Korean National Protection Profile for Network Device V1.1

2017. 4. 21

The certified Protection Profile is written in Korean. This document is a translation of the original from Korean into English.

Foreword

This Protection Profile has been developed with the support of National Security Research Institute (NSR) under the agreement between National Intelligence Service (NIS) and Ministry of Science, ICT and Future Planning (MSIP). The Protection Profile author presents a set of Common Criteria security requirements compliant with the national security requirements for Network Devices in Korea. The National Cyber Security Center (NCSC) of NIS offered advise for the accurate interpretation of those national security requirements. The Protection Profile includes application notes which give the additional interpretation and guidance for the evaluation and certification based on the Common Criteria, and the separated guidance supporting document (Korean only) for the Protection Profile is provided.

Revision History

Version	Date	Content
1.0	2016.06.10	o First Issue
1.1	2017.04.21	o Delete operation definition in assignment operation of FDP_IFC.2.1 o Add a description of the assignment operation in application notes of FTP_TRP.1 o Other : Correction of content reinforcement, editing error, etc.

Table of Contents

1. PP introduction

1.1. PP reference

Title	Korean National Protection Profile for Network Device
Version	1.1
Evaluation Assurance Level	EAL1+ (ATE_FUN.1)
Developer	National Security Research Institute Telecommunication Technology Association
Common Criteria Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4
Certification Number	KECS-PP-0714a-2016
Keywords	Network device, Switch, Router

1.2. TOE overview

1.2.1. Network device overview

LAN(Local Area Network) is a computer network to intercommunicate the independently operating IT device by connecting within the limited area, a network device transmits the packets from source IT entities to destination IT entities over the LAN communication equipments. Organizations can share the assets and functions by interconnecting the servers, PCs, printers, storage devices, etc. over the LAN. The typical LAN-based network services provided by the network device include a file server, network printer, remote access and management, and email, etc..

In general, LAN does not require the network path settings, but require it in case of a building two more subnetworks according to the internal network scale and purpose. In the organization that deals with a lot of massive network traffic, the LAN is separated by segment unit and connects each segment using the bridge filtering method. And after, switch transmits the packet to the destination by referring the packet address. Depending on the scale of network, there are a variety of the network device including switches, routers, firewalls, VPN gateways, etc.. with different roles in OSI L2 layer to OSI L7 layer. Switches transmit the packet in OSI L2 layer, and routers transmit the packet in OSI L3 layer after setting the optimal routing paths by interconnecting switches.

The recent network device, which are also known as L3 switch, transmits packets based on the IP address in layer 3 instead of existing switching function of transmitting packets in layer 2 based on the MAC address. The L3 switch can perform both the switching function in layer 2 and the routing function in layer 3, and be classified into the switch mounted a router module or a router card.

Both the L3 switch and the router transmit packets through the port connected to the destination by referring the IP address, but unlike the L3 switch that routes and controls packets based on the hardware, the router routes and controls packets based on the software installed in the device.

Upon receipt of the unicast packets without destination address, the multicast and the broadcast packets, the layer 2-based switch performs packet flooding to all ports except for the receiving port, but the L3 switch and the router provide the function that blocks all these packets.

1.2.2. TOE type and scope

The TOE defined in this Protection Profile provides the function that transmits and controls packets and is restricted to L3 or higher layer appliance switches and routers equipped with the network operating system that supports various communication security protocols such as IPSec, SSH, TLS, HTTPS and SNMP v3, etc.. This Protection Profile defines common minimum security requirements that must be provided by the network device.

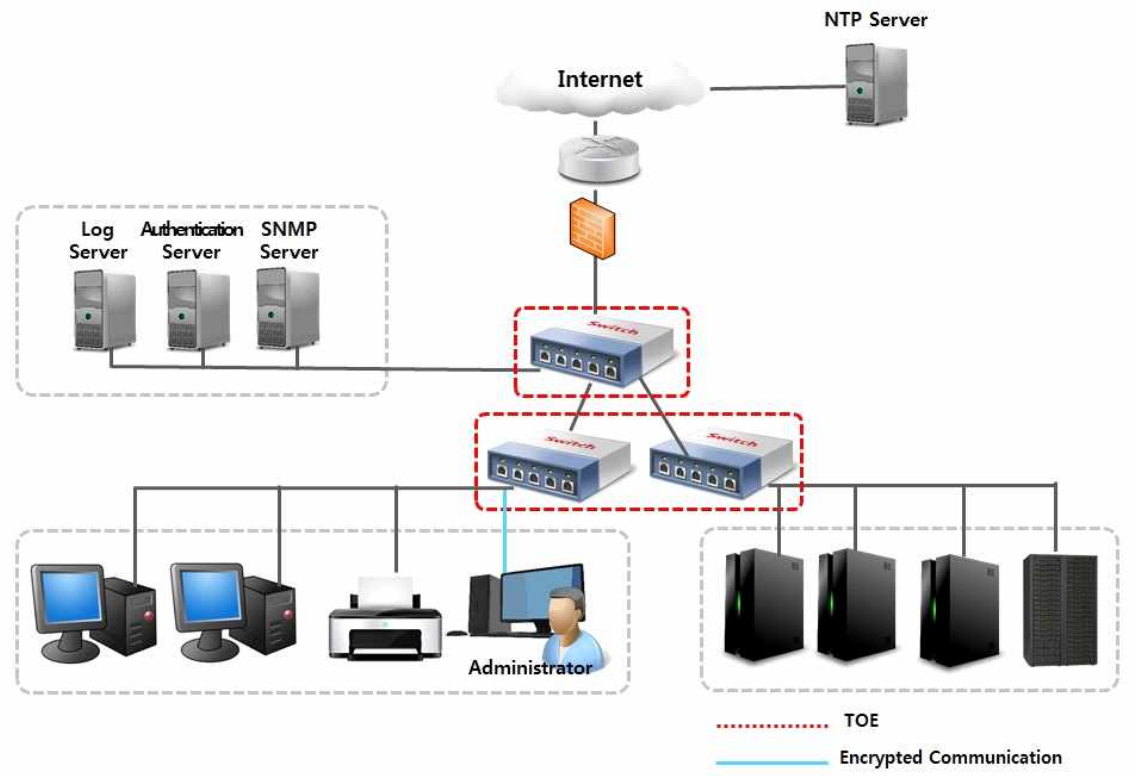
1.2.3. TOE usage and major security features

The TOE controls the traffic and transmits packets in accordance with the rule configured by the administrator in order to protect IT information assets connected to the internal network. The switch, located on the front of various IT device such as server, PC, printer, and storage device, etc., transmits packets sent by the device. The router, on the other hand, located on the junction that connects the network with different data link layers such as Ethernet, token ring, Point-to-Point, and FDDI(Fiber Distributed-Data Interface), transmits incoming packets to the designated destinations. The network traffic handled by the TOE may have different packet structures and security attributes depending on the OSI layer.

The TOE provides a variety of security features: security audit function that records the audit data for the critical events related to the security and management functions, network device administrator identification and authentication function including authentication failures handling, user data protection function that permits or denies corresponding packets based on the IP, port, and protocol of incoming packets in accordance with the rule set by the administrator, protection of data stored in the storage controlled by the TSF, and the TSF protection function such as TSF self-testing and testing of external entities, etc.. In addition, the TOE provides cryptographic support functions including the cryptographic key generation and destruction, and cryptographic operation to support cryptographic communications such as IPSec, TLS, SSH, and HTTPS for management access of administrator, security management functions to define administrator role and configure security functions, the TOE access function to manage the authorized administrator's interacting session, and the trusted path/channel function to provide the secure communications between the TOE and the administrator who accesses for management to it.

1.2.4. Non-TOE and TOE operational environment

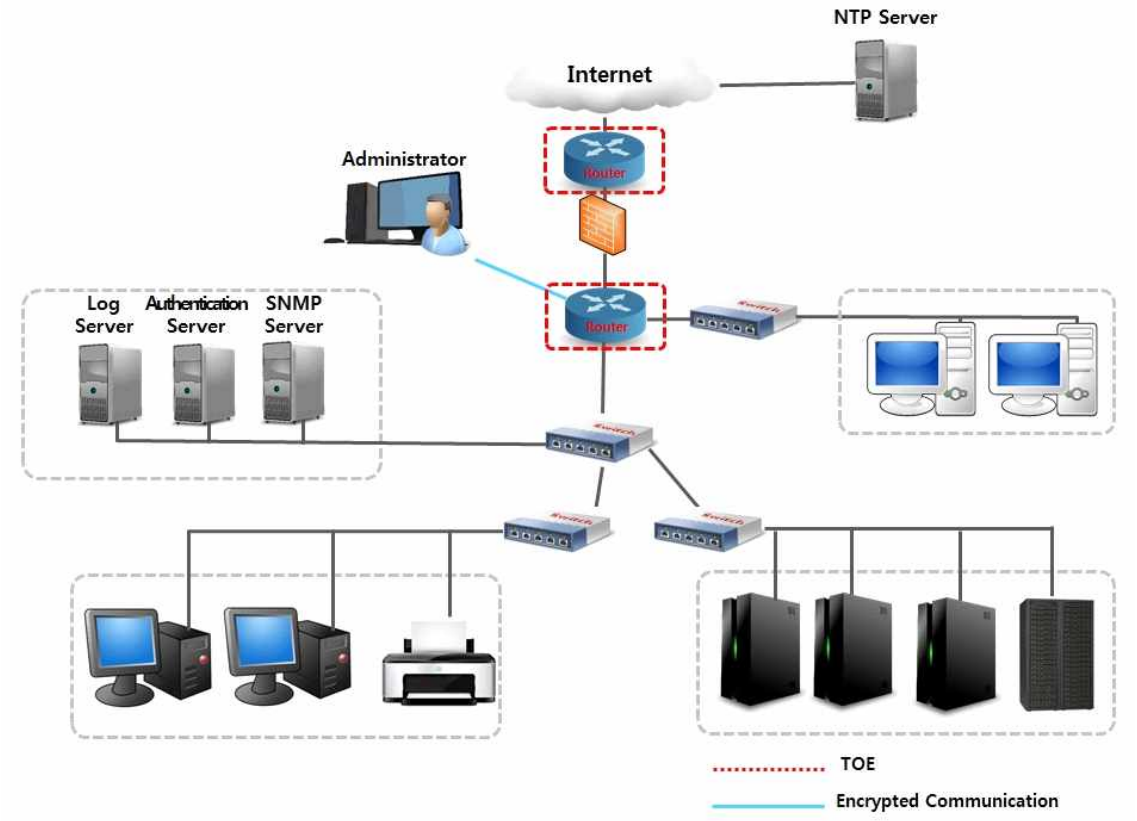
The switch located on the front of various IT device such as the server, PC, printer, and storage device handles packets transmitted by each terminal. The router located on the network junction that connects the different data link layers or between the networks that have different ranges of address handles packets. The operational environment of the switch and the router is as shown in [Fig. 1] and [Fig. 2].



[Fig. 1] Operational environment for switch

The organization's internal network is subdivided using VLAN and the L3 device is used for communications between VLANs. There is no need of router for communications between devices included in the same VLAN, but L3 network device such as L3 switch or router is required for communications between devices with different VLANs.

In the operational environment for switch, there may exist a log server to store and manage the audit data, an authentication server for authenticating administrators, an SNMP server for managing swtch, and an NTP server for synchronizing time. In addition, ST authors may introduce other external entities in the operational environment for switch to perform the security function of the switch. The others except for the switch(TOE) are operational environment.



[Fig. 2] Operational environment for router

The type of router depends on the organization's scale and network class. The operational environment for router can be similar to the switch, but unlike the switch, the router can be installed on the network junction that connects different data link layers. Therefore, the router is used not only to connect the networks with different address ranges but also to connect different types of data link layers such as Ethernet, token rink, Point-to-Point, and FDDI(Fiber Distributed-Data Interface), etc..

The a log server, authentication server, SNMP server and NTP server may exist with the same purpose of the switch. The others except for the router(TOE) are operational environment.

The switch and the router may provide protocols and management functions (e.g. Information flow control function to control in-bounded packets to the network device by the ARP protocol required to transmit traffics from L2 to L3 layer) to handle network traffics, those parts (e.g. routing protocols which are included for efficiency of the router, but are not related to the enforcement of the security functionality) which are not related to the security functional requirements (hereinafter called the "SFR") can be classified into the non-TSF of the TOE with consideration for the physical scope of the TOE, etc..

This PP has been developed considering various types of the TOE implementation. The ST author, which claims conformance to this PP, shall describe any non-TOE hardware, software or firmware required by the TOE to operate.

1.3. Conventions

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

The CC allows several operations to be performed for functional requirements: iteration, assignment, selection and refinement. Each operation is used in this PP.

Iteration

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

Assignment

This is used to assign specific values to unspecified parameters (e.g., password length). The result of assignment is indicated in square brackets like [assignment_value].

Selection

This 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*.

Refinement

This is used to add details and thus further restrict a requirement. The result of refinement is shown in **bold text.**

Security Target (ST) Author

This is used to represent the final decision of attributes being made by the ST author. The ST author's operation is denoted in braces, as in {decided by the ST author}. In addition, operations of SFR not completed in the Protection Profile must be completed by the ST author.

"Application notes" is provided to clarify the intent of requirements, provide the information for the optional items in implementation, define "Pass/Fail" criteria for a requirement. The application notes is provided with corresponding requirements if necessary.

1.4. Terms and definitions

Terms used in this PP, which are the same as in the CC, must follow those in the CC.

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

Measure of the effort to be expended in attacking a TOE expressed as an attacker's expertise, resources and motivation

Augmentation

Addition of one or more requirement(s) to a package

Authentication Data

Information used to verify a user's claimed identity

Authorized Administrator

Authorized user to securely operate and manage the TOE

Authorized user

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

Backbone Switch

Switch installed to the entry point of all network traffic passing through interconnects sever and other network devices

Can/could

The 'can' or 'could' presented in application notes indicates optional requirements applied to the TOE by ST author's choice

Class

Set of CC families that share a common focus

Component

Smallest selectable set of elements on which requirements may be based

Dependency

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

Indivisible statement of a security need

Evaluation Assurance Level (EAL)
Set of assurance requirements drawn from CC Part 3, representing a point on the CC predefined assurance scale, that form an assurance package

External Entity
Human or IT entity possibly interacting with the TOE from outside of the TOE boundary

Family
Set of components that share a similar goal but differ in emphasis or rigour

Identity
Representation uniquely identifying entities (e.g. user, process or disk) within the context of the TOE

Iteration
Use of the same component to express two or more distinct requirements

Local access
The access to the TOE by using the console port to manage the TOE by administrator, directly

L3 Switch
Network device that transmits the packet to the destination referred the IP address on layer 3. It is a switch with routing function which provides the connections and communications between VLAN

Management access
The access to the TOE by using the HTTPS, SSH, TLS, IPSec, etc. to manage the TOE by administrator, remotely

Object
Passive entity in the TOE containing or receiving information and on which subjects perform operations

Operation (on a component of the CC)
Modification or repetition of a component. Allowed operations on components are assignment, iteration, refinement and selection

Operation (on an object)
Specific type of action performed by a subject on an object

Organizational Security Policies
Set of security rules, procedures, or guidelines for an organization wherein the set is currently given by actual or virtual organizations, or is going to be given

Protection Profile (PP)

Implementation-independent statement of security needs for a TOE type

Port

Physical connection port on the outside of network device

Recommend/be recommended

The 'recommend' or 'be recommended' presented in application notes is not mandatorily recommended, but required to be applied for secure operations of the TOE

Refinement

Addition of details to a component

Role

Predefined set of rules on permissible interactions between a user and the TOE

Routing

The process of path selection from source to destination in a network based on the IP address

Routing Protocol

The protocol used for the exchange of routing information between routers and maintenance of routing path table(e.g. RIP, OSPF, BGP, etc.)

Router

Network device that connects two or more independent networks or divides networks. It transmits network traffic to the destination by referring the optimal path depending on the routing algorithm based on network path/routing table

Security Target (ST)

Implementation-dependent statement of security needs for a specific identified TOE

Selection

Specification of one or more items from a list in a component

Shall/must

The 'shall' or 'must' presented in application notes indicates mandatory requirements applied to the TOE

Subject

Active entity in the TOE that performs operations on objects

Target of Evaluation (TOE)

Set of software, firmware and/or hardware possibly accompanied by guidance

Threat Agent

Entity that can adversely act on assets

TOE Security Functionality (TSF)

Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs

TSF Data

Data for the operation of the TOE upon which the enforcement of the SFR relies

User

See "external entity", a user means administrator in network device

1.5. PP organization

Chapter 1 introduces to the Protection Profile, providing Protection Profile references and the TOE overview.

Chapter 2 provides the conformance claims to the CC, PP and package; and describes the claim's conformance rationale and PP conformance statement.

Chapter 3 describes the security objectives for the operational environment.

Chapter 4 defines the extended components for the network device.

Chapter 5 describes the security functional and assurance requirements. If required, application notes are provided to clarify the meaning of requirements and provide an explanation of detailed guidelines to the ST author for correct operations.

Reference describes the references for users who need more information about the background and related information than those described in this PP.

Abbreviated terms are listed to define frequently used terms in the PP.

2. Conformance claim

2.1. CC conformance claim

CC		Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4 • Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and General Model, Version 3.1, Revision 4 (CCMB-2012-09-001, Sep, 2012) • Common Criteria for Information Technology Security Evaluation. Part 2: Security Functional Components, Version 3.1, Revision 4 (CCMB-2012-09-002, Sep, 2012) • Common Criteria for Information Technology Security Evaluation. Part 3: Security Assurance Components, Version 3.1, Revision 4 (CCMB-2012-09-003, Sep, 2012)
Conformance claim	Part 2 Security functional components	Extended: FMT_PWD.1, FPT_PST.1, FPT_TUD.1, FTA_SSL.5
	Part 3 Security assurance components	*Conformant*
	Package	Augmented : EAL1 *augmented* (ATE_FUN.1)

2.2. PP conformance claim

This Protection Profile does not claim conformance to other PPs.

2.3. Package conformance claim

This Protection Profile claims conformance to assurance package EAL1 augmented with ATE_FUN.1.

2.4. Conformance claim rationale

Since this Protection Profile does not claim conformance to other Protection Profiles, it is not necessary to describe the conformance claim rationale.

2.5. PP conformance statement

This Protection Profile requires "strict PP conformance" of any ST or PP, which claims conformance to this PP.

3. Security objectives

The followings are the security objectives handled by technical and procedural method supported from operational environment in order to provide the TOE security functionality accurately.

3.1. Security objectives for the operational environment

OE.PHYSICAL_CONTROL

The TOE shall be located in physically secure environment to which only the authorized administrator is allowed to access and the protective facilities are provided.

OE.SECURITY_MAINTENANCE

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

OE.TRUSTED_ADMIN

The authorized administrator of TOE shall be non-malicious users, have appropriately trained for TOE management functions and accurately fulfill the duties in accordance with administrator guidance.

OE.PATCH_MANAGEMENT

The authorized administrator regularly applies the latest patches for the firmware of network device and software used in the device. If the source of patch files can not be verified, the installation of patch files shall be restricted. After updates, the authorized administrator checks that disused or unnecessary services are disabled and blocks the interfaces connected to the disused port.

OE.LOG_BACKUP

The authorized administrator periodically checks a spare space of audit data storage in case of the audit data loss, and carries out the audit data backup (external log server or separate storage device, etc.) to prevent audit data loss.

4. Extended components definition

4.1. Security management

4.1.1. ID and password

Family Behaviour

This family defines the capability that is required to control ID and password management used in the TOE, and set or modify ID and/or password by authorized users.

Component levelling

FMT_PWD.1 ID and password management, requires that the TSF provides the management function of ID and password.

Management: FMT_PWD.1

The following actions could be considered for the management functions in FMT:

a) Management of ID and password configuration rules.

Audit: FMT_PWD.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: All changes of the password.

4.1.1.1. FMT_PWD.1 Management of ID and password

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

FMT_PWD.1.1 The TSF shall restrict the ability to manage the password of [assignment: *list of functions*] to [assignment: *the authorized identified roles*].

1. [assignment: *password combination rules and/or length*]

2. [assignment: *other management such as management of special characters unusable for password, etc.*]

FMT_PWD.1.2 The TSF shall restrict the ability to manage the ID of [assignment: *list of functions*] to [assignment: *the authorized identified roles*].

1. [assignment: *ID combination rules and/or length*]
2. [assignment: *other management such as management of special characters unusable for ID, etc.*]

FMT_PWD.1.3 The TSF shall provide the capability for [selection, choose one of: *setting ID and password when installing, setting password when installing, changing the ID and password when the authorized administrator accesses for the first time, changing the password when the authorized administrator accesses for the first time*].

Application notes

- o If the TOE does not provide the capability for managing the ID and password combination rules by authorized roles, etc., 'none.' may be specified in assignment operations of FMT_PWD.1.1, FMT_PWD.1.2.
- o The ID and password combination rules that can be set by authorized roles may include minimum and maximum length setting, mixing rule setting involving English upper case/lower case/number/special characters, etc..

4.2. Protection of the TSF

4.2.1. Protection of stored TSF data

Family Behaviour

This family defines rules to protect TSF data stored within containers controlled by the TSF from the unauthorized modification or disclosure.

Component levelling

FPT_PST: Protection of stored TSF data	1

FPT_PST.1 Basic protection of stored TSF data, requires the protection of TSF data stored in containers controlled by the TSF.

Management: FPT_PST.1

There are no management activities foreseen.

Audit: FPT_PST.1

There are no auditable events foreseen.

4.2.1.1. FPT_PST.1 Basic protection of stored TSF data

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PST.1.1 The TSF shall protect [assignment: *TSF data*] stored in containers controlled by the TSF from the unauthorized [selection: *disclosure, modification*].

Application notes

o Containers controlled by the TSF mean storage in the TOE or external entities (DBMS, etc.) that interact with the TOE.

o Examples of TSF data to be protected as follows:

- User password, cryptographic key (pre-shared key, symmetric key, private key), TOE configuration values (security policy, configuration parameters), audit data, etc.

o The TSF data can be encrypted and stored, controlled to be accessed, or hided to be protected from the unauthorized disclosure.

4.2.2. TSF update

Family Behaviour

This family defines TOE firmware/software update requirements.

Component levelling

FPT_TUD: TSF update	1

FPT_TUD.1 TSF security patch update, requires trusted update of the TOE firmware/software including the capability to verify the validity on the update file before installing updates.

Management: FPT_TUD.1

The following actions could be considered for the management functions in FMT:

a) Management of update file verification mechanism

Audit: FPT_TUD.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: Update file verification result (success, failure)

4.2.2.1. FPT_TUD.1 TSF security patch update

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TUD.1.1 The TSF shall provide the capability to view the TOE versions to [assignment: *the authorized identified roles*].

FPT_TUD.1.2 The TSF shall verify validity of the update files using [selection: *hash value comparison, digital signature verification*] before installing updates.

Application notes

- o The TSF shall provide the capability to check the current version of the firmware/software that most recently installed and executed by authorized roles.
- o The latest updates and security patches are essential to remove security vulnerabilities. The validity verification on the update files is required since the installation of update files without any verification can result in system malfunction, or service failures, etc..

4.3. TOE access

4.3.1. Session locking and termination

Family Behaviour

This family defines requirements for the TSF to provide the capability for TSF-initiated and user-initiated locking, unlocking, and termination of interactive sessions.

Component levelling

In CC Part 2, the session locking and termination family consists of four components. In this PP, it consists of five components by extending one additional component as follows.

※ The relevant description for four components contained in CC Part 2 is omitted.

FTA_SSL.5 The management of TSF-initiated sessions, provides requirements that the TSF locks or terminates the session after a specified time interval of user inactivity.

Management: FTA_SSL.5

The following actions could be considered for the management functions in FMT:

a) Specification for the time interval of user inactivity that is occurred the session locking and termination for each user

b) Specification for the time interval of default user inactivity that is occurred the session locking and termination

Audit: FTA_SSL.5

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: Locking or termination of interactive session

4.3.1.1. FTA_SSL.5 Management of TSF-initiated sessions

Hierarchical to: No other components.

Dependencies: [FIA_UAU.1 authentication or No dependencies.]

FTA_SSL.5.1 The TSF shall [selection:

- *lock the session and/or re-authenticate the user before unlocking the session,*
- *terminate*] an interactive session after a [assignment: time interval of user inactivity].

Application notes

o This requirement may be applied to the local access and management access of users (SSH, HTTPS, etc.).

5. Security requirements

The security requirements specify security functional requirements and assurance requirements that must be satisfied by the TOE that claims conformance to this PP.

The security functional requirements included in this PP are derived from CC Part 2 and Chapter 4 Extended components definition.

In addition, the security functional requirements are classified into mandatory SFRs and optional SFRs, as follows.

- Mandatory SFRs: are required to be mandatorily implemented in the network device.
- Optional SFRs: are not required to be mandatorily implemented in the network device. However, when the TOE additionally provides related capabilities, the ST author must include the corresponding SFRs.

The following table summarizes the security functional requirements used in the PP.

Security functional class	Security functional component		Mandatory SFR / Optional SFR
FAU	FAU_GEN.1	Audit data generation	**Mandatory SFR**
	FAU_SEL.1	Selective audit	Optional SFR
	FAU_STG.1	Protected audit trail storage	**Mandatory SFR**
	FAU_STG.3	Action in case of possible audit data loss	**Mandatory SFR**
FCS	FCS_CKM.1	Cryptographic key generation	**Mandatory SFR**
	FCS_CKM.2	Cryptographic key distribution	Optional SFR
	FCS_CKM.4	Cryptographic key destruction	**Mandatory SFR**
	FCS_COP.1	Cryptographic operation	**Mandatory SFR**
FDP	FDP_IFC.2	Complete Information flow control	**Mandatory SFR**
	FDP_IFF.1	Simple security attributes	**Mandatory SFR**
FIA	FIA_AFL.1	Authentication failure handling	**Mandatory SFR**
	FIA_SOS.1	Verification of secrets	**Mandatory SFR**
	FIA_UAU.1	Timing of authentication	**Mandatory SFR**
	FIA_UAU.6	Re-authenticating	Optional SFR
	FIA_UAU.7	Protected authentication feedback	**Mandatory SFR**
	FIA_UID.1	Timing of identification	**Mandatory SFR**
FMT	FMT_MOF.1	Management of security functions behaviour	**Mandatory SFR**
	FMT_MSA.1	Management of security attributes	**Mandatory SFR**

Security functional class	Security functional component		Mandatory SFR / Optional SFR
	FMT_MSA.3	Static attribute initialization	**Mandatory SFR**
	FMT_MTD.1	Management of TSF data	**Mandatory SFR**
	FMT_PWD.1(Extended)	Management of ID and password	**Mandatory SFR**
	FMT_SMF.1	Specification of management functions	**Mandatory SFR**
	FMT_SMR.1	Security roles	**Mandatory SFR**
FPT	FPT_PST.1(Extended)	Basic protection of stored TSF data	**Mandatory SFR**
	FPT_STM.1	Reliable time stamps	**Mandatory SFR**
	FPT_TEE.1	Testing of external entities	**Mandatory SFR**
	FPT_TST.1	TSF testing	**Mandatory SFR**
	FPT_TUD.1(Extended)	TSF security patch update	**Mandatory SFR**
FTA	FTA_MCS.2	Per user attribute limitation on multiple concurrent sessions	Optional SFR
	FTA_SSL.5(Extended)	Management of TSF-initiated sessions	**Mandatory SFR**
	FTA_TSE.1	TOE session establishment	**Mandatory SFR**
FTP	FTP_ITC.1	Inter-TSF trusted channel	Optional SFR
	FTP_TRP.1	Trusted path	**Mandatory SFR**

[Table 1] Security functional requirements

5.1. Security functional requirements (Mandatory SFRs)

The network device that claims conformance to this PP must meet the following 'Mandatory SFRs'. The terms 'Refinement' and 'Iteration' in the remark field are correspond to the operations of CC component.

Security functional class	Security functional component		Remark
FAU	FAU_GEN.1	Audit data generation	
	FAU_STG.1	Protected audit trail storage	
	FAU_STG.3	Action in case of possible audit data loss	
FCS	FCS_CKM.1	Cryptographic key generation	
	FCS_CKM.4	Cryptographic key destruction	
	FCS_COP.1	Cryptographic operation	
FDP	FDP_IFC.2	Complete Information flow control	
	FDP_IFF.1	Simple security attributes	

Security functional class	Security functional component		Remark
FIA	FIA_AFL.1	Authentication failure handling	
	FIA_SOS.1	Verification of secrets	
	FIA_UAU.1	Timing of authentication	Refinement
	FIA_UAU.7	Protected authentication feedback	Refinement
	FIA_UID.1	Timing of identification	Refinement
FMT	FMT_MOF.1	Management of security functions behaviour	Refinement
	FMT_MSA.1	Management of security attributes	Refinement
	FMT_MSA.3	Static attribute initialization	Refinement
	FMT_MTD.1	Management of TSF data	Refinement
	FMT_PWD.1(Extended)	Management of ID and password	Extended
	FMT_SMF.1	Specification of management functions	
	FMT_SMR.1	Security roles	Refinement
FPT	FPT_PST.1(Extended)	Basic protection of stored TSF data	Extended
	FPT_STM.1	Reliable time stamps	
	FPT_TEE.1	Testing of external entities	Refinement
	FPT_TST.1	TSF testing	Refinement
	FPT_TUD.1(Extended)	TSF security patch update	Extended, Refinement
FTA	FTA_SSL.5(Extended)	Management of TSF-initiated sessions	Extended, Refinement
	FTA_TSE.1	TOE session establishment	Refinement
FTP	FTP_TRP.1	Trusted path	Refinement

[Table 2] Mandatory security functional requirements

5.1.1. Security audit

5.1.1.1. 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) [Refer to the "auditable event" in [Table 3] Audit events, [assignment: *other specifically defined auditable events*]].

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 PP/ST [Refer to the contents of "additional audit record" in [Table 3] Audit events, [assignment: *other audit relevant information*]].

Application notes

o The ST author shall perform assignment operation of FAU_GEN.1.1 with the audit records supported by the TOE using following table. But, it is strongly recommended to record audit data of critical events related to the operation of the TOE security functionality.

o If the audit function is working as a part of the major process in the TOE, 'start-up' of the audit function may be recorded within the audit record which is the start-up of major processes after the initial start-up of the TOE. 'Shutdown' of the audit function may be replaced with the function-level event similar to 'start-up' (e.g. audit records of process termination, etc.) or lower-level event (e.g. audit records of device shutdown, etc.).

o The audit records shall include the date and time of the event, type of event, subject identity (e.g. account, IP, etc.), and the outcome (success or failure) of the event.

Security functional component	Auditable event	Additional audit record
FIA_UAU.1	All use of the authentication mechanism	
FIA_UID.1	All use of the user identification mechanism, including the user identity provided	
FMT_MOF.1	All modifications in the behaviour of the functions in the TSF	
FMT_MSA.1	All modifications of the values of security attributes	
FMT_MSA.3	Modifications of the default setting of permissive or restrictive rules, All modifications of the initial values of security attributes	
FMT_MTD.1	All modifications to the values of TSF data	Modified TSF data
FMT_SMR.1	Modifications to the group of users that are part of	

Security functional component	Auditable event	Additional audit record
	a role	
FMT_PWD.1	All changes of the password	
FPT_TUD.1	Update file verification result (success, failure)	Cause of verification failure

[Table 3] Audit events

5.1.1.2. 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.

Application notes

- o The capability that allows only an authorized administrator can access to the audit records shall be provided.
- o An unauthorized access to the audit records by using the activated other service shall be totally blocked in the network device.

5.1.1.3. 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 **[** Notification to the authorized administrator, [assignment: *actions to be taken in case of possible audit storage failure*] if the audit trail exceeds [assignment: *pre-defined limit*]].

Application notes

- o The capability to notify that the amount of the audit trail exceeds the certain limit of disk capacity shall be provided for the administrator.
  - Method (e.g. alarms, LED display, sending the Syslog/SNMP, etc.)
  - Threshold information (e.g. 90%, etc.)
- o In case of possible audit data loss, the capability that audit records are transmitted to the external log server and backup server may be provided. When this capability is provided with secure communication, refer to 'Optional SFR' FTP_ITC.1 for more details.

5.1.2. Cryptographic support

5.1.2.1. FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *cryptographic key generation algorithm*] and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

Application notes

o This SFR is related to the cryptographic key generation for the IPsec, TLS, SSH, HTTPS, etc. to support the confidentiality and integrity of the administrator's management access, or cryptographic operation when storing the critical data. The ST author is recommended to perform iteration operation in accordance with the cryptographic algorithms provided by the TOE.

o In cryptographic communication protocol such as IPSec, TLS, SSH, HTTPS, etc., entities generate the asymmetric cryptographic key to establish the key between the communication entities. This requirement is defined in FCS_CKM.1, and key establishment protocol is defined in 'Optional SFR' FCS_CKM.2. If the TOE's role is to receive an asymmetric key in key establishment procedure, there is no need to generate the key.

o The cryptographic algorithm and cryptographic key sizes are recommended to meet the cryptographic complexity of 112 bits or more. In addition, it is recommended to use the cryptographic algorithm validated in Korea Cryptographic Module Validation Program (KCMVP).

5.1.2.2. FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *cryptographic key destruction method*] that meets the following: [assignment: *list of standards*].

5.1.2.3. FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

Application notes

o In cryptographic operation, it is recommended to perform iteration operation on FCS_COP.1 according to the used cryptographic algorithm (symmetric key, asymmetric key, hash, keyed-hash, etc.).

e.g. FCS_COP.1(1) Cryptographic operation (Symmetric key cryptographic operation)

FCS_COP.1(2) Cryptographic operation (MAC)

FCS_COP.1(3) Cryptographic operation (Hash)

FCS_COP.1(4) Cryptographic operation (Digital signature generation)

FCS_COP.1(5) Cryptographic operation (Digital signature verification)

o It is recommended to use cryptographic and hash algorithm which meet the cryptographic complexity of 112 bits or more.

- Hash: SHA-224/256/384/512, etc.
- Symmetric key cryptography: SEED, ARIA-128/192/256, etc.
- Public key cryptography: RSA 2048, etc.
- Digital signature: RSA-PSS-2048/3072, ECDSA/KCDSA/EC-KCDSA, etc.

o It is recommended to use the cryptographic algorithm validated in Korea Cryptographic Module Validation Program (KCMVP).

5.1.3. User data protection

5.1.3.1. FDP_IFC.2 Complete information flow control

Hierarchical to: FDP_IFC.1 Subset information flow control

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.2.1 The TSF shall enforce the [assignment: *information flow control SFP*] on [

The following lists of subjects and information] and all operations that cause that information to flow to and from subjects covered by the SFP.

[

- Subjects: IT entities that transmit and receive the information through the TOE
- Information: Packets transmitted through the TOE

]

FDP_IFC.2.2 The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

Application notes

o The network device that works on the network layer (L3 Layer) controls network packets by setting the IP address-based network paths. A server or a network device may be a subject of the network layer.
o The network device that works on the transport layer (L4 Layer) controls segments to transmit the data suitable for the network protocols (e.g. DNS, SNMP, SSH, DHCP, HTTPS, etc.) between hosts based on TCP/UDP ports. A subject of the transport layer is the servers interconnected through the network protocol.
o The subject of the session layer (L5, L6, L7 Layer) or higher may be a user who requested service or a client eligible to become an administrator.
o As above, due to the difference in attributes of packet header and the subject types depending on the operating layer of a network device, information flow control policies can be defined multiple times using iteration operation.
o The TOE shall mandatorily provide the ACL(Access Control List) as part of the information flow control policy. If it provides a variety of ACL functions such as standard ACL and extended ACL, it shall be defined as the assignment operation in FDP_IFC.2.1.
  - Standard ACL: controls traffic by checking the source address only (permit or deny)
  - Extended ACL: controls traffic by checking both the source address and destination address (permit or deny)
o If the TOE supports the VLAN, the ST author may define VLAN information flow control policy(VLAN ACL) using the assignment operation in FDP_IFC.2.1, and perform the iteration operation if it is required to differentiate it from the existing information flow control policy.
o In case of using the SNMP service, the unauthorized access may be blocked by permitting only the designated IP's access defined in that policy.
o If the TOE provides both IPv4 and IPv6, the ST author shall present the information flow control policy to be configured in IPv4 and IPv6 respectively.

5.1.3.2. FDP_IFF.1 Simple security attributes

Hierarchical to: No other components.

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

FDP_IFF.1.1 The TSF shall enforce the [assignment: *information flow control SFP*] based on the following types of subject and information security attributes: [The following list of subjects and information presented in FDP_IFC.2, and for each following security attributes].

[

- Subject: IT entities that transmit and receive data through the TOE, [assignment: *subject security attributes*]
- Information: Packets transmitted through the TOE, [assignment: *information security attributes*]

]

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

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

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: [assignment: *rules, based on security attributes, that explicitly authorize information flows*].

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

Application notes

o The security attributes which must be presented as one of the information flow control rules according to the operating layer of the TOE are as follow.

- L3 device : IP Address(Source, Destination)
- L4 device : IP Address(Source, Destination), Port(Source, Destination)
- L5 device and/or higher : IP Address(Source, Destination), Port(Source, Destination), Protocol

o As above, due to the difference in attributes of packet header and the subject types depending on the operating layer of the TOE, information flow control policies can be defined multiple times using iteration operation.

o The TOE optionally implements the VLAN function and interacts with separate authentication server.

- Referred standard: IEEE Std 802.1q-2011(Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks), or over

  IEEE Std 802.1X-2010(Port Based Network Access Control), or over

o For example, the denial rules which block the following network attacks are defined in FDP_IFF.1.5 assignment operation.

- Network Layer: ICMP Router Redirection, IP Spoofing, ARP Spoofing, ARP Redirect, ARP Cache Poisoning, LAND Attack, Ping of Death, smurf, Directed Broadcast Attack, etc.
- Transfer Layer: Syn Flooding, UDP Flooding, etc.
- Over the Session Layer: DNS Spoofing, RUDY(R-U-Dead-Yet) Attack, Slowloris, SQL Query Attack, etc.

o In FDP_IFF.1.3 and FDP_IFF.1.5, rules blocking such as anomalous packets may be specified. The anomalous packets mean those packets which are not TCP/IP packets defined in IETF RFC791, RFC792, RFC793, etc., and it can be spoofed packets, looping packets, packets which is not configured with the TCP flag, etc.. Additionally, the spoofing packet that source address IP is set as broadcast, or multicast loopback may be included.

o In case of using the SNMP service, the unauthorized access may be blocked by permitting only the designated IP's access defined in that policy.

o If the TOE provides both IPv4 and IPv6, the ST author shall present the packet controlled in IPv4 and IPv6 respectively.

5.1.4. Identification and authentication

5.1.4.1. 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 [selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].

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

Application notes

o In this SFR, a capability that restricts accesses to the TOE when the defined number of unsuccessful authentication attempts has been met shall be required, and this shall be applied to the local access(console port) and the management access(SSH, etc.) supported

by the TOE.

- o The number and time(e.g., time period for account locking) of authorized administrator's authentication failure may be fixed value (number of failures: 5 times or less, time period: 5 minutes or more) in the TOE, or configurable by the authorized administrator.
- o If the number of authentication failure and actions are set differently depending on the TOE user, services(e.g. SSH), etc., the ST author may apply the iteration operation.
- o In the event of consecutive authentication failure, the examples of actions may include the account locking, the time limit for re-authentication, etc.. However, if the most privileged administrator's account is locked, it is automatically unlocked after a certain period of time to prevent the situation that administrator's account is totally not available.

5.1.4.2. FIA_SOS.1 Verification of secrets

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [assignment: *a defined quality metric*].

Application notes

- o Verification of secrets may be applied in every creation and change of all passwords, such as changing passwords, creating a password of new administrator, and changing passwords at first access by the administrator. This requirement shall be applied to the local access(console port) and the management access(SSH, etc.) supported by the TOE.
- o The ST author can define the password combination rules and length, etc. in [assignment: *a defined quality metric*] of FIA_SOS.1.1, but password shall be able to be composed of combination of English upper/lower case letters/numbers/special characters and support 9 characters or more. And, this requirement is applied to the followings.
  - Administrator's password(local and management access)
  - Pre-shared key for interacting with an authentication server
  - SNMP authentication password
  - SNMP privacy password
- o In case of creation and change of passwords, password can be input 15 characters or more.
- o When deciding the password complexity verification method based on administrator-defined permission criteria, "*Administrator-defined permission criteria in FMT_PWD.1*" shall be defined in assignment operation.

5.1.4.3. FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

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

FIA_UAU.1.2 The TSF shall require each **administrator** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of **the administrator.**

Application notes

- o A user of network device is an administrator that operates management functions of the TOE, and administrator roles may be divided into multiple roles depending on the management function of access privileges. When dividing the administrator roles into multiple roles, requirements shall be defined in FMT_SMR.1. This requirement shall be applied to the local access(console port) and the management access(SSH, etc.) supported by the TOE.
- o In case of the password-based authentication method, identification and authentication are carried out simultaneously and thus 'list of TSF mediated actions' is the same defined in FIA_UID.1. In case of the certificate-based authentication, the function that enumerates the certificate list and stored certificate location/devices selection before identification and authentication can be provided. Therefore, the ST author shall consider the function list according to the authentication method supported by the TOE before identification and authentication, and perform the assignment operation.
- o If no actions are appropriate in assignment operation of FIA_UAU.1.1, it is recommended to use FIA_UAU.2 which is in a hierarchical relationship with FIA_UAU.1.

5.1.4.4. 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 [masked password input, [selection, choose one of: *No feedback about the failure reason when unsuccessful authentication attempts, none*]] to **the administrator** while the authentication is in progress.

Application notes

- o The input password shall be masked to make it unrecognizable and the followings are masked. Methods such as concealing user's input password on the screen are acceptable for preventing the input password disclosure. This requirement shall be applied to the local access(console port) and the management access(SSH, etc.) supported by the TOE.
  - When generating and changing the administrator's password

- When authenticating the administrator

o In case of identification and authentication failures, the TOE shall not provide the feedback for the cause of failure (e.g. You have inputted an incorrect account or password, etc.), and this may be optionally applied. It may be applicable to local access(console port) and management access(SSH, etc.) supported by the TOE.

5.1.4.5. FIA_UID.1 Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow [assignment: *list of TSF-mediated actions*] on behalf of **the administrator** to be performed before **the administrator** is identified.

FIA_UID.1.2 The TSF shall require each **administrator** to be successfully identified before allowing any other TSF-mediated actions on behalf of **the administrator.**

Application notes

o A user of network device is an administrator that operates management functions of the TOE, and administrator roles may be divided into multiple roles depending on the management function of access privileges. When dividing the administrator roles into multiple roles, requirements shall be defined in FMT_SMR.1. This requirement shall be applied to the local access(console port) and the management access(SSH, etc.) supported by the TOE.

o If no actions are appropriate in assignment operation of FIA_UID.1.1, it is recommended to use FIA_UID.2 which is in a hierarchical relationship with FIA_UID.1.

5.1.5. Security management

Security functional component	Management function	Management type
FAU_STG.3	Maintenance of the threshold	Management of TSF data threshold
	Maintenance (deletion, modification, addition) of actions to be taken in case of imminent audit storage failure	Management of security functions
FDP_IFF.1	Managing the attributes used to make explicit access based decisions	Management of security attributes
FIA_AFL.1	Management of the threshold for unsuccessful authentication attempts	Management of TSF data threshold

Security functional component	Management function	Management type
	Management of actions to be taken in the event of an authentication failure	Management of security functions
FIA_SOS.1	Management of the metric used to verify the secrets	Management of security functions
FIA_UAU.1	Management of the authentication data by an administrator Management of the authentication data by the associated user	Management of TSF data
	Management of the list of actions that can be taken before the user is authenticated	Management of security functions
FIA_UID.1	Management of the user identities	Management of TSF data
	If an authorized administrator can change the actions allowed before identification, the managing of the action lists	Management of security functions
FMT_MOF.1	Management of the group of roles that can interact with the functions in the TSF	Management of security roles
FMT_MSA.1	Management of the group of roles that can interact with the security attributes	Management of security roles
	Management of rules by which security attributes inherit specified values.	Management of security attributes
FMT_MSA.3	Management of the group of roles that can specify initial values	Management of security roles
	Management of the permissive or restrictive setting of default values for a given access control SFP Management of rules by which security attributes inherit specified values	Management of security attributes
FMT_MTD.1	Management of the group of roles that can interact with the TSF data	Management of security roles
FMT_PWD.1	Management of ID and password configuration rules	Management of security functions
FMT_SMR.1	Management of the group of users that are part of a role.	Management of security roles
FPT_STM.1	Management of the time	Management of security functions
FPT_TEE.1	Management of the conditions under which the testing	Management of TSF

Security functional component	Management function	Management type
	of external entities occurs, such as during initial start-up, regular interval, or under specified conditions Management of the time interval if appropriate	data
FPT_TST.1	Management of the conditions under which TSF self testing occurs, such as during initial start-up, regular interval, or under specified conditions Management of the time interval if appropriate	Management of TSF data
FPT_TUD.1	Management of update file verification mechanism	Management of security functions
FTA_SSL.5	Specification for time interval of user inactivity that is occurred the session locking and termination for each user Specification for the default time interval of user inactivity that is occurred the session locking and termination	Management of TSF data
FTA_TSE.1	Management of the session establishment conditions by the authorized administrator	Management of TSF data
FTP_TRP.1	Configuring the actions that require trusted path, if supported	Management of security functions

[Table 4] Security management action and management type by component

5.1.5.1. FMT_MOF.1 Management of security functions behavior

Hierarchical to: No other components.

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

FMT_MOF.1.1 The TSF shall restrict the ability to ***conduct management actions*** of the functions [assignment: *list of functions*] to [the authorized administrator].

Application notes

o "Management action" to which a refinement operation is applied includes the ability to determine the behavior, disable, enable, modify the behavior of some functions in the TSF. This requirement shall be applied to the local access(console port) and management access(SSH, etc.) supported by the TOE.

o The action that adds, deletes or modifies conditions or rules capable of determining the security functions behavior is included in the management of security functions behaviors. And, the action that adds, deletes or modifies behaviors taken by the TSF according to the

corresponding conditions and rules is also included in the management of security functions behaviors. In addition, the action of selecting mechanism, protocol, etc., when there are variously provided to support the same purpose, is included in the management of security functions behavior because it corresponds to the modification of behavior.

- o The ST author may perform assignment operation in FMT_MOF.1.1 with reference to '[Table 4] security management action and management type by component' for the case that the TOE supports management functions.
- o The ST author may define additional management actions of security function for each component in addition to management functions which are presented in '[Table 4] security management action and management type by component'. Management actions of security function may be included for the additional or extended requirements.

5.1.5.2. FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

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

FMT_MSA.1.1 The TSF shall enforce the [assignment: ***information flow control SFP(s)***] to restrict the ability to [selection: *change_default, query, modify, delete, [assignment: other operations]*] the security attributes [assignment: *list of security attributes]* to [the authorized administrator].

Application notes

- o The ST author shall define FMT_MSA.1.1 assignment operation with reference to '[Table 4] security management action and management type by component' if the TOE supports security attribute management functions. This requirement shall be applied to the local access(console port) and management access(SSH, etc.) supported by the TOE.
- o The TOE shall provide the ability that administrator maintains the packet denial rules to block the basic network attacks.
- o The ST author may define additional security attribute management actions for each component in addition to management function that are presented in '[Table 4] security management action and management type by component', and present security attribute management actions for additional or extended requirements in addition to security functional requirements stated in this document.

5.1.5.3. 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 [assignment: ***information flow control SFP***] to provide [selection, choose one of: *restrictive, permissive, [assignment: other property]*] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the [the authorized administrator] to specify alternative initial values to override the default values when an object or information is created.

5.1.5.4. FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of management functions

FMT_MTD.1.1	The TSF shall restrict the ability to ***manage*** the [assignment: *list of TSF data*] to [the authorized administrator].

Application notes

- o "Manage" to which a refinement operation is applied includes the ability to change default, query, modify, delete, clear, other operation, etc.. This requirement shall be applied to the local access(console port) and management access(SSH, etc.) supported by the TOE.
- o The ST author may perform assignment operation in FMT_MTD.1.1 with reference to '[Table 4] security management action and management type by component', for the case that a TOE supports the TSF data management function.
- o The ST author may define additional TSF data management actions for each component in addition to management function that are presented in '[Table 4] security management action and management type by component', and present TSF data management actions for additional or extended requirements in addition to security functional requirements stated in this document. For example, the configuration of device access time limit when the consecutive unsuccessful authentication attempts can be included in management actions.
- o The TOE can provide the ability to restrict that only authorized administrator shall manage the following critical commands to change the device status.

  - Configuration initialization

5.1.5.5. FMT_PWD.1 Management of ID and password (Extended)

Hierarchical to: No other components.

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

FMT_PWD.1.1 The TSF shall restrict the ability to manage the password of [assignment: *list of functions*] to [the authorized administrator].

1. [assignment: *password combination rules and/or length*]
2. [assignment: *other management such as management of special characters unusable for password, etc.*]

FMT_PWD.1.2 The TSF shall restrict the ability to manage the ID of [assignment: *list of functions*] to [the authorized administrator].

1. [assignment: *ID combination rules and/or length*]
2. [assignment: *other management such as management of special characters unusable for ID, etc.*]

FMT_PWD.1.3 The TSF shall provide the capability for [selection, choose one of: *setting ID and password when installing, setting password when installing, changing the ID and password when the authorized administrator accesses for the first time, changing the password when the authorized administrator accesses for the first time*].

Application notes

- o If the TOE does not provide the management functions that administrator manage the combination rules and length of ID and password, etc., 'none' may be specified in assignment operations of FMT_PWD.1.1 and FMT_PWD.1.2.
- o The ST author shall defines list of functions which require the password management in [assignment: *list of function*] of FMT_PWD.1.1 including the generation and modification of administrator's password.
- o This requirement shall be applied to the local access(console port) and management access(SSH, etc.) supported by the TOE.
- o The ID and password combination rules that can be set by the administrator in FMT_PWD.1.1 and FMT_PWD.1.2 may include minimum and maximum length setting, mixing rule setting involving English upper/lower case letters/numbers/special characters, etc..
- o The ST authors shall select FMT_PWD.1.3 depending on whether administrator's ID and password, or password are set during the installation/initial booting procedure of the TOE or the installation/initial booting is executed using the default ID and/or password provided by the TOE.

  In case of installation/initial booting using the default ID and/or password, if administrator succeeds in the identification and authentication after inputting administrator's ID and password at first access, the administrator shall be forced to change the default administrator's password by TOE's function.
- o The requirements in FMT_PWD.1.3 shall be applied to the TOE and service, and the function to force to change the default password shall be applied to the local access(console port) and management access(SSH, etc.) of the administrator.

Category	Timing	Requirements
Local access	administrator's first local access	When default ID and/or password are provided by the TOE, the function to force to change password shall be provided at administrator's first access to the product.
Management access	administrator's first management access - SSH - Other secure services(e.g. HTTPS, etc.)	When default ID and/or password for the service are provided by the TOE, the function to force to change password shall be provided at administrator's first access(or other time/other method) using a corresponding service.

o In case of 'setting ID and password when installing, setting password when installing' presented in FMT_PWD.1.3, the function to force to change the default password shall not be required at administrator's first access.

5.1.5.6. 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 management functions:

[

1. enable/disable [assignment: *management access service*] (default value: disable)
2. Supporting SNMP v3
3. Designating IP address for management access service
4. Setting access privileges per administrator account
5. Checking details and results of the testing by FPT_TST.1 and FPT_TEE.1
6. [assignment: *list of management functions to be provided by the TSF*]

]

Application notes

o The ST author lists up all the functions that support management actions. The listed management functions in FMT_SMF.1 shall ensure that it is consistent with the management actions of TSF function, TFS data and security attributes defined in FMT_MOF.1, FMT_MTD.1, FMT_MSA.1, and FMT_PWD.1, etc..

o The management of the TOE includes not only local access management by the administrator but also the management access, therefore, the ST author shall specify the

management functions by classifying local and management access respectively.

- o The status of management access service, for example 'disable' or 'enable', shall be adjustable by the configuration, but default status must be 'disable' when delivering.
- o "Management access services" in FMT_SMF.1.1 includes, for example, SSH, HTTPS, TLS, IPSec, etc., and the management functions by service can be defined in FMT_SMF.1.1 as assignment operation.
- o In case of using VTY(Virtual Teletype) for management access, the transmitted data on the communication path shall be protected using the secure communication.
- o In case of supporting SNMP, SNMP v3 or its successors shall be supported. And, when using SNMP(including v1 and v2), the security guideline to use them shall be followed. In addition, see the FCS class for more details regarding cryptography.
- o If only local accesses are used to properly block the unauthorized access attempts by unauthorized users, management accesses shall be denied.
- o The capability shall be provided so that an administrator can check the details and results of TSF testing and external entities testing. The means for checking the testing result may include any of screen display, LED, audit data, etc..
- o If the TSF testing fails, the appropriate action that is suitable for the tested TSF parts may be provided. For example, in case of TSF parts affecting the critical functions and security functions of the TOE, the capability may be provided so that administrators are immediately aware of abnormal status of the device's anomaly status using the LED on the hardware external or alarm, etc.. If the test of external entities fails, refer to FPT_TEE.1 for the action.

5.1.5.7. 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 [assignment: *the authorized identified roles*].

FMT_SMR.1.2 The TSF shall be able to associate users with **roles defined in FMT_SMR.1.1**.

Application notes

- o As presented in FIA_UID.1, the user of a network device is an administrator who performs the managements of the TOE, and the administrator roles shall be severally divided depending on access privileges of administrator account. This requirement shall be applied to the local access(console port) and management access(SSH, etc.) supported by the TOE.
- o It must be noted that the ST author shall suitably assign the access and command privileges in accordance with the administrator's roles. For example, monitoring administrators shall not change the TOE's configuration by assigning a wrong command

group to them.

o The TOE may introduce a variety of security roles: each user of the network device is defined as one administrator role and it set the different access privileges for each account, or, administrator roles are classified into the several roles such as the most privileged administrator and monitoring administrators, and access privileges are set differently based on the role, etc.

5.1.6. Protection of the TSF

5.1.6.1. FPT_PST.1 Basic protection of stored TSF data (Extended)

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PST.1.1 The TSF shall protect [the administrator password, [assignment: *TSF data*]] stored in the containers controlled by the TSF from the unauthorized *disclosure*.

Application notes

o Containers controlled by the TSF means storage in the TOE or external entities (DBMS, etc.) that interact with the TOE.

o This SFR shall be mandatorily applied to the password for the administrator's local access (console port) and management access (SSH, etc.). And, when the TOE protects other stored TSF data, it is defined as assignment operation in FPT_PST.1.1.

o As a method for protecting from the unauthorized disclosure, the administrator password which is the TSF data should be securely stored using cryptographic algorithm (asymmetric key cryptography, hash function, etc.). If passwords for changing the operating mode or elevating privileges are provided, it shall be included in the interpretation of 'administrator password' and be securely stored.

o All the secrete information (passwords, pre-shared keys, asymmetric keys, private keys, etc.) stored in containers controlled by the TSF shall not be read or inferred, that means information should not be read or inferred through the functions (interface) provided by the TOE. This SFR must be applied to the following:

- Password for administrator's local access and management access
- Pre-shared key for interacting with an authentication server
- Authentication password for supporting SNMP v3
- Privacy password for supporting SNMP v3
- Password for changing operating mode
- Password for elevating privilege, etc.

o When storing the audit data which is one of TSF data in the inside device, the function

that stores encrypted audit data may be provided.

o See the FCS class for more details regarding cryptography.

5.1.6.2. FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

Application notes

o The TSF provides the reliable time stamp by itself, or the TSF can provide a time stamp by synchronizing with reliable time information of external entities (e.g. reliable NTP server).

5.1.6.3. 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 the initial start-up,* [selection: *periodically during normal operation, at the request of* ***the authorized administrator****, [assignment: other conditions]*] to check the fulfillment of [operating status of major hardware components].

FPT_TEE.1.2 If the test fails, the TSF shall [assignment: *action(s)*].

Application notes

o When initial start-up (Power On), testing functions (a function for checking the normal operation status of the major hardware) for checking the error of major hardwares shall be provided. Entities such as CPU, memory, flash, network interface, power, etc. may be a testing target. In this PP, the TOE is appliance switches and routers, but the hardware is tested as external entity because it is not a part of the TSF.

o The ST author can select external entities to be tested, however, those external entities shall be tested if their abnormal operation (e.g. error, stop, etc.) affect the critical functions and security functions of the network device.

o The capability shall be provided so that an administrator can check the details and results of testing of external entities. Refer to 'FMT_SMF.1' for more details.

o If the test of external entities fails, the appropriate action that is suitable for the tested entities may be provided. For example, in case of external entities affecting the critical functions and security functions of the TOE, the capability may be provided so that administrators are immediately aware of abnormal status of the device's anomaly status using the LED on the hardware external or alarm, etc..

When the TOE provides no actions to be taken in case of failure of testing of external entities, the PP permits the ST author to assign 'none' in the assignment operation of FPT_TEE.1.2.

- o Testings of external entities do not need to be carried out at the same time, however, it is required to carry out each testing at certain necessary conditions per each external entity. For example, the TOE may implement that external entities affecting the critical functions and security functions of TOE shall be tested in full at initial start-up.
- o The ST author can select the interval (e.g. every one hour during normal operation or at the request of the authorized administrator) of external entities testing during normal operation. However, the testing interval shall be determined within certain reasonable bounds so that they do not adversely affect to the connected network when the network device operates abnormally.
- o The capability may be provided so that administrator directly executes the testing of external entities, and the ST author may select all or parts of external entities to be directly tested.
- o All external entities such as NTP server, authentication server, log server, DBMS, etc. that interact with the TOE can be additionally tested. And, it is recommended that other external entities required for secure and accurate operation of the TOE are to be tested.

5.1.6.4. 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 ***after loading firmware during the initial start-up,*** [selection: *periodically during normal operation, at the request of* ***the authorized administrator****, at the conditions [assignment: conditions under which self test should occur]*] to demonstrate the correct operation of [selection: *[assignment: parts of TSF], the TSF*].

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

FPT_TST.1.3 The TSF shall provide **[selection: *the authorized administrator, the TSF, none*]** with the capability to verify the integrity of [selection: [assignment: *parts of TSF], the TSF*].

Application notes

- o After loading firmware during the initial start-up (Power On), the TSF runs a suite of self tests of critical processes related to the operation of security functions such as identification and authentication, information flow control, security management, etc..
- o The ST author can select parts of the TSF to be tested, however, those parts of the TSF shall be tested if their abnormal operation (e.g. error, stop, etc.) affect the critical functions

and security functions of the TOE.

o The configuration file, cryptographic key file, configuration backup file, audit records for backup, device configuration for backup and recovery, other critical files, etc. can be included in the list to be verified for integrity in FPT_TST.1.2.

When the TOE provides the authorized administrator with no capability to verify integrity of the TSF data, the PP permits the ST author to assign 'none' in the assignment operation.

o In FPT_TST.1.3, the capability to directly verify integrity of the TSF such as critical processes is provided to the administrator.

When the TOE provides the authorized administrator with no capability to verify integrity of the TSF, the PP permits the ST author to assign 'none' in the assignment operation.

o The capability shall be provided so that an administrator can check the details and results of TSF testing. Refer to 'FMT_SMF.1' for details.

o TSF testings do not need to be carried out at the same time, however, it is required to carry out each testing at certain necessary conditions per each TSF part.

o The ST author can select the interval (e.g. every one hour during normal operation or at the request of the authorized administrator) of TSF testing during normal operation. However, the testing interval shall be determined within certain reasonable bounds so that they do not adversely affect to the connected network when the TOE operates abnormally.

o The capability may be provided so that administrator directly executes the TSF testing, and the ST author may select all or parts of the TSF to be directly tested.

o In case of the ST author selects 'the TSF' in [selection: *the authorized administrator, the TSF, none*] of FPT_TST.1.3, the capability that verifies the TSF integrity shall be provided during the initial start-up.

5.1.6.5. FPT_TUD.1 TSF security patch update (Extended)

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TUD.1.1 The TSF shall provide the capability to view the TOE versions to [the authorized administrator].

FPT_TUD.1.2 The TSF shall verify validity of the update files using [selection: *hash value comparison, digital signature verification*] before installing updates.

Application notes

o The TSF shall provide the capability to check the current version of the TOE which most

recently installed and executed by authorized administrator.

o Updates may be available either automatically or manually. If online update is available, update files shall be transmitted through a secure communication channel to protect the file. Refer to 'Optional SFR' FTP_ITC.1 for more details.

o When failing the firmware installation and update file verification of the network device, the TOE shall be securely started and operated using a previous firmware.

5.1.7. TOE access

5.1.7.1. FTA_SSL.5 Management of TSF-initiated sessions (Extended)

Hierarchical to: No other components.

Dependencies: [FIA_UAU.1 Timing of authentication or no dependencies]

FTA_SSL.5.1 The TSF shall [selection:

- *lock the session and/or re-authenticate the administrator before unlocking the session,*
- *terminate*] **the administrator's** interactive session after a [assignment: time interval of **the administrator** inactivity].

Application notes

o This SFR shall require the capability to lock or terminate the session after a time interval of the administrator inactivity, and it shall be applied to local access(console port) and management access(SSH, etc.) supported by the TOE.

o "A time interval of the authorized administrator inactivity" can be the fixed value in TOE (less than 10 minutes) or the TOE can provide capability to set the value to the authorized administrator.

o If inactivity time and actions (session locking or session termination) are differently provided depending on the TOE user, service(e.g. SSH), etc., the ST authors may apply the iteration operation.

o Session Locking means that the TSF shall lock an interactive session after inactivity time by disabling any activity of the administrator's data access/display devices other than unlocking the session, and clearing or overwriting display devices, making the current contents(TOE configuration values, etc.) unreadable.

5.1.7.2. FTA_TSE.1 TOE session establishment

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_TSE.1.1 The TSF shall be able to deny **administrator's management access session** establishment based on [connection IP, [selection: *connection time, whether or not to activate the management access session of the same account, whether or not to activate the management access session of administrator account with the same privilege, [assignment: critical management functions attribute], none*]].

Application notes

o The management access session of administrator shall be allowed only from the terminal with designated IP address for management access. That is, refer to 'Designate IP address for management access service' in FMT_SMF.1.1 for more details.

o The TOE may provide the ability to restrict that the following commands to change the device status are executed via local access only.

- Boot ROM access
- Factory initialization
- Engineer mode (debugging, memory modification/dump, etc.)

5.1.8. Trusted path/channels

5.1.8.1. FTP_TRP.1 Trusted path

Hierarchical to: No other components.

Dependencies: No dependencies

FTP_TRP.1.1 The TSF shall provide a communication path between itself and ***the management access*** **administrator** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from *modification, disclosure,* [assignment*: other types of integrity or confidentiality violation*].

FTP_TRP.1.2 The TSF shall permit [selection: *the TSF,* ***the management access administrator***] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [selection: ***the authentication of management access administrator***, [assignment: *other services for which trusted path is required*]].

Application notes

o The TOE shall provide a trusted channel using a cryptographic communication protocol in case of administrator's management access. The SSH, TLS, HTTPS, IPSec can be presented as a cryptographic communication protocol and see the FCS class for more details regarding cryptography.

- o If the TLS protocol is supported for the administrator's management access, it shall support TLS 1.2 (RFC 5246) or its successors. If the SSH protocol is supported, it shall support SSH v2(RFC 4251 ~ 4254) or its successors. See the FCS class for more details regarding cryptography, however, it is recommended to remove the publicly available vulnerabilities included in the protocol for secure use.
- o If the TOE does not provide the capability for other types of integrity or confidentiality violation, 'none' may be specified in assignment operations of FTP_TRP.1.1.

5.2. Security functional requirements (Optional SFRs)

'Optional SFRs' in this PP are as follows. 'Optional SFRs' are not required to be implemented mandatorily, however, when the TOE additionally provides related capabilities, the ST author must include the corresponding SFRs into the ST.

Security functional class	Security functional component		Remark
FAU	FAU_SEL.1	Selective audit	
FCS	FCS_CKM.2	Cryptographic key distribution	
FIA	FIA_UAU.6	Re-authenticating	
FTA	FTA_MCS.2	Per user attribute limitation on multiple concurrent sessions	Refinement
FTP	FTP_ITC.1	Inter-TSF trusted channel	

[Table 5] Optional security functional requirements

5.2.1. Security audit

5.2.1.1. FAU_SEL.1 Selective audit

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation
FMT_MTD.1 Management of TSF data

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

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

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

Application notes

- o FAU_SEL.1 Selective audit is an optional SFR that can be optionally implemented. When providing this capability in the TOE, the ST author shall include this requirement into SFRs.
- o If ST author includes this SFR, they shall additionally derive the security problem definition and security objectives when necessary.

5.2.2. Cryptographic support

5.2.2.1. FCS_CKM.2 Cryptographic key distribution

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [assignment: *cryptographic key distribution method*] that meets the following: [assignment: *list of standards*].

Application notes

- o FCS_CKM.2 Cryptographic key distribution is an optional SFR that can be optionally implemented. When providing this capability in the TOE, the ST author shall include this requirement into SFRs.
- o If ST author includes this SFR, they shall additionally derive the security problem definition and security objectives when necessary.
- o Keys used in the cryptographic key establishment method in FCS_CKM.2.1 shall be associated with the key generated in FCS_CKM.1.1.

5.2.3. Identification and authentication

5.2.3.1. FIA_UAU.6 Re-authenticating

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions [assignment: *list of conditions under which re-authentication is required*].

Application notes

- o FIA_UAU.6 Re-authenticating is an optional SFR that can be optionally implemented. However, if obtaining the higher administrator's privileges by using the privilege elevating command after administrator's login, the ST author shall include this requirement into SFRs.
  - This SFR is intended to provide a secure authentication capability for the TOE that provides access privilege configurations of operation mode for each account. And, it requires to restrict usable commands depending on the privileges set in the administrator's account. In addition, additional authentication(re-authentication) capability

is required if the TOE is allowed to obtain higher administrator privileges through the privilege elevating command after login.

- o This SFR can be excluded if privilege elevating commands are not provided after login.
- o If ST author includes this SFR, they shall additionally derive the security problem definition and security objectives when necessary.
- o If the TOE includes FIA_UAU.6 requirement, the capability that allows the administrator to create/reset a password for changing operating mode shall be included in FMT_SMF.1. Refer to FMT_PWD.1 for more details on creating a password.

5.2.4. TOE access

5.2.4.1. FTA_MCS.2 Per user attribute limitation on multiple concurrent sessions

Hierarchical to: FTA_MCS.1 Basic limitation on multiple concurrent sessions

Dependencies: FIA_UID.1 Timing of identification

FTA_MCS.2.1 The TSF shall restrict the maximum number of concurrent sessions that belong to the same **administrator** according to the rules [assignment: *rules for the number of maximum concurrent sessions*].

FTA_MCS.2.2 The TSF shall enforce, by default, a limit of [assignment: *default number*] sessions per **administrator**.

Application notes

- o FTA_MCS.2 Per user attribute limitation on multiple concurrent sessions is an optional SFR that can be optionally implemented. When providing this capability in the TOE, the ST author shall include this requirement into SFRs.
- o If ST author includes this SFR, they shall additionally derive the security problem definition and security objectives when necessary.
- o A session presented in FMT_MCS.2 means 'the access of user', the number of sessions shall be interpreted 'the number of user accesses.
- o When restricting the number of management access sessions to the TOE by each service (e.g. SSH, HTTPS, TLS, IPSec, etc.), it is defined in assignment operation of FTA_MCS.2.1.
- o In the case of administrator's management access session in FTA_MCS.2.1, the capability that restricts the maximum number of concurrent sessions to only one, or restricts the number of concurrent connection sessions may be provided.
- o Besides management access session, the maximum number of allowed concurrent accesses shall be defined in FTA_MCS.2.2.

5.2.5. Trusted path/channels

5.2.5.1. FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

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

Application notes

- o FTP_ITC.1 Inter-TSF trusted channel is an optional SFR that can be optionally implemented. When providing this capability in the TOE, the ST author shall include this requirement into SFRs.
- o If ST author includes this SFR, they shall additionally derive the security problem definition and security objectives when necessary.
- o Examples of the trusted IT product presented in FTP_ITC.1 are external log server, authentication server, update server, etc..
- o If the TSF interacts with the external log server or authentication server, etc., the TSF and each server shall protect the TSF data such as audit data, authentication data, TOE configuration files, network configuration files by providing trusted channel using cryptographic protocol. See the FCS class for more details regarding cryptography.
- o If the TLS protocol is supported when communicating between the TSF and trusted IT product, it shall support TLS 1.2 (RFC 5246) or its successors. And, if the SSH protocol is supported, it shall support SSH v2(RFC 4251 ~ 4254) or its successors. See the FCS class for more details regarding cryptography, however, it is recommended to remove the publicly available vulnerabilities included in the protocol for secure use.

5.3. Security assurance requirements

Assurance requirements of this Protection Profile are comprised of assurance components in CC part 3, and the evaluation assurance level is EAL1+. The following table summarizes assurance components.

Security assurance class	Security assurance component	
Security Target evaluation	ASE_INT.1	ST introduction
	ASE_CCL.1	Conformance claims
	ASE_OBJ.1	Security objectives for the operational environment
	ASE_ECD.1	Extended components definition
	ASE_REQ.1	Stated security requirements
	ASE_TSS.1	TOE summary specification
Development	ADV_FSP.1	Basic functional specification
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.1	Labelling of the TOE
	ALC_CMS.1	TOE CM coverage
Tests	ATE_FUN.1	Functional testing
	ATE_IND.1	Independent testing - conformance
Vulnerability assessment	AVA_VAN.1	Vulnerability survey

[Table 6] Security assurance requirements

5.3.1. Security Target evaluation

5.3.1.1. 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.

5.3.1.2. 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.

5.3.1.3. ASE_OBJ.1 Security objectives for the operational environment

Dependencies: No dependencies.

Developer action elements:

ASE_OBJ.1.1D	The developer shall provide a statement of security objectives.

Content and presentation elements:

ASE_OBJ.1.1C	The statement of security objectives shall describe the security objectives for the operational environment.

Evaluator action elements:

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

5.3.1.4. 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.

5.3.1.5. ASE_REQ.1 Stated security requirements

Dependencies: ASE_ECD.1 Extended components definition

Developer action elements:

ASE_REQ.1.1D	The developer shall provide a statement of security requirements.
ASE_REQ.1.2D	The developer shall provide a security requirements rationale.

Content and presentation elements:

ASE_REQ.1.1C	The statement of security requirements shall describe the SFRs and the SARs.
ASE_REQ.1.2C	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.1.3C	The statement of security requirements shall identify all operations on the security requirements.
ASE_REQ.1.4C	All operations shall be performed correctly.
ASE_REQ.1.5C	Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.
ASE_REQ.1.6C	The statement of security requirements shall be internally consistent.

Evaluator action elements:

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

5.3.1.6. 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.

Evaluator action 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.

5.3.2. Development

5.3.2.1. ADV_FSP.1 Basic functional specification

Dependencies: No dependencies.

Developer action elements:

ADV_FSP.1.1D	The developer shall provide a functional specification.
ADV_FSP.1.2D	The developer shall provide a tracing from the functional specification to the SFRs.

Content and presentation elements:

ADV_FSP.1.1C	The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.
ADV_FSP.1.2C	The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI. `
ADV_FSP.1.3C	The functional specification shall provide rationale for the implicit

	categorization of interfaces as SFR-non-interfering.
ADV_FSP.1.4C	The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.
	Evaluator action elements:
ADV_FSP.1.1E	The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.
ADV_FSP.1.2E	The evaluator *shall determine* that the functional specification is an accurate and complete instantiation of the SFRs.

5.3.3. Guidance documents

5.3.3.1. 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 fulfil 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.

5.3.3.2. 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_PRE1.1C	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_PRE1.2C	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.

5.3.4. Life-cycle support

5.3.4.1. ALC_CMC.1 Labelling of the TOE

	Dependencies: ALC_CMS.1 TOE CM coverage
	Developer action elements:
ALC_CMC.1.1D	The developer shall provide the TOE and a reference for the TOE.
	Content and presentation elements:
ALC_CMC.1.1C	The TOE shall be labelled with its unique reference.
	Evaluator action elements:
ALC_CMC.1.1E	The evaluator *shall confirm* that the information provided meet requirements for content and presentation of evidence.

5.3.4.2. ALC_CMS.1 TOE CM coverage

Dependencies: No dependencies.

Developer action elements:

ALC_CMS.1.1D The developer shall provide a configuration list for the TOE.

Content and presentation elements:

ALC_CMS.1.1C The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.

ALC_CMS.1.2C The configuration list shall uniquely identify the configuration items.

Evaluator action elements:

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

5.3.5. Tests

5.3.5.1. 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.

5.3.5.2. ATE_IND.1 Independent testing - conformance

Dependencies: ADV_FSP.1 Basic functional specification
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures

	Developer action elements:
ATE_IND.1.1D	The developer shall provide the TOE for testing.
	Content and presentation elements:
ATE_IND.1.1C	The TOE shall be suitable for testing.
	Evaluator action elements:
ATE_IND.1.1E	The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.
ATE_IND.1.2E	The evaluator *shall test* a subset of the TSF to confirm that the TSF operates as specified.

5.3.6. Vulnerability assessment

5.3.6.1. AVA_VAN.1 Vulnerability survey

Dependencies: ADV_FSP.1 Basic functional specification
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures

	Developer action elements :
AVA_VAN.1.1D	The developer shall provide the TOE for testing.
	Content and presentation elements:
AVA_VAN.1.1C	The TOE shall be suitable for testing.
	Evaluator action elements:
AVA_VAN.1.1E	The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.1.2E	The evaluator *shall perform* a search of public domain sources to identify potential vulnerabilities in the TOE.
AVA_VAN.1.3E	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 Basic attack potential.

5.4. Security requirements rationale

5.4.1. Dependency rationale of security functional requirements

The following table shows dependency of security functional requirements.

No.	Security functional requirements	Dependencies	Reference No.
1	FAU_GEN.1	FPT_STM.1	22
2	FAU_STG.1	FAU_GEN.1	1
3	FAU_STG.3	FAU_STG.1	2
4	FCS_CKM.1	FCS_CKM.2 or FCS_COP.1	6
		FCS_CKM.4	5
5	FCS_CKM.4	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	4
6	FCS_COP.1	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	4
		FCS_CKM.4	5
7	FDP_IFC.2	FDP_IFF.1	8
8	FDP_IFF.1	FDP_IFC.1	7
		FMT_MSA.3	16
9	FIA_AFL.1	FIA_UAU.1	11
10	FIA_SOS.1	-	-
11	FIA_UAU.1	FIA_UID.1	13
12	FIA_UAU.7	FIA_UAU.1	11
13	FIA_UID.1	-	-
14	FMT_MOF.1	FMT_SMF.1	19
		FMT_SMR.1	20
15	FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1	7
		FMT_SMF.1	19
		FMT_SMR.1	18
16	FMT_MSA.3	FMT_MSA.1	15
		FMT_SMR.1	20
17	FMT_MTD.1	FMT_SMF.1	19
		FMT_SMR.1	20
18	FMT_PWD.1	FMT_SMF.1	19
		FMT_SMR.1	20
19	FMT_SMF.1	-	-
20	FMT_SMR.1	FIA_UID.1	13
21	FPT_PST.1	-	-

No.	Security functional requirements	Dependencies	Reference No.
22	FPT_STM.1	-	-
23	FPT_TEE.1	-	-
24	FPT_TST.1	-	-
25	FPT_TUD.1	-	-
26	FTA_SSL.5	FIA_UAU.1 or No dependencies	11
27	FTA_TSE.1	-	-
28	FTP_TRP.1	-	-

[Table 7] Rationale for the dependency of security functional requirements

FDP_IFF.1 and FMT_MSA.1 have the dependency on FDP_IFC.1, and this is satisfied by FDP_IFC.2 that is in hierarchical relationship with FDP_IFC.1.

5.4.2. Dependency rationale of security assurance requirements

The dependency of EAL1 assurance package provided in the CC is already satisfied, the rationale is omitted.

The augmented SAR ATE_FUN.1 has dependency on ATE_COV.1. but, ATE_FUN.1 is augmented to require developer testing in order to check if the developer correctly performed and documented the tests in the test documentation, ATE_COV.1 is not included in this PP since it is not necessarily required to show the correspondence between the tests and the TSFIs.

References

Title	Author	Remark
Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4 • Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and General Model, Version 3.1, Revision 4 (CCMB-2012-09-001, Sep, 2012) • Common Criteria for Information Technology Security Evaluation. Part 2: Security Functional Components, Version 3.1, Revision 4 (CCMB-2012-09-002, Sep, 2012) • Common Criteria for Information Technology Security Evaluation. Part 3: Security Assurance Components, Version 3.1, Revision 4 (CCMB-2012-09-003, Sep, 2012)	CCMB	2012. 9
Checklist of security functional requirements for the network device	National Security Research Institute	2014

Abbreviated terms

ACL	Access Control List
CC	Common Criteria
CCMB	Common Criteria Maintenance Board
EAL	Evaluation Assurance Level
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
IP	Internet Protocol
IPSec	Internet Protocol Security
IT	Information Technology
LAN	Local Area Network
L3	Layer3
MAC	Media Access Control
NTP	Network Time Protocol
OSI	Open Systems Interconnection
SFP	Security Function Policy
SFR	Security Functional Requirement
SNMP	Simple Network Management Protocol
SSH	Secure Shell
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
VLAN	Virtual Local Area Network