informal functional specification

Developer action elements

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

Content and presentation of evidence elements

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

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

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

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

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

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

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

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

Evaluator action elements

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

5.1.2.4.2. AGD_USR.1 User guidance

Dependencies: ADV_FSP.1 Informal functional specification

Developer action elements

AGD_USR.1.1D The developer shall provide user guidance.

Content and presentation of evidence elements

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

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

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

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

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

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

Evaluator action elements

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

5.1.2.5. Life cycle support (ALC)

5.1.2.5.1. ALC_DVS.1 Identification of security measures

Dependencies: No dependencies

Developer action elements

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

Content and presentation of evidence elements

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

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

Evaluator action elements

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

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

5.1.2.5.2. ALC_LCD.1 Developer defined life-cycle model

Dependencies: No dependencies

Developer action elements

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

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

Content and presentation of evidence elements

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

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

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

5.1.2.5.3. ALC_TAT.1 Well-defined development tools

Dependencies: ADV_IMP.1 Subset of the implementation of the TSF

Developer action elements

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

ALC_TAT.1.2D The developer shall document the selected implementation-dependent optionsof the development tools.

Content and presentation of evidence elements

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

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

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

Evaluator action elements

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

5.1.2.6. Tests (ATE)

5.1.2.6.1. ATE_COV.2 Analysis of coverage

Dependencies: ADV_FSP.1 Informal functional specification
ATE_FUN.1 Functional testing

Developer action elements

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

Content and presentation of evidence elements

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

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

Evaluator action elements

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

5.1.2.6.2. ATE_DPT.1 Testing: high-level design

Dependencies: ADV_HLD.1 Descriptive high-level design
ATE_FUN.1 Functional testing

Developer action elements

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

Content and presentation of evidence elements

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

Evaluator action elements

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

5.1.2.6.3. ATE_FUN.1 Functional testing

Dependencies: No dependencies

Developer action elements

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

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation of evidence elements

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

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

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

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

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

Evaluator action elements

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all

requirements for content and presentation of evidence.

5.1.2.6.4. 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

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

Content and presentation of evidence elements

ATE_IND.2.1C The TOE shall be suitable for testing.
ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ATE_IND.2.2E The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.
ATE_IND.2.3E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.1.2.7. Vulnerability assessment (AVA)

5.1.2.7.1. 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

AVA_MSU.2.1D	The developer shall provide guidance documentation.
AVA_MSU.2.2D	The developer shall document an analysis of the guidance documentation.

Content and presentation of evidence elements

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.
AVA_MSU.2.2C	The guidance documentation shall be complete, clear, consistent and reasonable.
AVA_MSU.2.3C	The guidance documentation shall list all assumptions about the intended environment.
AVA_MSU.2.4C	The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).
AVA_MSU.2.5C	The analysis documentation shall demonstrate that the guidance documentation is complete.

Evaluator action elements

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

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

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.

5.1.2.7.2. 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

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

Content and presentation of evidence elements

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

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

Evaluator action elements

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

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

5.1.2.7.3. AVA_VLA.2 Independent vulnerability analysis

Dependencies: ADV_FSP1. 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

AVA_VLA.2.1D	The developer shall perform a vulnerability analysis.
AVA_VLA.2.2D	The developer shall provide vulnerability analysis documentation.

Content and presentation of evidence elements

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

AVA_VLA.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_VLA.2.2E	The evaluator ***shall conduct*** penetration testing, building on the developer vulnerability analysis, to ensure the identified vulnerabilities have been addressed.
AVA_VLA.2.3E	The evaluator ***shall perform*** an independent vulnerability analysis.
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.
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.

5.2. Security requirements for the IT environment

The security requirements for the IT environment of this ST are composed of the functional components from the CC Part 2.

The following table summarizes the functional components related to the IT environment.

Table 5-10 Security functional requirements for the IT environment

Functional class	Functional component	
Identification and authentication	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
Protection of the TSF	FPT_ITT.1	Basic internal TSF data transfer protection
	FPT_STM.1	Reliable time stamps
Trusted path/channels	FTP_ITC.1	Inter-TSF trusted channel

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication
Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2.1 The **IT environment** shall require each **log server manager** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that **log server manager**.

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification
Dependencies: No dependencies

FIA_UID.2.1 The **IT environment** shall require each **log server manager** to identify itself before allowing any other TSF-mediated actions on behalf of that **log server manager**.

FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to: No other components

Dependencies: No dependencies

FPT_ITT.1.1 The **IT environment** shall protect TSF data from *disclosure, modification* when it is transmitted between separate parts of the TOE.

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components

Dependencies: No dependencies

FPT_STM.1.1 The **IT environment** shall be able to provide reliable time stamps for **the TSF to use**.

FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components

Dependencies: No dependencies

FTP_ITC.1.1 The **IT environment** 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.

FTP_ITC.1.2 The **IT environment** shall permit *the TSF* to initiate communication via the trusted channel.

FTP_ITC.1.3 The **IT environment** shall initiate communication via the trusted channel for [access to the GUI administrator console, Signature update, malicious Website list update].

6. TOE summary specification

This chapter specifies the security functions the TOE provides to satisfy the TOE SFR and defines the assurance measures to meet the TOE SARs.

The TOE provides the following security functions.

6.1. TOE security functions

This section describes the security functions the TOE provides to satisfy the IT SFRs defined in “5.1.1 TOE security functional requirements.”

6.1.1. Security audit (Audit)

6.1.1.1. Audit generation and protection (Audit_Gen_Protect)

For supporting the security requirements defined in FAU_GEN.1, Audit generation and protection can generate audit records regarding the following:

- Start-up and shutdown of the audit functions
- Actions taken due to imminent security violations
- Enabling and disabling of any of the analysis mechanisms; Automated responses performed by the tool
- All modifications to the audit configuration that occur while the audit collection functions are operating
- Successful requests to perform an operation on an object covered by the administrator access control policy
- Decisions to permit requested information flows
- The reaching of the threshold for the unsuccessful authentication attempts and the actions taken and the subsequent, if appropriate, restoration to the normal state
- Rejection by the TSF of any tested secret
- Unsuccessful use of the authentication mechanism

- Attempts to reuse authentication data
- Unsuccessful use of the user identification mechanism, including the user identity provided
- Use of the management functions
- Modifications to the group of users that are part of a role
- Changes to the time
- Integrity errors
- If possible, the impossibility to return to a secure state after failure of a security function
- Any failure detected by the TSF
- Rejection of allocation operation due to resource limits
- Locking of an interactive session by the session locking mechanism; Successful unlocking of an interactive session
- Termination of an interactive session by the session locking mechanism
- Failure of the trusted channel fuctions; Identification of the initiator and target of failed trusted channel fuctions

The TSF can, for the events above, associate each auditable event with the identity of the authorized administrator that caused the event and the identifier of audit records on the network packets. The following are the audit records additional to those generated on the audit events above:

- Actions taken due to imminent security violations: Identity of recipient of the action
- Successful requests to perform an operation on an object covered by the administrator access control policy : Identification information of object
- Decisions to permit requested information flows: Identification information of object; Decision to deny

For the auditable events above, each audit record includes at least:

- Date and time of the event
- Type of event
- Subject identity
- Outcome (success or failure) of the event

Date and time of the event clearly identify the time, date, month, and year on which the event happened. Event type categorizes the types defined in FAU_GEN.1 into Warning, Counter Log, Counter Log for each server, Activity Log, and IPS.

The TOE is able to indicate potential violations using the following information:

- Accumulation of failed authentication of a user

- Accumulation of violations of the administrator access control policy
- Accumulation of violations of the rules of eXshield information flow control policy/eXshield IPS information flow control policy
- Accumulation of audited events on the integrity violations of the TSF data and executable code
- Excessive rejection of packet
- Too little traffic from the external network
- Too much traffic from the external network
- Interface down
- Excessive session use
- Excessive CPU use
- Excessive memory use
- Errors in HA mode
- Virtual IP Address error

The TOE generates audit data determining an event as one of the potential violations above; informs the authorized administrator using an alarm popup through the GUI administrator console; and sends an email to the address registered by the authorized administrator. Based on the generated warning audit data, the TOE detects any illegal access or attack.

The authorized administrator of the TOE can include or exclude auditable events from the set of audited events based on the type of events and eXshield information flow control policy for each.

Audit record is generated in a binary type, not a normal text file. Log does not allow MODIFY right but READ right only. The TOE therefore can prevent modification of the audit records.

To prevent audit storage exhaustion, the TOE allows the authorized administrator to specify a value from 1 through 100% (default 99%) of the file system use at which the authorized administrator will be informed by an alarm popup through the GUI administrator console and by the registered email to take action.

If the file system where audit data is stored is exhausted, the TOE blocks all sessions including the current one but for the administrator console and prevents all network packets from passing through. Sessions will be locked until the authorized administrator accesses TOE_LServer and performs backup or compression of the audit data to make a file system space.

The authorized administrator shall manage the capacity of audit data trail carefully and perform backup or compression of audit records on the GUI administrator console if the audit data threshold is passed.

The TOE receives time source from RTC(Real-Time Clock) and NTP(Network Time Protocol) server provided by the OS in the IT environment. RTC has a built-in battery in it so it can provide a reliable time in spite of the lack of the power. System time will be updated after the boot by the interrupt of CPU Clock so it can be used in recording security audit and provide reliable time stamps. The external NTP server is used to synchronize the time of the TOE with it so the TOE can provide a reliable time to be used in recording security audit.

6.1.1.2. Audit review (Audit_Review)

Only an administrator who accessed from the IT entity registered as a management access IP according to the Administrator access control policy and Identification and authentication can read all audit data.

The authorized administrator can review all TOE audit data that are translated into readable form through the administrator console. It can also search or sort the data by the subject identity, target object, date and time of the event, type of the event, importance, and outcome (success or failure) using one factor or combination of more than 2 factors.

Audit data review is only possible through the GUI administrator console. Review of the audit data is performed after the administrator checks the subject and cycle of review by reading the audit data review subject and setup file.

6.1.2. Identification and authentication (User_Auth)

6.1.2.1. Administrator registration (Admin_User_Register)

When an administrator wants to use the GUI administrator console or communicate with the TOE through the CLI administrator console, the administrator shall be identified and authenticated, which shall be preceded by the registration of administrator.

For an initial registration of administrator, the ID, password, and access right of an administrator are selected in the process of system installation using the CLI administrator console at the initial system boot. Generation of more than one administrators and generation on the GUI administrator console are allowed.

The TOE places the following restrictions on the password in registering an administrator:

Restrictions on a password
● From 6 through 32 letters ● Combination rule ■ More than one numeric number, alphabet (uppercase and lowercase), and special letter ■ More than 3 repeated characters or digits are disallowed ■ More than 3 consecutive numerical or alphabetical sequences are disallowed ■ ID and Password cannot have more than 3 consecutive letters in common ■ NAME and Password cannot have more than 3 consecutive letters in common ■ Well-Known Word(admin, admimistrator, test, qwe, user) is disallowed ● Cycle of change ■ Administrator's password: Change every 20 access

Table 6-1 Retrictions on a password

An authorized administrator can add/modify/delete an administrator using an administrator setup menu through the GUI administrator console. Any items necessary at the generation of an administrator shall be included with the ID and password at registration.

An administrator registers the IP address of the IT product to be managed to use the GUI administrator console. Neither registering an administrator of a higher level nor increasing the level of

an existing administrator is possible.

6.1.2.2. Administrator identification and authentication (Admin_InA)

Identification and authentication satisfies the SOF-medium for the minimum strength of a probabilistic or permutational mechanism. FIA_UAU.2 and FIA_UAU.4 also satisfy the SOF-medium. Administrator identification and authentication provides an administrator authentication function by ID/Password and by one-time password (S-key).

An administrator can access the administrator console of the TOE after being identified and authenticated. The TOE can perform identification and authentication by using Password or S/KEY system. An administrator, the access subject, attempts to access the administrator authentication process of the TOE that has already been initialized using the login screen of the administrator console. At the attempt, SSL communication is used between the administrator and the TOE, which will send and receive a message of request for a server information to determine which authentication system will be used. The difference between Password authentication system and S/KEY authentication system can be explained as the following:

Password system requires an administrator to input the authentication data, the ID and Password, which are compared with those stored in the TOE. If the result shows the same value is found, the identification and authentication process will be successfully completed; otherwise the connection will be terminated.

S/KEY system requires an administrator to send the ID and Password to the administrator identification and authentication process in the TOE. The process sends an Iteration Count, which is the ID and Password, and an S/Key Challenge, which is the Seed value, to the administrator. Then the administrator sends a Response value obtained using S/Key OTP Calculator back to the process, which will check the Response value.

- Iteration Count value: A random number generated by Random function at the administrator's attempt to log in, from 1 through 20
- Seed value: Combination of the name of the TOE system and the value obtained by Random function; e.g. "SE50964"

In S/Key system, the TOE calculates a Response value using S/Key OTP Calculator. The identification and authentication process in the TOE sends an Iteration Count value and Seed value, which are random values that will be used once at login and generated randomly to prevent the reuse of the authentication data. The S/Key OTP Calculator also does not store the Iteration Count value

and Seed value after calculating and let them be destroyed. Any character input by a user during authentication will be shown as a dot to the user.

An administrator that passed through the identification and authentication process of the TOE is able to use all of the TSF-mediated functions.

Information about the ID and password of an administrator are stored in the file system of the TOE and will be used as identification values to be compared to the ID and password an authorized administrator inputs when accessing the administrator console. The TOE allows the administrator to access if the values are confirmed to correspond.

When unsuccessful authentication attempts occur 1~10 (as specified by an authorized administrator; default 3) times consecutively, the TOE prevent authentication of the administrator before an authorized administrator takes action, inform the authorized administrator of the authentication failures, terminates the authentication screen, and records an audit log. The administrator of which authentication is prevented can restart the identification and authentication process if the administrator registered at installation selects it from administrator registration menu and allows reauthentication.

An administrator session is locked after 1~120 (as specified by an authorized administrator; default 10) minutes of the administrator inactivity. Re-authentication is required to unlock the session.

In order to use the CLI administrator console, an administrator shall be identified and authenticated for the TOE through the TOE console port. Input of the default ID and password given at the purchase of the TOE is first required. After the identification and authentication of the default are completed, a prompt for an administrator identification and authentication is shown for the input of the registered administrator ID and password. When the process is completed, the administrator can use the CLI administrator console.

6.1.3. User data protection (User_Data_protection)

6.1.3.1. Access control (Access_ctrl)

6.1.3.1.1. Administrator access control (Admin_acc_ctrl)

The TOE shall enforce an access control rule, when an administrator (access subject) intends to access all TSF data and TSF executable files (object) object based on the security attributes of the subject and object. Access control shall be performed on all operations between a subject and object based on the security attributes of an administrator (ID, IP address, access level) and of an object ("OK" button of the GUI administrator console, commands of the CLI administrator console). Access control will be performed in the way that the connection of an administrator is terminated if the administrator does not have the access right for the access object.

Administrator access control policy addresses the GUI administrator console and CLI administrator console.

In order to implement the administrator access control policy of the GUI administrator console, allow or deny access of an administrator as an access subject based on the IP address of the administrator previously registered and perform identification and authentication. The identified and authenticated administrator will be under the application of access control rules based on the security attributes of group authorities and have authorities as the following according to the attributes – either Level 1, 2, or 3 – of the group.

Table 6-2 Administrator group authorities

Administrator group	
Group attribute	**Group authority**
Level 1	Allow READ; deny WRITE, EXECUTE and HALT
Level 2	Allow READ, WRITE, and EXECUTE; deny HALT
Level 3	Allow READ, WRITE, EXECUTE, and HALT

In the case "READ only" is selected at the login to the GUI administrator console, even the administrator of Level 2 or 3 are given READ but not WRITE and HALT on an object.

In case of the attempt to access with the same ID as the one already connected to the TOE, deny

access based on the rule that denies connection with the same ID as the connected one.

Administrators of Level 2 and above are assigned through the CLI administrator console the authority to execute commands on objects. It should be remembered that Level 2 administrators are not allowed to have the authority for halt and reboot commands of the CLI administrator console.

6.1.3.2. Information flow control (Flow_control)

The TOE applies eXshield information flow control policy and eXshield IPS information flow control policy on an operation that causes information flow to or from a subject that sends and receives information through the TOE. Therefore, it ensures that all operations that cause information flow to and from all subjects in the TSF are covered by eXshield information flow control policy and eXshield IPS information flow control policy.

6.1.3.2.1. Packet filtering (Packet_filtering)

The default policy has a rule to deny all except for an administrator IP; that is, it restricts all information flow until another policy is generated. Rules to allow some information flow can be added in accordance with the administrator-established policy, which will be enforced by the TOE. The policies set by an administrator may include to allow, deny, and, after blocking a packet, ‘Reset’ and ‘ICMP’ that sends ‘Reset’ or ‘ICMP Unreachable Code’ repectively to disable connection or raise an alarm .

Packet filtering rules include a function to control access forcedly by checking the access level of the source. Access will be allowed if the security level of the source is higher than or same as that of the destination. An authorized administrator can set the security level from 1 through 20.

The TOE allows the services explicitly specified to be allowed; otherwise it denies all services. The TOE will be delivered with no policy setting, so during installation an authorized administrator can configure a packet filtering rule that clearly specifies the packets to be allowed.

The TOE will terminate all interactive sessions if the time of any internal/external IT entity’s inactivity exceeds 30 minutes.

As the default policy denies all services, it can prevent possible mistakes that can be made at the establishment of policy by an administrator.

6.1.3.2.2. Intrusion prevention (Intrusion_prevention)

There is a possibility of a hacking attack that exhausts the resources of host or network and exploits vulnerabilities to cause an availability problem. To prevent this threat, an intrusion prevention system (IPS) is necessary that detects any illegal access or attack.

Intrusion prevention function is to monitor the attributes of an information that passes through the TOE and compare them with the block list to perform an action defined by an administrator on the information found out to be an attack.

- **Normal hacking**
  - Block a packet from outside with an internal network IP address
  - Block a packet from inside with an external network IP address
  - Block a packet from outside with an abnormal address
  - Block abnormal IP packet fragments
  - Block Land attack
  - Block a TCP connection with the same source port and destianation port
  - Block Ping of Death attack
  - Block ICMP Destination Unreachable packet
  - Block a packet with a Source Route option
  - Block an abnormal TCP stream

- **Signature check**
  - Detection and blocking of a packet by Signature

- **Traffic anomaly**
  - Whitelist check
  - SYN Flooding
  - UDP Flooding
  - Ping Flooding
  - Scanning attack

- **Protocol anomaly**
  - Block ICMP responses from the external network that are not requested
  - Detect and block DNS Cache Poisoning

- **2-layer protection**

- **URL Blocker function**

URL Blocker function blocks a request for access to a specific site by a general user in the TOE.

When a general user in the TOE requires an URL that is blocked by an authorized administrator of the TOE to access a specific web server outside the TOE, URL Blocker blocks the request.

To perform its function, URL Blocker extracts the URL the user sent to access web and compares it with the Table containing the information of the object of Blocking. If the data is found on the Table, terminate connection to the web page and send the Blocking page to the user who requested the page. If a URL of Domain is blocked, URL Blocker stores its IP in the Blocking Table and generates audit data. When the IP is in the Blocking Table, adding the IP is not necessary. Audit data will be generated on the blocked pages.

URL Blocker function can be used with reference to the information of the objects of Blocking and Blocking exception list made by an authorized administrator. The Table containing the information of the objects of Blocking categorizes in the block list registered by an administrator and the ICEC, Information Communication Ethics Committee, Korea.

The TOE counters an illegal attack at the detection of hacking during intrusion prevention in the way described in Table 6-2.

Table 6-3 Intrusion prevention functions countering an attack

Function	Description
Alarm	Upon detection of hacking, inform an administrator based on Hacking Log.
Block	When an hacking attack exceeds the level of blocking, inform KLSM of the set of IP addresses to be blocked so they will be prevented for a specified time.
IPS Signature Action	● **Drop** : Destroy a packet and record a log. ● **Reset** ・ TCP : Send an RST message and record a log. ・ UDP : Send a Port Unreachable message and record a log.

	▪ Other : Record a log. ● **Log** : Record a log. ● **Alarm** : Record an alarm log and inform the administrator of detection by IPS Signature using an alarm popup through the administrator program.

6.1.3.2.3. Network address translation (NAT)

The consumers using the TOE can, when they want public IP addresses or want to cover the IP address of the internal network, cover the address of the internal network from the external network using NAT (Network Address Translation) function. This function ensures the internal IP address unknown to the external network and minimizes the possibility of attack due to the exposure of the address. An authorized administrator can configure NAT at the installation.

The TOE provides four types of NAT function – Static NAT, LS (Load Sharing) NAT, Dynamic NAT, and PAT – which can be described as below:

Static NAT – Each IP address in the internal network is assigned one IP address to be used in the external network to make a pair of addresses, which will be translated by the same process at the connection to the external network. It is used for the request for connection from the external network to the internal network, or the other way around.

Dynamic NAT – Sets Pool of the internal IP address to be translated and IP addresses to be used in the external network. If an internal host belonging to the internal IP Pool requests connection to the external network, assign an unused IP randomly (i.e. dynamically) from the external IP Pool to it to be translated to an external IP. Store the internal IP – external IP pair of the session in a Table so packets passing in/out can be translated based on the Table.

PAT – Port Address Translation; Used when multiple IP addresses intend to make a session with the external network using one external IP address. The TOE maintains an internal IP – external IP translation table regarding the session that maps an external IP and port; when a packet related to the session (with a public destination IP), the TOE translates the IP into a corresponding one according to the table. This enables the TOE to maintain the session by correct translation even when a host with multiple internal IP addresses makes multiple sessions simultaneously using one external IP.

LS NAT – Loading Sharing NAT; Makes one external IP address correspond to multiple internal IP addresses and performs distributed translation of all sessions with a destination of the IP address into the assigned internal IP address to do load balancing.

- Round Robin: Change an internal IP to make a session in the order of request.

Requests for connection will equally be distributed to the internal hosts.

- Weighted Round Robin: More weighted way compared to a Round Robin. The more requests for connection will be accepted for the more weighted IP. For example, if there are A, B, and C hosts possessing the internal IP on a list to be translated and the weight on their IP is 3, 2, and 1 respectively, A, B, and C will respond to the request in the proportion of 3:2:1.
- Least Connection: When a request for connection is made by an external host, allow a session with a host that maintains the least sessions among the hosts registered in the internal IP list. It makes the number of maintained sessions distributed equally.
- Weighted Least Connection: More weighted way compared to a Least Connection. The more sessions shall be maintained by the more weighted IP. For example, if there are A and B hosts possessing the internal IP on a list to be translated and their IPs are defined to have a weight of 2(A) and 1(B) and maintaining 190(A) and 100(B) sessions respectively with the external network. At the request for connection, A accepts it because it doubles B in weight, although it currently has more sessions than B.
- Hashing: The hosts having the same external IP will make a session with the host having a specific internal IP. The hash of an external IP address will be calculated so a session can be made only with the host having an internal IP corresponding to that hash value.

6.1.3.2.4. Network traffic control (Traffic_control)

The TOE determines the maximum level of resource use by each network traffic. Network resource utilization function categorizes into a bandwidth limit and a session limit. Bandwidth limit can be set by an authorized administrator from the minimum 1Kbps through 1,000,000Kbps. Session limit can range from the minimum 60 through the maximum 800.000 for the unmarked application, or from 30 through 3,600 for the application under each policy. These functions prevent a certain user or group from exclusively possessioning the network resources regardless of an administrator's intention.

Traffic limit rule is to make the traffic that agrees with the policy established in packet filtering occupy bandwidth to the specified extent. It can be used to prevent a specific traffic overload from affecting another network utilization and protect a traffic from others.

Session limit function can be divided into two: "Limit total number of sessions of this policy" and "Limit the number of sessions for each source IP."

"Limit total number of sessions of this policy" inputs the number of session for the policy of the packet filtering rule currently applied and limits sessions. "Limit the number of sessions for each source IP" manages the count for each Src IP to determine whether to drop or not.

When "Block all sessions of the IP when the number of session is exceeded" function is activated, all sessions of the source IP will be blocked if the number of sessions including previously allowed sessions exceeds the limit defined by an administrator. When the function is deactivated, block the extra sessions of each source IP.

6.1.4. Security management (Sec_Man)

6.1.4.1. Management of security functions (Man_Sec_Fun)

An administrator can determine the behavior of, disable, enable, and modify the behavior of the following functions through the GUI administrator console. An administrator shall be first identified and authenticated to operate the GUI administrator console and log in to the console, which ensures these authorities are restricted to an authorized administrator.

Table 6-4 Management of security functions

Function	Capability
Action in case of possible audit storage failure	Determine the behavior, disable, and modify the behavior
Action in case of audit storage failure	Determine the behavior, disable, enable, and modify the behavior
Maintain rules for potential violation analysis	
Specify maximum quota of the number of session	
eXshield IPS information flow control	
Audit data backup	Determine the behavior and modify the behavior
Establish the cycle of audit data compression	
eXshield information flow control	
Manage user group with authority to read security audit review	
Terminate the GUI administrator console after a specified time of the authorized administrator's inactivity	
Selective audit data generation	Disable and enable
Receive reliable timestamps from the NTP server	
SNMP function	
Activate the function of NAT rule	
Action in case of security alarms	Disable, enable, and modify the behavior
Disable and reactivate system	Determine the behavior and enable
Action requiring trusted channel	Modify the behavior
Manage the group of authorized administrators that are part of a	Determine the behavior, enable,

role	and modify the behavior
Determine emailing an administrator in case of authentication failure	Determine the behavior
Unlock a disabled administrator by an authorized administrator	
Manual testing of an abstract machine	Enable
Check the TOE state and network information	
System backup and recovery	
Specify maximum quota of network traffic	Determine the behavior, disable, and enable

6.1.4.2. Management of security attributes (Man_Sec_attr)

The TOE provides a restrictive default value of the security attributes used for the administrator access control policy, eXshield information flow control policy, and eXshield IPS information flow control policy.

The authorized administrator of the TOE can change the default of, query, modify, delete, and generate the following security attributes. The management actions are described under each security requirement.

Table 6-5 Management of security attributes

SFP	Security attribute	Operation
Administrator access control policy	Administrator IP address	Change_default, modify, delete, and generate
	Administrator ID	Modify, delete, and generate
	Access level	Change_default, modify, delete, and generate
	Login options, execution	Change_default and modify
eXshield information flow control policy	Security level (1~20)	Change_default and modify
	Subject group	Query, modify, and delete
	IP address	Modify, delete, and generate
	Service (Port number)	Modify and generate
	Destination URI	Modify, delete, and generate
	Time	Modify
	Data information	Modify, delete, and generate
eXshield IPS information flow control policy	Destination URI	Modify, delete, and generate
	Time	Modify
	Data information	Modify, delete, and generate

The TSF provides a default value for a security attribute that is to be modified or established. Only a safe security attribute is allowed for the value. Invalid security attribute is delied to input. An administrator can change the default value of security attributes.

When a subject that intends to access the security label of an object that is the target of access

control, the security label of the list about the subject and object is assigned 20, which is the lowest level, as a default value. This defaule value cannot be changed. An administrator can change the security label.

- When a group object to which an object that is the target of access control belongs, the default is No Group, which means it belongs to no group. This default value cannot be changed.

6.1.4.3. Management of TSF data (Man_TSF_Data)

6.1.4.3.1. Restriction of TSF data management to an authorized administrator

An authorized administrator of the TOE can manage the following TSF data only through the GUI administrator console.

- TSF data for management

TSF data	Operation
Important files that form the TOE	Back up to a semi-permanent auxiliary memory and recover
Identification data	Delete and generate
Authentication data	Modify, delete, and generate
Time	Query and modify
System	
The number of administrator's login failure	
Time of the authorized administrator inactivity	
Bandwidth control rule	
Session control rule	
Limits on the file system	
Administrator access control policy eXshield information flow control policy eXshield IPS information flow control policy	Query, modify, delete, and generate
Administrator information	
TOE_LServer configuration information	
High Availability configuration information	
SNMP configuration information	

URL block rule	
Network interface information	
Ethernet bridging information	
Interface trunking information	
Routing information	
DNS information necessary to email an authorized administrator	
IPS Signature	Modify
The number of unsuccessful authentication attempts	
IPS signature update information	Query
CPU use of each Zone of DashBoard; memory use; current session, BPS, PPS, IPS signature check state	
Current server state	
Current session, NAT change table, IPS block list, current access administrator	

6.1.4.3.2. Management of limits on TSF data

The limit on audit trail can range from 1% through 100% (default 99%). Values other than the range are denied in the GUI administrator console. An authorized administrator cannot change the highest and lowest value.

The number of unsuccessful authentication attempts can be from 1 through 10 (default 3). Any number outside this scope will be denied input by the administrator console. This minimum and maximum limit cannot be changed even by an authorized administrator.

The time interval of self testing will be determined by the day and time specified by an administrator.

When TSF data reaches or exceed the predefined limit, the following actions should be taken:

- If the audit trail exceeds the predefined limit, 99% of the memory capacity:
  - Record audit
  - Email the administrator to take action
  - Use an alarm popup to inform the administrator that is logged on to the GUI administrator console

- If the number of unsuccessful authentication attempts reaches or exceeds the predefined limit:
  - Prevent re-authentication of the inactive user before any action by the authorized administrator
  - Record audit
  - Inform the authorized administrator using an alarm popup through the GUI administrator console
  - Send an email to the address registered by the authorized administrator

- If the limit on the bandwidth control is met or exceeded:
  - Record audit

6.1.4.3.3. IPS Signature update

IPS Signature includes a regular update and an urgent update. Regular update can be configured by an administrator to perform update daily or on a specific day. Urgent update allows downloading the updates to an IP address set by an administrator immediately or at an urgent update is required by SECUI Update server.

6.1.4.4. Management of security roles (Man_Sec_Role)

The TSF maintains the security role of an authorized administrator in the following manner:

Administrator registration

“Administrator” can mean both the administrator of TOE_Gateway and the administrator provided by the underlying OS of TOE_LServer. When the administrator of TOE_Gateway is registered at the initial installation of TOE_Gateway or through the GUI administrator console, the ID, password, and access level are stored in the administrator information list file. The administrator of TOE_LServer is registered at the installation of the underlying OS and its ID and password are stored. The TOE maintains the authorized administrator’s role in this way.

6.1.5. TSF stability (TSF_Safer)

6.1.5.1. HA function (High_Availability)

HA (high availability) function is provided for the kernels of the TOE to synchronize the session information and check operation state and roles. If HA warning or HA Reset occurs, it sends a warning screen when an administrator is using the GUI administrator console, send an email to the administrator, and records an audit log, as appropriate to the configuration of the warning log.

HA function realizes high availability as it distributes load by controlling traffic during a normal state and makes traffic sent only to active systems when required by a system. In order to prevent an incorrect enforcement of the TSF due to the distribution of traffic, HA function synchronizes NAT session, packet filtering, and IPS function block list and sends the packets it does not control to another system.

When multiple parts of TOE operating in HA mode are installed, an administrator assigns roles to Master, Backup Master, and Slave. The roles of each part are stated below:

Master :

- Checks that systems operating in HA mode are operating and make a list of the systems to notify Slaves.
- Manages Virtual IP, and when other system requires, changes the configuration of the Virtual IP to make traffic go to active systems only.

* Backup Master :

- Normally operates as a Slave and works Master's authorities as a proxy when Master cannot operate.
- When Master can normally operate again, detects it and turns the authorities over again.
- Not in the TOE. Included as additional description.

* Slave :

- Operates only in Slave mode.
- Can establish the name of a system, Network Interface Card setting, and Routing setting only.
- Other than the second bullet, operates exactly the same with Master of HA Zone it belongs to. Synchronizes with Master every one minute.

6.1.5.2. Security function stability self test (Secui_Self_Test)

To demonstrate the assumptions related to the underlying abstract machine of the TSF are correctly upheld, the TSF performs self testing during initial start-up or at the request of an authorized administrator regarding the following:

- **Self testing list**
  - Check process operating state
  - Check Disk state
  - Check data integrity
  - Check the operation of each interface
  - Check HA Link
  - Check HA state
  - Check Virtual IP address state
  - Check Kernel Memory size
  - ping
  - traceroute

A module that performs self test on the security stability will first check the state of process operating in the TOE and the usage of all disks connected to the TOE in KB. Then it will check the validity of all TSFs except for the audit record, which is the list of files for integrity check, and perform integrity check on the TSF data files and executable files on the list. Integrity check will be performed during initial start-up, periodically during normal operation, and at the request of an authorized administrator. Then it will check the operation and state of the network interface on the TOE environment file and, when configuring HA, check the physical Link state between two systems on the TOE environment file. The operation of HA will also be checked at the HA configuration.

6.1.5.3. TSF protection (TSF_Protection)

The TOE located on the contact of networks so all traffic from the internal(external) network will pass through the TOE to comminucate with the external(internal) network. Non-bypassability of the TSP is satisfied in the following manner: When a traffic arrives at one of the internal(external) network ports in the TOE, it will unexceptionally pass through the kernel module and according to the packet contents an appropriate TSP will be enforced by the security functions and sent to the external(internal) network through the external(internal) network port.

The TOE implements a function to make a trusted management channel using SSL communication provided by the IT environment. An IT entity to which an administrator accesses downloads from the TOE a compressed file related to Java program through the Web browser. The file will be executed by JRE(Java runtime environment) to provide an administrator console based on Java. SSL (protocol version SSL V3) will be used to secure the integrity and confidentiality of the data transmitted during the communication between that administrator console and the TOE. The TSF keeps a server state with the TCP port setup open and makes an SSL session at the request for a session by the administrator console. Key exchange is done by RSA(1024bit), data encryption by 3DES (168bit; operational mode CBC), and message integrity check by HMAC SHA-1, which ensures TSF data transmission through a trusted channel during the communication between the administrator console and the TSF.

6.1.5.4. Process monitoring (Mon_Process)

The TOE supports an authorized administrator's activities through the GUI and CLI administrator consoles when any errors occur. This provides not only a function for security management but a function to safely recover the state in case of any error.

Trusted recovery is possible by a process monitoring function, which monitors the operation of Application Processes for each security function of the TOE. It enables an administrator to provide the services of the security functions set by the administrator continuously, not to be interrupted by an error.

When an administrator generates a security policy, it will be stored in the configuration file. Correct operation of the process corresponding to the policy is required to provide a security function correctly. It's impossible to provide the security function if the process is deleted or not operating due to an error.

It checks the requisite processes that correspond to the security functions established by an administrator in the configuration file. Then it checks if the process exists in the current system and is normally operating. In case that a process that should be operating is abnormally operating or not operating at all, it reactivates the process so a security function can be provided correctly.

It can also monitor the monitoring process to ensure its correct operation. In case that the monitoring process is abnormally operatinf or not operating at all, it reactivates it so a security function can be provided correctly.

6.2. Assurance measures

Table 6-6 Assurance measures

Assurance class	Assurance component		Assurance measures
Configuration management	ACM_AUT.1	Partial CM automation	eXshield V1.0.1.R Configuration Management Version 1.4
	ACM_CAP.4	Generation support and acceptance procedures	
	ACM_SCP.2	Problem tracking CM coverage	
Delivery and operation	ADO_DEL.2	Detection of modification	eXshield V1.0.1.R Delivery Guide Version 1.1
	ADO_IGS.1	Installation, generation, and start-up procedures	eXshield V1.0.1.R Installation Guide Version 1.0
Development	ADV_FSP.2	Fully defined external interfaces	eXshield V1.0.1.R Functional Specification Version 1.7
	ADV_HLD.2	Security enforcing high-level design	eXshield V1.0.1.R High-level Design Version 1.7
	ADV_IMP.1	Subset of the implementation of the TSF	eXshield V1.0.1.R Implementation Validation Version 1.2 Source code
	ADV_LLD.1	Descriptive low-level design	eXshield V1.0.1.R Low-level Design Version 1.3

	ADV_RCR.1	Informal correspondence demonstration	eXshield V1.0.1.R Correspondence Analysis Version 1.3
	ADV_SPM.1	Informal TOE security policy model	eXshield V1.0.1.R Security Policy Modeling Version 1.5
Guidance documents	AGD_ADM.1	Administrator guidance	eXshield V1.0.1.R Administrator Guidance Version 1.5
	AGD_USR.1	User guidance	Not provided
Life cycle support	ALC_DVS.1	Identification of security measures	eXshield V1.0.1.R Life Cycle Support Version 1.3
	ALC_LCD.1	Developer defined life-cycle model	
	ALC_TAT.1	Well-defined development tools	
Tests	ATE_COV.2	Analysis of coverage	eXshield V1.0.1.R Tests Version 1.4
	ATE_DPT.1	Testing: high-level design	
	ATE_FUN.1	Functional testing	
	ATE_IND.2	Independent testing – sample	
Vulnerability assessment	AVA_MSU.2	Validation of analysis	eXshield V1.0.1.R Vulnerability and Misuse Analysis Version 1.3
	AVA_SOF.1	Strength of TOE security function evaluation	
	AVA_VLA.2	Independent vulnerability analysis	

7. PP claims

This chapter describes the protection profile to which this ST claims conformance.

7.1. PP reference

This ST claims conformance to the following protection profile and thus satisfies the objectives and security requirements for the TOE in the following protection profile:

- Network Intrusion Prevention System Protection Profile v1.1(21 Dec. 2005)

7.2. PP tailoring

This ST claims PP tailoring against the PP to which it conforms as the following:

This ST has changed the description of O.Information in the PP into “The TOE shall control all unauthorized import or export of information between the internal and external.”

This ST has changed the security objective for the environment OE.Vulnerability in the PP into the security objective for the TOE O.Vulnerability.

From the security functional requirements in the PP, FIA_UAU.1 is changed into FIA_UAU.2 in this ST, as the TSF does not allow any TSF-mediated actions before successful authentication.

From the TOE security functional requirements in the PP, FPT_STM.1 and FTP_ITC.1 are changed into the security functional requirements for the IT environment.

This ST does not require a user guidance because the TOE does not use any functions from AGD_USR.1.

Table 7-1 PP tailoring

Functional component		Operation
FAU_ARP.1	Security alarms	Decided by the ST author
FAU_GEN.1	Audit data generation	Assignment
FAU_GEN.2	User identity association	-
FAU_SAA.1	Potential violation analysis	Assignment
FAU_SAR.1	Audit review	-
FAU_SAR.3	Selectable audit review	Assignment; selection
FAU_SEL.1	Selective audit	Assignment; selection
FAU_STG.1	Protected audit trail storage	Selection
FAU_STG.3	Action in case of possible audit data loss	Assignment
FAU_STG.4	Prevention of audit data loss	Assignment; selection
FDP_IFC.1(1)	Subset information flow control(1)	Refinement
FDP_IFC.1(2)	Subset information flow control(2)	Refinement
FDP_IFF.1	Simple security attributes	Assignment; Decided by the ST author; iteration
FIA_AFL.1	Authentication failure handling	Assignment; selection
FIA_ATD.1(1)	User attribute definition(1)	Decided by the ST author
FIA_ATD.1(2)	User attribute definition(2)	Decided by the ST author
FIA_UAU.1	Timing of authentication	-
FIA_UAU.7	Protected authentication feedback	Assignment
FIA_UID.2(1)	User identification before any action(1)	-
FIA_UID.2(2)	User identification before any action(2)	-
FMT_MOF.1	Management of security functions	Assignment; selection
FMT_MSA.1	Management of security attributes	Assignment; selection
FMT_MSA.3	Static attribute initialization	Assignment; selection
FMT_MTD.1	Management of TSF data	Assignment; selection
FMT_MTD.2	Management of limits on TSF data	Assignment
FMT_SMF.1	Specification of management functions	Assignment
FMT_SMR.1	Security roles	-
FPT_AMT.1	Abstract machine testing	Assignment; selection; refinement
FPT_FLS.1	Failure with preservation of secure state	Assignment
FPT_RVM.1	Non-bypassability of the TSP	-
FPT_SEP.1	TSF domain separation	-

Functional component		Operation
FPT_STM.1	Reliable time stamps	Refinement
FPT_TST.1	TSF testing	Selection; assignment; refinement
FRU_FLT.1	Degraded fault tolerance	Assignment
FRU_RSA.1	Maximum quotas	Selection; assignment; iteration; refinement
FTA_SSL.1	TSF-initiated session locking	Assignment
FTA_SSL.3	TSF-initiated termination	Assignment
FTP_ITC.1	Inter-TSF trusted channel	Selection; assignment; refinement

7.3. PP additions

Table 7-2 PP additions

	Additions
TOE security environment	A.Server
	T.Export
	T.AttackTSFdata
	TE.Time
Security objective	O.Access
	OE.IA
	OE.Timestamp
	OE.Channel
	OE.Server
Security requirements for the TOE	FDP_ACC.2 Complete access control
	FDP_ACF.1 Security attribute based access control
	FIA_SOS.1 Verification of secrets
Security requirements for the IT environment	FIA_UAU.2 User authentication before any action
	FIA_UID.2 User identification before any action
	FPT_ITT.1 Basic internal transfer protection
	FPT_RCV.4 Function recovery

8. Rationale

This chapter describes the evidence used in the evaluation of this ST. It supports the claims that the ST is a complete and cohesive set of requirements, that the conformant TOE provides an effective set of IT security countermeasures within the security environment, and that the TOE summary specification addresses the requirements.

8.1. Security objectives rationale

Security objectives rationale shows that the specified security objectives are suitable, sufficient to address security problem, and not onerous.

The security objectives rationale demonstrates that:

Each assumption, threat, and OSP is addressed by at least one security objective.
Each security objective addresses at least one assumption, threat, or OSP.

The following table shows the rationale for the security objectives.

Table 8-1 Security objectives rationale

Security objective / Security environment	Security objectives for the TOE											Security objectives for the environment									
	O.Availability	O.Audit	O.Administration	O.Packet	O.DoS	O.Identification	O.Authentication	O.Information	O.TSFdata	O.Vulnerability	O.Access	OE.Locate	OE.Security	OE.Administrator	OE.Administration	OE.OSpatch	OE.Connection	OE.IA	OE.Timestamp	OE.Channel	OE.Server
A.Locate												X			X						
A.Security													X								
A.Administrator														X							
A.OSpatch																X					
A.Connection																	X				
A.Server																					X
T.Masquerade		X				X	X											X			
T.Failure	X								X						X	X					
T.Record	X	X																			
T.Import			X					X													
T.Service			X					X													
T.Packet		X		X		X															
T.Vulnerability			X							X			X		X	X					
T.DoS		X			X	X															

Security objective / Security environment	Security objectives for the TOE											Security objectives for the environment									
	O.Availability	O.Audit	O.Administration	O.Packet	O.DoS	O.Identification	O.Authentication	O.Information	O.TSFdata	O.Vulnerability	O.Access	OE.Locate	OE.Security	OE.Administrator	OE.Administration	OE.OSpatch	OE.Connection	OE.IA	OE.Timestamp	OE.Channel	OE.Server
T.Authentication		X				X	X														
T.Bypass	X							X			X	X					X				
T.Spoofing		X		X	X	X															
T.ModifyTSFdata	X	X				X			X												
T.Export			X					X													
T.AttackTSFdata																				X	
TE.Administration			X											X	X						
TE.Delivery														X	X						
TE.Time																			X		
P.Audit		X				X															
P.Administration			X											X	X						

8.1.1. Rationale for the security objectives for the TOE

The following are the rationale for the security objectives for the TOE.

O.Availability

This objective provides the availability of the TOE to provide the minimum network services in case of a failure in the TOE or overload of the TOE due to an attack.

Thus it ensures the availability of the TOE against T.Failure, T.ModifyTSFdata, T.Bypass, and T.Record, which is a threat of an audit storage exhaustion.

O.Audit

This objective ensures that, when a user uses security functions, the TOE generates audit data about each user according to the audit policy and that the TOE provides a means to maintain and review the records in a safe manner. It ensures that the TOE provides a function to take actions in case of the audit data is full. Audit data generation ensures that the TOE can detect an attacker's identity using the audit records in case of consecutive authentication attempts. Audit records also enables the TOE to trace an IP spoofing attack, DoS attack, and an attack sending an abnormal packet.

Thus it counters T.Masquerade, T.Record, T.Packet, T.DoS, T.Authentication, T.Spoofing, and T.ModifyTSFdata, and supports P.Audit.

O.Administration

The TOE controls illegal access to the internal network and illegal export of data through the internal network based on the information flow control rules established in order to enforce the security policies. To this end, the TOE shall provide a means to securely administer the TSF data and the TOE such as the TOE configuration data generation and management, update vulnerability signature management.

Thus it counters T.Import, T.Service, T.Vulnerability, T.Export, and TE.administration, and supports P.Administration because it provides a means for an authorized administrator to administer the TOE securely.

O.Packet

This objective ensures that the packets that do not conforming to TCP/IP standard, the packets sent from the external network with an internal network address, broadcasting packets, or looping packets are not imported to the internal network.

Thus it counters T.Packet and T.Spoofing.

O.DoS

An attacker may launch a DoS attack on the internal computers through the TOE. One of the examples of DoS attack may be the case where a remote user requests for an abnormally excessive services from the internal computer finally to exhaust the computer resources. It is possible for the internal computer to assign too many resources to the attacker so another users cannot user the computer. To prevent this, the TOE ensures that normal users can use the computer by preventing the computer from assigning resources exclusively to a user.

Thus it counters T.DoS and T.Spoofing.

O.Identification

The TOE users include an administrator that manages the TOE through an authorized access and an external user (IT entity) that passes the TOE without authentication to user an internal computer. Both of them requires identification to handle security-related events. Identification of an administrator is necessary to give accountability to all actions by an administrator. Identification of an external IT entity is necessary to generate audit records on an abnormal packet transfer, blocking a DoS attack, blocking IP spoofing attack, and an external IT entity's attempt to access.

Thus it counters T.Masquerade, T.DoS, T.Spoofing, T.Packet, T.Authentication, and T.ModifyTSFdata, and supports P.Audit.

O.Authentication

Any user that intends to access the TOE shall be authenticated. The authentication required for the TOE access, however, may be vulnerable to consecutive authentication attempts by an external attacker. The TOE shall therefore ensure an authentication mechanism resistant to the level of the consecutive authentication attempts by the attacker.

Thus it counters T.Masquerade and T.Authentication.

O.Information

The TOE locates on the connection that separates an internal network and an external network and controls information flow based on a security policy. This objective ensures that the TOE identifies and blocks various attacks that can be made in the networks in accordance with a deny policy and allow policy. These attacks include a virus attack, email or Web service containing an illicit information, or access to services without permission. The TOE protects the security of the internal network by preventing the attacks from being imported.

Thus it counters T.Import, T.Service, and T.Bypass.

This also ensures that the TOE controls information flow from the internal network to external network

according to a security policy.

Thus it counters T.Export.

O.TSFdata

The security policy of the TOE may not be enforced appropriately due to a modification of the TSF data resulting from an unexpected attack or TOE failure without an administrator's recognition. This objective ensures that the TOE checks any intentional or unintentional modification to the TSF data for a correct operation of the TSF.

Thus it counters T.Failure and T.ModifyTSFdata.

O.Access(*)

This objective ensures that an access to the TOE is controlled.

Thus it counters T.Bypass.

O.Vulnerability

This object ensures that the TOE updates and manages the database on vulnerabilities to protect the TOE and resources of the internal network of the TOE from an external attack exploiting new vulnerabilities of the TOE and resources.

Thus it counters T.Vulnerability.

8.1.2. Rationale for the security objectives for the environment

The following are the rationale for the security objectives for the environment of the TOE.

OE.Locate

This objective ensures that the TOE is located and operating in a physically secure environment, consequently that it is protected from an external physical attack and an attempt to modify the TOE. Thus it upholds A.Locate and counters T.Bypass.

OE.Security

This objective ensures that, when the internal network environment changes due to a network configuration change, increase or decrease of host or services, the changed environment and security policies will immediately be reflected to the TOE operational policy to maintain the same security as before. Thus it upholds A.Security and counters T.Vulnerability.

OE.Administrator

This objective ensures that the authorized administrator of the TOE can be trusted. Thus it upholds A.Administrator and P.Administration, and counters TE.Delivery.

OE.Administration

This objective ensures that the TOE is delivered and installed in a secure manner and is configured, administered, and used in a secure way by an authorized administrator. Thus it counters T.Failure, T.Vulnerability, TE.Administration, and TE.Delivery, and upholds A.Locate and P.Administration.

OE.OSpatch

This objective ensures that services or measures not required by the TOE will be eliminated and patches for the vulnerabilities will be performed to ensure confidence and stability of the OS. Thus it upholds A.OSpatch and counters T.Failure and T.Vulnerability.

OE.Connection

This objective ensures that all communications between the external network and internal network will be mediated by the TOE. Thus it counters T.Bypass and upholds A.Connection.

OE.IA(*)

This objective ensures that the log server manager will be identified and authenticated by the

underlying OS before allowed to access TOE_LServer. Thus it counters T.Masquerade.

OE.Timestamp(*)

This objective ensures that the TOE receives reliable time source for audit data storage and regular Signature update. Thus it counters TE.Time.

OE.Channel(*)

This objective ensures that the TOE will be provided with a trusted channel using SSL for secure communication between TOE_Gateway and TOE_LServer, TOE and SECUI Update server, or the TOE and GUI administrator console. Thus it counters T.AttackTSFdata.

OE.Server(*)

This objective ensures that the external servers that the TOE interacts with for its functions are secure. Thus it upholds A.Server.

8.2. Security requirements rationale

This chapter demonstrates that the described IT security requirements are suitable to meet the security objectives and, consequently, to address security problem.

The security functional requirements described in this ST support each other and the combination of more than one security requirements satisfies the security objectives.

8.2.1. Rationale for the TOE security functional requirements

The table below shows a mapping between the SFRs and security objectives. Each security objective for the TOE is addressed by at least one TOE SFR.

Table 8-2 Mapping SFRs to the security objectives

Security objective / SFR	O.Availability	O.Audit	O.Administration	O.Packet	O.DoS	O.Identification	O.Authentication	O.Information	O.TSFdata TSF	O.Access	O.Vulnerability
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_ACC.2									X	X	
FDP_ACF.1									X	X	
FDP_IFC.1(1)								X			

Security objective / SFR	O.Availability	O.Audit	O.Administration	O.Packet	O.DoS	O.Identification	O.Authentication	O.Information	O.TSFdata TSF	O.Access	O.Vulnerability
FDP_IFC.1(2)								X			
FDP_IFF.1(1)								X			
FDP_IFF.1(2)				X				X			
FIA_AFL.1							X				
FIA_ATD.1(1)		X		X	X	X		X			
FIA_ATD.1(2)		X				X					
FIA_SOS.1							X				
FIA_UAU.2			X				X		X		
FIA_UAU.4							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	X	
FMT_MSA.3			X					X	X	X	
FMT_MTD.1			X						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_RCV.4	X										
FPT_RVM.1								X			
FPT_SEP.1								X	X		
FPT_TST.1	X								X		
FRU_FLT.1	X							X			
FRU_RSA.1(1)					X						
FRU_RSA.1(2)								X			

Security objective / SFR	O.Availability	O.Audit	O.Administration	O.Packet	O.DoS	O.Identification	O.Authentication	O.Information	O.TSFdata TSF	O.Access	O.Vulnerability
FTA_SSL.1									X		
FTA_SSL.3					X						

FAU_ARP.1 Security alarms

This component satisfies O.Audit because it ensures an ability to take actions at the detection of security violations.

FAU_GEN.1 Audit data generation

This component satisfies O.Audit because it ensures an ability to define auditable events and generate audit records.

FAU_GEN.2 User identity association

This component satisfies O.Audit because it requires a user to be identified to define auditable events and associate each audit record with a user.

FAU_SAA.1 Potential violation analysis

This component satisfies O.Audit because it ensures an ability to indicate a security violation by monitoring the audited events.

FAU_SAR.1 Audit review

This component satisfies O.Audit because it ensures an ability of an authorized administrator to review the audit records.

FAU_SAR.3 Selectable audit review

This component satisfies O.Audit because it ensures an ability to search and sort audit data based on criteria with logical relations.

FAU_SEL.1 Selective audit

This component satisfies O.Audit because it ensures an ability to include or exclude auditable events based on attributes.

FAU_STG.1 Protected audit trail storage

This component satisfies O.Audit because it ensures an ability to protect the audit records from unauthorized modification or deletion.

FAU_STG.3 Action in case of possible audit data loss

This component satisfies O.Audit because it ensures an ability to take actions if the audit trail exceeds pre-defined limit.

FAU_STG.4 Prevention of audit data loss

This component satisfies O.Audit because it ensures an ability to take actions if the audit trail is full.

FDP_ACC.2 Complete access control(*)

This component satisfies O.TSFdata and O.Access because it ensures that a security policy for an administrator access control is defined and that the scope covered by the policy is defined.

FDP_ACF.1 Security attribute based access control(*)

This component satisfies O.TSFdata and O.Access because it ensures that a defined security policy is enforced based on attributes.

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

This component satisfies O.Information because it ensures that a security policy for eXshield information flow control is defined and that the scope covered by the policy is defined.

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

This component satisfies O.Information because it ensures that a security policy for eXshield IPS information flow control is defined and that the scope covered by the policy is defined.

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

This component satisfies O.Information because it provides a function to control information flow based on the security attributes of a subject and information according to eXshield information flow control policy.

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

This component satisfies O.Packet and O.Information because it provides a function to control information flow based on the security attributes of a subject and information according to eXshield IPS information flow control policy.

FIA_AFL.1 Authentication failure handling

This component satisfies O.Authentication because it defines the number of unsuccessful authentication attempts of an administrator to be detected and provides an ability to take actions when the defined number is met or surpassed, thus ensures that an administrator cannot access the GUI administrator console without authentication.

FIA_ATD.1(1) User attribute definition(1)

This component requires that the TOE shall identify an external IT entity by the IP address of a computer, which is the ground to generate audit records on an external IT entity, to determine whether it is forged, to determine a DoS attack, and control information flow. Thus it satisfies O.Audit, O.Packet, O.DoS, O.Identification, and O.Identification.

FIA_ATD.1(2) User attribute definition(2)

This component satisfies O.Audit and O.Identification because it requires the security attributes of an administrator to be identified.

FIA_SOS.1 Verification of secrets(*)

This component satisfies O.Authentication because it provides a mechanism to verify that secrets meet the defined metric.

FIA_UAU.2 User authentication before any action

This component satisfies O.Administration, O.TSFdata (Authentication of an administrator is required for the TOE management and TSF data protection), and O.Authentication because it ensures an ability to authenticate an administrator before any action.

FIA_UAU.4 Single-use authentication mechanism(*)

This component O.Authentication because it ensures an ability to prevent reuse of authentication data.

FIA_UAU.7 Protected authentication feedback

This component O.Authentication because it ensures that only a specified authentication feedback will be provided to a user while the authentication is in progress.

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

This component requires that the TOE shall identify an external IT entity by the IP address of a computer, which is the ground to generate audit records on an external IT entity, to determine whether it is forged, to determine a DoS attack, and control information flow. Thus it satisfies O.Audit, O.Packet, O.DoS, O.Identification, and O.Information.

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

This component satisfies O.Audit and O.Administration, O.TSFdata, and O.Identification because it requires that an administrator identifies itself.

FMT_MOF.1 Management of security functions

This component satisfies O.Availability and O.Administration because it ensures that an authorized administrator is able to manage the security functions and securese the availability in case of the TOE failure.

FMT_MSA.1 Management of security attributes

This component satisfies O.Administration, O.TSFdata, O.Information, and O.Access because it ensures that only an authorized administrator can access the security attributes data, which is the TSF data required in performing the TOE security functions.

FMT_MSA.3 Static attribute initialization

This component satisfies O.Administration, O.TSFdata, O.Information, and O.Access because it ensures that only an authorized administrator can access the security attributes data, which is the TSF data required in performing the TOE security functions, to initialize it.

FMT_MTD.1 Management of TSF data

This component satisfies O.Administration and O.TSFdata because it requires a function for an authorized administrator to manage the TSF data. It also satisfies O.Vulnerability because it ensures regular update for the Signature update.

FMT_MTD.2 Management of limits on TSF data

This component satisfies O.Availability and O.Administration because it secures the availability of the TOE by defining the limits for the TSF data and and ensuring that actions will be taken if the TSF data are at or exceed the indicated limits.

FMT_SMF.1 Specification of management functions

This component satisfies O.Administration because it requires the specification of the security management functions of the security attributes, TSF data, and security functions that the TSF shall enforce.

FMT_SMR.1 Security roles

This component satisfies O.Administration, O.Identification, and O.Authentication because it requires the role of the TOE security administrator to be restricted to an administrator role.

FPT_AMT.1 Abstract machine testing

This component satisfies O.Availability and O.TSFdata because it requires a suite of tests to demonstrate the correct operation of the abstract machine that underlies the TSF.

FPT_FLS.1 Failure with preservation of secure state

This component satisfies O.Availability and O.Information because it ensures that the TOE preserves secure state for the operation of important security functions and performs information flow control when failure occurs in the TOE.

FPT_RCV.4 Function recovery(*)

This component satisfies O.Availability because it ensures that the TOE recovers the functions through reactivation of process in case of an abnormal termination of the application process that forms the TOE.

FPT_RVM.1 Non-bypassability of the TSP

This component O.Information because it ensures that TSP enforcement functions are invoked and succeed, thus prevents bypass of information flow control.

FPT_SEP.1 TSF domain separation

This component satisfies O.TSFdata and O.Information because it ensures that the TSF maintains a security domain for its own execution that protects it from untrusted subjects.

FPT_TST.1 TSF testing

This component satisfies O.Availability and O.TSFdata because it ensures the self tests of the TSF to demonstrate the correct operation of the TSF and requires a function to verify the integrity of the TSF data and TSF executable code, thus ensures prevention or a prompt detection of the TOE failure.

FRU_FLT.1 Degraded fault tolerance

This component satisfies O.Availability and O.Information because it ensures that the TOE maintains important security functions in case of failure and performs information flow control.

FRU_RSA.1(1) Maximum quotas(1)

This component satisfies O.DoS because it requires a function to restrict the quotas of resource usage of the assets protected by the TOE for each user, thus prevents a DoS attack.

FRU_RSA.1(2) Maximum quotas(2)

This component satisfies O.Information because it enforces maximum quotas of the network traffic and session used simultaneously by individual IT entity or defined group of users, thus controls an excessive use of the network by a specific user.

FTA_SSL.1 TSF-initiated session locking

This component satisfies O.TSFdata because it requires a function to lock an authorized session after a defined time of an authorized administrator's inactivity.

FTA_SSL.3 TSF-initiated termination

This component satisfies O.DoS because it secures the availability of the network services by requiring the session with the internal computer to be terminated after a defined time of an external IT entity's inactivity.

8.2.2. Rationale for the TOE assurance requirements

This ST is consistent with EAL4, the assurance level of Network Intrusion Prevention System Protection Profile.

8.2.3. Rationale for the security requirements for the IT environment

Table 8-3 IT Rational for the security requirements for the IT environment

Security objective / SFR	OE.Timestamp	OE.Channel	OE.IA
FIA_UAU.2			X
FIA_UID.2			X
FPT_ITT.1		X	
FPT_STM.1	X		
FTP_ITC.1		X	

FIA_UAU.2 User authentication before any action

The underlying OS satisfies OE.IA because it ensures an ability to successfully authenticate a log server manager before any action.

FIA_UID.2 User identification before any action

The underlying OS satisfies OE.IA because it ensures an ability to successfully identify a log server manager before any action.

FPT_ITT.1 Basic internal TSF data transfer protection

The IT environment of the TOE satisfies OE.Channel because it protects the TSF data from

disclosure using SSL communication during transmitted between TOE_Gateway and TOE_LServer, which are the components of the distributed TOE.

FPT_STM.1 Reliable time stamps

The IT environment of the TOE satisfies the requirements corresponding to OE.Timestamp because the TOE receives reliable time stamps from the NTP server and underlying OS.

FTP_ITC.1 Inter-TSF trusted channel

The IT environment of the TOE satisfies the requirements corresponding to OE.Channel because the TOE is provided with a management function for a secure channel when an authorized administrator accesses the GUI administrator console for the TOE management and when the TOE communicates with SECUI Update server for the vulnerability Signature list update.

8.3. Dependencies rationale

8.3.1. Dependencies between the TOE security functional requirements

Table 8-4 shows the dependencies between the functional components.

Table 8-4 Rationale for the dependencies between SFRs

No.	Functional component	Dependencies	Ref No.
1	FAU_ARP.1	FAU_SAA.1	4
2	FAU_GEN.1	FPT_STM.1	36
3	FAU_GEN.2	FAU_GEN.1	2
		FIA_UID.1	23
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	2
		FMT_MTD.1	27
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_ACC.2	FDP_ACF.1	12
12	FDP_ACF.1	FDP_ACC.1	11
		FMT_MSA.3	26
13	FDP_IFC.1(1)	FDP_IFF.1(1)	15
14	FDP_IFC.1(2)	FDP_IFF.1(2)	16
15	FDP_IFF.1(1)	FDP_IFC.1(1)	13
		FMT_MSA.3	26
16	FDP_IFF.1(2)	FDP_IFC.1(2)	14
		FMT_MSA.3	26
17	FIA_AFL.1	FIA_UAU.1	20
18	FIA_ATD.1	-	-

19	FIA_SOS.1	-	-
20	FIA_UAU.2	FIA_UID.1	23
21	FIA_UAU.4	-	-
22	FIA_UAU.7	FIA_UAU.1	20
23	FIA_UID.2	-	-
24	FMT_MOF.1	FMT_SMF.1	29
		FMT_SMR.1	30
25	FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1]	[11 or 13, 14]
		FMT_SMF.1	29
		FMT_SMR.1	30
26	FMT_MSA.3	FMT_MSA.1	25
		FMT_SMR.1	30
27	FMT_MTD.1	FMT_SMF.1	29
		FMT_SMR.1	30
28	FMT_MTD.2	FMT_MTD.1	27
		FMT_SMR.1	30
29	FMT_SMF.1	-	-
30	FMT_SMR.1	FIA_UID.1	23
31	FPT_AMT.1	-	-
32	FPT_FLS.1	ADV_SPM.1	SAR
33	FPT_RCV.4	ADV_SPM.1	SAR
34	FPT_RVM.1	-	-
35	FPT_SEP.1	-	-
36	FPT_STM.1	-	-
37	FPT_TST.1	FPT_AMT.1	31
38	FRU_FLT.1	FPT_FLS.1	32
39	FRU_RSA.1	-	-
40	FTA_SSL.1	FIA_UAU.1	20
41	FTA_SSL.3	-	-
42	FTP_ITC.1	-	-
43	FTP_ITT.1	-	-

FDP_ACF.1 is dependent on FDP_ACC.1, which is satisfied by FDP_ACC.2 hierarchical to

FDP_ACC.1.

FAU_GEN.2, FIA_UAU.2, and FMT_SMR.1 are dependent on FIA_UID.1, which is satisfied by FIA_UID.2 hierarchical to FIA_UID.1.

FMT_MSA.1 is dependent on FDP_ACC.1 or FDP_IFC.1, which is satisfied by FDP_ACC.2 hierarchical to FDP_ACC.1 or FDP_IFC.1.

8.3.2. Dependencies between the TOE assurance requirements

The assurance measures of the TOE are the same set of assurance families of EAL4 from CC Part 3. Consequently, the dependencies between each assurance package are satisfied.

The assurance level of this ST – EAL4 – is considered suitable for the environment of the TOE.

8.4. Rationale for complementary components

This section analyzes the complementary relations between the TOE security functional components that are used to prevent bypass and tampering.

8.4.1. Bypass

Bypass means when unauthorized users access the TSF and its data to which they don't have an access right. The following functions prevent bypass of the security functions.

FPT_RVM.1 ensures that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

FDP_IFC.1 and FDP_IFF.1 prevent bypass because they ensure that eXshield information flow control policy will apply to all packets that pass through the TOE.

8.4.2. Tampering

The following functions prevent and detect tampering with the TSF and TSF data.

FPT_SEP.1 requires that the TSF maintains a security domain for its own execution that protects it from interference and tampering by untrusted subjects and the the TSF enforces separation between the security domains of subjects in the TSC.

FDP_IFC.1 and FDP_IFF.1 support prevention of modification because they ensure that the external network and internal network are separated so that they cannot tamper with each other through the TOE.

8.4.3. Disabling

The TOE provides the following functions to prevent attacks trying to disable security enforcement.

Security audit (FAU) class gives a ground to generate audit data on the security relevant events, to

determine an address forgery, to decide a DoS attack, and to control information flow. FAU also provides an administrator with a function to review audit data so the malicious attacks disabling security functions are detected. It supports FDP_IFC.1 and FDP_IFF.1.
FPT_TST.1 detects when the TOE is disabled as it verifies the integrity of data.

8.4.4. Deactivation

The following functions prevent the deactivation of the security functions.

FMT_MOF.1 prevents the deactivation of the security functions because it ensures that only an authorized administrator can manage the TOE security functions and TSF data.
FAU_STG.3 and FAU_STG.4 prevent the deactivation of the security audit functions.

8.5. SOF rationale

The information protected by the TOE in this ST is a general material possessing a medium value of assets. A threat agent is assumed to have low-level expertise, resources, and motivation. The CEM recommends that the TOE shall provide a minimum SOF-medium to counter a threat agent possessing a low attack potential. This ST determines and claims SOF-medium based on the probabilistic permutational mechanism considering the attack potential and value of assets.

The security functions in the ST to which a minimum SOF is claimed conform the corresponding functional components in Table 8-5 Functional components mapped to the security function with SOF claimed. The specified SOF flaim and minimum SOF satisfy the security objectives for the TOE Table 8-6 TOE security objectives mapped to the claimed SOF-medium

Table 8-5 Functional components mapped to the security function with SOF claimed

Functional component		Security function
FIA_UAU.2	User authentication before any action	Administrator identification and authentication (Admin_InA)
FIA_UAU.4	Single-use authentication mechanism	

Table 8-6 TOE security objectives mapped to the claimed SOF-medium

SOF	Security function	Security objective
Medium	Administrator identification and authentication (Admin_InA)	O.Authentication

8.6. TOE summary specification rationale

This chapter show that the TOE security functions are suitable to meet the IT security requirements.

8.6.1. Security functions corresponding to IT security requirements

The following Table 8-7 shows that the IT security requirements satisfy the security functions described above.

Table 8-7 Security functions mapped to the IT security requirements

Security function	IT security requirement
Audit generation and protection (Audit_Gen_Protect)	FAU_ARP.1
	FAU_GEN.1
	FAU_GEN.2
	FAU_SAA.1
	FAU_SEL.1
	FAU_STG.1
	FAU_STG.3
	FAU_STG.4
Audit review (Audit_Review)	FAU_SAR.1
	FAU_SAR.3
Administrator registration (Admin_Register)	FIA_ATD.1(2)
	FIA_SOS.1
	FMT_MTD.1
Administrator identification and authentication (Admin_InA)	FIA_AFL.1
	FIA_ATD.1(2)
	FIA_UAU.2
	FIA_UAU.4
	FIA_UAU.7
	FIA_UID.2(2)

	FTA_SSL.1
Administrator access control (Admin_acc_ctrl)	FDP_ACC.2
	FDP_ACF.1
Packet filtering (Packet_filtering)	FDP_IFC.1(1)
	FDP_IFF.1(1)
	FIA_ATD.1(1)
	FIA_UID.2(1)
	FTA_SSL.3
Intrusion prevention (Intrusion_Prevention)	FDP_IFC.1(2)
	FDP_IFF.1(2)
	FRU_RSA.1(1)
Network address translation (NAT)	FDP_IFC.1(1)
	FDP_IFF.1(1)
Network traffic control (Traffic_Control)	FRU_RSA.1(2)
Management of security functions (Man_Sec_Fun)	FMT_MOF.1
	FMT_SMF.1
Management of security attributes (Man_Sec_Attr)	FMT_MSA.1
	FMT_MSA.3
	FMT_SMF.1
Management of TSF data (Man_TSF_Data)	FMT_MTD.1
	FMT_MTD.2
	FMT_SMF.1
Management of security roles (Man_Sec_Role)	FMT_SMR.1
HA function (High_availability)	FPT_FLS.1
	FRU_FLT.1
Security function stability self test (Secui_Self_Test)	FPT_AMT.1
	FPT_TST.1
TSF protection (TSF_Protection)	FPT_RVM.1
	FPT_SEP.1
Process monitoring (Mon_Process)	FPT_RCV.4
	FPT_FLS.1

Audit generation and protection

This SF associates the user identity that created an audit event using the defined potential security violation rules, generates audit records, and detects auditable events and potential security violation;

Detects an attack and ensures that it cannot disable other security functions; Ensures only an authorized administrator can read all audit data; And provides selective audit, protected audit trail storage, action in case of possible audit data loss, prevention of audit data loss, and timestamp that ensures audit records are generated in the order it happens. Therefore, this SF satisfies FAU_ARP.1, FAU_GEN.1, FAU_GEN.2, FAU_SAA.1, FAU_SEL.1, FAU_STG.1, FAU_STG.3, and FAU_STG.4.

Audit review

This SF provides audit records such that an authorized administrator can read all audit data from the audit records and a user can interpret the information; And provides an ability to search and sort audit data based on the subject identity, object, the time, type, importance, and outcome of the event. Therefore, this SF satisfies FAU_SAR.1 and FAU_SAR.3.

Administrator registration

This SF registeres an administrator based on the list of security attributes of an administrator and maintains the list for each user. Therefore, it satisfies FIA_ATD.1(2). It checks the metrics for a password at the registration of administrator. Therefore, it satisfies FIA_SOS.1 and FMT_MTD.1.

Administrator identification and authentication

This SF detects 3~10 (as specified by an administrator) unsuccessful authentication attempts and executes defined TSF list if the defined number is met or surpassed; maintains the list of security attributes of each user; satisfies the metrics for a password, successfully authenticates a user before allowing any TSF-mediated actions on behalf of that user, and prevents reuse of a password by using OTP mechanism; keeps password input hidden by showing dots instead of each letter; and identifies successfully a user before allowing any TSF-mediated actions on behalf of that user. Therefore, this SF satisfies FIA_AFL.1, FIA_ATD.1(2), FIA_UAU.2, FIA_UAU.4, FIA_UAU.7, and FIA_UID.2(2). It provides a function to lock an interactive administrator session after 1~120 (default 10) minutes of inactivity and requires re-authentication before unlocking the session, therefore satisfies FTA_SSL.1.

Administrator access control

This SF controls all operations in the TSC using the security attributes according to the policy when an administrator (subject) accesses the TSF data or executable file (object). Therefore, it satisfies FDP_ACC.2 and FDP_ACF.1.

Packet filtering

This SF is applied to an operation causing information flow to and from controlled subjects according to eXshield information flow control policy; It controls information flow between a subject and object

by DAC and MAC. Therefore, it satisfies FDP_IFC.1(1) and FDP_IFF.1(1).

In addition, it identifies a user before allowing any actions by the TSF base on the IP address and security level of the IT entity of the internal/external network and terminates a session after 30 minutes of inactivity. Therefore, it satisfies FIA_ATD.1(1), FIA_UID.2(1), and FTA_SSL.3.

Intrusion prevention

This SF is applied to an operation causing information flow to and from controlled subjects according to eXshield IPS information flow control policy; It controls information flow to and from a subject based on the URL block rule, normal hacking list, traffic anomaly list, and 2-layer protection list. Therefore, it satisfies FDP_IFC.1(2) and FDP_IFF.1(2).

It also prevents a SYN Flooding attack by enforcing maximum quotas of a TCP transport layer representation, therefore satisfies FRU_RSA.1(1).

Network address translation

This SF is applied to an operation causing information flow to and from controlled subjects according to eXshield information flow control policy; It controls information flow to and from a subject. Therefore, it satisfies FDP_IFC.1(1) and FDP_IFF.1(1).

Network traffic control

This SF provides a function to enforce maximum quotas of a transport layer representation that individual IT entities can use simultaneously. Therefore, it satisfies FUR_RSA.1(2).

Management of security functions

This SF restricts the ability to determine the behavior of, disable, enable, and modify the behavior of the TSF functions; performs security management functions of the TSF; and prevents deactivation of other TSFs. Therefore, it satisfies FMT_MOF.1 and FMT_SMF.1.

Management of security attributes

This SF enforces the administrator, eXshield information flow control policy, and eXshield IPS information flow control policy by restricting the ability to modify, delete, generate, and query the security attributes. It also requires that the security attributes used for the enforcement of the SFP provide a restrictive default value and has an authorized administrator specify a selective initial value in the place of the default value when generating an object or information. Therefore, it satisfies FMT_MSA.1, FMT_MSA.3, and FMT_SMF.1.

Management of TSF data

This SF restricts the ability to operate the TSF data list specified by an author to an authorized administrator; and restricts the ability to specify limits on the audit storage capacity, the number of unsuccessful authentication attempts, and the time interval of self tests to an authorized administrator. Therefore, it satisfies FMT_MTD.1, FMT_MTD.2, and FMT_SMF.1.

Management of security roles

This SF can maintain the roles of an authorized administrator and associate a user with the roles. Therefore, it satisfies FMT_SMR.1.

HA function

This SF preserves a secure state in case of an error in the network circuit. Therefore, it satisfies FPT_FLS.1 and FRU_FLT.1.

Security function stability self test

This SF performs a suite of tests during initial start-up and at the request of an authorized administrator to demonstrate the correct applications of the security assumptions related to the underlying abstract machine of the TSF; performs a suite of self tests to demonstrate the correct operation of the TSF; and provides an authorized administrator with a function to verify integrity. Therefore, it satisfies FPT_AMT.1 and FPT_TST.1.

TSF protection

This SF ensures that packet flow to each function will be successful only after the packet filtering function that enforces the TSP is invoked, before each function in the TSC is allowed to proceed; and maintains a security domain for its own execution that protects it from interference and tampering by untrusted subjects, since all functions of the TOE are security-related. Therefore, it satisfies FPT_RVM.1 and FPT_SEP.1.

Process monitoring

This SF provides a function to preserve a secure state when an application-level process that comprises the TOE is abnormally terminated. Therefore, it satisfies FPT_FLS.1 and FPT_RCV.4.

8.7. TOE assurance measures rationale

The assurance measures of the TOE are the same as the assurance families for EAL4 from the CC Part 3 as shown in the following table.

Table 8-8 TOE assurance measures rationale

Assurance class	Assurance component		Assurance measures
Configuration management	ACM_AUT.1	Partial CM automation	eXshield V1.0.1.R Configuration management Version 1.4
	ACM_CAP.4	Generation support and acceptance procedures	
	ACM_SCP.2	Problem tracking CM coverage	
Delivery and operation	ADO_DEL.2	Detection of modification	eXshield V1.0.1.R Delivery Guide Version 1.1
	ADO_IGS.1	Installation, generation, and start-up procedures	eXshield V1.0.1.R Installation Guide Version 1.0
Development	ADV_FSP.2	Fully defined external interface	eXshield V1.0.1.R Functional specification Version 1.7
	ADV_HLD.2	Security enforcing high-level design	eXshield V1.0.1.R High-level design Version 1.7
	ADV_IMP.1	Subset of the implementation of the TSF	eXshield V1.0.1.R Implementation Validation Version 1.1 Source code
	ADV_LLD.1	Descriptive low-level design	eXshield V1.0.1.R Low-level design Version 1.3

	ADV_RCR.1	Informal correspondence demonstration	eXshield V1.0.1.R Correspondence Analysis Version 1.3
	ADV_SPM.1	Informal TOE security policy model	eXshield V1.0.1.R Security Policy Modeling Version 1.5
Guidance documents	AGD_ADM.1	Administrator guidance	eXshield V1.0.1.R Administrator guidance Version 1.5
	AGD_USR.1	User guidance	-
Life cycle support	ALC_DVS.1	Identification of security measures	eXshield V1.0.1.R Life cycle support Version 1.3
	ALC_LCD.1	Developer defined life-cycle model	
	ALC_TAT.1	Well-defined development tools	
Tests	ATE_COV.2	Analysis of coverage	eXshield V1.0.1.R Tests Version 1.4
	ATE_DPT.1	Testing: high-level design	
	ATE_FUN.1	Functional testing	
	ATE_IND.2	Independent testing – sample	
Vulnerability assessment	AVA_MSU.2	Validation of analysis	eXshield V1.0.1.R Vulnerability and misuse analysis Version 1.3
	AVA_SOF.1	Strength of TOE security function evaluation	
	AVA_VLA.2	Independent vulnerability analysis	
	AVA_SOF.1	Strength of TOE security function evaluation	
	AVA_VLA.2	Independent vulnerability analysis	

The following TOE assurance requirements are satisfied by the assurance measures as specified below:

ACM_AUT.1 Partial CM automation

The assurance measures satisfy this requirement, as Configuration Management describes the automated tools required for the generation of the TOE.

ACM_CAP.4 Generation support and acceptance procedures

The assurance measures satisfy this requirement, as Configuration Management describes the generation support and acceptance procedures, which are part of the CM procedures.

ACM_SCP.2 Problem tracking CM coverage

The assurance measures satisfy this requirement, as Configuration Management provides the problem tracking CM coverage.

ADO_DEL.2 Detection of modification

The assurance measures satisfy this requirement, as Delivery Guide provides how to confirm the detection of modification.

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

The assurance measures satisfy this requirement, as Installation Guide provides the installation, generation, and start-up procedures.

ADV_FSP.2 Fully defined external interfaces

The assurance measures satisfy this requirement, as Functional Specification provides the TSF and the fully defined external interfaces.

ADV_HLD.2 Security enforcing high-level design

The assurance measures satisfy this requirement, as High-level Design provides security enforcing high-level design for each subsystem of the TSF.

ADV_IMP.1 Subset of the implementation of the TSF

The assurance measures satisfy this requirement, as Implementation Validation and Source Code provide subset of the implementation of the TSF that forms the TOE.

ADV_LLD.1 Descriptive low-level design

The assurance measures satisfy this requirement, as Low-level Design provides the descriptive low-level design for each module of the TSF.

ADV_RCR.1 Informal correspondence demonstration

The assurance measures satisfy this requirement, as Correspondence Analysis provides the correspondence analysis between ST-TSS and FSP, FSP and HLD, HLD and LLD, and LLD and IMP.

ADV_SPM.1 Informal TOE security policy model

The assurance measures satisfy this requirement, as Security Policy Modeling provides informal security policy model.

AGD_ADM.1 Administrator guidance

The assurance measures satisfy this requirement, as Administrator Guidance provides guidance for an administrator.

AGD_USR.1 User guidance

As the TOE does not define general users, User Guidance is not applied and can be replaces by Administrator Guidance.

ALC_DVS.1 Identification of security measures

The assurance measures satisfy this requirement, as Life Cycle Support provides the information of security in development and identification of security measures.

ALC_LCD.1 Developer defined life-cycle model

The assurance measures satisfy this requirement, as Life Cycle Support provides the developer defined life-cycle model.

ALC_TAT.1 Well-defined development tools

The assurance measures satisfy this requirement, as Life Cycle Support provides the description of well-defined development tools.

ATE_COV.2 Analysis of coverage

The assurance measures satisfy this requirement, as Tests provides the analysis of coverage.

ATE_DPT.1 Testing: high-level design

The assurance measures satisfy this requirement, as Tests provides the procedures of testing of high-level design.

ATE_FUN.1 Functional testing

The assurance measures satisfy this requirement, as Tests provides the procedures of functional testing.

ATE_IND.2 Independent testing – sample

The assurance measures satisfy this requirement, as Tests gives a ground for independent testing.

AVA_MSU.2 Validation of analysis

The assurance measures satisfy this requirement, as Vulnerability and Misuse Analysis provides the misuse analysis of the guidance documents.

AVA_SOF.1 Strength of TOE security function evaluation

The assurance measures satisfy this requirement, as Vulnerability and Misuse Analysis provides the analysis of the strength of TOE security function.

AVA_VLA.2 Independent vulnerability analysis

The assurance measures satisfy this requirement, as the evaluator can perform independent vulnerability analysis of the TOE based on Vulnerabililty and Misuse Analysis.

8.8. PP claims rationale

This ST claims conformance to Network Intrusion Prevention System Protection Profile V1.1, 21 Dec. 2005, KISA, with the following additions or modifications.

Table 8-9 Additions to the TOE security environment

Category	Item	Description
Assumption	A.Server	Added because the TOE uses services from the NTP server and SECUI Update server that are outside the TOE.
Threat	T.Export	Added because an internal user may export information illegally through the network.
	TE.Time	Added because it is possible for the TOE to receive a wrong time source, which results in an incorrect generation of audit records and regular Signature update.
	T.AttackTSFdata	Added because a threat agent may expose or modify the TSF data without permission during communication between TOE_Gateway and TOE_LServer, the TOE and Secui Update server, and the TOE and GUI administrator console.

Table 8-10 Modified or added security objectives

Category	Item	Description
Security objectives for the TOE	O.Information	Unauthorized import or export of information from the internal to external is added as the TOE controls information flow both from external to internal and from internal to external.
	O.Access	Added because the TOE shall control access to it according to the security policy rules.

Category	Item	Description
Security objectives for the environment	OE.IA	Added because the TOE allows a log server manager to click on the button for login before identification and authentication in the underlying OS and requires identification and authentication before allowing any other actions.
	OE.Timestamp	Added because the TOE shall receive secure time source from the NTP server or underlying OS.
	OE.Channel	Added because the TOE shall be provided with a trusted channel using SSL for secure communication between TOE_Gateway and TOE_LServer, the TOE and SECUI Update server, and the TOE and GUI administrator console.
	OE.Server	Added because the NTP server and SECUI Update server that locate outside the TOE for the secure operation of the TOE functions shall be secure.

Table 8-11 Additions of the IT security requirements

Category	Item	Description
TOE SFRs	FDP_ACC.2	Added because the TSF ensures that all operations between any subject in the TSC and any object within the TSF are covered by the administrator access control policy.
	FDP_ACF.1	Added because the TSF enforces the administrator access control policy to objects based on the list of subjects and objects, and the security attributes for each.
	FIA_SOS.1	Added because the TSF provides a mechanism to verify that secrets meet the metric defined by Secui.com Corp.
	FIA_UAU.4	Added because the TSF prevents reuse of authentication data related to administrator authentication mechanism.

	FPT_RCV.4	Added because the TSF ensures reactivation of process in case of abnormal termination of the application processes that form the TOE.
SFRs for the IT environment	FIA_UAU.2	Added because the IT environment ensures the ability to authenticate a log server manager successfully before allowing any other TSF-mediated actions on behalf of that manager.
	FIA_UID.2	Added because the IT environment ensures the ability to identifies a log server manager before allowing any other TSF-mediated actions on behalf of that manager.
	FPT_ITT.1	Added because the IT environment protects TSF data from disclosure and modification when it is transmitted between separate parts of the TOE.
	FPT_STM.1	Added because the IT environment receives reliable time stamps that ensure the orderly generation of audit data from underlying OS or NTP server.
	FTP_ITC.1	Added because the IT environment provides a trusted channel when the TSF initializes communication for Signature update, malicious Website list update, and accessing the log server.

Reference

[1] Common Criteria V2.3 Part 1 : Introduction and general model, August 2005

[2] Common Criteria V2.3 Part 2 : Security functional requirements, August 2005

[3] Common Criteria V2.3 Part 3 : Security assurance requirements, August 2005

[4] Common Methodology for Information Technology Security Evaluation, version 2.3, August 2005