SECUI NXG W V1.0.1

Security Target

Version 1.2

SECUI

Revision History

ST_SECUI NXG W V1.0.1_V1.2.doc		
Revision	**Date**	**Desc.**
V1.0.	2008.02.27	– Initial draft
V1.1	2008.07.04	– Reflected the EOR-01 – For TOE operational environment, it is specified in the mode of Gateway, Bridge and Reverse proxy – Modified assumptions of A.Physical, A.Admin, and A. Operating System Reinforcement – Added security objectives for the operational environment, OE. Time Stamp – Added definition of Subjects, Objects and the Security Attributes, Operations in the Table 6-1 – Modified the operations of FDP_IFF.1.4(1) and FDP_IFF.1.4(2) – Added list of information controlled under the indicated SFP, packet direction, in FDP_IFF.1.1(4) – Modified assignment of information flow control SFP, SECUI NXG W Information flow packet filtering policy, in FDP_IFC.1(4) – Modified editing error and supplemented contents in 8.2. Reference
V1.2	2008.08.30	– Reflected the EOR-02 – Modified the Scheme, Notification no.2008-26 by the MOPAS in ST identification – Changed the TOE operational environment from Gateway mode and Bridge, Reverse proxy to Gateway and Transparent-bridge, Transparent-gateway – Modified as the following in Non-TOE scope : • Added MGMT port and modified NIC in the Table 1-1 • Supplemented contents of XLR Processor in 8.1. Glossary – Modified as the following in security problem definition : • Deleted T. Vulnerability and T. DoS – Modified as the following in security objectives : • Deleted O. Vulnerability as well as Security objectives rationale and in the Table 4-3 since it is satisfied with

		consistency • Deleted OE. PreventDoS – Modified as the following in security requirements : • Changed the refinement in FAU_GEN.1.1 from '*minimum*' to '*not specified*' • Added Items of Table 6-8 List of functions(2), Execution of CLI commands, super administrator, and server administrator, in FMT_MOF.1(2) • Added description of external entities • Modified list of subjects in FDP_IFF.1.1(3) • Modified in FDP_IFF.1.1(4): Policy name changed • Modified contents of Table 6-7, 6-8, and 6-9 in FMT_MOF • Modified contents of Table 6-14, 6-15, 6-16, and 6-18 in FMT_MTD • Changed FTA_SSL.1 to FTA_SSL.3 • Modified Security functional requirements rationale in the Table 6-21 – Changed as the following in the TOE summary specification • Changed the identifier of web server attack protection from 'WS_AP' to 'SW_DP_AP' • Changed the identifier of web server data learning from 'WS_AP_LEARN' to 'SW_DP_AP_LEARN' • Changed the identifier of web server data protection from 'WS_AP_PROTECT' to 'SW_DP_AP_PROTECT' • Changed the identifier of Service contents protection from 'WS_AP_CONTENTS' to 'SW_DP_AP_CONTENTS' • Changed name of 'TSF data administration limited to an authorized administrator' to 'Management of TSF data' • Changed the name of 'Self testing' changed to 'External entity testing' • Added identifier of 'Management of limits on TSF data', 'SW_MAN_DATA_LIMIT' • Supplemented contents of 'TSF data integrity check and action'

Table of Contents

List of Figures

List of Tables

1. ST introduction

This Security Target describes the security functionality and evaluation scope of SECUI NXG W V1.0.1 provided by SECUI.com Corp. and presents the conformance claim, security problem definition, security objectives, security requirements, and TOE summary specification. This ST will be referenced that is defined requirements as secure management of web application firewall.

1.1. ST identification

File name	ST_SECUI NXG W V1.0.1_V1.2.doc
ST Title	SECUI NXG W V1.0.1 Security Target Version 1.2
Document history	Refer to Revision History
Author	Youngsik Kim, Yujin Choo / Technical planning team / Technology department, SECUI.com Corp.
Date	30 Aug 2008
Evaluation Criteria	Common Criteria for Information Technology Security Evaluation (CC, Notification no.2008-26 by the MOPAS)
Common Criteria Version	Common Criteria V3.1r2
PP Identification	None
Evaluation Assurance Level	EAL4
TOE Identification	SECUI NXG W V1.0.1
Product Line	SECUI NXG 4000W-4C. SECUI NXG 4000W-12C, SECUI NXG 4000W-12F, SECUI NXG 2000W-4C, SECUI NXG 2000W-12C, SECUI NXG 2000W-12F
Product Type	Web application firewall
Key words	Command insertion, I&A, web server, web application, web application firewall, web client, information flow control, cookie poisoning, cross site scripting (XSS), heuristics, HTTP header buffer overflow attack, SQL query insertion
Evaluation Facility	Korea System Assurance, Inc.
Certification body	IT Security Certification Center, National Intelligence Service

1.2. TOE overview

The TOE described in this ST refers to a software-based web application firewall, which detects and prevents intrusion against the web application and web server data on web zone.

The TOE locates on the point that connects internal and external the web zone or the Internet network in order to detect and prevent malicious web traffics.

1.2.1. Usage of the TOE

As the Table 1-1, TOE operational environment is comprised of SECUI NXG 4000W product line (SECUI NXG 4000W-4C, SECUI NXG 4000W-12C, SECUI NXG 4000W-12F) and SECUI NXG 2000W product line (SECUI NXG 2000W-4C, SECUI NXG 2000W-12C, SECUI NXG 2000W-12F). The TOE locates on the connection point of external and internal of the web zone connected to the Internet and protects the web traffic that the network firewall fails to protect from unauthorized attack from external. It also helps SSL communication between web server and web client, which consequently will decrease the load on the server and provide services more than faster.

After installed, the TOE will be learned web tree database by heuristics of the web access patterns on the network. Then it will be allowed only learned heuristics patterns, which provides appropriate countermeasure for an unknown attack (Zero-Day Attack) in possible. It is also performed monitoring the hacking of the web application and web server data through the HTTP protocol check and HTML parsing, which ensure from sophisticated intrusion of detection and blocking in real-time.

1.2.2. Major security features of the TOE

The TOE provides packet filtering and web server protection for user data protection. Packet filtering allows or denies access of a packet passing through the TOE to the web server or TOE itself according to the policy defined by an authorized administrator. Packets allowed access will be sent to the TOE web protection proxy daemon to perform web server attack protection, which is a basic security function of a web application firewall, including web server data heuristics, web server data protection, and service contents protection.

The TOE monitors the requests for web clients for a defined time to collect web traffic data (web

server data heuristics) and protects web server data (web server data protection). It also prevents corruption of personal information such as SSN or credit card numbers and web page (Service contents protection). An authorized administrator defines security policies for the web server attack protection and upon which performs security action on all web traffic input to the TOE. “Security action” refers to the specific security behaviors performed according to the violations detected by the web server attack protection. Security behaviors include transferring detected results by log (LOG), destroying violating traffic (Drop), emailing an administrator, sending a warning page, page redirection, and replacing characters.

The TOE also provides functions of I&A, security audit, secure management, and TSF protection:
I&A, identification and authentication of an administrator, ensures actions to be taken in case of authentication failure. Secure audit generates, makes log of audit records, and reviews to detect potential security violation and take an action. Security management addresses security functions, security attributes, TSF data, and security roles. TSF protection performs self testing to verify integrity of the TSF data and executable code; tests external entities to maintain secure state; and provides a function to manage a session after a specified period of administrator inactivity.

1.2.3. Operational environment of the TOE

The Operational environment of the TOE may be configured Gateway mode, Transparent-bridge mode, and Transparent-gateway mode as the following figures.

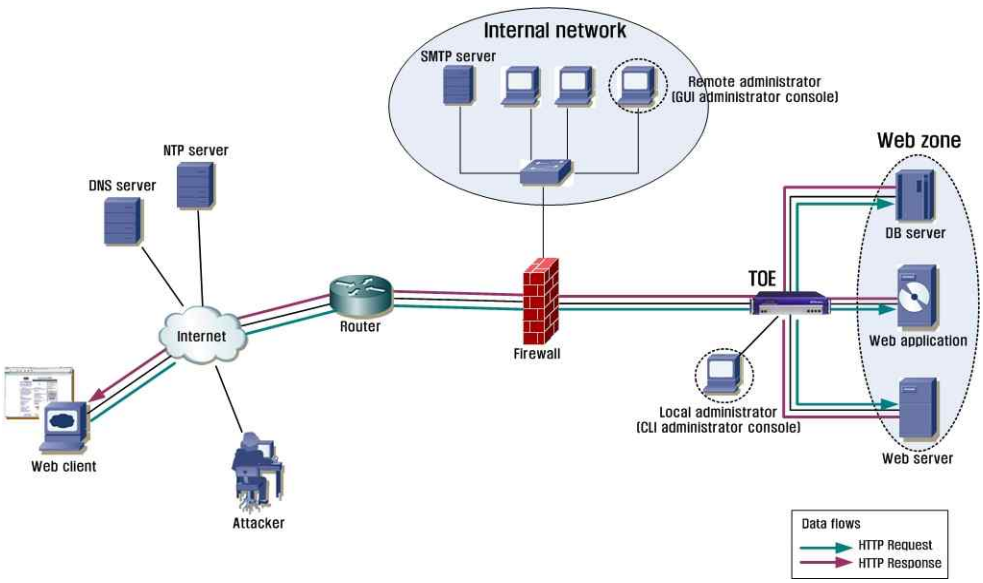


Figure 1-1 Gateway mode

Gateway mode is a general forward proxy type, which gets the address of web server inside the web zone to be protected to the TOE and analyzes all web traffic trying to access the web server from outside to protect the web server that is defined as an internal network.

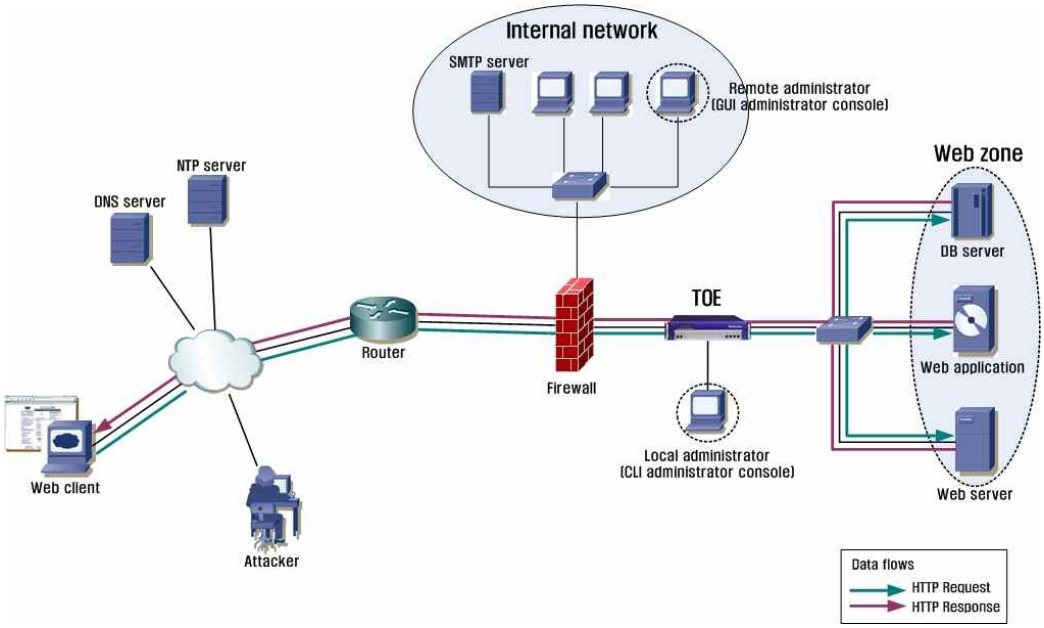


Figure 1-2 Transparent-bridge mode

Transparent-bridge mode is configured in in-line type as a general firewall. The TOE checks web traffic between the web client and web zone. This mode offers network transparency, where a web server user cannot recognize the TOE, and doesn't require the network configuration changed.

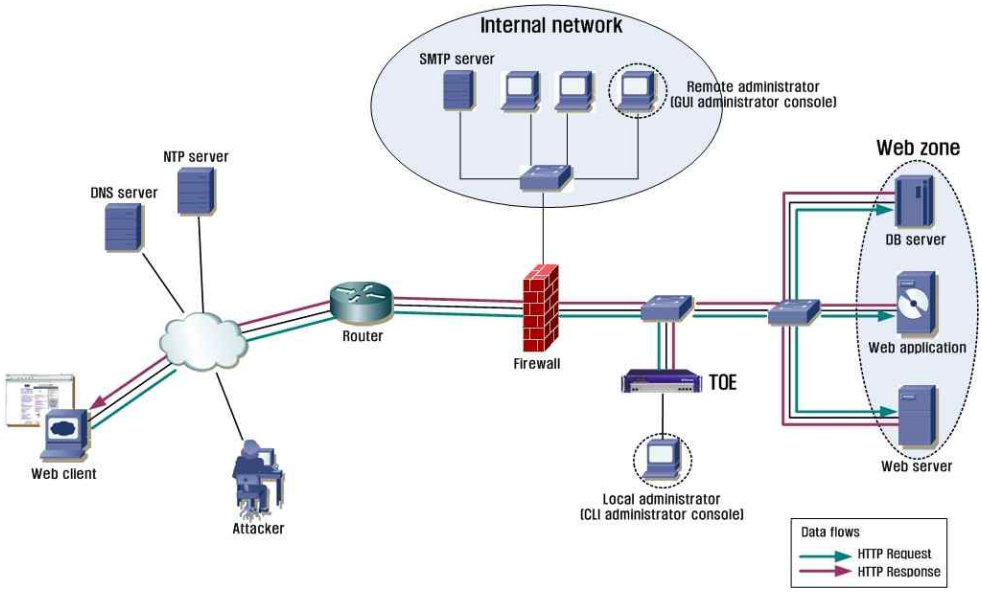


Figure 1-3 Transparent-gateway mode

Transparent-gateway mode is where the TOE operates as a web proxy; it is recommended that the TOE be installed in the same network bandwidth with the web server and that the web server address be changed into the TOE IP address by DNS. When a web server user requires access to the web server, the TOE checks the contents and sends it back to the web server. Result of request will go the opposite direction. In this case, any traffic other than the web traffic and traffic for administration will not be transferred to the TOE.

GUI and CLI administrator console can manage the TOE according to the remote or local administrator guidance. They allow an authorized administrator to set and change the initial configuration of the TOE. The administrator can access the GUI administrator console through the web browser to start, stop, and terminate the security functions.

NTP server is used to get exact time information when the TOE generates an audit data. DNS server provides name services about the host name of the web server used by the TOE. Both of them can be located either in the same network with the TOE operational system or in an external network.

SMTP server sets the security action of sending an email regarding the security relevant events occurred in the TOE and is normally located in the same network with the TOE operational system or in an internal network.

When an attacker accesses using HTTPS protocol that uses SSL encryption between the web server and web client, the TOE terminates HTTPS connection and provides security functions, which will operate in real time to prevent attack that may affect the protected system.

1.3. TOE description

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

1.3.1. Physical scope of the TOE

Target of evaluation comprises SECUI NXG W V1.0.1 (software) and SECUI NXG W V1.0.1 User Operational Manual.

The software will be delivered to the customers loaded to the dedicated hardware as specified in the Table 1-1 Configuration of the TOE and the manual as both a hard copy and a PDF file in a CD.

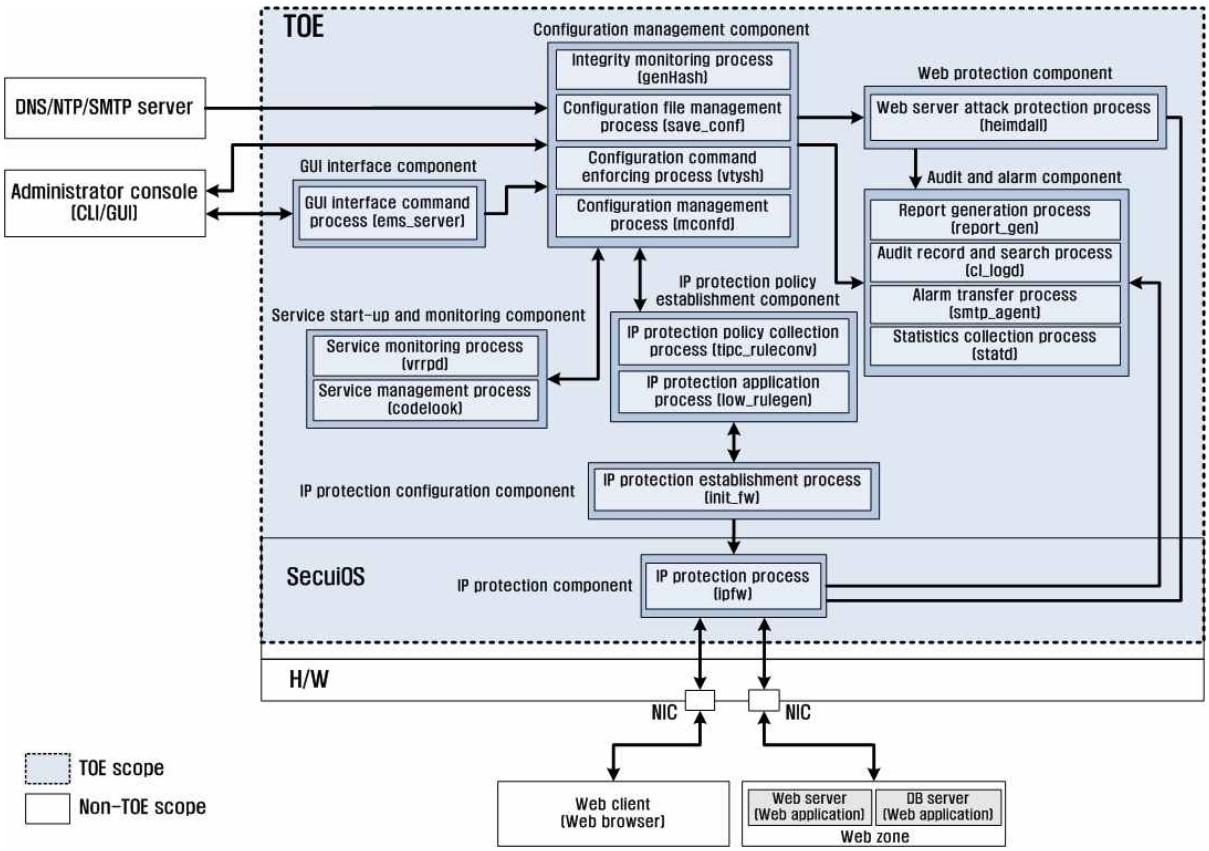


Figure 1-4 Physical scope of the TOE

The TOE is physically comprised of the following:

- GUI interface component comprises of GUI interface command process (ems_server), which

transfers the administrator command to the configuration management process (mconfd).

- Configuration management component comprises of configuration management process (mconfd), configuration command enforcing process (vtysh), configuration file management process (save_config), and integrity monitoring process (genHASH). Configuration management process (mconfd) performs IPC communication to interpret an administrator command sent from GUI interface command handling process (ems_server) of GUI interface component and send it to the other components. It also performs administrator identification and authentication. Configuration command enforcing process (vtysh) processes the interpreted command and performs the functions. Configuration file management process (save_config) stores what is set by an administrator in a configuration file or applies what is set by opening it from the stored files. Integrity monitoring process (genHASH) monitors whether integrity of the TSF data (TOE configuration file, TOE executable file, administrator identification and authentication data, etc.) is damaged and, when it is, restores it.
- Web protection component comprising web server attack protection process (heimdall), which addresses all web server attack protection functions provided by the TOE while operating based on multi thread.
- Service start-up and monitoring component are comprised of service monitoring process (vrrpd) and a service management process (codelook). Service monitoring process (vrrpd) enables the processes of each component in the TOE and monitors operation of each process to restart it if service stops due to malfunction. Service management process (codelook) processes command sent from configuration management process (mconfd) and controls start/stop/restart of each process.
- Audit and alarm component comprises audit record and search process (cl_logd), alarm transfer process (smtp_agent), statistics collection process (statd), report generation process (report_gen). Audit record and search process (cl_logd) provides a function to generate and search all security audit records by the TSF. Alarm transfer process (smtp_agent) sends an email to an administrator when a potential violation is detected. Statistics collection process (statd) provides statistical material for each type of allow/deny transaction and web intrusion attack. Report generation process (report_gen) generates a report out of the statistics.
- IP protection configuration component comprises IP protection policy collection process (tipc_ruleconv) and IP protection policy application process (low_rulegen). IP protection policy collection process (tipc_ruleconv) transforms packet filtering policy set by an administrator and provides it for IP protection process (ipfw) in the kernel of OS. IP protection policy application process (low_rulegen) applies the policy.
- IP protection policy establishment components comprising IP protection establishment process

(init_fw) transforms a packet filtering policy and sends it to an IP protection process (ipfw).

- IP protection components comprising IP protection process (ipfw) performs packet filtering on all packets coming into or out of the TOE network. Therefore, all packets are controlled through an IP protection process (ipfw).

1.3.2. Logical scope of the TOE

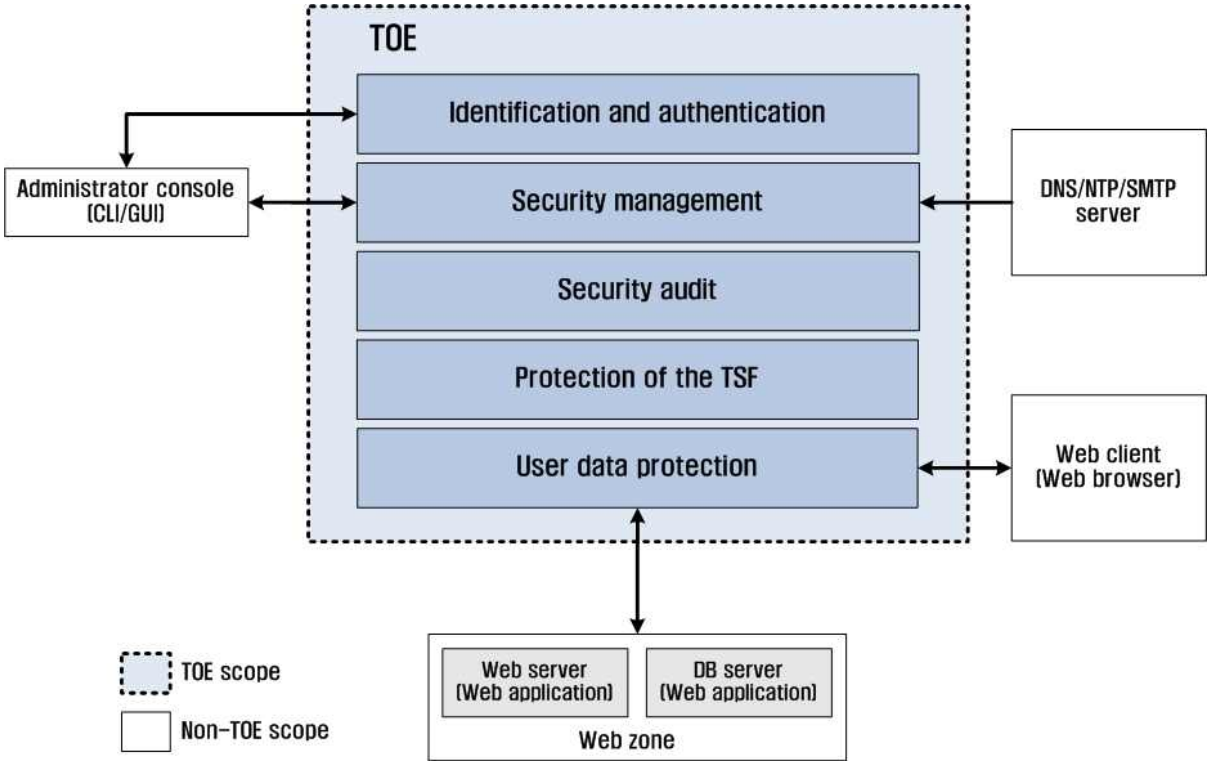


Figure 1-5 Logical scope of the TOE

The TOE is comprised logically of identification and authentication, security management, security audit, protection of the TSF, and user data protection.

- **Identification and Authentication**

The TOE identifies and authenticated an authorized administrator using ID/Password through the GUI/CLI administrator console. It defines an administrator group and manages it for each web server and domain, which is necessary for the management of many different web servers and domains. When an authentication attempt consecutively fails three times, the TOE will block login access from the failed administrator ID for the next 5 minutes.

- **Security Management**

An administrator establishes and manages security policies regarding web server data learning, web server data protection, and service contents protection through the GUI administrator console. The TOE provides a function to configure DNS server, NTP server, network, and interface that are required for the TOE to operate on an Internet. It also provides a function to manage the TOE state and configuration files.

Administrator that can access the administrator interface includes a super administrator, server administrator, and user. Super administrator has all authorities for management of the TOE; server administrator has all except for the restart of the TOE; and user has a read-only authority.

- **Security Audit**

An administrator is provided with a function to review and search audit records using search conditions and a statistical report generated out of the audit records. Analysis of potential security violation is possible using the audit records. When audit data storage meets the threshold, the TOE alarms an authorized administrator by an email; when the stored data surpasses the threshold (99%), the TOE deletes the oldest audit record without security function ceasing and generates an audit record.

- **Protection of the TSF**

TSF data transmitted between components of the TOE is encoded using SSL before transmission, which ensures its protection against disclosure or illegal modification. The TOE checks the state of CPU, memory, hard disk, TOE process, and network interface regularly during normal operation and, upon detection of anomaly, enables an administrator to restart TSF services. The TOE provides a function to monitor integrity of TSF data such as the TOE configuration file and TOE executable file. After the lock of a session by session management function after a certain period of administrator inactivity, re-authentication is required.

- **User Data Protection**

Packets coming into the TOE from outside shall be applied the packet filtering security policy set by an authorized administrator before it is allowed or denied access. Checking packets starts from a server access check. SECUI NXG W Information flow control policies will be applied to the header and body of those packets that passed the server access check.

The TOE sends the packets that passed through packet filtering to the web server and monitors request of a web client for a specific period of time to build a web tree database based on collected web traffic data. Then it detects and blocks intrusion against the web server exploiting vulnerabilities

of web. This should be based on a thorough analysis of http protocol. The TOE performs the following security behaviors:

- URL check: Checks URL accessing the web server; performs URL analysis, heuristics, access control, and directory access control.
- Query phrase and value check: Checks query of Header and Body sent by GET or POST method.
- Cookie corruption check: Checks the cookie made by the web server; performs cookie encryption, cookie forge/corruption protection, and domain cookie management.
- Cross-site scripting (XSS) protection: Checks whether the query or cookie data sent to the web server includes an enforceable script or HTML tag.
- Hidden field manipulation protection: Checks if each URL includes a hidden field.
- Header method check: Checks if the header method of each URL is allowed.
- SQL syntax injection protection: Blocks an attack where a user forges query and cookie value sent to the web server so they have an SQL syntax error and enforces SQL command randomly.
- Command injection protection: Checks if any forbidden system command is being used.
- URL-based access control: Establishes a policy for a URL of the web server to allow or block access from specific IP addresses.
- Base64 encoding check: Checks if a query used base64 encoding method.
- Header buffer overflow check: Specifies the maximum size of an HTTP header to prevent buffer overflow.
- URL extension check: Checks URL extension and determines whether to allow or block.
- Password check: Checks if a password is made to be a vulnerable combination and length.
- SSL application protection: Protect a web page on which policies have been set by applying SSL to it.

The TOE protects personal credit information included in the protected web server from being leaked. Personal credit information includes an SSN and credit card number. It also blocks transmission of the type and version information of the web server to prevent an attack specialized against the web server. It blocks transmission of an HTTP error page, which usually includes critical information of the server, to prevent unintended leakage of information. In addition, it prevents leakage of forged page and footnote. The TOE performs the following to protect web server service:

- Personal credit information protection: Protects personal information like an SSN and credit card number in the web service contents.
- Error page handling: Protects information of a web server that can be included in an error page.
- Footnote deletion: Checks whether the content from the protected web server includes a footnote and, if it does, deletes the footnote and sends it to a web client.

- Checksum protection: Checks the length or hash value of a web page that the protected web server sends as a respond to a web client and protects modified contents from being leaked.
- Forbidden work check: Checks if the contents from the web server or query value delivered to the web server include a forbidden word and, if they do, protects the contents from being leaked.

The TOE provides a function to define specific actions to be taken upon detection of violation based on the security policies set by an authorized administrator. Security actions configurable by the TOE include log sent in the form of security audit record, packet destroy, sending email to an administrator, transferring a warning page, page redirection, and replacing characters.

1.3.3. Non-TOE scope

The following are not included in the evaluation.

- SSL protocol for secure communication between the TOE and GUI administrator console
  - ✓ SSL library type: OpenSSL
- Time stamp that the TOE uses when it generates audit data
  - ✓ There are two ways for the TOE to get a trusted time stamp: using time information provided by the OS and using one provided by an external NTP server. In case of the system time, the TOE will regularly bring a value stored in Real-Time Clock (RTC) in its operational environment and compares it with its own time. The TOE time can only be changed by an authorized administrator. In case of the external NTP server, the TOE as an NTP client requires the NTP server for a correct current time. By exchanging time, the TOE can calculate the time of link delay using the gap between the time of NTP server and of its own and set its clock to be consistent with the server's. The first clock settlement will require 6 exchanges of time during 5~10 minutes. Once the time synchronization is finished, the TOE can modify its clock by exchanging messages at the time defined by the GUI administrator console to get a trusted time stamp.
- Domain information that is provided by the external DNS server that changes domain names into IP addresses to find out the location
- E-mail information that will be used when notifying an authorized administrator of security relevant events detected in the TOE
- Operation software of the TOE (SecuiOS V1.2)
  - ✓ SecuiOS V1.2 is an embedded OS that SECUI.COM has developed for the operation of the TOE.

- Configuration of the TOE (Table 1-1 Configuration of the TOE)
  - ✓ The following specifications are needed for hardware to operate the TOE. SECUI is not responsible for arbitrary addition of hardware other than the evaluated environment. The environment for installation and operation of the TOE is assumed to be used independently for the TOE. It is also assumed that only the least administrator ID will be produced as necessary for operation of the TOE and it will be a non-malicious administrator that manages the ID, password, and security patch correctly.

Table 1-1 Configuration of the TOE

Component	SECUI NXG 4000W – 4C	SECUI NXG 4000W – 12C	SECUI NXG 4000W – 12F	SECUI NXG 2000W – 4C	SECUI NXG 2000W – 12C	SECUI NXG 2000W – 12F	Note
CPU	XLR 732 1.2 GHz XLR 532 1.2 GHz	XLR 732 1.2 GHz XLR 532 1.2 GHz	XLR 732 1.2 GHz XLR 532 1.2 GHz	XLR 732 1.2 GHz	XLR 732 1.2 GHz	XLR 732 1.2 GHz	*RMI XLR Processor (See Glossary)
Main Memory	8 GB	8 GB	8 GB	4 GB	4 GB	4 GB	
CF Card	2 GB * 2	2 GB * 2	2 GB * 2	2 GB	2 GB	2 GB	Where the TOE will be installed
HDD	500 GB	500 GB	500 GB	500 GB	500 GB	500 GB	Where the audit records will be stored
NIC	4*10/100/1000 BASE-T	12*10/100/1000 BASE-T	12*1000 BASE-X	4*10/100/1000 BASE-T	12*10/100/1000 BASE-T	12*1000 BASE-X	
Mgmt. Port	1*10/100/1000 BASE-T	1*10/100/1000 BASE-T	1*10/100/1000 BASE-T	1*10/100/1000 BASE-T	1*10/100/1000 BASE-T	1*10/100/1000 BASE-T	Communication port for the CLI/GUI administrator console
Serial Port	1 * RJ-45	1 * RJ-45	1 * RJ-45	1 * RJ-45	1 * RJ-45	1 * RJ-45	

- Hardware for operation of the CLI/GUI administrator console for management of the TOE (See Table 1-2 Configuration of a CLI/GUI administrator console)
  - ✓ The following specifications are recommended for the hardware to install and operate the TOE administrator console that manages access to the TOE:

Table 1-2 Configuration of a CLI/GUI administrator console

Component	Required specification	Note
CPU	Pentium III 133 MHz and above	
Main memory	256 MB and above	
HDD	40 GB and above	Hard disk for installation of the administrator console program
NIC	1 EA or more	
Serial port	1 EA	RS-232 Serial, 38400 Baud (DB-9 Type)
OS	Windows XP Service Pack 2	
Java library	jre-1_5_0_11-windows-i586-p	Program for operating the GUI administrator console program

Component	Required specification	Note
web browser	Internet Explorer Version 5.5 and above	Program for accessing the GUI administrator console (Patch more than 128 bits providing SSL)
Administrator console program	Tera Term Professional Version 4.56	Communication emulator for accessing the CLI administrator console

- Web client and web server/web application transferring web traffic through the TOE
  - ✓ Web Client refers to the User Agent of a user that means to use the web server or web application, which is the protected system; User Agent means web browser.
  - ✓ Web server and web application refers to the web server data and web application data providing web services respectively, not the web server and web application server.

1.4. Conventions

The notation, formatting and conventions used in this Security Target are consistent with the Common Criteria for Information Technology Security Evaluation.

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

Assignment

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

Iteration

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

Refinement

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

Selection

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

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

2. Conformance claims

Conformance claim describes the CC, PP and package conformance claim, conformance rationale, PP conformance statement.

2.1. CC conformance claim

This ST claims conformance to

- Common Criteria reference
  - ✓ Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 3.1r1, September 2006, CCMB-2006-09-001
  - ✓ Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, Version 3.1r2, September 2007, CCMB-2007-09-002
  - ✓ Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, Version 3.1r2, September 2007, CCMB-2007-09-003
- Common Criteria Conformance
  - ✓ Part 2 Conformant
  - ✓ Part 3 Conformant

2.2. PP claim

There is no PP conformed by this ST.

2.3. Package claim

This ST conforms the following package of security assurance requirements.

- Assurance Package: EAL4 conformance

2.4. Conformance rationale

This ST did not claim conformance of other PPs, therefore it is not necessary to describe the conformance rationale.

3. Security problem definition

The security problem definition defines the intended threats, organizational security policies and assumptions so as to be handled by the TOE and the TOE operation environment.

This section identifies the threats to the IT assets against which protection is required by the TOE or by the security environment. The IT assets are divided into two categories:

- The IT assets against which protection is required by the TOE
  : Web server, web service, resources used by the web service, web application, data processed by the web application, and web contents
- The IT assets against which protection is required by the security environment
  : The TOE including the TSF data, executable code, etc.

3.1. Threats

The Threat agent is generally IT entities and human users who exert damage to the TOE and internal assets of the web zone in abnormal methods or attempt illegal access to the TOE and internal assets of the web zone from outside. The Threat agent has enhanced-basic level of expertise, resources and motivation.

Table 3-1 Threats of the TOE

T. Impersonation
The threat agents can access TOE by masquerading as authorized administrator.
T. Breakdown
The TOE may not provide normal services to user as it is in use or breakdown occurred due to external attacks, etc.
T. Recording Failure
The threat agent can disable recording of security-related events of the TOE by exhausting storage capacity.
T. Illegal Service Access
The threat agent can interrupt the web service provision of host by accessing services not

approved to the host of internal network.
T. Abnormal Web Request
The threat agent may cause erroneous operation in web server of internal network of web zone by transmitting web traffic that holds abnormal structure.
T. Continuous Authentication Attempt
The threat agent can acquire the authorized administrator rights by attempting continuous authentication to access the TOE.
T. Web Contents Attack
The threat agent may forge the data of the web application on the web server or leak web server data or personal credit information and misuse them.
T. Unauthorized TSF Data Change
TSF data may be changed without authentication as threat agent makes buffer overflow attack to TOE.

3.2. Organizational security policies

This section describes the organizational security policies (OSPs) that should be addressed by the TOE that conforms to this ST.

Table 3-2 Organizational Security Policies

P. Audit
To trace responsibilities on all security-related activities, security-related events shall be recorded and maintained and reviewed.
P. Secure Management
The TOE shall provide management means for the authorized administrator to manage the TOE in secure manner[1].

3.3. Assumptions

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

Table 3-3 Assumptions

A. Physical Security
The TOE shall be located in physically secure environment that can be accessed only by the authorized administrator.
A. Security Maintenance
When the internal network environment changes due to change in the network configuration, web server increase/ decrease, web application increase/ decrease and web service increase/ decrease, etc., the changed environment and security policy shall immediately be reflected in the TOE operation policy so that security level can be maintained to be the same as before.
A. Trusted Administrator
The authorized administrator of the TOE shall not have any malicious intention, receive proper training on the TOE management, and follow the administrator guidelines.

[1] To manage this web application firewall in safety, no one can delete or modify configuration files (not include the user data) except for authorized administrators of the TOE.

A. Operating System Reinforcement
Unnecessary services or means shall be removed from the operating system, and security shall be enhanced to better protect against vulnerabilities in the operating system thereby ensuring its reliability and stability.
A. Single Point of Connection
All communications between the external and internal networks of web zone are carried out only through the TOE.
A. Transfer Data Protection
The TOE shall protect transferred TSF data between a remote administrator and the TOE from unauthorized exposure, modify and deletion.

4. Security objectives

This ST defines security objectives by categorizing them into the TOE and the environment. Security objectives for the TOE are directly handled by the TOE. Security Maintenance objectives for operation environment shall be handled by technical/procedural means supported by the operation environment in order for the TOE to accurately provide security functions.

4.1. Security objectives for the TOE

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

Table 4-1 Security objectives for the TOE

O. Availability
The TOE shall provide normal service by maintaining the minimum security function at occurrence of breakdown by incidental attack or external attack.
O. Audit
The TOE shall record and maintain security-related events in order to enable tracing of responsibilities for security-related acts and shall provide means to review the recorded data.
O. Management
The TOE shall provide means for the authorized administrator of the TOE to efficiently manage the TOE in a secure manner.
O. Abnormal Web Request Cut-off
The TOE shall cut off the web traffic to hold abnormal structure among web traffics from web client to web server that pass through the TOE.
O. Identification and Authentication
The TOE shall identify users intending to access TOE and all external IT entities that are subject to information flow control by the TOE and authorize identity of administrator before permitting TOE access after administrator identification.
O. Web Contents Protection
The TOE can identify if the web contents registered on the web server, which is an IT entity, are altered and stop personal credit information such as SSN or credit card number from being leaked.

O. TSF Self Test Protect
The TOE shall protect itself in terms of TSF data management, change and deactivation in the security functionality during start-up, periodically, and at the request of an authorized administrator.
O. Information Flow Control
The TOE shall control outflow and inflow of unauthorized web traffic from inside to outside or from outside to inside in the web zone
O. Heuristics
The TOE shall provide a function that monitors the information of packets required by a web client, which is an IT entity, for a specific period of time and makes a profile out of it with application of the security policy that the TOE provides.
O. TSF Data Protection
The TOE shall protect TSF data from unauthorized exposure, change and deletion.

4.2. Security objectives for the operational environment

The followings are security objectives handled in relation to IT fields or by nontechnical/procedure-related means.

Table 4-2 Security objectives for the operational environment

OE. Physical Security
The TOE shall be located in physically secure environment that can be accessed only by the authorized administrator.
OE. Security Maintenance
When the internal web zone environment changes due to change in the network configuration, web server increase/ decrease, web application increase/ decrease and web service increase/ decrease, etc., the changed environment and security policy shall immediately be reflected in the TOE operation policy so that security level can be maintained to be the same as before.
OE. Trusted Administrator
The authorized administrator of the TOE shall not have any malicious intention, receive proper training on the TOE management, and follow the administrator guidelines.
OE. Secure Management
The TOE shall be distributed and installed in secure method and be configured, managed and used in secure method by authorized administrator.
OE. Operation System Reinforcement
Unnecessary services or means shall be removed from the operating system, and security shall be enhanced to better protect against vulnerabilities in the operating system thereby ensuring its reliability and stability.
OE. Single Point of Connection
All communications between the external and internal networks of web zone are carried out only through the TOE.
OE. Transfer Data Protection
The TOE shall protect the TSF data from being transferred between a remote administrator and the TOE in unauthorized methods.
OE. Time Stamp
The TOE shall accurately record the security related events by using the reliable time stamps

provided by the TOE operational environment.

4.3. Security objectives rationale

The security objectives rationale demonstrates that the specified security objectives are appropriate, sufficient to trace security problems and are essential, rather than excessive.

The rationale of security objectives demonstrates the following.

- Each threat, organizational security policy and assumption has at least one security objective tracing to it.
- Each security objective traces to at least one threat, organizational security policy and assumption.

Table 4-3 Summary of Mappings between Security Problem Definition and Security Objectives

Security objectives / Security problem definition	Security objectives for the TOE										Security objectives for the operational environment							
	O. Availability	O. Audit	O. Management	O. Abnormal Web Request Cut-off	O. Identification and Authentication	O. Web Contents Protection	O. TSF Self Test Protect	O. Information Flow Control	O. Heuristics	O. TSF Data Protection	OE. Physical Security	OE. Security Maintenance	OE. Trusted Administrator	OE. Secure Management	OE. Operation System Reinforcement	OE. Single Point of Connection	OE. Transfer Data Protection	OE. Time Stamp
T. Impersonation		X			X													
T. Breakdown	X						X			X								
T. Recording Failure	X	X																
T. Illegal Service Access			X					X	X									
T. Abnormal Web Request		X		X	X			X	X									
T. Continuous Authentication Attempt		X			X													
T. Web Contents Attack		X				X												
T. Unauthorized TSF Data Change		X								X								

Security objectives / Security problem definition	Security objectives for the TOE										Security objectives for the operational environment							
	O. Availability	O. Audit	O. Management	O. Abnormal Web Request Cut-off	O. Identification and Authentication	O. Web Contents Protection	O. TSF Self Test Protect	O. Information Flow Control	O. Heuristics	O. TSF Data Protection	OE. Physical Security	OE. Security Maintenance	OE. Trusted Administrator	OE. Secure Management	OE. Operation System Reinforcement	OE. Single Point of Connection	OE. Transfer Data Protection	OE. Time Stamp
P. Audit		X																X
P. Secure Management			X											X				
A. Physical Security											X			X				
A. Security Maintenance												X						
A. Trusted Administrator													X					
A. Operating System Reinforcement															X			
A. Single Point of Connection																X		
A. Transfer Data Protection																	X	

4.3.1. Rationale for the security objectives for the TOE

O. Availability
This TOE security objective is to provide TOE availability in order for the minimum web service provision when TOE is in overload state due to attack by attacker or at occurrence of breakdown in TOE. Therefore, this security objective assures TOE availability in response to T. Breakdown, and T. Record failure, the threat to saturation in audit record storage capacity of TOE.
O. Audit
As for this TOE security objective, TOE records audit event per user according to audit record policy when user is using security function. Also, the TOE assures to provide the means of safely maintaining and reviewing the recorded audit events. In other words, the TOE provides handling function when audit data reaches saturation state. Audit record creation assures to detect identity of attacker through audit record in case continuous attempts for authentication are made. Spoofing attack, service denial attack and attack to produce and transmit abnormal packet can also be traced through audit record. Therefore, this security objective handles T. Impersonation, T. Recording Failure, T. Abnormal Web Request, T. Continuous Authentication Attempt, T. Web Contents Attack, and T. Unauthorized TSF Data Change through audit record and supports P. Audit on security policy of organization.
O. Management
In order to execute security policy, TOE sets rules of information flow control, therefore controls illegal access to internal network. For this, the TOE shall provide means to safely manage TOE and TSF data, such as on TOE configuration data creation and management as well as the positive based rule management, etc. Therefore, this TOE security objective supports P. Secure Management on security policy of organization as it handles T. Illegal Service Access and provides means for the authorized administrator to safely manage TOE.
O. Abnormal Web Request Cut-off
This objective shall ensure that web request will be shut down if there is traffic, among web-related traffic coming to the internal of the TOE that does not conform to the web protocol or contains abnormal information. Thus it counters T. Abnormal Web Request.
O. Identification and Authentication
Users to use TOE are divided into administrator who manages TOE by connecting to TOE with authentication and external user (IT entity) passing through the TOE without authentication simply

to use web server of internal network. Two of the above cases require the function of identification to process security-related events. Administrator identification function is required because responsibilities are given to all acts used by administrator. External IT identification is necessary for manipulating (or reusing) cookies and creating audit record on attempts of connection to external IT. And user intending to access TOE shall obtain authentication. However, authentication required at access to TOE can be vulnerable to the attack of continuous authentication attempt by outside attacker. Therefore, TOE shall assure authentication mechanism to endure the attack of continuous authentication attempt to suit the level of external attacker. Therefore, this TOE security objective handles threats of T. Impersonation, T. Abnormal Web Request, and T. Continuous Authentication Attempt and supports P. Audit.
O. Web Contents Protection
This objective enables the TOE to check if web contents registered on the web server is manipulated and, if so, ensures generation of audit record and recovery of the web contents. Therefore, this TOE security objective handles threats of T. Web Contents Attack.
O. TSF Self Test Protect
This objective ensures that the TOE protects itself against an unexpected attack from outside by performing TSF data protection, change or deactivation of security functionality. Therefore, this TOE security objective handles threats of T. Breakdown.
O. Information Flow Control
TOE controls information flow according to security policy by being installed at the point where internal and external networks are separated. This security objective assures identifying and avoiding diverse attacks possible to occur in network according to deny and allow policies. Diverse attacks in network refer to virus attack, e-mail or web service including illegal information and access to web application service that is not allowed. The TOE ensures security of internal network of the web zone by controlling these attacks and preventing them from being flown into internal network of the web zone according to the set rules. Therefore, security objective handles threats of T. Illegal Service Access and T. Abnormal Web Request.
O. Heuristics
This objective ensures that the TOE monitors the information of packets required by the web client for a certain amount of time and makes a profile about the results with applying the security policies that the TOE provides. Therefore, this TOE security objective handles threats of T. Illegal Service Access and T. Abnormal Web Request.
O. TSF Data Protection
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. Therefore, this TOE security objective handles threats of T. Breakdown and T. Unauthorized TSF Data Change.

4.3.2. Rationale for the security objectives for the operational environment

OE. Physical Security
This security objective for the operational environments ensures physically secure environment of the TOE, therefore is required to support assumption of A. Physical Security.
OE. Security Maintenance
When the internal network environment changes due to change in the internal network configuration of web zone, increase/decrease of web server, increase/decrease of web application and increase/decrease of web service etc., this security objective for the operational environments ensures to immediately reflect the changed environment and security policy to operation policy, therefore to maintain security in the same level as before. Therefore, this security objective is required to support assumption of A. Security Maintenance.
OE. Trusted Administrator
This security objective for the operational environments ensures that the authorized administrator of the TOE can be trusted. Therefore, this is required to support assumption of A. Trusted Administrator.
OE. Secure Management
This objective ensures that the TOE is delivered and installed in a physically secure environment and is configured, administered, and used in a secure manner by an authorized administrator. Thus it upholds A. Physical Security and enforces P. Secure Management.
OE. Operation System Reinforcement
This security objective for the operational environments ensures for operation system to be reliability and stability by executing operation to remove all services or means in operation system not required and reinforcement on vulnerabilities of operation system. Therefore, this security objective is required to support assumption of A. Operation System Reinforcement.
OE. Single Point of Connection
This security objective for the operational environments ensures that all communications between the external and internal networks of the web zone are carried out only through the TOE, therefore is required to support assumption of A. Single Point of Connection
OE. Transfer Data Protection
This security objective ensures that the TOE protects TSF data transferred between the TOE and a remote administrator from unauthorized disclosure and modification. Therefore is required to support assumption of A. Transfer Data Protection.

OE. Time Stamp
This security objective for this operational environment ensures to accurately record the security-related events by using reliable time stamps provided by the TOE operational environment, therefore is required to enforcing organizational security policies of P. Audit.

5. Extended components definition

There are no defined extended components by this ST.

6. Security requirements

Security requirements describe security functional and assurance requirements to be satisfied by the TOE that conform this ST.

This ST defines all subjects, objects, operations, security attributes and external entities, etc. used in security requirements as follows.

a) Subjects, objects, and related security attributes and operations

Table 6-1 Definition of Subjects, Objects and the Related Security Attributes, Operations

Subject (User)	Subject (User) security attributes	Object (Information)	Object (Information) security attributes	Operation
Unauthorized web client on the side of information sender	IP address	Web traffic sent from subject to another place through the TOE	Cookie domain, cookie, web server address, URL	Allow if an allow-rule exists; block any other access
			Web server address, cookie, HTTP Request Message (Method, Request-URI, Request Headers)	Block if a block-rule exists; allow any other access
Web server or web application program on the side of information sender	IP address	Web contents sent from subject to another place through the TOE	MIME, HTTP Response Message (Response-Header, Entity-Header, Message-Body)	Protect contents if an appropriate rule (to transform, allow, block) exists - Transform: allow access after transformation into the transferred data value - Allow: allow access - Block: block access
IT entity on the side of information sender	IP address	Traffic sent from subject to another place through the TOE	IP address, net mask, port number, protocol, priority, packet direction	Allow if an allow-rule exists; Block if a block-rule exists
Authorized administrator	Identifier	Audit data	See audit review list of Table 6-5 Audit review criteria	Read, search
		TSF data	See Table 6-14 TSF data list(1)	Query
			See Table 6-15 TSF data list(2)	Query, modify
			See Table 6-16 TSF data list(3)	Query, delete, generate
			See Table 6-17 TSF data list(4)	Change default, query, modify, generate, heuristics
			See Table 6-18 TSF data list(5)	Query, modify, delete, generate
			See Table 6-19 Action taken in case of exceeded TSF data limit	Specify limits
		Security	SECUI NXG W Information flow	Query, modify, delete,

Subject (User)	Subject (User) security attributes	Object (Information)	Object (Information) security attributes	Operation
		attributes	denial policy; See Table 6-10 Management of security attributes(1)	generate, heuristics
			SECUI NXG W Information flow permission policy; See Table 6-11 Management of security attributes(2)	Query, modify, delete, generate, heuristics
			SECUI NXG W Information flow web contents protection policy; See Table 6-12 Management of security attributes(3)	Query, modify, delete, generate, heuristics
			SECUI NXG W Information flow packet filtering policy; See Table 6-13 Management of security attributes(4)	Query, modify, delete, generate
			SECUI NXG W Information flow packet filtering policy, packet direction and protocol	Query, modify
		Security function	See Table 6-7 List of functions(1)	Disable, enable
			See Table 6-8 List of functions(2)	Enable
			See Table 6-9 List of functions(3)	Modify behavior

b) External entity

- Administrator console (CLI/GUI): An external entity that provides an interface for an authorized administrator to access the TOE and manage security functions; web browser and administrator console program.
- Web server (web application): Server and application protected by the TOE that provide web services.
- Web client (web browser): A user accessing an object of protection of the TOE, i.e. an external IT entity that accesses a web server using a web browser.
- DB server (web application): A server program for processing DB data on a web application.
- DNS server: A server that provides domain name service; a web client can access the web server using a domain name.
- NTP server: A server program that provides time information to the TOE; it supports audit functions using a trusted time stamp.
- SMTP server: A server that provides mailing service; it sends TSF-related a warning message produced by the TOE to an email specified by an administrator.

6.1. Security functional requirements

The security functional requirements defined in this Security Target consist of the following components from Part 2 of the CC, summarized in the following Table 6-2.

Table 6-2 Security Functional Requirements

Security Functional Class	Security Functional Components	
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_STG.1	Protected audit trail storage
	FAU_STG.3	Action in case of possible audit data loss
	FAU_STG.4	Prevention of audit data loss
User Data Protection	FDP_IFC.1(1)	Subset information flow control(1)
	FDP_IFC.1(2)	Subset information flow control(2)
	FDP_IFC.1(3)	Subset information flow control(3)
	FDP_IFC.1(4)	Subset information flow control(4)
	FDP_IFF.1(1)	Simple security attributes(1)
	FDP_IFF.1(2)	Simple security attributes(2)
	FDP_IFF.1(3)	Simple security attributes(3)
	FDP_IFF.1(4)	Simple security attributes(4)
	FDP_SDI.2	Stored data integrity monitoring
Identification and Authentication	FIA_AFL.1	Authentication failure handling
	FIA_ATD.1(1)	User attribute definition(1)
	FIA_ATD.1(2)	User attribute definition(2)
	FIA_UAU.2	User authentication before any action
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	User identification before any action
Security Management	FMT_MOF.1(1)	Management of security functions behavior(1)
	FMT_MOF.1(2)	Management of security functions behavior(2)
	FMT_MOF.1(3)	Management of security functions behavior(3)
	FMT_MSA.1(1)	Management of security attributes(1)
	FMT_MSA.1(2)	Management of security attributes(2)
	FMT_MSA.1(3)	Management of security attributes(3)
	FMT_MSA.1(4)	Management of security attributes(4)

Security Functional Class	Security Functional Components	
	FMT_MSA.1(5)	Management of security attributes(5)
	FMT_MSA.3	Static attribute initialization
	FMT_MTD.1(1)	Management of TSF data(1)
	FMT_MTD.1(2)	Management of TSF data(2)
	FMT_MTD.1(3)	Management of TSF data(3)
	FMT_MTD.1(4)	Management of TSF data(4)
	FMT_MTD.1(5)	Management of TSF data(5)
	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_TEE.1	Testing of external entities
	FPT_FLS.1	Failure with preservation of secure state
	FPT_TST. 1	TSF testing
Resource Utilization	FRU_FLT. 1	Degraded fault tolerance
TOE Access	FTA_SSL.3	TSF-initiated termination

6.1.1. Security Audit (FAU)

6.1.1.1. 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 [send the email to the address registered by the authorized administrator] upon detection of a potential security violation.

6.1.1.2. 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 *not specified* level of audit; and

c) [information specified in the Auditable Events column and categorized as "Others" in the Category column of Table 6-3]

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 (if applicable), 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, [information specified in the Additional audit record contents column of Table 6-3]

Table 6-3 Auditable events

Functional Components	Auditable Events	Category	Additional audit record contents
FAU_ARP. 1	Actions taken due to imminent security violations	Others	Recipient identity of actions
FAU_SAA.1	Enabling and disabling of any of the analysis mechanisms, Automated responses performed by the tool	Others	-
FDP_IFF.1	Decisions to permit requested information flows	Others	Identified information of Object
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	Others	-
FIA_UAU.2	Unsuccessful use of the authentication mechanism	Others	-
FIA_UID.2	Unsuccessful use of the user identification mechanism, including the user identity provided	Others	-
FMT_SMF.1	Use of the management functions	Others	-
FMT_SMR.1	Modifications to the group of users that are part of a role	Others	-
FPT_TST. 1	Execution of the TSF self tests and the results of the tests	Others	-
FRU_FLT. 1	Any failure detected by the TSF	Others	-
FTA_SSL.3	Termination of an interactive session by the session locking mechanism	Others	-

FAU_GEN.2 User identity association

Hierarchical to: No other components

Dependencies: FAU_GEN.1 Audit data generation

FID_UID.1 Timing of identification

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.1.1.3. 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 enforcement of the SFRs.

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

a) Accumulation or combination of [audit event of unsuccessful authentication among the auditable events in FIA_UAU.2, audit event of Table 6-4 Information flow controlled rule violation among the auditable events in FDP_IFF.1, audit event of integrity violation among the auditable events in FPT_TST. 1] known to indicate a potential security violation;

b) [none]

Table 6-4 Audit event of information flow controlled rule violation

Information flow controlled rule	Audit event of rule violation
SECUI NXG W Information flow denial policy	Audit event where an audit record is generated that information requested by a web client is considered an attack because it does not match the cookie domain, cookie, web server address, and URL list registered by the TOE through heuristics.
SECUI NXG W Information flow permission policy	Audit event where an audit record is generated that information requested by a web client is considered an attack because it matches the block-rule that the TSF provides based on the web server, cookie, and HTTP request message registered by the TOE through heuristics.
SECUI NXG W Information flow web contents protection policy	Audit event where an audit record is generated that information requested by a web client is considered an attack because it matches the MIME attribute provided by the protected web server and a rule to protect contents – to transform, allow, or block.

6.1.1.4. 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 **authorized administrator** 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 apply [search] of audit data based on [the criteria in the Table 6-5 Audit review criteria].

Table 6-5 Audit review criteria

Type of auditable events	Audit review item	Criteria
Web intrusion blocking	Level, URL, Time, Method, Subject ID (Client IP), Object ID (Server IP, Real Dest IP), Result, Attack Type	• Search by keywords for each audit review item. • Search by for more than one audit review item and in condition 'AND'
Packet filtering rule Check	Timestamp, Subject ID (Src IP, Src Port), Object ID (Dst IP, Dst Port), Protocol, Packet filtering rule number (Rule ID), Action	
Security management behavior	Level, Timestamp, Subject ID (From ID), Object ID (To ID), User ID	
TOE testing and TSF error detection	Level, Time	

6.1.1.5. 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 in the audit trail 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 [send an email to the address registered by the authorized administrator] if the audit trail exceeds [95% of the audit storage capacity].

FAU_STG.4 Prevention of audit data loss

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

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4.1 The TSF shall *overwrite the oldest stored audit records* and [none] if the audit trail is full.

6.1.2. User Data Protection (FDP)

6.1.2.1. 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(1) The TSF shall enforce the [SECUI NXG W Information flow denial 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 web client on the side of information sender

b) Information: Web traffic sent from subject to another place through the TOE

c) Operation: Pass when allowing rules exist, otherwise block]

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

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

Hierarchical to: No other components

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1(2) The TSF shall enforce the [SECUI NXG W Information flow permission 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 web client on the side of information sender

b) Information: Web traffic sent from subject to another place through the TOE

c) Operation: Block when blocking rules exist, otherwise allow]

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

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

Hierarchical to: No other components

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1(3) TSF shall enforce the [SECUI NXG W Information flow web contents protection 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: Web server or web application program on the side of information sender

b) Information: Web contents sent from subject to another place through the TOE

c) Operation: Protect contents when protecting of web contents rules in transforming, allowing and blocking, exists

- Allow after transforming into the transferred data when transforming rules exist
- Allow when allowing rules exist
- Block when blocking rules exist]

Application notes: This security policy is defined to rules in order to protect web contents provided by the web service and required data if it is specified to be protected. For the web contents protecting, the TOE is provided by rules to allow, block, and transform. Web contents can be an initial homepage, image, file, personal credit information (i.g. SSN, credit card number, etc.), footnote in a web page, or an error page and etc.

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

Hierarchical to: No other components

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1(4) The TSF shall enforce [SECUI NXG W Information flow packet filtering 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: IT entity on the side of information sender

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

c) Operation: Allow when allowing rules exist, block when blocking rules exist]

Application notes: This security policy is packet filtering policy to control flow of all packets that inflow and outflow through the TOE, and it is allowing and blocking rule. Also, it is in control of information flow of packet by using packet direction and priority.

6.1.2.2. FDP_IFF Information flow control functions

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

Hierarchical to: No other components

Dependencies: FDP_IFC.1Subset information flow control

FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1(1) The TSF shall enforce the [SECUI NXG W Information flow denial policy] on the following types of subject and information security attributes:

a) [List of subjects: Unauthorized web client on the side of information sender
Subject security attributes: IP address

b) List of information: Web traffic sent from subject to another place through the TOE
Information security attributes: cookie domain, cookie, web server address, URL]

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

a) [The TOE shall permit requests for access of services where the presumed web server address by request of web client is included in the set of registered or heuristic IP addresses by the TOE.

b) The TOE shall permit requests for access of services where the URL by request of web client is included in the set of heuristic or registered URL by authorized administrator.

c) The TOE shall permit requests for access of services where the cookie domains by request of web client is included in heuristic cookie domains or not included in the set of matched rules of default domain policy specified by authorized administrator and by unregistered domain, when allowing rules exist.

d) The TOE shall permit requests for access of services where the cookie by request of web client is included in the set of heuristic cookies or not included in the set of matched rules by the DEFAULT_COOKIE policy for all cookies specified by authorized administrator and by unregistered cookie, when

allowing rules exist.]

FDP_IFF.1.3(1) The TSF shall enforce the [none].

FDP_IFF.1.4(1) The TSF shall explicitly authorize an information flow based on the following rules:

a) [The TOE shall permit requests for access of services where the IP address by request of web client is included in the set of bypass addresses in bypass group policy of the TOE.]

FDP_IFF.1.5(1) The TSF shall explicitly deny an information flow based on the following rules:

a) [The TOE shall reject requests in which the information received by the TOE contains abnormal structure of cookie.]

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

Hierarchical to: No other components

Dependencies: FDP_IFC.1Subset information flow control

FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1(2) The TSF shall enforce the [SECUI NXG W Information flow permission policy] based on the following types of subject and information security attributes:

a) [List of subjects: Unauthorized web client on the side of information sender
Subject security attributes: IP address

b) List of information: Web traffic sent from subject to another place through the TOE
Information security attributes: web server address, cookie, HTTP request message (method, request-URI, request headers)]

FDP_IFF.1.2(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) [The TOE shall permit to reject access of services in which the information received by the TOE contains expired cookie session time and invalid cookie value issued in cookie session of information.

b) The TOE shall permit to reject access of services in which the information received by the TOE contains http request message known to heuristics or matching rulesets by the following security policy rulesets of web server URL :
URL check, header buffer overflow check, password check, URL-based access control, URL extension check, get query check, post query check, header method check, sql syntax injection protection, cross-site scripting protection, command injection protection, hidden field operation protection,

base64 encoding check.

FDP_IFF.1.3(2) The TSF shall enforce the [none].

FDP_IFF.1.4(2) The TSF shall explicitly authorize an information flow based on the following rules:

a) [The TOE shall permit HTTPS traffic that in web session by request for web client contains HTTP protocol when transforming HTTP protocol into HTTPS protocol rulesets exist.

b) The TOE shall permit requests for access of services that contains registered web client by administrator.]

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

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

Hierarchical to: No other components

Dependencies: FDP_IFC.1Subset information flow control

FMT_MSA.3 Static attribute initialization

FDP_IFF.1.1(3) The TSF shall enforce the [SECUI NXG W Information flow web contents protection policy] based on the following types of subject and information security attributes:

a) [List of subjects: Web server or web application program on the side of information sender

Subject security attributes: IP address

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

Information security attributes: MIME, HTTP response message (response-header, entity-header, message-body)]

FDP_IFF.1.2(3) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

a) [The TOE shall permit requests for access of services where the information received by the TOE is included in the set of transforming a requested information if a rule to transform among the web contents check rules applies to the contents such as MIME or HTTP response message that the web server or web application provides at the request of the web client

b) The TOE shall permit requests for access of services where the information received by the TOE is included in the set of allowing rulesets if a rule to allow among the web contents check rules applies to the contents such as MIME or

HTTP response message that the web server or web application provides at the request of the web client.

c) The TOE shall permit to reject access of services in which the information received by the TOE contains rules to block among the web contents rules applies to the contents such as MIME or HTTP response message that the web server or web application provides at the request of the web client.]

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

FDP_IFF.1.4(3) The TSF shall explicitly authorize an information flow based on the following rules: [none].

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

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

Hierarchical to: No other components

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

FDP_IFF.1.1(4) The TSF shall enforce the [SECUI NXG W Information flow packet filtering policy] based on the following types of subject and information security attributes:

a) [List of subjects: IT entity on the side of information sender
Subject security attributes: IP address

b) List of information: Traffic sent from subject to another place through the TOE
Information security attributes: IP address, net mask, port number, protocol, priority, packet direction]

FDP_IFF.1.2(4) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

a) [The TOE shall permit requests for access of services that not contains deny of information flow based on the IP address, net mask, port number, protocol, and packet direction of a destination blocked according to the priority set up by authorized administrator.

b) The TOE shall permit requests for access of services that allow of information flow based on the IP address, net mask, port number, protocol, and packet direction of a destination allowed according to the priority set up by an authorized administrator.]

FDP_IFF.1.3(4) The TSF shall enforce the [none].

FDP_IFF.1.4(4) The TSF shall explicitly authorize an information flow based on the following rules: [none].

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

6.1.2.3. FDP_SDI Stored data integrity

FDP_SDI.2 Stored data integrity monitoring and action

Hierarchical to: FDP_SDI.1

Dependencies: No dependencies

FDP_SDI.2.1 The TSF shall monitor user data stored in containers controlled by the TSF for [integrity errors] on all objects, based on the following attributes:

[Types of MIME: text/plain, text/css, multipart/form-data, application/x-www-form-urlencoded, application/x-hwp, application/unknown, application/octet-stream, application/pdf, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, application/x-shockwave-flash, message/http, image/bmp, image/gif, image/jpeg, video/mpeg, video/x-msvideo]

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall [take actions as in the Table 6-6 Actions to be taken upon detection of an integrity error].

Table 6-6 Actions to be taken upon detection of an integrity error

Case	Actions
DROP	To destroy requests for packet, to send an email, to generate audit records
Warning page	To display a warning page that setting up administrator, to send an email, to generate audit records
Redirect	To redirect to a page that setting up administrator, to send an email, to generate audit records

Application notes: User data attributes, web contents, include an initial homepage, image and file. The TOE may specify the user data attributes as a MIME type; integrity monitoring should only be performed on the objects that have the specified attributes.

6.1.3. Identification and Authentication (FIA)

6.1.3.1. 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 *[3]* unsuccessful authentication attempts occur related to [administrator authentication attempts].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *surpassed*, the TSF shall [blocking the login from failed identifier (administrator ID) for the next 5 minutes].

6.1.3.2. 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(1) The TSF shall maintain the following list of security attributes belonging to individual **authorized administrator**:

a) [Identifier

b) Password

c) Authority]

Application notes: Authorized administrators are comprised of super administrator, server administrator, and user. 'Authority' among the security attributes means the permitted range of security functions that can be performed in each role.

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

Hierarchical to: No other components

Dependencies: No dependencies

FIA_ATD.1.1(2) The TSF shall maintain the following list of security attributes belonging to individual **IT entities**: [IP address]

Application notes: An IT entity of the TSF refers to the equipment of an administrator who intends to access the TOE through an identification and authentication. It helps for blocking the replay attack to maintain IP address in security attributes

6.1.3.3. FIA_UAU User Authentication

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

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 [to display input characters as an asterisk ('*')] to the user while the authentication is in progress.

6.1.3.4. FIA_UID User Identification

FIA_UID.2 User identification before any action

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

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

6.1.4. Security Management (FMT)

6.1.4.1. FMT_MOF Management of functions in TSF

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

Hierarchical to: No other components

Dependencies: FMT_SMF.1 Specification of management Functions
FMT_SMR.1 Security roles

FMT_MOF.1.1(1) The TSF shall restrict the ability to *disable, enable* the functions [of Table 6-7 List of functions(1)] to [the authorized administrator].

Table 6-7 List of functions(1)

Functions	Authorities
Operate the function of system monitoring	Super administrator
Operate the function for each TOE information flow controlled ruleset	Super administrator, server administrator
Operate the function of automatic heuristics in redirect server	Super administrator, server administrator
Operate the function of each web server	Super administrator, server administrator

FMT_MOF.1(2) Management of security functions behavior(2)

Hierarchical to: No other components

Dependencies: FMT_SMF.1 Specification of Management Functions
FMT_SMR.1 Security roles

FMT_MOF.1.1(2) The TSF shall restrict the ability to *enable* the functions [of Table 6-8 List of functions(2)] to [the authorized administrator].

Table 6-8 List of functions(2)

Function	Authority
Initialize the system configuration	Super administrator

Restart the services (TSF process)	Super administrator
Restart the system	Super administrator
Backup and recovery the TOE configuration data	Super administrator
Execute the CLI commands	Super administrator, Server administrator, user
Check the integrity	Super administrator
Print out reports	Super administrator, server administrator, user

FMT_MOF.1(3) Management of security functions behavior(3)

Hierarchical to: No other components

Dependencies: FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security roles

FMT_MOF.1.1(3) The TSF shall restrict the ability to *modify the behavior of* the functions [of Table 6-9 List of functions(3)] to [the authorized administrator].

Table 6-9 List of functions(3)

Function	Authority
Operate the operational mode of the TOE	Super administrator
Trail audit records	Super administrator
Operate the heuristic mode of the TOE	Super administrator, server administrator
Apply the security policy of cookie domain	Super administrator, server administrator
Apply the security policy of cookie	Super administrator, server administrator
Operate the heuristic mode of web server URL	Super administrator, server administrator
Apply the security policy of web server URL	Super administrator, server administrator
Apply the monitoring traffic policy in heuristics	Super administrator, server administrator
Apply the non-monitoring traffic policy	Super administrator,

	server administrator
Operate the heuristic mode of each web server	Super administrator, server administrator
Apply the heuristics policy of each web server	Super administrator, server administrator
Apply the permit or not for abnormal escape word	Super administrator, server administrator

6.1.4.2. FMT_MSA Management of security attributes

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

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(1) The TSF shall enforce the [SECUI NXG W Information flow denial policy] to restrict the ability to *query, modify, delete, [generate, learn by heuristics]* the security attributes [in the Table 6-10 Management of security attributes(1)] to [the authorized administrator].

Table 6-10 Management of security attributes(1)

Security attributes	Authorities
Cookie domain	Super administrator, server administrator
Cookie	Super administrator, server administrator
web server address	Super administrator, server administrator
URL	Super administrator, server administrator

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

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(2) The TSF shall enforce the [SECUI NXG W Information flow permission policy] to *query, modify, delete, [generate, learn by heuristics]* the security attributes [in the Table 6-11 Management of security attributes(2)] to [the authorized administrator].

Table 6-11 Management of security attributes(2)

Security attributes	Authorities
web server address	Super administrator, server administrator
Cookie	Super administrator, server administrator
HTTP Request Message	Super administrator, server administrator

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

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(3) The TSF shall enforce the [SECUI NXG W Information flow web contents protection policy] to *query, modify, delete, [generate, learn by heuristics]* the security attributes [in the Table 6-12 Management of security attributes(3)] to [the authorized administrator].

Table 6-12 Management of security attributes(3)

Security attributes	Authorities
MIME	Super administrator, server administrator
HTTP Response Message	Super administrator, server administrator

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

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(4) The TSF shall enforce the [SECUI NXG W Information flow packet filtering policy] to *query, modify, delete, [generate]* the security attributes [in the Table 6-13 Management of security attributes(4)] to [the authorized administrator].

Table 6-13 Management of security attributes(4)

Security attributes	Authorities
Source IP address	Super administrator, server administrator
Source net mask	Super administrator, server administrator
Destination IP address	Super administrator, server administrator
Destination port number	Super administrator, server administrator
Priority	Super administrator, server administrator

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

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(5) The TSF shall enforce the [SECUI NXG W Information flow packet filtering policy] to *query, modify, [none]* the security attributes [packet direction, protocol] to [the authorized administrator].

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 [SECUI NXG W Information flow denial policy, SECUI NXG W Information flow permission policy, SECUI NXG W Information flow web

contents protection policy, SECUI NXG W Information flow packet filtering 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 [super administrator, server administrator] to specify alternative initial values to override the default values when an object or information is created.

6.1.4.3. FMT_MTD Management of TSF data

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

Hierarchical to: No other components

Dependencies: FMT_SMF.1 Specification of Management Functions
FMT_SMR.1 Security roles

FMT_MTD.1.1(1) The TSF shall restrict the ability to *query* the [TSF data in the Table 6-14 List of TSF data(1)] to [the authorized administrator].

Table 6-14 List of TSF data(1)

TSF data	Authorities
System configuration information	Super administrator
Information of real-time traffic status	Super administrator, server administrator, user
Statistics of the TOP5 among blocked web intrusion events	Super administrator, server administrator, user
Real-time monitoring information of blocked web intrusion events	Super administrator, server administrator, user
Log search information of an audit review items for each type of audit event	Super administrator
Statistics of an audit for a specific period of time	Super administrator

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

Hierarchical to: No other components

Dependencies: FMT_SMF.1 Specification of Management Functions
FMT_SMR.1 Security roles

FMT_MTD.1.1(2) The TSF shall restrict the ability to *query, modify* the [TSF data in the Table 6-15 List of TSF data(2)] to [the authorized administrator].

Table 6-15 List of TSF data(2)

TSF data	Authorities
Version and information of the TOE	Super administrator
Time information of the TOE	Super administrator
Time limit of an administrator session	Super administrator
Permitted number of login sessions	Super administrator
Administrator interface information	Super administrator
Information of the TOE network interface communication mode	Super administrator
Address of each operation mode of the TOE network	Super administrator
Interface information of each operation mode of the TOE network	Super administrator
Address of other servers (DNS, NTP)	Super administrator
Information about enabling audit functions	Super administrator
Configuration information of a policy bypass group for the purpose of administration	Super administrator, server administrator
Email configuration information of an administrator of a policy bypass for the purpose of administration	Super administrator, server administrator
URL property information of each web server	Super administrator, server administrator

FMT_MTD.1(3) Management of TSF data(3)

Hierarchical to: No other components

Dependencies: FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security roles

FMT_MTD.1.1(3) The TSF shall restrict the ability to *query, delete, [generate]* the [TSF data in the Table 6-16 List of TSF data(3)] to [the authorized administrator].

Table 6-16 List of TSF data(3)

TSF data	Authorities

Address of other servers (DNS, NTP)	Super administrator
Configuration information of a site (automatic) heuristics	Super administrator, server administrator
Information of an SSL configurable MIME type	Super administrator, server administrator

FMT_MTD.1(4) Management of TSF data(4)

Hierarchical to: No other components

Dependencies: FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security roles

FMT_MTD.1.1(4) The TSF shall restrict the ability to *change_default, query, modify, delete, [generate, learn by heuristics]* the [TSF data in the Table 6-17 List of TSF data(4)] to [the authorized administrator].

Table 6-17 List of TSF data(4)

TSF data	Authorities
Configuration information of SECUI NXG W Information flow denial policy	Super administrator, server administrator
Configuration information of SECUI NXG W Information flow permission policy	Super administrator, server administrator
Configuration information of SECUI NXG W Information flow web contents protection policy	Super administrator, server administrator

FMT_MTD.1(5) Management of TSF data(5)

Hierarchical to: No other components

Dependencies: FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security roles

FMT_MTD.1.1(5) The TSF shall restrict the ability to *query, modify, delete, [generate]* the [TSF data in the Table 6-18 List of TSF data(5)] to [the authorized administrator].

Table 6-18 List of TSF data(5)

TSF data	Authorities

TSF data	Authorities
Configuration information of an administrator mail	Super administrator
Warning page	Super administrator
Configuration information of a policy bypass for the purpose of administration	Super administrator
Information about identification and authentication of an administrator	Super administrator
Configuration information of a host name	Super administrator
Routing configuration information	Super administrator
Configuration information of each web server URL host	Super administrator, server administrator
IP address and Port configuration information of each web server	Super administrator, server administrator
Configuration of each web server heuristics: MIME list, method list, and header list	Super administrator, server administrator
Configuration information of an SSL certificate	Super administrator
Configuration information of SECUI NXG W Information flow packet filtering policy	Super administrator, server administrator

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 [the TSF data in the Table 6-19] to [the super administrator, server administrator].

FMT_MTD.2.2 The TSF shall take the following actions, if the TSF data are at, or exceed, the indicated limits: [actions in the Table 6-19]

Table 6-19 Actions in case of reached or exceeded TSF data limits

TSF data	Limits	Actions
Time limit of an administrator session	1~1440 (minutes)	Terminate GUI and re-authenticate
Permitted number of login	1~64	Block access to GUI

TSF data	Limits	Actions
sessions		
Cookie session timeout	60~86400 (seconds)	Terminate the cookie session
HTTP header size	1024 ~ 16384 bytes	Deny requested web traffic, email an administrator, make an audit record
		Display a warning message, email an administrator, make an audit record
		Redirect to a URL designated by an administrator, email an administrator, make an audit record
Number of hidden SSN figures	1~13	Replace the figure with '*'
Number of hidden credit card figures	1~16	Replace the figure with '*'
Number of GET query	0~65535	Deny requested query, email an administrator, make an audit record
		Display a warning message, email an administrator, make an audit record
		Redirect to a URL designated by an administrator, email an administrator, make an audit record
Number of POST query	0~65535	Deny requested query, email an administrator, make an audit record
		Display a warning message, email an administrator, make an audit record
		Redirect to a URL designated by an administrator, email an administrator, make an audit record

6.1.4.4. 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]

6.1.4.5. 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: [the authorized administrator].

FMT_SMR.1.2 The TSF shall be able to associate **authorized administrators** with roles.

6.1.5. Protection of the TSF (FPT)

6.1.5.1. FPT_FLS Fail secure

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components

Dependencies: No dependencies

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [Failure due to the CPU usage and memory resource exhaustion]

6.1.5.2. FPT_TEE Testing of external entities

FPT_TEE.1 Testing of external entities

Hierarchical to: No other components

Dependencies: No dependencies

FPT_TEE.1.1 The TSF shall run a suite of tests *during initial start-up, periodically during normal operation, [at the restart of the TOE by an authorized administrator]* to check the fulfillment of [the properties of the external entities: Disk, Memory, TSF process, each network interface].

FPT_TEE.1.2 If the test fails, the TSF shall [make a restart the TOE by authorized administrator].

6.1.5.3. FPT_TST TSF self test

FPT_TST. 1 TSF testing

Hierarchical to: No other components

Dependencies: No dependencies

FPT_TST. 1.1 The TSF shall run a suite of self tests *during initial start-up, at the request of the authorized administrator* to demonstrate the correct operation of *the TSF*.

FPT_TST. 1.2 The TSF shall provide **authorized administrators** with the capability to verify the integrity of *[TSF configuration file, identification and authentication data]*.

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

6.1.6. Resource Utilization (FRU)

6.1.6.1. 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 [service restart] when the following failures occur: [Types of TSF failures in FPT_FLS.1]

6.1.7. TOE Access (FTA)

6.1.7.1. FTA_SSL Session locking and termination

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 [1~1440 minutes of an administrator inactivity after identification of that administrator].

6.2. Security assurance requirements

The security assurance requirement (SAR)s 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 shows the assurance components.

Table 6-20 Security assurance requirements: EAL4

Assurance class	Assurance component	
Security target evaluation	ASE_INT. 1	ST introduction
	ASE_ECD.1	Extended components definition
	ASE_CCL.1	Conformance claims
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Development	ADV_ARC.1	Security architecture description
	ADV_FSP. 4	Complete functional specification
	ADV_IMP. 1	Implementation representation of the TSF
	ADV_TDS.3	Basic modular design
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life cycle support	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.4	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedures
	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. 2	Testing: security enforcing modules
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability assessment	AVA_VAN.3	Focused vulnerability analysis

6.2.1. Security target evaluation (ASE)

6.2.1.1. ASE_INT. 1 ST introduction

Dependencies: No dependencies

Developer action elements

ASE_INT. 1.1D The developer shall provide an ST introduction.

Content and presentation elements

ASE_INT. 1.1C The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.

ASE_INT. 1.2C The ST reference shall uniquely identify the ST.

ASE_INT. 1.3C The TOE reference shall identify the TOE.

ASE_INT. 1.4C The TOE overview shall summarise the usage and major security features of the TOE.

ASE_INT. 1.5C The TOE overview shall identify the TOE type.

ASE_INT. 1.6C The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.

ASE_INT. 1.7C The TOE description shall describe the physical scope of the TOE.

ASE_INT. 1.8C The TOE description shall describe the logical scope of the TOE.

Evaluator action elements

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

ASE_INT. 1.2E The evaluator *shall confirm* that the TOE reference, the TOE overview, and the TOE description are consistent with each other.

6.2.1.2. ASE_ECD.1 Extended components definition

Dependencies: No dependencies

Developer action elements

ASE_ECD.1.1D The developer shall provide a statement of security requirements.

ASE_ECD.1.2D The developer shall provide an extended components definition.

Content and presentation elements

ASE_ECD.1.1C The statement of security requirements shall identify all extended security requirements.

ASE_ECD.1.2C The extended components definition shall define an extended component for each extended security requirement.

ASE_ECD.1.3C The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.

ASE_ECD.1.4C The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.

ASE_ECD.1.5C The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.

Evaluator action elements

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

ASE_ECD.1.2E The evaluator *shall confirm* that no extended component can be clearly expressed using existing components.

6.2.1.3. ASE_CCL.1 Conformance claims

Dependencies: ASE_INT. 1 ST introduction
ASE_ECD.1 Extended components definition
ASE_REQ.1 Stated security requirements

Developer action elements

ASE_CCL.1.1D The developer shall provide a conformance claim.

ASE_CCL.1.2D The developer shall provide a conformance claim rationale.

Content and presentation elements

ASE_CCL.1.1C The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.

ASE_CCL.1.2C The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.

ASE_CCL.1.3C The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.

ASE_CCL.1.4C The CC conformance claim shall be consistent with the extended components definition.

ASE_CCL.1.5C The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.

ASE_CCL.1.6C The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.

ASE_CCL.1.7C The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.

ASE_CCL.1.8C The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.

ASE_CCL.1.9C The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.

ASE_CCL.1.10C The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.

Evaluator action elements

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

6.2.1.4. ASE_OBJ.2 Security objectives

Dependencies: ASE_SPD.1 Security problem definition

Developer action elements

ASE_OBJ.2.1D The developer shall provide a statement of security objectives.

ASE_OBJ.2.2D The developer shall provide a security objectives rationale.

Content and presentation elements

ASE_OBJ.2.1C The statement of security objectives shall describe the security objectives for the TOE and the security objectives for the operational environment.

ASE_OBJ.2.2C The security objectives rationale shall trace each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective.

ASE_OBJ.2.3C The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.

ASE_OBJ.2.4C The security objectives rationale shall demonstrate that the security objectives counter all threats.

ASE_OBJ.2.5C The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.

ASE_OBJ.2.6C The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.

Evaluator action elements

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

6.2.1.5. ASE_REQ.2 Derived security requirements

Dependencies: ASE_OBJ.2 Security objectives
ASE_ECD.1 Extended components definition

Developer action elements

ASE_REQ.2.1D The developer shall provide a statement of security requirements.

ASE_REQ.2.2D The developer shall provide a security requirements rationale.

Content and presentation elements

ASE_REQ.2.1C The statement of security requirements shall describe the SFRs and the SARs.

ASE_REQ.2.2C All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.

ASE_REQ.2.3C The statement of security requirements shall identify all operations on the security requirements.

ASE_REQ.2.4C All operations shall be performed correctly.

ASE_REQ.2.5C Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.

ASE_REQ.2.6C The security requirements rationale shall trace each SFR back to the security objectives for the TOE.

ASE_REQ.2.7C The security requirements rationale shall demonstrate that the SFRs meet all

security objectives for the TOE.

ASE_REQ.2.8C The security requirements rationale shall explain why the SARs were chosen.

ASE_REQ.2.9C The statement of security requirements shall be internally consistent.

Evaluator action elements

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

6.2.1.6. ASE_SPD.1 Security problem definition

Dependencies: No dependencies

Developer action elements

ASE_SPD.1.1D The developer shall provide a security problem definition.

Content and presentation elements

ASE_SPD.1.1C The security problem definition shall describe the threats.

ASE_SPD.1.2C All threats shall be described in terms of a threat agent, an asset, and an adverse action.

ASE_SPD.1.3C The security problem definition shall describe the OSPs.

ASE_SPD.1.4C The security problem definition shall describe the assumptions about the operational environment of the TOE.

Evaluator action elements

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

6.2.1.7. ASE_TSS.1. TOE summary specification

Dependencies: ASE_INT. 1 ST introduction
ASE_REQ.1 Stated security requirements
ADV_FSP. 1 Basic functional specification

Developer action elements

ASE_TSS.1.1D The developer shall provide a TOE summary specification.

Content and presentation elements

ASE_TSS.1.1C The TOE summary specification shall describe how the TOE meets each SFR.

Evaluator action elements

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

ASE_TSS.1.2E The evaluator *shall confirm* that the TOE summary specification is consistent with the TOE overview and the TOE description.

6.2.2. Development (ADV)

6.2.2.1. ADV_ARC.1 Security architecture description

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

Developer action elements

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

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

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

Content and presentation elements

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

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

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

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

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

Evaluator action elements

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

6.2.2.2. ADV_FSP. 4 Complete functional specification

Dependencies: ADV_TDS.1 Basic design

Developer action elements

ADV_FSP. 4.1D The developer shall provide a functional specification.

ADV_FSP. 4.2D The developer shall provide a tracing from the functional specification to the SFRs.

Content and presentation elements

ADV_FSP. 4.1C The functional specification shall completely represent the TSF.

ADV_FSP. 4.2C The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP. 4.3C The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP. 4.4C The functional specification shall describe all actions associated with each TSFI.

ADV_FSP. 4.5C The functional specification shall describe all direct error messages that may result from an invocation of each TSFI.

ADV_FSP. 4.6C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

Evaluator action elements

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

ADV_FSP. 4.2E The evaluator *shall determine* that the functional specification is an accurate and complete instantiation of the SFRs.

6.2.2.3. ADV_IMP. 1 Implementation representation of the TSF

Dependencies: ADV_TDS.3 Basic modular design
ADV_TAT. 1 Well-defined development tools

Developer action elements

ADV_IMP. 1.1D The developer shall make available the implementation representation for the entire TSF.

ADV_IMP. 1.2D The developer shall provide a mapping between the TOE design description and the sample of the implementation representation.

Content and presentation elements

ADV_IMP. 1.1C The implementation representation shall 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 in the form used by the development personnel.

ADV_IMP. 1.3C The mapping between the TOE design description and the sample of the implementation representation shall demonstrate their correspondence.

Evaluator action elements

ADV_IMP. 1.1E The evaluator *shall confirm* that, for the selected sample of the implementation representation, the information provided meets all requirements for content and presentation of evidence.

6.2.2.4. ADV_TDS.3 Basic modular design

Dependencies: ADV_FSP. 4 Complete functional specification

Developer action elements

ADV_TDS.3.1D The developer shall provide the design of the TOE.

ADV_TDS.3.2D The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

Content and presentation elements

ADV_TDS.3.1C The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.3.2C The design shall describe the TSF in terms of modules.

ADV_TDS.3.3C The design shall identify all subsystems of the TSF.

ADV_TDS.3.4C The design shall provide a description of each subsystem of the TSF.

ADV_TDS.3.5C The design shall provide a description of the interactions among all subsystems of the TSF.

ADV_TDS.3.6C The design shall provide a mapping from the subsystems of the TSF to the modules of the TSF.

ADV_TDS.3.7C The design shall describe each SFR-enforcing module in terms of its purpose and interaction with other modules.

ADV_TDS.3.8C The design shall describe each SFR-enforcing module in terms of its SFR-related interfaces, return values from those interfaces, interaction with and called interfaces to other modules.

ADV_TDS.3.9C The design shall describe each SFR-supporting or SFR-non-interfering module in terms of its purpose and interaction with other modules.

ADV_TDS.3.10C The mapping shall demonstrate that all behavior described in the TOE design is

mapped to the TSFIs that invoke it.

Evaluator action elements

ADV_TDS.3.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ADV_TDS.3.2E The evaluator *shall determine* that the design is an accurate and complete instantiation of all security functional requirements.

6.2.3. Guidance documents (AGD)

6.2.3.1. AGD_OPE.1 Operational user guidance

Dependencies: ADV_FSP. 1 Basic functional specification

Developer action elements

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

Content and presentation elements

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

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

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

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

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

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

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

Evaluator action elements

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

6.2.3.2. AGD_PRE.1 Preparative procedures

Dependencies: No dependencies

Developer action elements

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

Content and presentation elements

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

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

Evaluator action elements

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

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

6.2.4. Life-cycle support (ALC)

6.2.4.1. ALC_CMC.4 Production support, acceptance procedures and automation

Dependencies: ALC_CMS.1 TOE CM coverage
ALC_DVS.1 Identification of security measures
ALC_LCD.1 Developer defined life-cycle model

Developer action elements

ALC_CMC.4.1D The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.4.2D The developer shall provide the CM documentation.

ALC_CMC.4.3D The developer shall use a CM system.

Content and presentation elements

ALC_CMC.4.1C The TOE shall be labelled with its unique reference.

ALC_CMC.4.2C The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.4.3C The CM system shall uniquely identify all configuration items.

ALC_CMC.4.4C The CM system shall provide automated measures such that only authorised changes are made to the configuration items.

ALC_CMC.4.5C The CM system shall support the production of the TOE by automated means.

ALC_CMC.4.6C The CM documentation shall include a CM plan.

ALC_CMC.4.7C The CM plan shall describe how the CM system is used for the development of the TOE.

ALC_CMC.4.8C The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

ALC_CMC.4.9C The evidence shall demonstrate that all configuration items are being maintained under the CM system.

ALC_CMC.4.10C The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.

Evaluator action elements

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

6.2.4.2. ALC_CMS.4 Problem tracking CM coverage

Dependencies: No dependencies

Developer action elements

ALC_CMS.4.1D The developer shall provide a configuration list for the TOE.

Content and presentation elements

ALC_CMS.4.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation representation; and security flaw reports and resolution status.

ALC_CMS.4.2C The configuration list shall uniquely identify the configuration items.

ALC_CMS.4.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

Evaluator action elements

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

6.2.4.3. ALC_DEL.1 Delivery procedures

Dependencies: No dependencies

Developer action elements

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

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

Content and presentation elements

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

Evaluator action elements

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

6.2.4.4. 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 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.

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.

6.2.4.5. 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 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.

6.2.4.6. ALC_TAT. 1 Well-defined development tools

Dependencies: ADV_IMP. 1 Implementation representation of the TSF

Developer action elements

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

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

Content and presentation elements

ALC_TAT. 1.1C Each development tool used for implementation shall be well-defined.

ALC_TAT. 1.2C The documentation of each development tool shall unambiguously define the meaning of all statements as well as all conventions and directives used in the

implementation.

ALC_TAT. 1.3C The documentation of each development tool 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.

6.2.5. Tests (ATE)

6.2.5.1. ATE_COV.2 Analysis of coverage

Dependencies: ADV_FSP. 2 Security-enforcing 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 elements

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

ATE_COV.2.2C The analysis of the test coverage shall demonstrate that all TSFIs in the functional specification have been tested.

Evaluator action elements

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

6.2.5.2. ATE_DPT. 2 Testing: security enforcing modules

Dependencies: ADV_ARC.1 Security architecture description
ADV_TDS.3 Basic modular design
ATE_FUN.1 Functional testing

Developer action elements

ATE_DPT. 2.1D The developer shall provide the analysis of the depth of testing.

Content and presentation elements

ATE_DPT. 2.1C The analysis of the depth of testing shall demonstrate the correspondence between the tests in the test documentation and the TSF subsystems and SFR-enforcing modules in the TOE design.

ATE_DPT. 2.2C The analysis of the depth of testing shall demonstrate that all TSF subsystems in the TOE design have been tested.

ATE_DPT. 2.3C The analysis of the depth of testing shall demonstrate that the SFR-enforcing modules in the TOE design have been tested.

Evaluator action elements

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

6.2.5.3. ATE_FUN.1 Functional testing

Dependencies: ATE_COV.1 Evidence of coverage

Developer action elements

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

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation elements

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

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

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

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

Evaluator action elements

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

6.2.5.4. ATE_IND.2 Independent testing – sample

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

Developer action elements

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

Content and presentation elements

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

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

Evaluator action elements

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

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

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

6.2.6. Vulnerability assessment (AVA)

6.2.6.1. AVA_VAN.3 Focused vulnerability analysis

Dependencies: ADV_ARC.1 Security architecture description
ADV_FSP. 2 Security-enforcing functional specification
ADV_TDS.3 Basic modular design
ADV_IMP. 1 Implementation representation of the TSF
AGD_OPE.1 Operational user guidance
AGE_PRE.1 Preparative procedures

Developer action elements

AVA_VLA.3.1D The developer shall provide the TOE for testing.

Content and presentation elements

AVA_VLA.3.1C The TOE shall be suitable for testing.

Evaluator action elements

AVA_VLA.3.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

AVA_VLA.3.2E The evaluator *shall perform* a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VLA.3.3E The evaluator *shall perform* an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design, security architecture description and implementation representation to identify potential vulnerabilities in the TOE.

AVA_VLA.3.4E The evaluator *shall conduct* penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Enhanced-Basic attack potential.

6.3. Security requirements rationale

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

6.3.1. Security functional requirements rationale

Security functional requirements rationale demonstrates that:

Each security objective for the TOE is addressed by at least one security functional requirement.

Each security functional requirement is addressed by at least one security objective.

Table 6-21 shows a mapping between the security objectives and SFRs.

Table 6-21 Mapping SFRs to the security objectives

Security objective / SFR	O. Availability	O. Audit	O. Management	O. Abnormal Web Request Cut-off	O. Identification and Authentication	O. Web Contents Protection	O. TSF Self Test Protect	O. Information Flow Control	O. Heuristics	O. TSF Data Protection
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_STG.1		X								
FAU_STG.3		X								
FAU_STG.4		X								
FDP_IFC.1(1)								X	X	

Security objective / SFR	O. Availability	O. Audit	O. Management	O. Abnormal Web Request Cut-off	O. Identification and Authentication	O. Web Contents Protection	O. TSF Self Test Protect	O. Information Flow Control	O. Heuristics	O. TSF Data Protection
FDP_IFC.1(2)				X				X		
FDP_IFC.1(3)						X				
FDP_IFC.1(4)								X		
FDP_IFF.1(1)								X	X	
FDP_IFF.1(2)				X				X		
FDP_IFF.1(3)						X				
FDP_IFF.1(4)								X		
FDP_SDI.2						X				
FIA_AFL.1					X					
FIA_ATD.1(1)					X					
FIA_ATD.1(2)					X					
FIA_UAU.2					X					
FIA_UAU.7					X					
FIA_UID.2					X					
FMT_MOF.1(1)			X							
FMT_MOF.1(2)			X							
FMT_MOF.1(3)			X							
FMT_MSA.1(1)			X							
FMT_MSA.1(2)			X							
FMT_MSA.1(3)			X							
FMT_MSA.1(4)			X							
FMT_MSA.1(5)			X							
FMT_MSA.3			X	X						
FMT_MTD.1(1)			X							
FMT_MTD.1(2)			X							

Security objective / SFR	O. Availability	O. Audit	O. Management	O. Abnormal Web Request Cut-off	O. Identification and Authentication	O. Web Contents Protection	O. TSF Self Test Protect	O. Information Flow Control	O. Heuristics	O. TSF Data Protection
FMT_MTD.1(3)			X							
FMT_MTD.1(4)			X							
FMT_MTD.1(5)			X							
FMT_MTD.2			X		X					
FMT_SMF.1			X							
FMT_SMR.1			X							
FPT_TEE.1							X			
FPT_FLS.1	X						X			
FPT_TST. 1							X			X
FRU_FLT. 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_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_IFC.1(1) Subset information flow control(1)

This component satisfies O. Information Flow Control and O. Heuristics because it ensures that SECUI NXG W Information flow denial policy, which is defined based on the security attributes, will be enforced.

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

This component satisfies O. Abnormal Web Request Cut-offand O. Information Flow Control because it ensures that SECUI NXG W Information flow permission policy, which is defined based on the security attributes, will be enforced.

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

This component satisfies O. Web Contents Protection because it ensures that SECUI NXG W Information flow web contents protection policy, which is defined based on the security attributes, will be enforced.

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

This component satisfies O. Information Flow Control because it ensures that SECUI NXG W Information flow packet filtering policy, which is defined based on the security attributes, will be enforced.

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

This component satisfies O. Information Flow Control and O. Heuristics because it provides a rule to control information flow based on security attributes.

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

This component satisfies O. Abnormal Web Request Cut-off and O. Information Flow Control because it provides a rule to control information flow based on security attributes.

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

This component satisfies O. Web Contents Protection because it provides a rule to control information flow based on security attributes.

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

This component satisfies O. Information Flow Control because it provides a rule to control information flow based on security attributes.

FDP_SDI.2 Stored data integrity monitoring and action

This component satisfies O. Web Contents Protection because it monitors integrity of the web contents stored in an external IT entity and provides an appropriate action.

FIA_AFL.1 Authentication failure handling

This component satisfies O. Identification and 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 satisfies O. Identification and Authentication because it requires identification and authentication of each authorized administrator.

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

This component satisfies O. Identification and Authentication because it requires identification and authentication of each user.

FIA_UAU.2 User authentication before any action

This component satisfies O. Identification and Authentication because it ensures an ability to authenticate an authorized administrator successfully.

FIA_UAU.7 Protected authentication feedback

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

FIA_UID.2 User identification before any action

This component satisfies O. Identification and Authentication because it ensures an ability to identify a user successfully.

FMT_MOF.1(1) Management of security functions(1)

This component satisfies O. Management because it ensures that an authorized administrator is able to manage the security functions.

FMT_MOF.1(2) Management of security functions(2)

This component satisfies O. Management because it ensures that an authorized administrator is able to manage the security functions.

FMT_MOF.1(3) Management of security functions(3)

This component satisfies O. Management because it ensures that an authorized administrator is able to manage the security functions.

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

This component satisfies O. Management because it ensures that an authorized administrator manages the security attributes based on which the information flow control policies are applied.

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

This component satisfies O. Management because it ensures that an authorized administrator manages the security attributes based on which the information flow control policies are applied.

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

This component satisfies O. Management because it ensures that an authorized administrator manages the security attributes based on which the information flow control policies are applied.

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

This component satisfies O. Management because it ensures that an authorized administrator manages the security attributes based on which the information flow control policies are applied.

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

This component satisfies O. Management because it ensures that an authorized administrator manages the security attributes based on which the information flow control policies apply.

FMT_MSA.3 Static attribute initialization

This component satisfies O. Management and O. Abnormal Web Request Cut-off because it provides initial values of the security attributes on which the information flow control policies apply.

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

This component satisfies O. Management because it ensures that only an authorized administrator can manage the TSF data related to security.

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

This component satisfies O. Management because it ensures that only an authorized administrator can manage the TSF data related to security.

FMT_MTD.1(3) Management of TSF data(3)

This component satisfies O. Management because it ensures that only an authorized administrator can manage the TSF data related to security.

FMT_MTD.1(4) Management of TSF data(4)

This component satisfies O. Management because it ensures that only an authorized administrator can manage the TSF data related to security.

FMT_MTD.1(5) Management of TSF data(5)

This component satisfies O. Management because it ensures that only an authorized administrator can manage the TSF data related to security.

FMT_MTD.2 Management of limits on TSF data

This component satisfies O. Management and O. Identification and Authentication because it ensures that an authorized administrator defines limits for the number of failed authentication attempts and that actions will be taken if the limits are reached.

FMT_SMF.1 Specification of Management Functions

This component satisfies O. Management 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. Management because it provides roles related to security that the TSF can recognize.

FPT_TEE.1 Testing of external entities

This component satisfies O. TSF Self Test Protect because it ensures that testing of external entities is performed to demonstrate the correct operation of the external entities of the TSF.

FPT_FLS.1 Failure with preservation of secure state

This component satisfies O. Availability and O. TSF Self Test Protect because it ensures that the TOE preserves secure state for the operation of important security functions.

FPT_TST. 1 TSF testing

This component satisfies O. TSF Self Test Protect and O. TSF Data Protection because it ensures self tests of the TSF to demonstrate the correct operation of the TSF and a function that an authorized administrator verifies the integrity of the TSF data and TSF executable code.

FRU_FLT. 1 Degraded fault tolerance

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

FTA_SSL.3 TSF-initiated termination

This component satisfies O. Management because it requires a function to terminate an authorized session after a defined time of an authorized administrator’s inactivity.

6.3.2. Security assurance requirements rationale

The evaluation assurance level of this web application firewall is EAL4.

EAL4, which requires methodical design, test, and review, permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.

EAL4 provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and complete interface specification, guidance documentation, a description of the basic modular design of the TOE, and a subset of the implementation, to understand the security behavior. The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification and TOE design, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, implementation representation, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with an Enhanced-Basic attack potential.

6.4. Dependencies rationale

6.4.1. Dependencies between the SFRs

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

No.	Functional components	Dependencies	Reference no.
22	FMT_MTD.2	FMT_MTD.1 FMT_SMR.1	21 24
23	FMT_SMF.1	-	-
24	FMT_SMR.1	FIA_UID.1	17
25	FPT_TEE.1	-	-
26	FPT_FLS.1	-	-
27	FPT_TST. 1	-	-
28	FRU_FLT. 1	FPT_FLS.1	26
29	FTA_SSL.3	-	-

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

FIA_AFL.1 and FIA_UAU.7 are dependent on FIA_UAU.1, which is satisfied by including FIA_UAU.2 that is hierarchical to FIA_UAU.1.

FAU_GEN.1 is dependent on FPT_STM.1, which is satisfied by OE. Time Stamp as the TOE uses trusted time stamp provided in the operational environment to record security-relevant events correctly.

6.4.2. Dependencies between the SARs

Dependencies in each assurance package provided in the CC are considered satisfied.

7. TOE summary specification

This chapter describes the IT security functions that satisfy the functional requirements and how the security functions satisfy the TOE security functional requirements.

7.1. Security Audit (SW_AUDIT)

7.1.1. Audit record generation (SW_AUDIT_GEN)

Audit generation and protection can generate audit records regarding the following:

- Start-up and shutdown of the audit functions
- Actions taken due to potential security violations
- Enabling and disabling of any of the analysis mechanisms; Automated responses performed by the tool
- 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
- Unsuccessful use of the authentication mechanism
- 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
- Integrity errors
- Termination of an interactive session by the session locking mechanism
- Successful attempts to check the integrity of user data, including an indication of the results of the check.
- Any failure detected by the TSF

The following are audit records additional to those generated on the auditable events above:

- Decisions to permit requested information flows: Identification information of an object and a decision to deny
- Actions taken due to potential security violations: Identity of a recipient of those actions

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

- Date and time of the event
- Event type
- 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. Audit records for each type of audit log are categorized into Allow transaction log, Deny transaction log, L3 firewall log, audit log (configuration log), and system log; generation of each audit record may either be included or excluded.

For each type of audit log, audit record is generated in the following log fields. An audit record can verify the user identity required by FAU_GEN.2.

Allow/deny transaction log is the audit record about the attack types of web intrusion. Table 7-1 shows its log fields.

Table 7-1 Allow/deny transaction log fields

Field	Description
Timestamp	Shows date and time
Server IP	Shows server IP
Server Port	Shows server Port
Attack Type	Shows the attack type of web intrusion
Method	Shows methods like GET, POST, etc.
URL	Shows URL after the root URL
Message	Explains detected message
Real Server IP	Shows actual IP address of the protected web server
Real Server Port	Shows Port of the protected web server
Out bytes	Shows the data size transmitted from a server to a client
In bytes	Shows the data size transmitted from a client to a server
Client IP	Shows IP address of a client
Level	Shows ‘Minor’ in case of allowed transaction; shows ‘Major’ in case of denied transaction
Result	Shows the result of an attack – either allowed or denied; shows the result in a basic configuration – Drop/Redirect

Field	Description
Response Code	Shows an HTML status code
Weekday	Shows a weekday
ID	Shows an ID information regarding a security audit event
Content Type	Shows the type of MIME
User Agent	Shows a user web browser such as Internet Explorer, Mozilla, or Opera
Full Transaction	Shows the whole contents of all transactions in a pop-up window

L3 firewall log is an audit record about allowed or blocked packets as a result of packet filtering. Table 7-2 shows its log fields.

Table 7-2 L3 firewall log fields

Field	Description
Timestamp	Shows date and time
Out bytes	Shows the size of data flowing from In Bound (internal: LAN-T) to Out bound (external: WAN-T)
In bytes	Shows the size of data flowing from Out bound (external: WAN-T) to In Bound (internal: LAN-T)
Time Started	Shows the time that started packet filtering
Time Ended	Shows the time that ended packet filtering
Source IP	Shows the source IP address
Destination IP	Shows the destination IP address
Rule ID	Shows the packet filtering rule ID
Source Port	Shows the source port number
Destination Port	Shows the destination port number
Protocol	Shows the type of protocol used in packet filtering
Level	Shows the priority of packet filtering rules
Action	Shows the result of allowed or blocked packets

Audit log, or configuration log, is an audit record about an administrator's TOE management behavior on the GUI or CLI administrator console. Table 7-3 shows its log fields.

Table 7-3 Audit log (Configuration log) fields

Field	Description
Timestamp	Shows date and time

Field	Description
From ID	Shows a subject ID that generates a configuration log
To ID	Shows an object ID on which a configuration log is generated
Command	Shows the commands enforced by an administrator
Result	Shows the result of an administrator's behavior
Length	Shows the message length that is recorded as a configuration log
Level	Shows the importance of a configuration log
User ID	Shows a user ID of a configuration log
Description	Shows a detailed explanation of a configuration log

System log is an audit record about integrity violation that can occur under the TOE operation mode such as the TOE self testing or testing of external entities and about all kinds of failure detected by the TSF. Table 7-4 shows its log fields.

Table 7-4 System log fields

Field	Description
Level	Shows the importance of a system log
Time	Shows the date and time when the system log is generated
Message	Shows a detailed explanation of a system log

The TOE is able to indicate, by FAU_SAA.1, potential violations analysis using the following information:

Table 7-5 Target of potential violation analysis

✓ Accumulation of administrator authentication failure
✓ Accumulation of audit events of information flow control rule violation
✓ Accumulation of audit events of TSF data and executable code integrity violation

Table 7-6 shows the audit events of information flow control rule violation.

Table 7-6 Audit event of information flow controlled rule violation

Information flow controlled rule	Audit event of a rule violation
SECUI NXG W Information flow denial policy	Audit event where an audit record is generated that information requested by a web client is considered an attack because it does not

Information flow controlled rule	Audit event of a rule violation
	match the cookie domain, cookie, virtual web server, and URL list that are registered by the TOE through heuristics.
SECUI NXG W Information flow permission policy	Audit event where an audit record is generated that information requested by a web client is considered an attack because it matches the block-rule that the TSF provides based on the web server, cookie, and HTTP Request Message registered by the TOE through heuristics.
SECUI NXG W Information flow web contents protection policy	Audit event where an audit record is generated that information requested by a web client is considered an attack because it matches the MIME attribute provided by the protected web server and a rule to protect contents – to transform, allow, or block.

If any of those events in the Table 7-6 is considered by FAU_ARP. 1 as potential violation, an email will be sent to an address registered by an administrator through the GUI administrator console.

7.1.2. Audit record review (SW_AUDIT_REVIEW)

According to FAU_SAR.1, an administrator can review all audit data that are translated into readable form with network connection through the GUI administrator console. Audit trail results are provided in a report form to be interpreted easily. The TOE provides a report function that makes chart and graph of daily, weekly, monthly, and yearly statistics about top-listed attacks and prints out the result in a report format in a PDF or Excel file.

According to FAU_SAR.3, an administrator also can review audit data after filtering it with a defined rule or with a specific criteria with logical relations (using audit review items). Types of auditable events that allow review are web intrusion block event, Packet filtering rule check event, Security management behavior event, and TOE self test and TSF failure detection event. These can be reviewed for the following types of events in the Table 7-7 if Audit data generation enables audit function on the Allow/deny transaction log, L3 firewall log, audit log (configuration log), and system log.

Table 7-7 Audit review criteria

Type of auditable event	Audit review item	Criteria
Web intrusion block event	Level, URL, Time, Method, Subject ID (Client IP), Object ID (Server IP, Real Destination IP),	• Search by keywords for each audit review

Type of auditable event	Audit review item	Criteria
	Result, Attack Type	item. • Search for more than one audit review item and in condition 'AND'
Packet filtering rule check event	Timestamp, Subject ID (Src IP, Src Port), Object ID (Dst IP, Dst Port), Protocol, Packet filtering rule number (Rule ID), Action	
Security management behavior event	Level, Timestamp, Subject ID (From ID), Object ID (To ID), User ID	
TOE self test and TSF failure detection event	Level, Time	

7.1.3. Audit record protection (SW_AUDIT_PROTECT)

According to FAU_STG.1, the TOE generates an audit record in a binary type, not a normal text file. Log does not allow MODIFY but READ right only. The TOE therefore can prevent modification of the audit records.

According to FAU_STG.3, the TOE checks audit storage every 10 seconds and, if more than 95% of the file system in which audit data is stored is used, send an alarm email to an authorized administrator.

According to FAU_STG.4, the TOE sends an alarm email to an administrator if the audit storage is full (more than 99% of the capacity is being used) and starts deleting the oldest audit record. Therefore the authorized administrator shall manage the capacity of audit data trail carefully and delete audit records using the GUI administrator console (initializing system configuration) if the audit data threshold is passed.

7.2. Identification and Authentication (SW_INA)

7.2.1. Administrator group generation and administrator registration (SW_INA_REGISTER)

When an administrator wants to use the GUI administrator console or access the TOE through the CLI administrator console, the administrator shall be identified and authenticated. When the TOE is enabled, an administrator can access the TOE and log in with the administrator information set as a default values from the point of delivery. The TOE defines an administrator group and manages it for each web server and domain separately, which is necessary for the management of many different web servers and domains.

The TOE can register an administrator in the administrator group through the GUI administrator console.

- **User ID**: Input administrator ID (Valid from 4 to 32 bits)
- **Password**: Input password (Valid from 4 to 32 bits)
- **Password confirmation**: Input password again
- **Name**: Input administrator name
- **Email**: Input administrator email address
- **Tel. no.**: Input administrator phone number
- **Other**: Input other information
- **Level**: Set administrator level (See Table 7-13 Authorized administrator roles)
- **Group list**: Select administrator group

Authority of administrator is categorized into a super administrator, server administrator, and user. Management of administrators is only possible by a super administrator.

7.2.2. Administrator identification and authentication (SW_INA_AUTH)

All accesses to the TOE are through the GUI or CLI administrator console. The TOE provides a function to identify and authenticate an administrator before any action (FIA_UID.2, FIA_UAU.2). Identification and authentication of an administrator use password based process.

Information of the ID (identifier), password, and authority are stored in the TOE file system according to FIA_ATD.1(1) and used for confirmation of the ID and password an authorized administrator will input when accessing the GUI administrator console. Access will be allowed only when the values match the stored data.

According to FIA_ATD.1(2), the TOE identifies an external IT entity accessing the protected web server and checks whether it is authorized using an IP address. If an IT entity that is not registered by an authorized administrator accesses a specific URL of the protected web server, the TOE identifies it and generates an audit record.

An administrator cannot enforce any security functions before authentication. While authentication is in progress, the password input by a user will be displayed as '*' according to FIA_UAU.7 to protect authentication data. In case of authentication failure, the TOE will display a login failure message.

According to FIA_AFL.1, when an authentication attempt fails three consecutive times, the TOE will block login access from the failed administrator ID for the next 5 minutes.

7.3. User Data Protection (SW_DP)

The TSF applies SECUI NXG W Information flow denial policy, SECUI NXG W Information flow permission policy, SECUI NXG W Information flow web contents protection policy, and SECUI NXG W Information flow packet filtering policy on operations causing information flow between a subject and information, which sends and receives information through the TOE.

7.3.1. Web server attack (SW_DP_AP)

7.3.1.1. Web server data learning (SW_DP_AP_LEARN)

The TOE monitors the protected web server for the request of a web client for a specific period of time and, based on collected web traffic data, builds a web tree database to be used in applying SECUI NXG W Information flow denial policy defined in FDP_IFC.1(1) and FDP_IFF.1(1).

The TOE collects web traffic data through heuristics about the following items, which are defined as information security attributes in FDP_IFF.1(1).

- Cookie
- Cookie domain
- URL
- Web server address

Cookie domain is necessary for management at each domain when maintaining session information at the request for a cookie of a web client. Cookie information is managed in it.

'Cookie' means a session cookie, in which ID information of a session allowed access to the web server is included. Functions to protect a cookie can be divided into SQL syntax injection protection, cross-site scripting protection, and command injection protection. Table 7-8 shows actions of each function.

Table 7-8 Cookie policies

Cookie policy	Action

Cookie policy	Action
Command injection protection	Check or pass
	Transform into an HTML entity code or do not transform
Cross-site scripting protection	Check or pass
	Transform into an HTML entity code or do not transform
SQL syntax injection protection	Check or pass
	Transform into an HTML entity code or escape special characters
	Duplicate special characters or do not transform

In case that a domain in the protected web server is configured as a name an administrator specified as an alias, the TOE will collect web traffic data about the web server by interpreting the domain information.

URL information is collected as a part of heuristics about URLs in the web server at the request of a web client and under application of information flow functions.

The TOE can set a bypass policy on a specific web page or URL in the web server for the purpose of management if the protected web server is known by heuristics. Then a web client that intends to access the TOE can access the web server regardless of the TOE information flow control policy.

7.3.1.2. Web server data protection (SW_DP_AP_PROTECT)

Intrusion detection and block function shall be performed on the web server protected by the TOE by analyzing web intrusion types exploiting vulnerabilities of web based on the web traffic data collected by web server data learning. To this end, SECUI NXG W Information flow permission policy will be applied as defined in FDP_IFC.1(2) and FDP_IFF.1(2).

Checking web traffic is based on a thorough analysis of a source IP address, destination IP address, and HTTP protocol. Attack pattern will be checked in accordance with the policies set by each module composed. Packets generated by the TOE and those delivered to a web server that is not protected are not related to the security functions. web traffics with a host name not specified in the security policy and of a size larger than allowed will be destroyed immediately. The following are the security functions applied for web server attack protection.

Base64 encoding check

If an external user transfers data that did not use base64 encoding method while the policy is

established that any query transferred to the web server should use base64 encoding method, performs security behaviors (LOG, destroying packet, page redirection, sending a warning page, and emailing an administrator) as set by an administrator.

Command injection protection

Checks if an external user uses command on the web server using a query or cookie data or reads a data file stored in the system and, if it is the case, performs security behaviors (LOG, destroying packet, page redirection, sending a warning page, emailing an administrator, and replacing characters) as set by an administrator.

Cookie corruption check

If a stolen cookie value is detected or a cookie (domain) not permitted is transferred from the web server through an analysis, performs security behaviors (LOG, destroying packet, page redirection, sending a warning page, and emailing an administrator) as set by an administrator. Provides cookie encryption to protect the cookie, which makes prevention of illegal access through manipulating cookies and a Replay attack possible.

Cross-site scripting protection

Checks if an external user intends to operate a malicious HTML tag or script on his web browser or another's web browser that displayed a web page and, if any violation is detected, performs security behaviors (LOG, destroying packet, page redirection, sending a warning page, and emailing an administrator) as set by an administrator.

Header buffer overflow check

If an external user attempts to transfer a header of a bigger size than specified by an administrator to cause an error in the web server, performs security behaviors (LOG, destroying packet, page redirection, sending a warning page, and emailing an administrator) as set by an administrator.

Header method check

If a method of an accessing URL is not one of the header methods that are allowed for each URL or learnt to be allowed, performs security behaviors (LOG, destroying packet, page redirection, sending a warning page, and emailing an administrator) as set by an administrator.

Hidden field manipulation protection

If an external user manipulates a hidden field into the web server using POST query, performs security behaviors (LOG, destroying packet, page redirection, sending a warning page, and emailing

an administrator) as set by an administrator.

Password check

Analyzes password of an external user accessing the web server and, if a vulnerability is detected, performs security behaviors (LOG, destroying packet, page redirection, sending a warning page, and emailing an administrator) as set by an administrator.

Query phrase check

Analyzes query of an external user accessing the web server; performs security behaviors (LOG, destroying packet, page redirection, sending a warning page, and emailing an administrator) as set by an administrator if its number exceeds the limit for each URL, its phrase does not match the rule, the URL does not include a core query for each URL, or it matches the query value check pattern.

SQL syntax injection protection

Checks if an external user causes an SQL syntax error to enforce SQL command randomly on the web server and, if it is the case, performs security behaviors (LOG, destroying packet, page redirection, sending a warning page, emailing an administrator, and replacing characters) as set by an administrator.

SSL application protection

Protect data transferred between a web client and the web server using SSL protocol as specified by SECUI NXG W Information flow permission policy. Application of the policy can be configured for each URL of the web server. To protect SSL, a security function will confirm that the requested URL of a web browser needs to be protected by SSL and recommend the request to use HTTPS access that uses SSL.

URL-based access control

Checks an IP address and network of an external user accessing the web server and, on the sessions denied by an administrator, performs security behaviors (LOG, destroying packet, page redirection, sending a warning page, and emailing an administrator) as set by the administrator.

URL check

Analyzes URL of an external user accessing the web server and, if an attempt to access from not permitted URL or wrong data is detected, performs security behaviors (LOG, destroying packet, page redirection, sending a warning page, and emailing an administrator) as set by an administrator. The URL information analyzed by URL check modules are also used by another security modules.

URL extension check

If the URL of an external user accessing the web server includes a file extension not registered, performs security behaviors (LOG, destroying packet, page redirection, sending a warning page, and emailing an administrator) as set by an administrator. Registration of an extension on the web server can be manually, or by automatic heuristics.

7.3.1.3. Service contents protection (SW_DP_AP_CONTENTS)

Response traffic from the web server may contain various kinds of vulnerable information. The TOE applies SECUI NXG W Web contents protection policy defined in FDP_IFC.1(3) and FDP_IFF.1(3) to prevent the information from being leaked. All response traffic that is sent to a web client from the web server will be transmitted through the TOE. The TOE will first analyze the traffic and perform web contents protection as specified by the policy.

Personal credit information like an SSN and credit card number included in the page serviced by the web server will be protected by the following security functions:

Credit card number protection

If the web server transfers data including a credit card number at an external user's request or the requested contents include a credit card number, performs security behaviors (LOG, DROP, and modify data) as set by an administrator. Attached files will also be checked for a credit card number.

Response from the web server may include information about the web server itself such as types of server and application, different error values, or footnote, which will be protected by the following security functions:

Checksum protection

Performs a checksum operation on the contents (web page) of the web server to detect corruption and, if it is corrupted, performs security behaviors (LOG, DROP, page redirection, sending a warning page, and emailing an administrator) as set by an administrator.

Error page handling

When a response message from the web server is an HTTP error page, performs security behaviors (LOG, DROP, page redirection, sending a warning page, and emailing an administrator) as set by an administrator to prevent the server information from being leaked.

Footnote deletion

When an external user uses web service provided by the web server, deletes a footnote among the sources of the web page to protect information about the web server and web page from being leaked and performs security behaviors (LOG and emailing an administrator) as set by an administrator.

Forbidden word check

If an external user accessing the web server uploads a forbidden word or attempts to access the contents including a forbidden word, performs security behaviors (LOG, DROP, page redirection, sending a warning page, and emailing an administrator) as set by an administrator or replaces the word by another permitted word.

Social security number protection

If the web server transfers data including an SSN at an external user's request or the requested contents include an SSN, performs security behaviors (LOG, DROP, and modify data) as set by an administrator. Attached files will also be checked for an SSN.

The web server may have risk of having corruption of contents of the web page by a malicious user through a channel not protected by the TOE. In this case, the following security function can prevent leakage of the corrupted page in accordance with FDP_SDI.2.

Web traffic that passed through SECUI NXG W web contents protection policy will be transmitted to a web client that requested the web page.

7.3.2. Packet filtering (SW_DP_PF)

The TOE applies SECUI NXG W Information flow packet filtering policy according to FDP_IFC.1(4) and FDP_IFF.1(4) to provide a packet filtering function for network packets being sent to the web server or a web client. SECUI NXG W Information flow packet filtering policy set by an authorized administrator will be applied to packets sent to the TOE from outside to decide whether to allow or deny access to the TOE. Checking packets starts from a server access check. SECUI NXG W Information flow control policies will be applied to the header and body of those packets that passed the server access check.

Rules of packet filtering will be decided based on the source IP and net mask, destination IP and net mask, destination port number, protocol, priority, and packet direction.

Security action will perform specific security behaviors based on the violations detected by above-mentioned web server data protection and service contents protection. Upon detection of security attribute violation on an object protected by the TOE, security behavior to be performed will be decided among the following:

- LOG
- Destroying packet (DROP)
- Send a warning page
- Redirection of a web page
- Email an administrator
- Replace characters

7.4. Security management (SW_MAN)

7.4.1. Management of Security Functions (SW_MAN_FUN)

According to FMT_MOF.1 and FMT_SMF.1, an administrator can disable, enable, and modify the behavior of the security functions through the CLI/GUI administrator console. It is ensured that the ability to perform these functions are restricted to an authorized administrator as in the Table 7-9 List of management of security functions.

Table 7-9 List of management of security functions

Function	Ability	Role
Operate the function of system monitoring	Disable, enable	Super administrator
Operate the function for each TOE information flow controlled ruleset	Disable, enable	Super administrator, server administrator
Operate the function of automatic heuristics in redirect server	Disable, enable	Super administrator, server administrator
Operate the function of each web server	Disable, enable	Super administrator, server administrator
Initialize the system configuration	Enable	Super administrator
Restart the services (TSF process)	Enable	Super administrator
Restart the system	Enable	Super administrator
Backup and recovery the TOE configuration data	Enable	Super administrator
Execute the CLI commands	Enable	Super administrator, server administrator, user
Check the integrity	Enable	Super administrator
Print out reports	Enable	Super administrator, server administrator, user
Operation mode of the TOE network	Modify behavior	Super administrator
Trail audit records	Modify behavior	Super administrator

Function	Ability	Role
Operate the heuristic mode of the TOE	Modify behavior	Super administrator, server administrator
Apply the security policy of cookie domain	Modify behavior	Super administrator, server administrator
Apply the security policy of cookie	Modify behavior	Super administrator, server administrator
Operate the heuristic mode of web server URL	Modify behavior	Super administrator, server administrator
Apply the security policy of web server URL	Modify behavior	Super administrator, server administrator
Apply the monitoring traffic policy in heuristics	Modify behavior	Super administrator, server administrator
Apply the non-monitoring traffic policy	Modify behavior	Super administrator, server administrator
Operate the heuristic mode of each web server	Modify behavior	Super administrator, server administrator
Apply the heuristics policy of each web server	Modify behavior	Super administrator, server administrator

7.4.2. Management of Security Attributes (SW_MAN_ATTR)

An authorized administrator can query, generate, modify, delete, or learn by heuristics the security attributes of information flow control policies defined in FMT_MSA.1(1), FMT_MSA.1(2), FMT_MSA.1(3), FMT_MSA.1(4), and FMT_MSA.1(5).

Table 7-10 Management of security attributes

Information flow control policy	Security attribute	Operation
		Super administrator / server administrator
SECUI NXG W Information flow denial policy	Cookie domain	Query, generate, modify, delete, learn
	Cookie	Query, generate, modify, delete, learn
	web server address	Query, generate, modify, delete, learn
	URL	Query, generate, modify, delete, learn
SECUI NXG W	web server address	Query, generate, modify, delete, learn

Information flow control policy	Security attribute	Operation
		Super administrator / server administrator
Information flow permission policy	Cookie	Query, generate, modify, delete, learn
	HTTP Request Message	Query, generate, modify, delete, learn
SECUI NXG W Information flow web contents protection policy	MIME	Query, generate, modify, delete, learn
	HTTP Response Message	Query, generate, modify, delete, learn
SECUI NXG W Information flow packet filtering policy	Source IP address	Query, generate, modify, delete
	Source net mask	Query, generate, modify, delete
	Destination IP address	Query, generate, modify, delete
	Destination port number	Query, generate, modify, delete
	Priority	Query, generate, modify, delete
	Packet direction	Query, modify
	Protocol	Query, modify

According to FMT_MSA.3 and FMT_SMF.1, the TOE provides a restrictive default value used in SECUI NXG W Information flow denial policy and SECUI NXG W Information web contents protection policy; receives a safe value of corresponding security attributes; and sends an alarm in case of an insecure value. The TSF provides a default value for a security attribute that it intends to modify or establish. Invalid security attributes cannot be input. The TOE can decide an alternative initial value to override the default value provided by the TOE when an authorized administrator generates an Information flow control policy.

7.4.3. Management of TSF data (SW_MAN_DATA)

7.4.3.1. Management of TSF data (SW_MAN_DATA_ADMIN)

An authorized administrator of the TOE can manage the TSF data stated below as specified in FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3), FMT_MTD.1(4), FMT_MTD.1(5), and FMT_SMF.1 through the GUI administrator console.

Table 7-11 Management of TSF data

TSF data	Operation		
	Super administrator	Server administrator	User

TSF data	Operation		
	Super administrator	Server administrator	User
System configuration information	Query	-	-
Version and information of the TOE	Query, modify	-	-
Time information of the TOE	Query, modify	-	-
Time limit of an administrator session	Query, modify	-	-
Permitted number of login sessions	Query, modify	-	-
Administrator interface information	Query, modify	-	-
Information of the TOE network interface communication mode	Query, modify	-	-
Address of each operation mode of the TOE network	Query, modify	-	-
Interface information of each operation mode of the TOE network	Query, modify	-	-
Routing configuration information	Query, modify, delete, generate	-	-
Address of other servers (DNS, NTP)	Query, delete, generate	-	-
Configuration information of a host name	Query, modify, delete, generate	-	-
Warning page	Query, modify, delete, generate	-	-
Configuration information of a policy bypass for the purpose of administration	Query, modify	-	-
Configuration information of a policy bypass group for the purpose of administration	Query, modify	-	-
Configuration information of an administrator email of a policy	Query, modify	-	-

TSF data	Operation		
	Super administrator	Server administrator	User
bypass for the purpose of administration			
Configuration information of an administrator mail	Query, modify, delete, generate	-	-
Information about enabling audit functions	Query, modify	-	-
Information of real-time traffic status	Query	Query	Query
Statistics of the TOP5 among blocked web intrusion events	Query	Query	Query
Real-time monitoring information of blocked web intrusion events	Query	Query	Query
Log search information of an audit review items for each type of audit event	Query	Query	Query
Statistics of an audit for a specific period of time	Query	Query	Query
Configuration information of a site (automatic) heuristics	Query, delete, generate	Query, delete, generate	-
URL property information of each web server	Query, modify	Query, modify	-
Configuration information of each web server URL host	Query, modify, delete, generate	Query, modify, delete, generate	-
IP address and Port configuration information of each web server	Query, modify, delete, generate	Query, modify, delete, generate	-
Configuration of each web server heuristics: MIME list, method list, and header list	Query, modify, delete, generate	Query, modify, delete, generate	-
Configuration information of an SSL certificate	Query, modify, delete, generate	Query, modify, delete, generate	-
Administrator identification and authentication information	Query, modify, delete, generate	-	-

TSF data	Operation		
	Super administrator	Server administrator	User
Permission/prevention of an abnormal Escape text	Query, modify	Query, modify	-
Information of an SSL configurable MIME type	Query, delete, generate	Query, delete, generate	-
Configuration information of SECUI NXG W Information flow denial policy	Change_default, query, modify, delete, generate, learn	Change_default, query, modify, delete, generate, learn	-
Configuration information of SECUI NXG W Information flow permission policy	Change_default, query, modify, delete, generate, learn	Change_default, query, modify, delete, generate, learn	-
Configuration information of SECUI NXG W Information flow web contents protection policy	Change_default, query, modify, delete, generate	Change_default, query, modify, delete, generate	-
Configuration information of SECUI NXG W Information flow packet filtering policy	Query, modify, delete, generate	Query, modify, delete, generate	-

7.4.3.2. Management of limits on TSF data (SW_MAN_DATA_LIMIT)

The TOE takes actions below when defined limits on TSF data are reached or exceeded in accordance with FMT_MTD.2 and FMT_SMF.1.

Table 7-12 Management of limits on TSF data and actions

TSF data	Limit	Action
Time limit of an administrator session	1~1440 (minutes)	Terminate GUI and re-authenticate
Permitted number of login sessions	1~64	Block access to GUI
Cookie session timeout	60~86400 (seconds)	Terminate the cookie session
HTTP header size	1024 ~ 16384 bytes	Deny requested web traffic, email an administrator, make an audit record
		Display a warning message, email an administrator, make an audit record

TSF data	Limit	Action
		Redirect to a URL designated by an administrator, email an administrator, make an audit record
Number of hidden SSN figures	1~13	Replace the figure with '*'
Number of hidden credit card figures	1~16	Replace the figure with '*'
Number of GET query	0~65535	Deny requested query, email an administrator, make an audit record
		Display a warning message, email an administrator, make an audit record
		Redirect to a URL designated by an administrator, email an administrator, make an audit record
Number of POST query	0~65535	Deny requested query, email an administrator, make an audit record
		Display a warning message, email an administrator, make an audit record
		Redirect to a URL designated by an administrator, email an administrator, make an audit record

7.4.4. Security Management Roles (SW_MAN_ROLE)

The TOE maintains authorized administrator roles as in the Table 7-13 in accordance with FMT_SMR.1.
An administrator shall be identified and authenticated to interact with the TOE directly through the GUI/CLI administrator console; which will only be possible after that administrator's identifier is registered.

Super administrator has all authorities provided by the TOE including specifying server administrator, who has all authorities but initializing/restarting the system, and user, who only has an authority to review the TSF security management.

When an administrator is registered, the identifier (Admin ID), password, authority, and group

information of that administrator will be stored in the TOE administrator information list file. Therefore, an administrator ID can always be associated to the corresponding password and authority; which is the way to maintain authorized administrator roles.

Table 7-13 Authorized administrator roles

Authority	Role
Super Admin	Authority to perform all security management functions of the TSF
Server Admin	Authority to enforce the security policies of the web server defined in an administrator group
USER	Authority to review the list of TSF security management

7.5. Protection of the TSF (SW_PT)

7.5.1. TSF data integrity check and action (SW_PT_CHK)

This function ensures the integrity of files when an administrator stores, deletes, or modifies TSF data in the TOE listed below through the GUI administrator console according to FPT_TST. 1. Integrity check will be performed during initial start-up or at the request of an administrator.

- Identification and authentication data
- TSF configuration file
- TSF executable file

Whenever the TSF data is changed, the system will calculate Hash value using an integrity hash algorithm and store it in the TOE, which will be checked by Hash value check program.

Hash value check program calculates the Hash value of the TSF executable file, configuration file, and authentication data currently stored in the system and compares it with that stored in the TOE to ensure integrity of the TSF data.

If an attacker tries to change the object of integrity check by circumventing, not through the CLI/GUI administrator console, the Hash value of the TSF data and that stored in the TOE would differ from each other, which will be detected as an integrity error. Then the integrity check result will be recorded in an audit record and the data will be recovered to the state before the error.

7.5.2. External entity testing (SW_PT_ENTITYTEST)

The TSF run a test of external entities during initial start-up and normal operation of the TOE to show the correct operation of the external entities.

- CPU usage
- Disk state check
- Memory usage
- Network interface operation check
- TOE process operation state

- TSF data integrity check

Testing of external entities will monitor the state of process operating in system; which will ensure the security functions provide services continuously and not stopped by an unexpected error. If a process is not operating or operating abnormally, re-start all processes related to security functions to continue regular services.

See “7.5.1. TSF data integrity check and action” for the TSF data integrity check.

Usage of disk, memory, and CPU will be checked periodically and its result will be sent to an administrator in real-time. Operation and state of network interface will also be checked.

7.5.3. Maintenance of secure state and session management (SW_PT_AVAILABILITY)

If a failure occurred in the TOE due to the CPU or memory resource exhaustion, an administrator shall re-start services to preserve secure state in accordance with FPT_FLS.1 and FRU_FLT. 1.
To prevent this, the TOE shall regularly check the usage of CPU and memory and make a log about detected failure.

Super administrator can define limited time of an administrator session (1~1440 minutes). The session will be terminated after the defined time of authorized administrator inactivity as specified in FTA_SSL.3. Once a session is terminated, re-authentication is required to unlock the session.

All accesses for an administrator authentication will be mediated by SSL communication, which is not included in the TOE. Cryptographic key and an integrity monitoring key will be generated randomly each time identification and authentication occur through SSL communication in order to prevent reuse of authentication data.

8. Annex

8.1. Glossary and abbreviation

Administrator console

A console to manage the TOE; GUI administrator console allows access through a virtual Java machine on the Internet explorer; CLI administrator console allows direct access to the TOE through a serial port of SECUI NXG web Application Firewall V1.0.1.

Assets

Entities that the owner of the TOE presumably places value upon.

Assignment

The specification of an identified parameter in a component (of the CC) or requirement.

Attack Potential

A measure of the effort to be expended in attacking a TOE, expressed in terms of an attacker's expertise, resources and motivation.

Audit Trail

Collection of disk records on which log and action of a user who accessed the system are recorded.

Augmentation

The addition of one or more requirement (s) to a package.

Authentication Data

Information used to verify the claimed identity of a user.

Authority

A permitted scope to perform security functions for each authorized administrator role.

Authorized administrator is categorized into a super administrator, server administrator, and user. Authorities of each are as follows:

- Super Admin: Can read/write/enforce all security management functions of the TOE.

- Server Admin: Can read/write/enforce all security management functions except “restart service/system.”
- User: Can read/write his ID information only; Can read any other security management functions.

Authorized administrator

An administrator that securely operates and manages the web application firewall in accordance with the TOE security policies.

Authorized user

A user who may, in accordance with the SFRs, perform an operation.

Base64 encoding check

Checks if a query uses base64 encoding method.

Checksum protection

Checks the length or hash value of a web page that the protected web server sends as a respond to a web client and protects modified contents from being leaked.

Class

A grouping of CC families that share a common focus.

Common Criteria

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 V3.1r2 was translated into Korean and announced by the Minister of Public Administration and Security by notification no.2008-26.

Command injection protection

Checks if a forbidden system command is being used.

Connectivity

The property of the TOE which allows interaction with IT entities external to the TOE. This includes exchange of data by wire or by wireless means, over any distance in any environment or configuration.

Component

The smallest selectable set of elements on which requirements may be based.

Contents

Program or information provided by the Internet or PC communication. web contents means web-related data provided by web services.

Cookie

Recorded information of access to the Internet web site, which mediates between a user and the web site.

Cookie corruption check

Checks the cookie made by the web server; performs cookie encryption, cookie forge/corruption protection, and domain cookie management.

Cookie Poisoning

A type of attack where an attacker masquerades as somebody else by manipulating the information of a cookie to access a web site.

Cross-site scripting

An attack where an attacker uploads a client side script to a web server to enforce a malicious code on someone else's browser.

Cross-site scripting (XSS) protection

Checks whether the query or cookie data sent to the web server includes an enforceable script or HTML tag.

Cryptographic communication

Communication encoded in a section by HTTPS or other methods.

Dependency

A relationship between components such that if a requirement based on the depending component is included in a PP, ST or package, a requirement based on the component that is depended upon must normally also be included in the PP, ST or package.

Element

An indivisible statement of security need.

Error message handling

Server script error messages the web server displays such as JSP, ASP, and PHP, and a DB error message may give an attacker information that might threaten the security of the web server. Error message handling stops the messages from being transferred to a user from the web server.

Evaluation

Assessment of a PP, an ST or a TOE, against defined criteria.

Evaluation assurance level (EAL)

An assurance package, consisting of assurance requirements drawn from CC Part 3, representing a point on the CC predefined assurance scale.

Evaluation authority

A body that implements the CC for a specific community by means of an evaluation scheme and thereby sets the standards and monitors the quality of evaluations conducted by bodies within that community.

Evaluation scheme

The administrative and regulatory framework under which the CC is applied by an evaluation authority within a specific community.

Extension

The addition to an ST or PP of functional requirements not contained in Part 2 and/or assurance requirements not contained in Part 3 of the CC.

External IT entity

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

External user

A session user that passes through the TOE without authentication to use services of the web server.

Family

A grouping of components that share a similar goal but may differ in emphasis or rigor.

File-upload attack

An attack where a user uploads to the web server .exe, .jsp, and .php files applicable on it and enforces malicious commands.

Footnote deletion

Checks if the contents provided by the protected web server includes a footnote; if they do, deletes the footnote before transferring them to a web client.

Forbidden word check

Checks if the contents from the web server or query value delivered to the web server include a forbidden word and, if they do, protects the contents from being leaked.

Gateway Mode

Gateway mode is operated in a proxy mode. Proxy was originally used in a firewall for Internet protection, but now for the access to a Proxy server on a web browser. When a web browser specifies a Proxy, URL required by a web client will be connected to the Proxy server, not a server indicated by the URL. A Proxy server will send the request to the server indicated by the URL, then receive a response instead of the client and deliver it to the client.

Header buffer overflow check

Specifies the maximum size of an HTTP header to prevent buffer overflow.

Header method check

Checks if the header method of each URL is allowed.

Hidden field

A hidden field in an HTML is used, though not being seen on a web browser, to transmit data.

Hidden field manipulation protection

Checks if each URL includes a hidden field.

HTML parsing

Displaying an HTML document on a screen in a user-friendly format through a web browser program.

HTTP 1.1 standard

HTTP (HyperText Transfer Protocol) is a protocol that enables information transfer on WWW. Compared to HTTP 1.0, HTTP 1.1 standard has an enhanced rate, more methods added, and uses

Host request-header.

HTTP communication

Communication using HTTP.

HTTP header buffer overflow attack

An attack where an attacker causes internal buffer to overflow while an executable code is operating on a web server in order to enforce malicious commands.

HTTPS communication

Using SSL as a subordinate layer of HTTP, encodes and decodes pages requested by a user and returned by a web server.

Human User

Any person who interacts with the TOE.

(Learning by) heuristics

Produces a web tree database about the protected web server with the purpose of generating Positive security rule.

Identifier

A name with which one can uniquely identify and differentiate an object. In this ST, it is an administrator ID, which is an identification name of an authorized administrator accessing the TOE.

Identity

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

Inter-TSF transfer

Communicating data between the TOE and the security functionality of other trusted IT products.

Internal communication channel

A communication channel between parts of the TOE.

Internal TOE transfer

Communicating data between separated parts of the TOE.

Invalid HTTP

Request or response that is against the HTTP standards.

Iteration

The use of the same component to express two or more distinct requirements.

Object

A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Organizational security policy (OSP)

A set of security rules, procedures, or guidelines imposed (or presumed to be imposed) now and/or in the future by an actual or hypothetical organization in the operational environment.

Package

A named set of either functional or assurance requirements (e.g. EAL 3).

Packet

A block of data used in data transfer on the Internet. Unlike traditional transfer where data is transmitted consecutively between two points, packet transfer divides data into a certain size and sends a packet one by one. Each packet contains not only a certain size of data but also information such as its addressee, address, or control code.

Password

An input string required for a login to a specific system to confirm the identity of a user.

Password check

Checks whether a password is vulnerable in terms of its combination and length.

Personal credit information

Information about a living individual such as a name and SSN, combination of which can identify an individual.

As far as the TOE is concerned, personal information means an SSN and credit card number that can be used illegally by a malicious attacker.

Personal credit information leak protection

Protects personal credit information like SSN or credit card in web service contents.

Positive Rule

A web application firewall security policy that denies all accesses except those allowed.

Product

A package of IT software, firmware, and hardware that is designed to be used or included by a various types of system so that it can provide functions.

Protection Profile (PP)

An implementation-independent statement of security needs for a TOE type.

Query phrase and value check

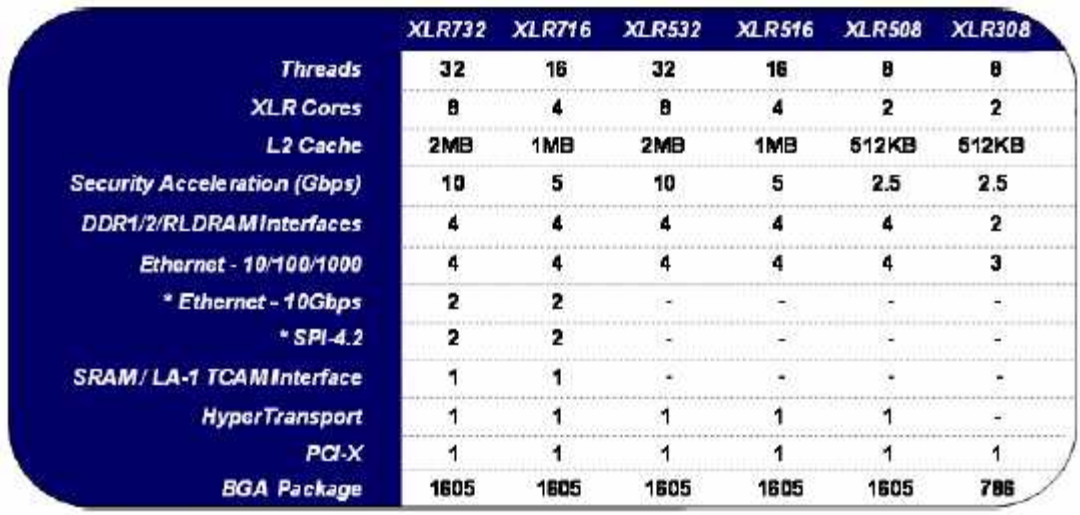
Checks query of Header and Body sent by GET or POST method.

Refinement

The addition of details to a component.

***RMI XLR™ Processor**

RMI XLR™ Processor is a general-purpose MIPS64® process that supports a safe line speed, multi platforms, and software-based application. It provides XLR-enhanced simplicity and is combined with a strong and innovative multi-processing and multi-thread-based architecture. XLR Processor based on a programmable SuperSOC™ solution does not require micro-coding or scripting usable only for the XLR itself. In addition, its industry standard media interface provides a variety of connectivity options to intensify compatibility.



	XLR732	XLR716	XLR532	XLR516	XLR508	XLR308
Threads	32	16	32	16	8	8
XLR Cores	8	4	8	4	2	2
L2 Cache	2MB	1MB	2MB	1MB	512KB	512KB
Security Acceleration (Gbps)	10	5	10	5	2.5	2.5
DDR1/2/RLDRAM Interfaces	4	4	4	4	4	2
Ethernet - 10/100/1000	4	4	4	4	4	3
* Ethernet - 10Gbps	2	2	-	-	-	-
* SPI-4.2	2	2	-	-	-	-
SRAM / LA-1 TCAM Interface	1	1	-	-	-	-
HyperTransport	1	1	1	1	1	-
PCI-X	1	1	1	1	1	1
BGA Package	1605	1605	1605	1605	1605	786

Figure 8-1 RMI XLR™ Processor Family

Figure 8-1 shows the types and specifications of XLR Processor Family.

Table 8-1 summarizes main features of XLR Processor Family.

Next Generation XLR Cores • A enhanced XLR processor of a 64-bit MIPS64 type • Supports more than 32 threads (virtual CPU) • More than 8 cores: Supports 4 way multi thread • Supports 1.5 GHz	**Expansible network interface** • Provides 2 SPI-4.2 interfaces (16 port) *§ • Provides 2 10G Ethernets (XGMII) *§ • Provides 4 10/100/1000 Ethernets • Provides a networking hardware acceleration function for each enhanced interface • Provides PCI-X-64/32 bit/133 MHz (PCI 2.2) Master or Target • Provides HyperTransport 8 bit, 3.2 GB/s PIC
Cache subsystem • Provides a completely consistent multi-level memory subsystem • Provides each core with system on-chip level 1 split cache • Provides 32 KB ECC L1 data and 32 KB parity L1 command • Provides ECC L2 cache that contains more than 2 MB • 8 ways of combination in all caches	**Integrated system interfaces** • PCMCIA interface • Flash memory interface • Provides dual I2C interface • Provides dual 16550 UART interface • Provides 32 bit GPIO interface • Provides IEEE 1149.1 EJTAG and memory BIST functionality
High-speed dispersed inter-connection • Supports connection between all cores, caches, and processing agents • Implements inter-connection providing inter-connectivity and expansibility for high performance by system on-chip;	**High performance configurable memory controllers** • DDR1/DDR2/RLD2 DRAM that support ECC (400 MHz) • 4 x 36 or 2 x 72 mixed memory that uses perx72 DRAM • QDR2 or DDR2 SRAM that supports ECC (400 MHz) § •Supports TCAM/NSE / NPF-LA1 interface §

Supports Non-blocking • Supports a high-speed messaging network for an measurable communication between main processing and I/O components	• 4-channel DMA
Networking hardware acceleration • Provides a packet dispersion engine for processing line bitrates • Flexible packet tagging and packet dispersion management • Verify and generate TCP checksum	**Power management** • An on-chip heat sensor • Supports software-programming clock throttling
Strong points of a security acceleration engine • Provides more than 10 Gbps for bulk encoding/decoding • Provides more than 4 high-performance crypto cores • Supports DES / 3DES, ARC4, AES (128, 192, 256) • Supports MD5, SHA-1, SHA-256 (in all HMAC) • Supports RSA/ DH for SSL / IPSec • Random number generator	**General-purpose programming** • Allows virtualization of a domain that is not mapped to a core divided as a virtual MIPS mode • Supports 3 fine and coarse drained scheduling mode / CPU • Supports parallel·pipe line & hybrid processing mode • Supports debugging performance monitoring in the system on-board
*§: Shared interface that only supports XLR732 / XLR716	

Table 8-1 Main features of XLR Processor Family

To summarize main features of XLR Processor Family shown in the Table 8-1, it is a cost-effective single-chip solution implemented with expansibility, multi service system, and the next generation Key building block, which can be provided for a variety of operational environments of users.

Role

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

Secret

Information that must be known only to an authorized administrator and/or the TOE security functionality (TSF) in order to enforce a specific Security function policy (SFP).

Security attribute

A property of subjects, users (including external IT products), objects, information, sessions and/or resources that is used in defining the SFRs and whose values are used in enforcing the SFRs.

Security function policy (SFP)

A set of rules describing specific security behavior enforced by the TSF and expressible as a set of

SFRs.

Security objective

A statement of intent to counter identified threats and/or satisfy identified organization security policies and/or assumptions.

Security Target (ST)

An implementation-dependent statement of security needs for a specific identified TOE.

Selection

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

SQL (Structured Query Language)

A database sublanguage used to operate and manage a relational database.

SQL Injection

An attack to manipulate an SQL syntax and send it to a web server in order to manipulate the DB of the web server.

SQL syntax injection protection

Blocks an attack where a user forges query and cookie value sent to the web server so they have an SQL syntax error and enforces SQL command randomly.

Stream

Socket information used by an input socket and output socket that can be sent and received on a network.

Subject

An active entity in the TOE that performs operations on objects.

System

IT equipment with a specific purpose and operational environment.

Target of evaluation (TOE)

A set of software, firmware and/or hardware possibly accompanied by guidance.

Threat agent

An unauthorized user or external IT entity that causes a threat such as illegal access, modification, and deletion to an asset.

TOE resource

Anything useable or consumable in the TOE.

TOE Security Functionality (TSF)

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

Traffic

The amount of data transmitted through a network or of transaction and message.
web traffic refers to the data or message that is used in the section of web service.

Transfers outside of the TOE

TSF mediated communication of data to entities not under control of the TSF.

TSF Data

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

TSF Interface (TSFI)

A means by which external entities (or subjects in the TOE but outside of the TSF) supply data to the TSF, receive data from the TSF and invoke services from the TSF.

Transparent-bridge mode

One of modes of operation of the TOE where it is configured in an in-line type like a firewall.

Transparent-gateway mode

One of modes of operation of the TOE where it operates as a web proxy. By modification of DNS configuration, HTTP (S) communication between a web server and web client will be through the TOE.

Trusted channel

A means by which a TSF and a remote trusted IT product can communicate with necessary confidence.

Trusted path

A means by which a user and a TSF can communicate with necessary confidence.

Unicode Directory Traversal

An attack using Unicode to access a directory file that is not allowed by a web server.

URI (Uniform Resource Identifier)

An identification system of united information resources with the Internet services provided. The most common type of URI is URL, an web page address.

URL (Uniform Resource Locator)

A logical address that shows resources such as a file and news group on the Internet. When HTTP is used, resources may be an HTML page, image file, programs like CGI or Java applet, and files supported by HTTP.

URL check

Checks a URL that is accessing the web server; performs URL analysis, heuristics, access control, and directory access control.

URL extension check

Checks URL extension and determines whether to allow or block.

User agent

A client application used by a specific network protocol. User agent HTTP refers to a web browser.

User

Any entity outside the TOE that interacts with the TOE. It can be a human user or external IT entity.

User data

Data created by and for the user, which does not affect the operation of the TSF.

Web application

Software developed since web for the Internet/Intranet using various languages to search database or process general business logic. Script and service like Java script or JSP access database to search for the latest data and provide the result to a user through a browser or client program.

Web browser

A client program that uses HTTP to request for data on the Internet web server.

Web client

A user that receives web services from a web server.

Web Server

A server computer that provides services on web. The TOE provides Apache, Microsoft, sun, and Zeus.

Web tree database

Analyzes the structure of a web server in terms of a directory, web page, and parameters of URL and stores it in a DB. Positive security rule applies to the DB.

Web zone

Contrary concept to an Intranet; a domain protected by the TOE, where assets like a system that provides web application are placed.

Zero-Day Attack

Personal information leakage increases due to an increase of computer worm virus that searches vulnerable PCs on the Internet that were hit by computer crimes. It usually takes 2 weeks before one takes actions after recognizing that a computer was exposed to a crime. Zero-day attack exploits those computers before patches are made in order to disclosure personal information.

8.2. Reference

- Common Criteria Part 1: Introduction and general model, Version 3.1 R1, Sep. 2006
- Common Criteria Part 2: Security functional requirements, Version 3.1 R2, Sep. 2007
- Common Criteria Part 3: Security assurance requirements, Version 3.1 R2, Sep. 2007
- Common Methodology for Information Technology Security Evaluation, Version 3.1 R2, Sep. 2007