Safegate
Security Target

February 22 2000

Version 1.2e

FUJITSU LIMITED

1. INTRODUCTION

1.1. ST identification

Product name: Safegate

TOE:

This ST corresponds to the following target of evaluation (TOE):

Manufacturer: Fujitsu Limited
Product name: Safegate
Version number: 2.0.2
Product code: D238E22H2

1.2. ST overview

This security target (ST) describes the security functions of Safegate, a Firewall provided by Fujitsu Limited. The Safegate TOE is composed of the IP packet filtering function, Application gateway function and Audit function.

1.3. CC conformance

As the purpose of Safegate is to protect private networks operating under Safegate from numerous kinds of attacks from intruders from other networks, Safegate is required to conform to close to the highest security level on a commercial basis.

- Security functional requirements conform to CC Version 2.0 Part 2.
- Security assurance requirements conform to EAL3 in CC Version 2.0 Part 3.

1.4. Reference Materials

CC-1 Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model
CCEB-98-026, Version 2.0, May, 1998

CC-2 Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements
CCEB-98-027, Version 2.0, May, 1998

CC-3 Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements
CCEB-98-028, Version 2.0, May, 1998

CC-4 CS2-Protection Profile Guidance for Near-Term COTS
Version 0.4, December 10, 1998

1.5. Acronyms

CC	Common Criteria for Information Technology Security Evaluation

EAL	Evaluation Assurance Level
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IT	Information Technology
LAN	Local Area Network
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Function
TSP	TOE Security Policy
UDP	User Datagram Protocol

2. TOE DESCRIPTION

A number of resources on the Internet are made available to private network users (hosts) when such private networks are connected to the Internet. But resources on a private network may be exposed to numerous kinds of attacks from intruders through the Internet if the private network is directly connected to the Internet. This TOE works as a Firewall that serves as a single point connecting the private network to the Internet and eliminates various kinds of potential threats of attacks on the private network through the Internet. This TOE is composed of the following TSFs.

- IP packet filtering function (TSF_IPPF)
- Application gateway/Transparent mode (TSF_APTC)
- Application gateway/Non-transparent mode (TSF_APRC)
- Audit function (TSF_AUDT)

2.1. Execution environment

Each function of the TOE works on Solaris version 2.6 and assumes that the following network environment is being used.

- Ethernet LAN (10M and 100M) based on STREAMS of SVR4 on which IP and ICMP work with all TCP/IP network protocols

2.2. Function overview

2.2.1. IP packet filtering function (TSF_IPPF)

TSF_IPPF controls the IP packet flow between the Internet and private networks by using TCP or UDP interface. TSF_IPPF examines IP packets to determine whether to pass them through Safegate or block them, in accordance with the IP packet-filtering rule. IP packet-filtering runs between the network drivers layer and IP layer in kernel space of Solaris.

2.2.2. Application gateway/Transparent mode (TSF_APTC)

TSF_APTC provides TCP, UDP and ICMP proxy function between the Internet and private networks without exposing the private network IP addresses to the Internet. Private network IP addresses in an IP packet being sent to the Internet are changed into Safegate's global IP address, and the Global IP addresses in IP packet being received from the Internet are changed into private IP addresses in TSF_APTC. In this manner, private network addresses are protected against potential threats coming through the Internet.

TSF_APTC needs IP packet filtering function (TSF_IPPF) to run. TSF_APTC can handle only the IP packets permitted by TSF_IPPF.

2.2.3. Application gateway/Non-transparent mode (TSF_APRC)

TSF_APRC also controls the IP packet flow between the Internet and the private network, but handles only the IP packet data with telnet and ftp protocols and blocks the other protocol's IP packet data. In Application gateway/Non-transparent mode, the connection between networks is made in two steps. First of all, the users on the private network establish a connection with TSF_APRC, then TSF_APRC establishes a connection with the Internet. TSF_APRC first receives packet data sent from the private network and stores the data to TSF_APRC itself. Then, the IP addresses in the IP packet are changed to Safegate's IP address. Afterwards, the IP packets are sent to the Internet. Accordingly, private network addresses are concealed to protect them against potential threats coming through the Internet.

TSF_APRC needs IP packet filtering function (TSF_IPPF) to run. TSF_APRC can handle only the IP packets permitted by TSF_IPPF.

2.2.4. Audit function (TSF_AUDT)

TSF_AUDT has the facilities given below for analyzing or monitoring communications through the Safegate system, and alerting the user when it detects unauthorized accessing of the Safegate system or the private network itself. TSF_AUDT also has the facilities to access the filtering rule file and the environment definition file.

- Logging function
- Alert notification function
- Monitoring function
- Environment definition function

2.3. TOE Structure

1) Execution environment for Safegate

Safegate (TOE) runs in the network environment shown below.

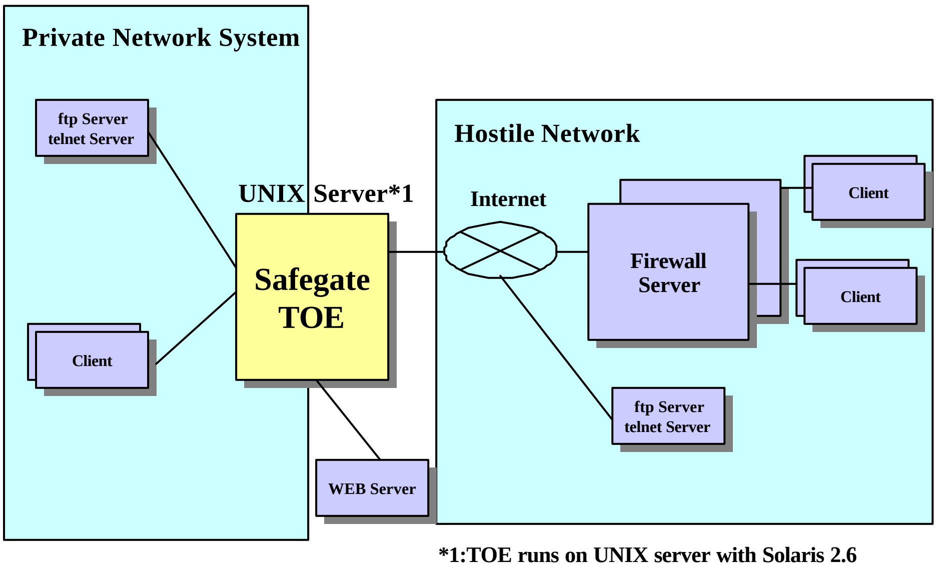

Figure2.1 Hardware/Network Environment for Safegate

2) Structure of Safegate

Figure 2.2 illustrates TOE for this ST. This TOE does not include the TCP/UDP/IP process in figure 2.2 that is provided by the operating system. Application Gateway/Non-transparent mode needs to be run after the execution of IP packet filtering.

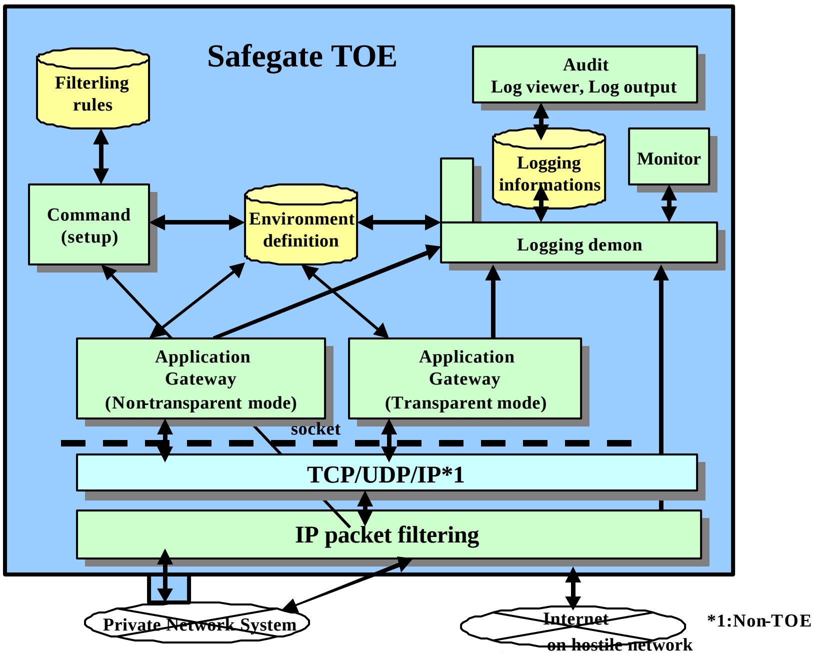

Figure2.2 **Structure of Safegate**

2.4. Resources protected

The TOE shall protect the private network system itself in accordance with the rule (3.3 Organizational Security Policies) defined by the organization. The TOE protects the following resources:

1) Private network system

This TOE connects the private network with the external network (hostile network) as shown in Figure 2.1 and protects the private network from potential threats from the hostile network. What resources on the private network the TOE protects depends on the security policy defined by the user's organization.

2) Firewall system

This TOE protects the TOE relevant resources that include the data for protecting resources on the private network. These resources include the following:

- Safegate execution code
- Environment definition file
- Filtering rule file
- Log file

This TOE does not protect the content of packet data.

3. Security Environment

This section addresses the TOE security environment which identifies and explains (as per CC requirements ASE_ENV.1.1C to ASE_ENV.1.3C) all:

- assumptions about the intended use of the TOE and the use environment of the TOE; (ASE_ENV.1.1C)
- known or presumed threats to the assets against which protection will be required, either by the TOE or by its environment; (ASE_ENV.1.2C)
- organizational security policies with which the TOE must comply; (ASE_ENV.1.3C)

3.1. Secure Use Assumptions

The following secure use assumptions are made:

ASM1 Safegate must be protected so that only the administrator can access it.

ASM2 Safegate is assumed to be a host connected to two or more networks.

ASM3 Only one network connection point on Safegate must exist between private networks and hostile networks.

ASM4 The Safegate administrator, assigned responsibility for the day-to-day management and configuration of Safegate, shall operate Safegate legally. Following violation may occur.

- Violation of the network security policy as a result of inaction, or irresponsible action on the part of careless, willfully negligent, or unethical authorized administrators

ASM5 Reserved.

ASM6 Reserved.

ASM7 Reserved.

ASM8 The configuration of Safegate should be reviewed on a regular basis to ensure that the configuration continues to meet the organization’s security objectives in the face of:

- changes to Safegate configuration (for whatever reason);
- changes in the security objectives;
- changes in the potential threats posed by a hostile network;
- changes in the hosts and services made available to a hostile network by the private network.

ASM.9 Reserved.

ASM.10 The Safegate administrator follows the administrative procedures, ensures users are trained and checks the audit trail on a regular basis for unauthorized operations.

3.2. Threats

This section identifies and explains presumed threats to IT assets against which protection is required, depending on the TOE or security environment in use.

3.2.1 Threats Countered

The general threats to be countered are:

- inappropriate access of the private network by attackers from an external network (hostile network);
- inappropriate exposure of private network data or resources to a hostile network by users on the private network.

In this document, the meaning of the term 'network' includes hosts on the network, services provided by these hosts and data accessible via these hosts.
The following specific threats are countered:

T1 Attackers on a hostile network posing as private network users may modify, destroy or disclose resources on the private network.

T21 Attackers on a hostile or private network may intrude into Safegate to make changes to filtering rules and the environment definition file, and as the result they have unauthorized packets and services passed through Safegate.

T22 Attackers on a hostile or private network may intrude into Safegate to make changes to the logging information, and as the result they make obscure the evidence of their unauthorized activity.

T3 Private network users accessing hostile networks may inadvertently expose the addresses and the physical configuration of the private network to hostile network users.

T4 Reserved.

T5 Information on the private network system may be exposed to hostile network users by using ICMP attacks on the target system that includes the Safegate system and the private network.

T6 Reserved.

T7 As a result of incorrect definition of packet filtering rules, the TSF may permit packets and services that violate security policy.

3.2.2 Threats Countered by the Environment

Threats not addressed by the TOE are listed below. These threats must be countered by technical and/or non-technical measures in the IT environment.

TE1, TE2 and TE3 Reserved.

TE4 Attackers on a hostile network may exploit new, previously unknown, attack methods (e.g., by using previously trustworthy services).
For example, unauthorized commands or programs are inserted into the TOE itself by using services (e.g., www, mail ftp) by way of well-known port numbers, and the commands or the programs modify the filtering rule or the TOE itself.

TE5 Attackers on a hostile network may attack unsecured configurations of hosts on the private network (e.g., configurations that do not conform to the network policy).

TE6 Attackers on a hostile network may attack the Safegate host and machines on the private network by using methods that take advantage of security relevant defects in existing

TE7 and TE8 Reserved.

TE9 Attackers may attack Safegate itself to modify it and pass unauthorized packets through the Safegate host.

3.2.3 Threats Not Countered

Threats not addressed by the TOE are listed below. These threats must be accepted as potential security risks.

TNC1 Attackers on a hostile network may successfully hi-jack an open session on an internal host.

TNC2 Viruses contained within incoming traffic.
In general, Firewalls don’t scan the details of incoming data. The number of viruses in the wild, the number of ways that viruses can be hidden within data, and the continually changing nature of the threat make it impractical for a Firewall to effectively counter the threat of viruses. Even if a Firewall were able to block any incoming traffic containing a virus, this would still not fully protect the private network from the introduction of viruses (for example, viruses introduced as a

result of the import of data on a floppy disk). This threat can be most effectively countered by using a combination of host-based virus protection software and by educating users.

TNC3 By issuing RIP packets, routers set up as Safegate host peripheral equipment may expose the configuration of the private network to the hostile network.

TNC4 Attackers on a hostile network attack the Safegate system and the private network by issuing source routing packets with unauthorized routing information of routers.

3.3 Organizational Security Policies

A Firewall compliant with this Security Target does not impose its own rules, but rather can be configured to implement a number of different organizational policies. Such a Firewall is also flexible, so that it can be modified to reflect changes in the relevant organization's security policy.

4. SECURITY OBJECTIVES

This section provides the statement of security objectives, distinguishing between IT and relevant non-IT security objectives (as per CC requirement ASE_OBJ.1.1C to ASW_OBJ.1.5C). The rationale for these security objectives is provided in Section 8 of this Security Target.

4.1. IT Security Objectives

The principle IT security objective of Safegate compliant with this Security Target is to reduce the vulnerabilities of a private network exposed to a hostile network by limiting the hosts and services available. Additionally, Safegate has the objective of providing the ability to monitor established connections and attempted connections between the private network and the hostile network.

The specific IT security objectives are as follows:

O.I Safegate must, be capable of identifying a single host or a group of hosts prior to Safegate allowing a connection to be established.

O.DAC1 Safegate must limit the valid range of addresses expected on each of the private and hostile networks (i.e. an external host cannot spoof an internal host).

O.DAC2 Safegate must limit the hosts and service ports on the private network that can be accessed from the hostile network.

O.DAC3 Safegate must limit the hosts and service ports on the hostile network that can be accessed from the private network.

O.AG1 Safegate has the ability to conceal from hostile networks the IP addresses of clients on the private network.

O.ADMIN Safegate must provide a single focus of administrative control of Safegate, ensuring that only the authorized administrator can exercise such control.

O.AUDMON Safegate must provide a facility for monitoring successful and unsuccessful attempts at connections between the private network and the hostile network.

O.AUDREC Safegate must provide measures for recording, searching and retrieving an audit trail in a format that enables recognition of security related events that include accurate date and time records.

4.2. Security Objectives for the Environment

Security objectives for the environment (OE1 through OE6) are defined as follows.

OE1 Those responsible for the Safegate must ensure that it is delivered, installed, managed and operated in a manner that maintains the security policy.

This objective is required to help ensure that the IT security objectives (O.DAC1 to O.AUDREC) and ASM8 are satisfied in practice.

OE2 The Safegate host must be established in the environment where only administrators can enter and Safegate itself must be protected from unauthorized modification by the operating system's function.

This objective is required to help ensure that ASM1 is satisfied in practice.

OE3 Those responsible for the Safegate must train administrators to establish and maintain sound security policies and practices.

This objective is required to help ensure that the ASM4, ASM8 and ASM10 are satisfied in practice.

OE4 Administrators of Safegate must ensure that the audit facilities are used and managed effectively. In particular, appropriate action must be taken to ensure continued audit logging, e.g. by regular archiving of logs, to ensure that sufficient free space is available. Furthermore, audit logs should be inspected on a regular basis and appropriate action should be taken upon detecting security breaches, or events that are likely to lead to a security breach in the future.

This objective is required in support of O.AUDMON and O.AUDREC, and is required to help ensure that ASM8 is satisfied in practice.

OE5 Safegate is designed or configured solely to act as a firewall on a host and does not provide any user services that are not related to Safegate's execution.

This objective is required to help ensure that ASM1 is satisfied in practice.

OE6 Safegate must be configured as the only network connection point between the private network and the hostile network.

This objective is required to help ensure that ASM2 and ASM3 are satisfied in practice.

5. IT security requirements

5.1 TOE security requirements

5.1.1. IP packet filtering function

Safegate controls IP packet flow between the private network and the hostile network on the basis of information flow control SFP; SFP_IPPF.

(1) FDP_IFC Information flow control policy

FDP_IFC.1 Subset information flow control

Audit: None

FDP_IFC.1.1 The TSF shall enforce *the information flow control SFP; SFP_IPPF* on *the following list*.

- Subjects: IT entities (i.e., hosts on the private network or the hostile network) that send or receive information through Safegate.
- Information: IP packet that attempts to pass through Safegate from one subject to another.
- Operations: permit or deny passing of information

(2) FDP_IFF Information flow control functions

FDP_IFF.1 Simple security attributes

Audit level: Basic
Audit: All decisions (permit and deny) on the information flow

FDP_IFF.1.1 TSF shall enforce *the information control SFP; SFP_IPPF* based on the following types of subject and information security attributes.

[Subject Security Attributes]

- Subject: IP address
- Subject: Network address

[Information Security Attributes]

- Packet direction

- Packet processing type (pass/block packets)
- Protocol of IP packet (TCP/UDP/ICMP)
- Source subnet-mask address
- Source IP address
- Destination subnet-mask address
- Destination IP address
- Source port number (for TCP/UDP)
- Destination port number (for TCP/UDP)
- TCP flag (for TCP)

  NO_CHK: pass SYN packet

  S_BLK: block SYN packet
- ICMP message type (for ICMP)
- ICMP message code (for ICMP)

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

[Rules]

Packet flow is controlled by the filtering condition based on the security policy. The filtering condition is defined by using possible following combinations of values of information security attributes, and the TSF permits packets to pass through Safegate if the filtering condition is satisfied.

- Packet direction

  Packet direction (up stream or down stream) through IP filtering are able to be restricted.
- Network interface

  Network interface can be restricted to protect it from sending/receiving packets to/from unauthorized network.
- Packet processing type

  Administrator can select whether to pass or reject the packets to be filtered.
- Logical conditions

  Logical conditions using following attributes can be specified to pass or reject packets.

Source port number (for TCP/UDP)
Destination port number (for TCP/UDP)
Port numbers
TCP flag (for TCP)
ICMP message type (for ICMP)
ICMP message code (for ICMP)

FDP_IFF.1.3 The TSF shall enforce the *additional information flow control SFP rules*.

- None

FDP_IFF.1.4 The TSF shall provide the following *additional SFP capabilities*.

- None

FDP_IFF.1.5 The TSF shall explicitly authorize an information flow based on the following rules *based on security attributes, that explicitly authorize information flows*.

- None

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules *that explicitly deny information flow based on security attributes*.

[Rules]

The packet flow is denied under the following conditions.

- There is no filtering condition available (The default setting, no filtering condition, is available.)
- The filtering condition defined in FDP_IFF.1.2 is not satisfied.

5.1.2. Application gateway/Transparent mode

Application gateway/Transparent mode provides TCP, UDP and ICMP proxy function based on the IP packet filtering function between the private network and the Internet.

(1) FDP_IFC Information flow control policy

FDP_IFC.1 Subset information flow control

Audit: None

FDP_IFC.1.1 The TSF shall enforce *the information flow control SFP; SFP_IPPF* on *the following list*.

- Subjects: IT entities (i.e., hosts on the private network or the hostile network) that send or receive information through Safegate.
- Information: IP packet that attempts to pass through Safegate from one subject to another.
- Operations: permit or deny passing of information

(2) FDP_IFF Information flow control functions

FDP_IFF.1 Simple security attributes

Audit level: Basic

Audit: All decisions (permit and deny) on the information flow
All address changes in transparent mode (See FDP_IFF.1.4)

FDP_IFF.1.1 TSF shall enforce *the information control SFP; SFP_IPPF* based on the following types of subject and information security attributes.

[Subject Security Attributes]

- Subject: IP address
- Subject: Network address

[Information Security Attributes]

- Packet direction
- Packet processing type (pass/block packets)
- Protocol of IP packet (TCP/UDP/ICMP)
- Source subnet-mask address

- Source IP address
- Destination subnet-mask address
- Destination IP address
- Source port number (for TCP/UDP)
- Destination port number (for TCP/UDP)
- TCP flag (for TCP)

  NO_CHK: pass SYN packet

  S_BLK: block SYN packet
- ICMP message type (for ICMP)
- ICMP message code (for ICMP)

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

[Rules]

Packet flow is controlled by the filtering condition based on the security policy. The filtering condition is defined by using possible following combinations of values of information security attributes, and the TSF permits packets to pass through Safegate if the filtering condition is satisfied.

- Packet direction

  Packet direction (up stream or down stream) through IP filtering are able to be restricted.
- Network interface

  Network interface can be restricted to protect it from sending/receiving packets to/from unauthorized network.
- Packet processing type

  Administrator can select whether to pass or reject the packets to be filtered.
- Logical conditions

  Logical conditions using following attributes can be specified to pass or reject packets.

  Source port number (for TCP/UDP)

  Destination port number (for TCP/UDP)

  Port numbers

TCP flag (for TCP)
ICMP message type (for ICMP)
ICMP message code (for ICMP)

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

- None

FDP_IFF.1.4 The TSF shall provide the following *additional SFP capabilities*.

- IP addresses of the private network in the IP packet being sent to the Internet are changed to Safegate's global IP address, and the Global IP address in the IP packet being received from the Internet are changed to the private IP addresses

FDP_IFF.1.5 The TSF shall explicitly authorize an information flow based on the following rules *based on security attributes, that explicitly authorize information flows*.

- None

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules *that explicitly deny information flow based on security attributes*.

[Rules]

The packet flow is denied under the following conditions.

- There is no filtering condition available (The default setting, no filtering condition, is available.)
- The filtering condition defined in FDP_IFF.1.2 is not satisfied.

5.1.3. Application gateway/Non-transparent mode

Application gateway/Non-transparent mode provides telnet and ftp proxy function based on the IP packet filtering function between the private network and the Internet.

(3) FDP_IFC Information flow control policy

FDP_IFC.1 Subset information flow control

Audit: None

FDP_IFC.1.1 The TSF shall enforce *the information flow control SFP; SFP_IPPF* on *the following list*.

- Subjects: IT entities (i.e., hosts on the private network or the hostile network) that send or receive information through Safegate.
- Information: IP packet that attempts to pass through Safegate from one subject to another.
- Operations: permit or deny passing of information

(4) FDP_IFF Information flow control functions

FDP_IFF.1 Simple security attributes

Audit level: Basic
Audit: All decisions (permit and deny) on the information flow

FDP_IFF.1.1 TSF shall enforce *the information control SFP; SFP_IPPF* based on the following types of subject and information security attributes.

[Subject Security Attributes]

- Subject: IP address
- Subject: Network address

[Information Security Attributes]

- Source IP address
- Destination IP address
- Port numbers (telnet or ftp)

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

[Rules]

Packet flow is controlled by the filtering condition based on the security policy. The filtering condition is defined by using possible following combinations of values of information security attributes, and the TSF permits packets to pass through Safegate if the filtering condition is satisfied.

- Network interface
  Network interface can be restricted to protect it from sending/receiving packets to/from unauthorized network.
- Packet processing type
  Administrator can select whether to pass or reject the packets to be filtered.
- Logical conditions
  Logical conditions using following attributes can be specified to pass or reject packets.
  Client IP address on private network
  Server IP address on the Internet
  Source port number (for telnet/ftp)
  Destination port number (for telnet/ftp)

FDP_IFF.1.3 The TSF shall enforce the *additional information flow control SFP rules.*

- None

FDP_IFF.1.4 The TSF shall provide the following *additional SFP capabilities.*

- IP addresses of the private network in the IP packet being sent to the Internet are changed to Safegate's global IP address, and the Global IP address in the IP packet being received from the Internet are changed to the private IP addresses

FDP_IFF.1.5 The TSF shall explicitly authorize an information flow based on the following rules *based on security attributes, that explicitly authorize information flows.*

- None

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules *that explicitly deny information flow based on security attributes.*

[Rules]

The packet flow is denied under the following conditions.

- There is no filtering condition available (The default setting, no filtering condition, is available.)
- The filtering condition defined in FDP_IFF.1.2 is not satisfied.

5.1.4. Security audit

(1) FAU_ARP.1 Security alarms

Management: The management (addition, removal, or modification) of actions.

Audit level: Minimal

Audit: Actions taken due to imminent security violations.

FAU_ARP.1.1 The TSF shall take *following disruptive actions* upon detection of a potential security violation.

- Console output

  Displays on console.

- Mail sending

  Sends mail.

- Monitor notification

  An alert detected during operation is notified by the real time monitor in real time.

- Command execution

  A specified command can be executed upon alert detection.

(2) FAU_GEN.1 Audit data generation

Management: None

Audit: None

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 audit functions;

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

- Audit level: Basic

c) *other specifically defined auditable events*.

- If the audit level selected is not "basic," enter the reason for making such selection.

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

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

Functional Component	Level	Auditable Event	Additional Audit Record Contents
FAU_ARP.1	minimal	Actions taken due to imminent security violations	
FAU_SAA.1	minimal	Automated responses performed by the tool	
FAU_SAR.1	basic	None	
FAU_SAR.3	detailed	None	
FAU_SEL.1	minimal	None	
FAU_STG.4	basic	Actions taken due to audit storage failure	
FDP_IFF.1	basic	All decisions (permit and deny) on the information flow All address changes in IP packets	
FMT_MOF.1	basic	None	
FMT_MSA.1	basic	None	
FMT_MTD.1	basic	None	

(4) FAU_SAA.1 Potential violation analysis

Management: maintenance of the rules by (adding, modifying, or deleting) rules from the set of rules.

Audit level: Minimal

Audit: Automated responses performed by the tool.

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

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

a) Accumulation or combination of *following subset of defined auditable events* known to indicate a potential security violation;

- Same source alert:
  when the number of discarded packets from a certain IP address exceeds the specified number within a certain time (IP-filtering/Transparent mode)
- Same destination alert:
  when the number of discarded packets to a certain IP address exceeds the specified number within a certain time (IP-filtering/Transparent mode)
- Monitor port alert:
  when detecting a packet for the monitor port set in the alert setting (IP-filtering/Transparent mode)

b) *any other rules.*

None.

(5) FAU_SAR.1 Audit review

Management: maintenance (addition to, modification of, or deletion from) of the group of users having read access privileges for audit records.

Audit level: Basic

Audit: Reading of information from the audit records.

- Notes: As the logging information, or audit records is managed only by the administrator with the root privilege authorized by OS, the TSF does not record the audit records defined in this requirement.

FAU_SAR.1.1 The TSF shall provide *following authorized users* with the capability to read *following audit information* from the audit records.

- *Authorized users* shall be the administrator.
- *The audit information defined* in FDP_GEN.1 is the data (all audit trail data) stored on log files.

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

- The following audit review tools output on a screen the results of editing the logging data for an authorized administrator:
  [Output of logging data in the TSFs;
  Log viewer in the TSFs.]

(6) FAU_SAR.3 Selectable audit review

Management: None

Audit level: Detailed

Audit: the parameters used for viewing

- Notes: As the logging information, or audit records is managed only by the administrator with the root privilege authorized by OS, the TSF does not record the audit records defined in this requirement.

FAU_SAR.3.1 The TSF shall provide the ability to perform *searches* of audit data based on *following criteria with logical relations.*

- The TSF shall provide the ability to perform *searches* of audit data based on *source IP address, destination IP address, destination protocol (TCP, UDP, ICMP), and destination service port number; and the logical "AND" and "OR" of any of these attributes.*

(7) FAU_SEL.1 Selective audit

Management: maintenance of audit event view/modify privileges for.

Audit level: Minimal

Audit: All modifications to the audit configuration that occur while the audit collection functions are operating.

- Notes: As the logging information, or audit records is managed only by the administrator with the root privilege authorized by OS, the TSF does not record the audit records defined in this requirement.

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

a) *following object identity and event type*

- *object identity*: TCP, UDP or ICMP
- *event type*: status of connection, disconnection or denying packets

b) *following list of additional attributes that audit selectivity is based upon.*

- The following are able to include or exclude objects and events as auditable events.

(1) Logging of IP packet filtering

object: protocol:

[TCP/UDP;

ICMP;

all<default>.]

event: type of data:

[connection/disconnection packet;

rejection packet;

all<default>.]

(2) Logging of application gateway/Non-transparent mode

event: logging level:

[connection status of telnet/ftp<default>;

ftp protocol information;

ftp transfer data byte.]

(8) FAU_STG.4 Prevention of audit data loss

Management: maintenance (deletion, modification, addition) of actions to be taken in case of audit storage failure.

Audit level: Basic

Audit: Actions taken due to audit storage failure.

FAU_STG.4.1 The TSF shall 'ignore auditable events', 'overwrite the *oldest stored audit records*' and *following actions to be taken in case of audit storage failure* if the audit trail is full.

- The following error message is displayed:
  "There is not enough hard disk space for log file."

(9) FMT_MOF.1 Management of security functions behavior

Management: managing the group of roles that can interact with the functions in the TSF;

Audit level: Basic

Audit: All modifications in the behavior of the functions in the TSF.

- Notes: As the logging information, or audit records is managed only by the administrator with the root privilege authorized by OS, the TSF does not record the audit records defined in this requirement.

FMT_MOF.1.1 The TSF shall restrict the ability to *operate following* functions to *the authorized identified roles.*

- Functions in TSFs:
  [create, delete, modify and view of configuration.]
- Only an authorized administrator may manage the behavior of the security functions in TSFs.

(10) FMT_MSA.1 Management of security attributes

Management: managing the group of roles that can interact with the security attributes.

Audit level: Basic

Audit: All modifications to the values of filtering rules.

- Notes: This TOE does not support this audit because of assumptions ASM1and ASM4.

FMT_MSA.1.1 The TSF shall enforce the *information flow control SFP* to restrict the ability to *following other operations* the *following list of security attributes* to *the authorized administrator roles.*

- *The information flow control SFP*:
  SFP_IPPF defined in FDP_IFC.1.1.
- *Other operations*:
  Manipulation of the attributes in the filtering rules
- *Security attributes*:
  Filtering rules containing the subject security attributes and Information security attributes defined in FDP_IFF.1.1
- *The authorized administrator roles*
  Only authorized administrator with the root privilege can access the filtering rules.

(11) FMT_MTD.1 Management of TSF data

Management: managing the group of roles that can interact with the TSF data.

Audit level: Basic

Audit: All modifications to the values of TSF data.

- Notes: As the logging information, or audit records is managed only by the administrator with the root privilege authorized by OS, the TSF does not record the audit records defined in this requirement.

FMT_MTD.1.1 The TSF shall restrict the ability to *change_default, query, modify, delete, clear, following other operations* the *following list of TSF data* to *the authorized administrator roles.*

- *other operations*:
  view the Environment definition.
- *TSFs data*:
  [Logging information files;
  Environment definition file (except security attribute);]

.

5.1.5. Strength of TOE security function

As Safegate will be used in general commercial systems, it will provide the SOF-medium that provides adequate protection against intruders with moderate attack potential.

5.2. TOE security assurance requirements

Safegate, designed for use in general commercial systems, also has the capability to assure security from the point of view of operations and management. This is because only an authorized administrator may manage systems with Safegate installed. Accordingly, Safegate offers EAL3-level of quality, which is a very adequate quality assurance level for a general commercial system.

Also, because only an authorized administrator can be the Safegate user, the user guidance assurance requirement (AGD_USR.1) is not provided.

5.3. Security requirements for the IT environment

This section describes the functional requirements that rely on OS functions. Accordingly, these functional requirements are not described in “8. Rational”.

5.3.1. Security audit

Safegate runs on an underlying operating system (OS). The OS is required to provide the functional requirements described below. These functional requirements are related to the management of configuration data and audit data in Safegate. Moreover, an authorized administrator is allowed access to TSF data.

For purposes of clarification, "OS" is used in place of "TSF" in each of the following functional requirements:

(1) FAU_SAR.2 Restricted audit review

Management: None

Audit level: Basic

Audit: Unsuccessful attempts to read information from the audit records.

FAU_SAR.2.1 The *OS* shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

- Only an authorized administrator may access to the audit records.

(2) FAU_STG.1 Protected audit trail storage

Management: None

Audit: None

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

- Only an authorized administrator may access to the audit records.

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

(3) FPT_RVM Non-bypassability of the TSP

Management: There are no management activities foreseen.

Audit: There are no actions.

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

(4) FPT_SEP TSF domain separation

Management: There are no management activities foreseen.

Audit: There are no actions.

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

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

Subject: The user process generated for each service such as telnet or ftp

Domain separation between the user processes is realised by OS function.

(5) FPT_STM.1 Reliable time stamps

Management: time management.

Audit level: Detailed

Audit: providing a timestamp.

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

- Provide reliable time stamps for logging.

5.3.2. Identification and authentication

Safegate runs on an underlying operating system (OS). The OS is required to provide the functional requirements described below. These functional requirements are related to the management of configuration data and audit data in Safegate. Moreover, an authorized administrator is allowed access to TSF data.

For purposes of clarification, "OS" is used in place of "TSF" in each of the following functional requirements:

(1) FMT_SMR.1 Security roles

Management: Managing the group of users that are part of a role.

Audit level: Detailed

Audit: All uses of the privileges of a role.

FMT_SMR.1.1 The *OS* shall maintain the roles: *following authorized identified roles.*

- Requires authorized identified roles as an authorized administrator in Safegate.

FMT_SMR.1.2 The *OS* shall be able to associate users with roles.

- The user of Safegate must be authenticated as an authorized administrator by the *OS*.

6. TOE summary specification

6.1. Introduction

This chapter describes security functionality in a form more understandable than function requirements. (Functional requirements are described in the previous chapter.) TOE Summary Specification shall include:

a) a definition of the TOE security functions which satisfy the identified security function requirements;

b) optionally, references to security mechanisms or techniques used to implement the IT security functions;

c) a references to rule documentation for associating the components of assurance requirements in EAL3 and a definition of assurance measures which satisfy the identified assurance requirements.

6.2. TOE security functions

6.2.1. IP packet filtering function

IPF.1: IP packet filtering function (called IP filtering) works between network drivers and IP in the kernel space on Solaris.

IP packet filtering is a function that permits or denies the transmission of IP packets through Safegate, between the hostile network and the private network, in accordance with the filtering rules defined by the authorized administrator.

Filtering rules can control IP packet flow in accordance with the security attributes of the subject or the information. The filtering rules determine whether to permit or deny the passage of a packet through Safegate, in accordance with filtering condition, by using following elements;

- Network communication interface that IP forwards IP packets:
- Source/target IP address (including subnet mask):
- Protocol, that is TCP, UDP, ICMP:
- Application protocol, such as telnet, ftp, smtp which runs on the TCP, UDP:
- Direction of packet flow:

The packet filtering rules examine the following filtering conditions in the sequence given below (from top to bottom):

- packet process type (block>transparent>pass)
- protocol (TCP/UDP/ICMP)

< in case of TCP/UDP >

- source port number (ascending)
- target port number (ascending)

< in case of ICMP >

- message type (ascending)
- message code (ascending)
- source subnet mask (descending)
- source IP address (ascending)
- target subnet mask (descending)
- target IP address (ascending)
- entry order of the specifications made by the authorized administrator

If any filtering condition is not satisfied for the IP packet, the IP packet is discarded.

6.2.2. Application gateway/Transparent mode

Application gateway/Transparent mode works on the basis IPF1.

AGW.1:

Application gateway/transparent mode connects directly a client on a private network to a target host on Internet and establishes a session between both network. Transparent mode provides following services.

a) Various services on TCP/UDP/ICMP such as telnet, ftp, mail, news, http, wais, gopher, ping (except for r command such as rcp, rsh and services based on RPC)

b) Multimedia services such as RealAudio Ver.5.0, VDO Live Ver.2.0, Stream Works Ver.3.0

Safegate communicates through packets passing between a private network and Internet. Safegate converts source IP addresses in packets into global IP addresses of Safegate itself when to send the packet to the target host. In the reply packet from the target host, the destination IP address is converted back to the local IP address of the original client.

6.2.3. Application gateway/Non-transparent mode

Application gateway/Non-transparent mode works on the basis IPF1.

AGW.2:

Application gateway/Non-transparent mode mediates only ftp and telnet services between a client on a private network and a host on Internet and does not mediate the other services.

Application gateway/Non-transparent mode establishes the connection between a private network and Internet in two steps.

First of all, a client on a private network establishes the session with the Safegate. Afterwards, Safegate has another session with a host on the Internet. Two simultaneous sessions lead to establish logically the connection between the client on the private network and the host on the Internet.

The address information constructing the private network system are completely concealed to the Internet because the private network connects indirectly to the Internet.

6.2.4. Security management

1) Safegate provides the following security management.

AUD.1 Logging functions

Safegate provides the logging functions that log the following audit information on files:

(1) Logging of IP packet filtering

a) Statistics information

The following are recorded as statistics information in services:

[number of passed packets;
number of discarded packets;
number of deliveries to each user stream.]

b) Connection information

The following packet data items are logged as connection information:

[passed packet (TCP; UDP);
discarded packet (all packets).]

(Note: TCP = packet with SYN, FIN, and RST bits on
UDP = first and last packets detected in communication between certain hosts)

The following are logged as connection information:

[date and time;
type of log(connection established packet; connection release packet; pass rejection packet; relay packet to user process);
interface;
source IP address;
destination IP address;
protocol(TCP; UDP);
source port number;
destination port number;
user ID.]

c) The following are able to include or exclude auditable events:

[protocol;
[TCP/UDP;
ICMP;
all<default>.]
type of data;

[connection establishment/release;
rejection;
all<default>.]]

(2) Logging of application gateway

(2-1) Non-transparent mode

a) Logging of connection information:
[status of connection or disconnect in telnet;
status of connection or disconnect in ftp.]

b) The following four levels are able to specify auditable events:
[no logging;
connection and disconnection status of telnet and ftp <default>;
connection and disconnection status, and ftp protocol information;
connection and disconnection status, ftp protocol information, and ftp transfer data byte.]

(2-2) Transparent mode

The following are logged as statistics information and relay information in gateway.

a) Statistics information:
[number of relay connections;
total bytes of relay data.]

b) relay information:
[date and time;
connection between client;
connection between destinations;
used protocol and service;
type of connection (normal connection; back connection);
volume of relayed data.]

(3) Common function

a) The following are able to specify when the audit trail is full:
[discard auditable events;
old file deletion (delete the oldest stored audit records and write the new file.]

b) The following error message is displayed when the audit trail is full:
"There is not enough hard disk space for the log file."

c) The following are able to specify when the audit trail is full:

[send mail<default>;

no send mail.]

AUD.2 Alert function

If it detects an invalid packet, Safegate provides the alert function that gives notification about, and logs such event as an alert event.

(1) IP packet filtering alert and application gateway alert

a) Alert notifications are able to specify the following:

[console output;

mail send;

notification via monitor;

command execution;

SNMP manager notification.]

(2) Immediately generate the following alert events and logging upon detection of events deemed indicative of a possible security violation:

[alert for the same source address;

alert for the same destination address.]

(3) The following are logged as alert information:

a) alert for same source address:

[detect time;

initial access time;

source IP address;

protocol (TCP; UDP);

packet count;

alert log number.]

b) alert for same destination address:

[detect time;

initial access time;

destination IP address;

protocol (TCP; UDP);

destination port;

packet count;

alert log number.]

AUD.3 Monitoring function

Safegate provides following monitoring function that displays alert information, statistics information and connection information currently.

a) Alert information

Monitoring function shows alert information defined in AUD.2 (3).

b) Statistics information

Monitoring function shows the total number of packets, passed packets and denied packets through starting Safegate time to the current time.

c) Connection information

Monitoring function shows the current session status connected with the Internet host.

AUD.4 Log output functions

Safegate provides the log output functions that edit and display logging data.

(1) Log output of IP packet filtering

[Type of information (statistics; connection; alert);
Date and time of start/end;
Source/destination IP address;
Port number;
Result of packet pass attempt (pass; block).]

(2) Log of application gateway/Non-transparent mode

[Type of information (telnet; ftp);
Date and time of start/end.]

(3) Log of application gateway/Transparent mode

[Type of information (statistics; relay);
Date and time of start/end;
IP address, host-name, or Domain-name of server;
IP address, host-name, or Domain-name of client;
Protocol(TCP; UDP; ICMP);
Port number.]

AUD.5 Log viewer

Safegate provides the log viewer functions for searching, editing and displaying logging data.

(1) Log viewer of IP packet filtering

[Type of information (connection; alert);

Date and time of start/end;
Source/destination IP address or host-name;
Protocol (TCP; UDP; ICMP);
Service (telnet; ftp);
Result of packet pass attempt (pass; block).]

(2) Log viewer of application gateway/Non-transparent mode
[Date and time of start/end;
IP address, or server-name of server;
IP address, or client-name of client;
Service (telnet; ftp).]

(3) Log viewer of application gateway/Transparent mode
[Type of information (connection; disconnect);
Date and time of start/end;
IP address, or server -name of server;
IP address, or client -name of client;
Protocol (TCP; UDP; ICMP);
Service (telnet; ftp).]

2) External interface

AUD.6 Environment setting

(1) Environment definition and Filtering rules

An authorized administrator has the authority to define the environment setting for Safegate, as follows:

Table 6.1 Settings required for IP filtering and application gateway

operating form setting item	IP filtering	IP filtering, Non-transparent GW	IP filtering, Transparent GW
Network configuration diagram	Y	Y	Y
Interface	Y	Y	Y
Host	Y	Y	Y
Host group	*	*	*
Network environment	*	*	*
Non-transparent GW environment	N	Y	N
Transparent GW environment	N	N	Y
Service	*	*	*
Service group	*	*	*
Logging	*	*	*

Alert	*	*	*
Packet filtering condition	Y	Y	Y

Y : required GW= gateway

* : optionally required

N: not required

(2) The Environment definition file

The Environment definition file is stored using protect mode; all persons except the authorized administrator are restricted from having access to this file.

6.3. Security mechanisms or techniques

The security functions do not refer to any particular security mechanisms or techniques.

6.4. Assurance Measures

The following table describes the rule documentation for associating the components of assurance requirements in EAL3.

Table 6.2 Assurance requirements and rule documentation

Assurance requirement	Component	Rule documentation
Configuration management	ACM_CAP.3	ACM_CAP.3.1D The developer shall provide a reference for the TOE. ACM_CAP.3.2D The developer shall use a CM system. ACM_CAP.3.3D The developer shall provide CM documentation.
	ACM_SCP.1	ACM_SCP.1.1D The developer shall provide CM documentation. Rule documentation: * Development process regulations * Configuration management procedures * Program configuration management procedures * Quality record management procedures * Cording conventions
Life cycle support	ALC_DVS.1	ALC_DVS.1.1D The developer shall produce development security documentation. Rule documentation: * Quality record management procedures * Document management procedures * Provisions for training in projects
Functional specification	ADV_FSP.1	ADV_FSP.1.1D The developer shall provide a functional specification. Refer to security target.
High-level design	ADV_HLD.2	ADV_HLD.2.1D The developer shall provide the high-level design of the TSF. Refer to functional specification.
Representation correspondence	ADV_RCR.1	ADV_RCR.1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

(cont.)

Assurance requirement	Component	Rule documentation
Tests	ATE_COV.2 ATE_DPT.1 ATE_FUN.1 ATE_IND.2	ATE_COV.2.1D The developer shall provide an analysis of the test coverage. ATE_DPT.1.1D The developer shall provide the analysis of the depth of testing. ATE_FUN.1.1D The developer shall test the TSF and document the results. ATE_FUN.1.2D The developer shall provide test documentation. ATE_IND.2.1D The developer shall provide the TOE for testing.
Administrator guidance	AGD_ADM.1	AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel. Documentation: * Safegate Description Manual
User guidance	AGD_USR.1	Not required for Safegate
Operation	ADO_IGS.1	ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.
Delivery	ADO_DEL.1	ADO_DEL.1.1D The developer shall document procedures for delivery of the TOE or parts of it to the user. ADO_DEL.1.2D The developer shall use the delivery procedures. Rule documentation: * Distribution rules
Vulnerability analysis	AVA_VLA.1	AVA_VLA.1.1D The developer shall perform and document an analysis of the TOE deliverables, searching for obvious ways in which a user can violate the TSP. AVA_VLA.1.2D The developer shall document the disposition of obvious vulnerabilities.
Misuse	AVA_MSU.1	AVA_MSU.1.1D The developer shall provide guidance documentation.
Strength of TOE security functions	AVA_SOF.1	AVA_SOF.1.1D The developer shall perform a strength-of-TOE security function analysis for each mechanism identified in the ST as having a strength-of-TOE security function problem.

7. PP Claims

There is no PP conforming to this ST

8. Rationale

8.1. Security objectives rational

Threat Security policy	T1	T21	T22	T3	T5	T7	TE4	TE5	TE6	TE9
O.I	✓	✓	✓		✓					
O.DAC1	✓	✓	✓	✓	✓					
O.DAC2		✓	✓		✓		✓		✓	
O.DAC3		✓	✓	✓						
O.AG1				✓						
O.ADMIN		✓	✓							
O.AUDMON				✓	✓	✓	✓	✓	✓	
O.AUDREC				✓	✓	✓	✓	✓	✓	
OE1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
OE2		✓	✓							✓
OE3	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
OE4	✓			✓	✓	✓	✓	✓	✓	
OE5		✓	✓							✓
OE6	✓	✓	✓	✓	✓	✓	✓	✓	✓	
ASM1		✓	✓							✓
ASM2	✓	✓	✓	✓	✓	✓	✓	✓	✓	
ASM3	✓	✓	✓	✓	✓	✓	✓	✓	✓	
ASM4					✓	✓	✓	✓	✓	
ASM8	✓			✓		✓		✓		
ASM10		✓	✓							✓

Table 8.1: Mapping of threats to IT Security Objectives

- Explanation of security policy against threat

T1 It is indispensable for identifying the attribute information of packets entering from the network interface of an external network, determine that a packet is forged from the packet attribute information and prevent invasion of a private network in order to guard against a T1 threat.

O.I reads the packet attribute information about the external network host attempting to invade the private network, and identifies the transmitter address information. O.DAC1 decides whether proper transmitter address information is set for the packet identified by the O.I as a packet to be sent through the external network interface. When this decision is made, the packet with transmitter address information set for a private network address band is blocked if coming from the external network interface. According to the IT security policy mentioned above, the counteraction ability against such threat can be fully reserved.

It is mandatory to organize the Safegate in the ASM2 and ASM3 compliant configuration and conduct ASM8-based configuration management in order to maintain technical countermeasures against this threat. To satisfy these assumptions, the OE3 must be performed to train good administrators, the OE4 must be performed to maintain high-level management, and the OE1 and OE6 must be performed properly at installation, configuration, and management of the Safegate in order to conduct the technical countermeasures safely and successfully.

T21 It is indispensable for limiting the access to the firewall host and restrict the resources on that host in order to guard against a T21 threat. This can be implemented by limiting the firewall host administrator using O.ADMIN and restricting access using O.I, O.DAC1, O.DAC2, and O.DAC3. The O.ADMIN limits the firewall host access right to specific users so that only those users can control a filtering rule base or operating environments. The O.I reads packet attribute information from the host attempting to establish a connection with the firewall host, in order to identify the transmitter address. The O.DAC1 restricts the O.I-identified packet on the address band of a network capable of accessing the firewall host in order to prevent any unauthorized hosts from gaining access. If any access to the firewall host is inhibited, the O.DAC1 restricts all firewall host accessible address bands. The O.DAC2 completely inhibits the O.I-identified packet from accessing the firewall host from an external network. Also, the O.DAC3 completely inhibits the O.I-identified packet from accessing the firewall host. According to the IT security policy mentioned above, the counteraction ability against such threat can be fully reserved.

It is mandatory to organize the Safegate in the ASM1, ASM2 and ASM3 compliant configuration, train users according to the ASM10 and keep their morals good in order to back up technical countermeasures against this threat. In order to back up these assumptions and technical countermeasures against this threat, the OE1 and OE6 must be performed properly at installation, configuration, and management of the Safegate, OE2 and OE5 must be performed for hardware and software protection, and the OE4 must be performed in order to maintain high-level management.

T22 It is indispensable for limiting the access to the firewall host and restricting the administrators who can access the resources on that host, in order to guard against a T22 threat. The firewall host administrators can be restricted by the O.ADMIN to limit access using the O.I, O.DAC1, O.DAC2, and O.DAC3 as protections. The O.ADMIN limits the firewall host access right to specific users so that only the administrators having the access right can control firewall audit logging information. The O.I reads packet attribute information from the host attempting to establish a connection with the firewall host, in order to identify the transmitter address. The O.DAC1 restricts the O.I-identified packet on the address band of a network capable of accessing the firewall host in order to prevent any unauthorized hosts from gaining access. If any access to the firewall host is inhibited, the O.DAC1 restricts all firewall host accessible address bands. The O.DAC2 completely inhibits the O.I-identified packet from accessing the firewall host from an external network. Also, the O.DAC3 completely inhibits the O.I-identified packet from accessing the firewall host. According to the IT security policy mentioned above, the counteraction ability against such threat can be fully reserved.

It is mandatory to organize the Safegate in the ASM1, ASM2 and ASM3 compliant configuration, train users according to the ASM10 and keep their morals good in order to back up technical countermeasures against this threat. To satisfy these assumptions, the OE3 must be performed to train good administrators, OE2 and OE5 must be performed for hardware and software protection, and the OE1 and OE6 must be performed properly at installation, configuration and management of the Safegate in order to conduct the technical countermeasures safely and successfully.

T3 It is indispensable for protecting the address system of the private network from leaking outside, limiting the hosts on the private network accessible to external networks, and preventing unnecessary access in order to guard against a T3 threat. The O.DAC1 and O.DAC3 are used to limit the hosts accessible to external networks, and the O.AG1 is used to protect the address system. The O.DAC1 limits the address band within the private network accessible to external networks. The O.DAC3 authorizes only the minimum access by limiting both accessible hosts and services that are available to the hosts within the internal network authorized by the O.DAC1 for access to the external networks. The O.AG1 translates a client address on the private network into a global address (an address assigned to the external network interface of Safegate) which causes no security risk even if disclosed outside, in order to hide the network system of the private network from outside. Also, to reduce the risks accompanied with access to external networks, the O.AG1 monitors illegal access attempts, collects information on security policy violators by organization or illegal acts, and provides information analysis using both O.AUDMON and O.AUDREC together. According to the IT security policy mentioned above, the counteraction ability against such threat can be fully reserved.

It is mandatory to organize the Safegate in the ASM2 and ASM3 compliant configuration and conduct configuration management according to the ASM8 in order to maintain technical countermeasures against this threat. To satisfy these assumptions, the OE3 must be performed to train good administrators, the OE1 must be performed properly at installation, configuration, and management of the Safegate in order to conduct the technical countermeasures safely and successfully, and then the OE4 must be performed in order to maintain high-level management. Also, the OE6 must be performed to be able the Safegate to manage all the communications between the private network and hostile networks.

T5 It is indispensable for limiting the access both to the firewall host from external networks and to a private network in order to guard against a T5 threat. A packet type and an access source can be handled by limiting access using the O.I, O.DAC1, and O.DAC2. The O.I reads packet attribute information from the host on an external network that attempts to transmit an illegal packet to the firewall host or private network host, in order to identify the transmitter address. The O.DAC1 restricts the O.I identified packet on the address band of an external network capable of accessing the firewall host and private network. The O.DAC2 detects the ICMP packet (hereinafter including a ping and a traceroute) transmitted from the external network, and cancels the ICMP packet transmitted from the host on an illegal external network not authorized by the O.DAC1. Also, the O.DAC2 reduces the risks arising from illegally transmitted packets using both O.AUDMON and O.AUDREC together. To do this, the O.DAC2 collects illegal access information and analyzes the information to provide the information on packets to be canceled. According to the IT security policy mentioned above, the counteraction ability against such threat can be fully reserved.

Also, it is mandatory to organize the Safegate in the ASM2 and ASM3 compliant configuration and conduct fair, routine management according in order to the ASM4 and maintain technical countermeasures against this threat. To satisfy these assumptions, the OE3 must be performed to train good administrators, the OE1 must be performed properly at installation, configuration and management of the Safegate in order to conduct the technical countermeasures safely and successfully, and then the OE4 must be performed in order to maintain high-level management. Also, the OE6 must be performed to be able the Safegate to manage all the communications between the private network and hostile networks.

T7 It is indispensable for monitoring packets to be passed or canceled on the firewall host, quickly detecting a packet which is controlled by the security policy in an organization, and correcting wrong packet control in order to guard against a T7 threat. Both O.AUDMON and O.AUDREC detect wrong packet control. The O.AUDMON and O.AUDREC can monitor packets which are passing through the firewall host, detect the distribution of packets violating the security polity of the organization, and acquire information on the services or address bands to be restricted. Based on the information obtained from the O.AUDMON and O.AUDREC, the administrator corrects packet filtering rule setting errors or any other security settings conforming to the organization's security. According to the IT security policy mentioned above, the counteraction ability against such threat can be fully reserved.

Also, it is mandatory to organize the Safegate in the ASM2 and ASM3 compliant configuration, conduct fair, routine management according to the ASM4, and then manage the configuration according to the ASM8 in order to maintain technical countermeasures against this threat. To satisfy these assumptions, the OE1 and OE6 must be performed properly at installation, configuration, and management of the Safegate in order to conduct the technical countermeasures safely and successfully. Then the OE3 must be performed to train good administrators and the OE4 must be performed to maintain high-level management.

TE4 It is indispensable for allowing the Safegate administrator to acquire hints for detecting an illegally used service by efficiently using and managing the audit function for maintaining good security policy, in order to guard against TE4 threat. The hints may be acquired by both

O.AUDMON and O.AUDREC, and at least some action can be taken against a service protocol detected from the information. This means that full action can be taken by limiting the use of services from external networks using the O.DAC2.

It is mandatory to organize the Safegate in the ASM2 and ASM3 compliant configuration, and conduct fair, routine management according to the ASM4 in order to maintain technical countermeasures against this threat. To satisfy these assumptions, the OE1 must be performed properly at installation, configuration, and management of the Safegate in order to conduct the technical countermeasures safely and successfully. Then the OE3 must be performed to train good administrators and the OE4 must be performed to maintain high-level management. Also, the OE6 must be performed to be able the Safegate to manage all the communications between the private network and hostile networks.

TE5 It is indispensable for allowing the Safegate administrator to efficiently use and manage the audit function for maintaining the good security policy, in order to guard against a TE5 threat. Both O.AUDMON and O.AUDREC can collect and analyze audit information to back up quick detection of an attack against a private network and help construction of a secure private network configuration.

It is mandatory to organize the Safegate in the ASM2 and ASM3 compliant configuration, conduct fair, routine management according to the ASM4, and manage the configuration according to the ASM8 in order to maintain technical countermeasures against this threat. To use the audit function efficiently, the OE1 must be performed properly at installation, configuration, and management of the Safegate. Then the OE3 must be performed to train good administrators and the OE4 must be performed to maintain high-level management. Also, the OE6 must be performed to be able the Safegate to manage all the communications between the private network and hostile networks.

TE6 It is indispensable for allowing the Safegate administrator to efficiently use and manage the audit function to maintain good security policy, in order to guard against a TE6 threat. Both O.AUDMON and O.AUDREC can collect and analyze audit information to acquire hints for detecting service security defects. At least the information on the defect obtained from the hints can be used to take proper action. There is a great expectation of possibly taking action by providing a time grace even if proper action information is not established. (It can depend on technological advances of a security expert organization.) Limiting the use of services from external networks using the O.DAC2 is sufficient for temporary action.

Also, it is mandatory to organize the Safegate in the ASM2 and ASM3 compliant configuration, and conduct fair, routine management according to the ASM4 in order to maintain technical countermeasures against this threat. To use the audit function efficiently, the OE1 must be performed properly at installation, configuration, and management of the Safegate. Then the OE3 must be performed to train good administrators and the OE4 must be performed to maintain high-level management. Also, the OE6 must be performed to be able the Safegate to manage all the communications between the private network and hostile networks.

TE9 It is indispensable for allowing the Safegate administrator to install the system in a safe environment and protect it from unauthorized personnel's modification or destruction of the Safegate itself, in order to guard against a TE9 threat. For physical protection, the ASM1, OE2, and OE5 must be performed. To take these protections, the OE1 must be performed properly at installation, configuration, and management of the Safegate. And then the OE3 must be performed to train good administrators. Also, it is mandatory to train users according to the ASM10, and keep their morals good in order to maintain technical countermeasures against this threat.

8.2. Security requirements rational

Security Functional Requirement	IT Security Objective							
	O.I	O.DAC1	O.DAC2	O.DAC3	O.AG1	O.ADMIN	O.AUDMON	O.AUDREC
FDP_IFC.1	✓	✓	✓	✓	✓			
FDP_IFF.1	✓	✓	✓	✓	✓			
FAU_ARP.1							✓	✓
FAU_GEN.1							✓	✓
FAU_SAA.1								✓
FAU_SAR.1							✓	✓
FAU_SAR.3								✓
FAU_SEL.1								✓
FAU_STG.4								✓
FMT_MOF.1						✓		
FMT_MSA.1						✓		
FMT_MTD.1						✓		
FAU_SAR.2						✓		
FAU_STG.1								✓
FPT_RVM.1	✓	✓	✓	✓	✓			
FPT_SEP.1	✓	✓	✓	✓	✓			
FPT_STM.1								✓
FMT_SMR.1						✓		

Table 8.2: Mapping of IT Security Objectives for Security Functional Requirements

O.I, O.DAC1 to O.DAC3 and O.AG1 need FPT_RVM.1 and FPT_SEP.1 to protect the function from bypassing or tampering by untrusted subjects.

O.I Safegate must, be capable of identifying a single host or a group of hosts prior to Safegate allowing a connection to be established.

FDP_IFC and FDP_IFF.1 together provide the information flow control security requirements that identify the source host address in a packet from both hostile and private networks. As the capability of identifying a single host or a group of hosts is performed by only this security objective, O.I is independent on the other security objectives.

O.DAC1 Safegate must limit the valid range of addresses expected on each of the private and hostile networks (i.e. an external host cannot spoof an internal host).

FDP_IFC and FDP_IFF.1 together provide the information flow control security requirements, which permit or deny a packet flow based on the source/destination IP address in a private or hostile network. Also, these requirements have the capability of limiting the valid range of addresses expected on each of the private and hostile networks.

O.DAC2 Safegate must limit the hosts and service ports that can be accessed from the hostile network.

FDP_IFC and FDP_IFF.1 together provide the information flow control security requirements, which permit or deny a packet flow based on the destination IP address and the service port in a private network. Also, these requirements have the capability of limiting the hosts and service ports that can be accessed from the hostile networks.

O.DAC3 Safegate must limit the hosts and service ports that can be accessed from the private network.

FDP_IFC and FDP_IFF.1 together provide the information flow control security requirements, which permit or deny a packet flow based on the destination IP address and the service port in a hostile network. Also, these requirements have the capability of limiting the hosts and service ports that can be accessed from the private networks.

O.AG1 Safegate has the ability to conceal from hostile networks the IP addresses of clients on the private network.

FDP_IFC and FDP_IFF.1 together provide the information flow control security requirements, which convert IP addresses of hosts in a private network to an IP address of Safegate, so as not to expose private network addresses to a hostile network.

O.ADMIN Safegate must provide a single focus of administrative control of Safegate, ensuring that only the authorized administrator can exercise such control.

FMT_MOF.1, FMT_MSA.1 and FMT_MTD.1 is necessary to allow the authorized administrator to control the management functions of Safegate (i.e. setting rules and parameters) in a secure manner. FAU_SAR.2 is necessary to prohibit all users read access to the audit records except for the authorized administrator. Also, FMT_SMR.1 is necessary to maintain the authorized roles.

O.AUDMON Safegate must provide a facility for monitoring successful and unsuccessful attempts at connections between the private network and the hostile network.

FAU_SAR.1 is necessary to allow the authorized administrator to review audit records. O.AUDMON also needs FAU_ARP.1 to show potential security violations on a display device as the function of the action defined in this requirement. FAU_GEN.1 defines the audit events to be shown.

O.AUDREC Safegate must provide measures to recording, searching and retrieving an audit trail in a format that enables recognition of security related events that include accurate date and time records.

FAU_GEN.1 and FAU_SEL1 are necessary to generate audit record. FAU_ARP.1 is necessary to take the actions when potential violations are detected. O.AUDREC needs FAU_SAA.1 to apply a set of rules in monitoring the audited events, and FAU_SAR.3 to selectively review audit records with the search capabilities. These audited events are shown on a display device according with FAU_SAR.1. FAU_STG.4 is necessary to prevent the loss of audit records when the audit storage is full and FAU_STD.1 is necessary to protect the audit records from unauthorized deletion and modifications. Also, O.AUDREC needs FPT_STM.1 to record correct time in audit records.

8.3. Security Requirements Dependency Analysis

Functional Component		Dependent on	
Number	Name	Name	Reference
1	FDP_IFC.1	FDP_IFF.1	2
2	FDP_IFF.1	FDP_IFC.1	1
3	FAU_ARP.1	FAU_SAA.1	5
4	FAU_GEN.1	FMT_MOF.1 FMT_MTD.1 FAU_STG.4	10 12 9
5	FAU_SAA.1	FAU_GEN.1	4
6	FAU_SAR.1	FAU_GEN.1	4
7	FAU_SAR.3	FAU_SAR.1	6
8	FAU_SEL.1	FMT_MTD.1 FAU_GEN.1	12 4
9	FAU_STG.4	FAU_SAA.1	5
10	FMT_MOF.1	None	-
11	FMT_MSA.1	FDP_IFC.1	1
12	FMT_MTD.1	None	-

Table 8.3: Dependencies of Functional Components

No.1: FDP_IFC.1 (Subset information flow control)

Depends on FDP_IFF.1 (Simple security attributes).

No.2: FDP_IFF.1 (Simple security attributes)

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

No.3: FAU_ARP.1 (Security alarms)

Depends on FAU_SAA.1 (Potential violation analysis).

No.4: FAU_GEN.1 (Audit data generation)

Depends on FMT_MOF.1 (Management of security functions behavior), FMT_MTD.1 (Management of TSF data) and FAU_STG.4 (Prevention of audit data loss).

No.5: FAU_SAA.1 (Security audit analysis)

Depends on FAU_GEN.1 (Audit data generation).

No.6: FAU_SAR.1 (Audit review)

Depends on FAU_GEN.1 (Audit data generation).

No.7: FAU_SAR.3 (Selectable audit review)

Depends on FAU_SAR.1 (Audit review).

No.8: FAU_SEL.1 (Selective audit)

Depends on FMT_MTD.1 (Management of TSF data) and FAU_GEN.1 (Audit data generation).

No.9: FAU_STG.4 (Prevention of audit data loss)

Depends on FAU_SAA.1 (Security audit analysis).

No.10: There is no dependency on FMT_MOF.1 (Management of functions in TSF)

No.11: There is no dependency on FMT_MSA.1 (Management of security attributes)

No.12: There is no dependency on FMT_MTD.1 (Management of TSF data)

8.4. Security Requirements Mutually Supportive

This section shows that the security requirements are mutually supportive and internally consistent. No detailed analysis is given with respect to the assurance requirements because:

- EAL3 is an established set of mutually supportive and internally consistent assurance requirements.
- By definition, assurance requirements naturally support the functional requirements, by providing assurance that the functional requirements are met by the TOE. Inconsistency between functional and assurance requirements can only arise if there are functional-assurance dependencies that are not being met, a possibility which has been shown not to arise by the preceding section.

Therefore, it is only necessary to provide a detailed analysis to demonstrate mutual support and internal consistency between the functional requirements. In so doing, it is asserted that all dependencies between functional requirements are satisfied, as demonstrated in the previous section. The dependency analysis itself demonstrates a certain degree of mutual support and internal consistency. The analysis provided here builds on this by showing how the security requirements work together to provide comprehensive protection against the forms of *indirect attack* given below, by which the intent of the security requirement could be defeated.

- *Bypassing* attacks, which involve an attacker exploiting interfaces to the TOEs that do not enforce the security requirement.
- *Tampering* (*or corruption*) attacks, which involve attacks on the integrity of data used by the security requirement;
- *De-activation* attacks, including misconfiguration of the TSF

Requirement	Requirement Providing Protection Against		
	Bypassing	Tampering (or corruption)	De-activation
FDP_IFC.1	FPT_RVM.1	FPT_SEP.1	N/A
FDP_IFF.1	FPT_RVM.1	FPT_SEP.1	FAU_GEN.1
FPT_RVM.1	N/A	N/A	N/A
FPT_SEP.1	N/A	N/A	N/A
FAU_ARP.1	FPT_RVM.1	N/A	FAU_GEN.1
FAU_GEN.1	FPT_RVM.1	N/A	FAU_GEN.1
FAU_SAA.1	FPT_RVM.1	FPT_SEP.1	FAU_GEN.1
FAU_SAR.1	N/A	N/A	N/A
FAU_SAR.3	N/A	N/A	N/A
FAU_SEL.1	N/A	FPT_SEP.1	N/A
FAU_STG.4	N/A	FPT_SEP.1	N/A
FMT_MOF.1	N/A	N/A	N/A
FMT_MTD.1	N/A	N/A	N/A

Table 8.4: Demonstration of Mutual Support between Functional Components

N/A: Not Applicable

Note:

In general:

- Bypassing attacks are ‘N/A’ if the requirement defines an invariant property of the TOE (e.g., FPT_SEP.1) or if the decision to invoke the functionality resides with the user rather than the TOE (e.g., FMT_XXX).
- Tampering attacks are ‘N/A’ if the correct behavior of the stated security requirement is not dependent on the integrity of any data.
- Deactivation attacks are ‘N/A’ if the security requirement as stated is not dependent on the configuration of the TSF.

Bypassing attacks are prevented by:

- FPT_RVM.1 with respect to security enforcement functions.

  FPT_RVM.1 ensures that the TSF invokes the security policies of SFP_IPPF for the IP packet filtering, SFP_APRC for Application Gate Way and SP_AUDT for the audit.

Tampering attacks are prevented by:

- FPT_SEP.1 which maintains domain separation, and in particular prevents an attacker from tampering with the security functions.

  FPT_SEP.1 ensures that the security policies of SFP_IPPF, SFP_APRC and SFP_APRC are enforced in the domain which is protected from interference and tampering by not trusted subject or the other TSF.

De-activation attacks are prevented by:

- FAU_GEN.1 which has the capability of auditing (and hence detecting) potential misconfiguration of the security function, thereby enabling the authorized administrator to take appropriate action.

  FAU_GEN.1 ensures that the administrator of the TOE collects the information to audit incorrect environment definitions or unauthorized modification of environment, and that the administrator performs an appropriate treatment.

8.5. TOE summary specification rational

The following table shows that a mapping between TOE summary specifications and functional requirements, and each functional requirement covered by a TOE summary specification or by a set of these specifications.

TOE summary Specification Functional Requirements	IPF.1	AGW.1	AGW.2	AUD.1	AUD.2	AUD.3	AUD.4	AUD.5	AUD.6
FDP_IFC.1	✓	✓	✓						
FDP_IFF.1	✓	✓	✓						
FAU_ARP.1					✓	✓			
FAU_GEN.1				✓	✓	✓			
FAU_SAA.1					✓				
FAU_SAR.1				✓		✓	✓	✓	
FAU_SAR.3								✓	
FAU_SEL.1				✓					
FAU_STG.4				✓					
FMT_MOF.1									✓
FMT_MSA.1									✓
FMT_MTD.1									✓
FAU_SAR.2 FAU_STG.1 FMT_SMR.1 FPT_RVM.1 FPT_SEP.1 FPT_STM.1	These functional requirements are realised by underlining Operating System								

Table 8.5: Mapping of security function for security functional requirements

FDP_IFF.1: The TSF shall provide the following capability. *Information (IP packets) defined in FDP_IFC.1.1 is examined to pass/deny between Subjects (private network and hostile network) defined in FDP_IFC.1.1.*

This requirement is met by the following security function. To determine whether a packet matches a condition in the TOE, the rules (that is, conditions) must first be established using IPF.1, specifying the particular combination of attributes for a “match” on a condition and an action of “trans” (note that “trans” is equivalent to “permit” with the additional functionality provided by AGW.1 or AGW.2). AGW.1 or AGW.2 is called to perform the address conversion from a private IP address to a temporary global IP address, or from a temporary global IP address to a private IP address to protect a private network configulation from unauthorized disclosure.

FAU_ARP.1: The TSF shall provide following actions upon detection of a potential security violation.

- *The TSF displays a message on console.*
- *The TSF sends a message by mail.*
- *The TSF notifies an alert on the real time monitor if the condition is satisfied. The condition is defined in FAU_SAA.1.*
- *The TSF executes a specified command.*
- *The TSF sends an alert data to SNMP manager.*

This requirement is met by AUD.2 that controls the actions to be taken when a potential security violation is detected. These actions are described above list. If AUD.2 determines to notify an alert on the real time monitor, then AUD.3 is performed to display the alert information, the statistics information or the connection information.

FAU_GEN.1: The TSF shall provide the following capability to generate an audit record.

This requirement is met by AUD.1, AUD.2 and AUD.3 according with each auditable event.

Functional Component	**Level**	**Auditable Event**	**Summary function**
FAU_ARP.1	Minimal	Actions taken due to imminent security violations	AUD.2 and AUD.3
FAU_SAA.1	Minimal	Automated responses performed by the tool	AUD.2
FAU_SAR.1	Basic	None	-
FAU_SAR.3	Detailed	None	-
FAU_SEL.1	Minimal	None	-
FAU_STG.4	Basic	Actions taken due to audit storage failure	AUD.1
FDP_IFF.1	Basic	All decisions (permit and deny) on the information flow All address changes in IP packets	AUD.1
FMT_MOF.1	Basic	None	-
FMT_MSA.1	Basic	None	-
FMT_MTD.1	Basic	None	-

FAU_SAA.1: The TSF shall provide the capability to apply a set of rules in monitoring the audited events based upon following attributes.

- *The same source IP address*
- *The same destination address*
- *The specified port set*

This requirement is met by AUD.2 that gives notification when the following condition is satisfied.

- More than specified numbers of packets with same source address or same destination address are detected.

FAU_SAR.1: The TSF shall provide *the authorized administrator* with the capability to read *following audit information* from the audit record and the audit records in a manner suitable for the authorized administrator to interpret the information.

- *Audit information for IP filtering, Transparent mode and Non-transparent mode*

This requirement is met by AUD.1, AUD.3, AUD.4 and AUD.5. AUD.1 records the audit information in the logging file. AUD.3, AUD.4 and AUD.5 show the audit record in a manner suitable for the authorized administrator.

FAU_SAR.3: The TSF shall provide the ability to perform *searches* of audit data based on the criteria *by using following keys. Searches are performed by using the one or multiple keys.*

- *Connection information or alert information*
- *Date and time of start or end*
- *Protocol (TCP/UDP/ICMP)*
- *Service (telnet/ftp)*
- *Result of handling packets (pass/block)*

This requirement is met by AUD.5 that gives a log viewer function. The log viewer provides the function to search the information related to the keys specified by an authorized administrator and shows them on a display device in a manner suitable for him.

FAU_SEL.1: The TSF shall be able to include or exclude auditable events from the set of audited events based on the attributes such as *object identity, user identity, subject identity, host identity and event type. These attributes are composed of following.*

- *Date and time*
- *Protocol (TCP/UDP/ICMP)*
- *IP address*
- *Port number*
- *User ID*

This requirement is met by AUD.1 that generates audit records according with the above attributes.

FAU_STG.4: The TSF shall *ignore auditable events or overwrite the oldest stored audit records* and *other actions to be taken in case of audit storage failure* if the audit trail is full.

This requirement is met by AUD.1 that ignore auditable events or overwrite the oldest stored audit record when the audit trail is full. AUD.1 also has the ability to issue the massage (“There is not enough hard disk space for the log file.”) to the authorized administrator.

FMT_MOF.1: The TSF shall restrict the ability *to operate following functions to the authorized administrator.*

- *Create, delete, modify and view of the Environment definition*

This requirement is met by AUD.6. AUD.6 checks the person who accesses the Environment definition must have the root privilege.

FMT_MSA.1: The TSF shall enforce *the access control SFP* to restrict the ability to *change_default, query, modify and delete following* security attributes to *the authorized administrator.*

- *Security attributes: Filtering rules*
- *The access control SFP: The authorized administrator with the root privilege can access above security attributes.*

This requirement is met by AUD.6 that checks an authorized administrator who accesses the filtering rules must have the root privilege provided by OS, and that only the administrator can access the filtering rules.

FMT_MTD.1: The TSF shall restrict the ability to *change_default, query, modify or delete following TSF data to the authorized administrator.*

- Logging information file
- Environment definition file

This requirement is met by AUD.6 that provides the function to change_default, query, modify or delete information in the Logging information file and the Environment definition file defined in AUD.6.

8.5.4 Underlining operating functions

The functional requirements in FPT do not appear in SFs, because those are realised by the underlining operating system. And the functional requirements in FAU_STG.1, FPT_STM.1 and FMT_SMR.1 for the protection of the audit trail, reliable time stamps and the identification of the authorized administrator are also realised by the underlining operating system.

8.6. Strength of Security Functions Consistency

This section shows how the minimum strength of function level for the ST is consistent with the security objectives for the TOE.

This ST claims SOF-medium for the strength of function level of the TOE, as the TOE is used in general commercial systems that may be attacked by intruders with moderate attacks (see 5.1.5).

The TOE assumes that Safegate is physically protected, Safegate is designed or configured solely to act as a firewall on its host, and that OS protects the TOE executable code itself and its resources. Accordingly there are no potential attacks to the TOE directly from the Safegate host inside and the TOE may be attacked only through packets from hostile networks. To counter these threats from hostile networks, IT security objectives require the TOE to provide functions to block unauthorized packets and detect the attacking the Safegate system and the private network system. And non-IT security objectives require the administrator to maintain the sound Safegate environment to meet the secure use assumptions defined by ASM1, ASM3, ASM4, ASM7, ASM8, ASM9 and ASM10. So the TOE can consistently counter against the threats according with IT security objectives and non-IT security objectives.

8.7. Assurance Measures Rational

The evaluation assurance level for this ST is EAL3. See 5.2.