국가용

침입차단시스템 보호프로파일

V1.0

2016. 6. 10

NIS

NSR
국가보안기술연구소
National Security Research Institute

전 문

본 '국가용 침입차단시스템 보호프로파일'은 국가정보원과 미래창조과학부의 협의 하에 국가보안기술연구소의 후원으로 개발되었다. 보호프로파일 작성자는 국가정보원 국가사이버안전센터의 「침입차단시스템 보안요구사항」에 서술된 국가용 보안요구사항을 공통평가기준에 적합하게 전환하였으며, 요구사항에 대한 정확한 해석은 국가정보원 국가사이버안전센터의 자문을 통해 이루어졌다. 공통평가기준을 적용한 평가·인증 시 추가적인 해석 및 가이드를 제공하기 위해 보호프로파일 내에 응용 시 주의사항을 서술하고 있으며, 보호프로파일에 대한 별도의 보조문서가 함께 제공된다.

개정 이력

버 전	일 자	개정 내용
1.0	2016.06.10	o 국가용 침입차단시스템 보호프로파일 V1.0 발간

목 차

1. 보호프로파일 소개

1.1. 보호프로파일 참조

제목	국가용 침입차단시스템 보호프로파일
버전	1.0
평가보증등급	EAL1+(ATE_FUN.1)
작성자	국가보안기술연구소, 한국정보통신기술협회
평가기준	정보보호시스템 공통평가기준(미래창조과학부고시 제2013-51호, 2013.8.8.)
공통평가기준 버전	CC V3.1 r4
인증번호	KECS-PP-0715-2016
주요 단어	침입차단시스템, 정보흐름통제, 접근통제

1.2. TOE 개요

1.2.1. 침입차단시스템 개요

본 보호프로파일은 네트워크 간 전송되는 패킷들을 정해진 규칙에 따라 차단하거나 통과시켜 공격자로부터 내부 자산을 보호하는 침입차단시스템(Firewall)에 대한 보안기능요구사항 및 보증요구사항을 정의한다.

침입차단시스템의 주요 기능은 외부 네트워크에서 내부 네트워크로 접근하는 트래픽을 제어하는 기능과 내부 네트워크와 외부 네트워크의 논리적/물리적인 분리를 통해 내부 자산에 대한 외부 사용자의 침입, 내부 사용자의 비 인가된 정보 유출 등을 방지하는 것이다.

침입차단시스템은 구성되는 방식, 적용되는 네트워크 계층, 접근통제 방식 등 다양한 정책적, 기술적 분류에 따라 구분된다.

1.2.2. TOE 유형 및 범위

본 보호프로파일에서 정의하는 TOE는 OSI 3~4계층(IP, 포트, 프로토콜 기반)에서 동작하는 상태기반 트래픽 필터링 기능을 제공하는 침입차단시스템으로 하드웨어 일체형 장비 형태로 제공된다. 본 보호프로파일에서는 상태기반 트래픽 필터링 침입차단시스템 장비가 제공해야 하는 공통적인 최소 보안기능을 정의하며, TOE는 이러한 보안기능을 제공해야 한다. 만일 TOE에서 OSI 5~7계층(세션, 어플리케이션 기반)에서 동작하는 어플리케이션 트래픽 필터링 침입차단시스템 기능을 제공한다면, "5.2 보안기능 요구사항(선택)"을 참고하여 관련 SFR을 도출해야 한다.

1.2.3. TOE 용도 및 주요 보안특성

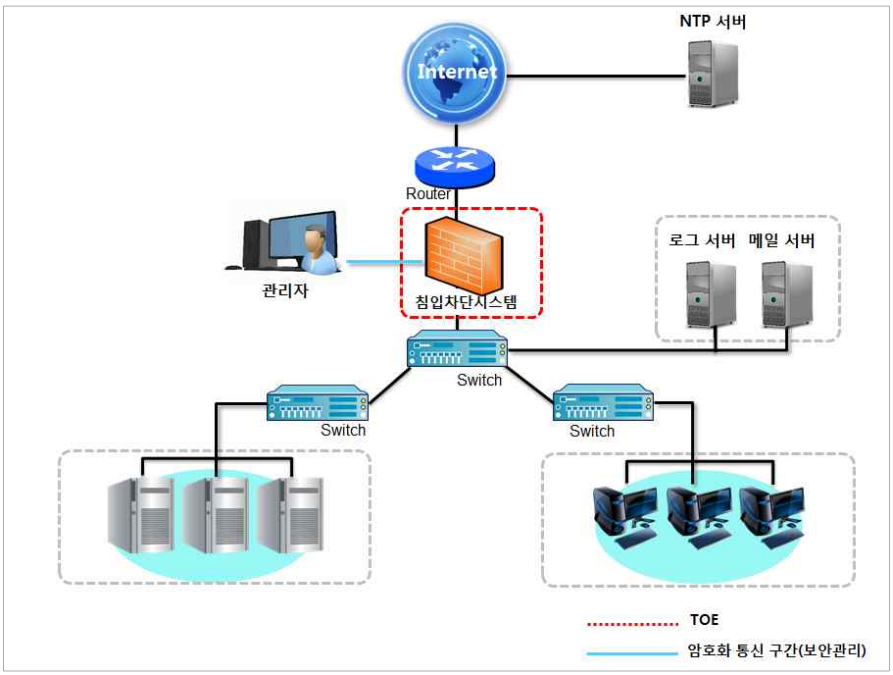
TOE는 내부망에 연결되어 있는 자산을 외부로부터 보호하기 위해 인가된 관리자가 설정한 규칙에 따라 트래픽을 제어하는 기능을 기본으로 제공한다.

TOE는 인가된 관리자가 설정한 IP 주소나 포트를 통해 송수신되는 네트워크 트래픽에 대해 패킷 필터링, 상태기반 검사, 세션 임계값에 따른 트래픽 필터링 등 상태기반 트래픽 필터링 기능을 제공한다. 또한 선택적으로 HTTP 컨텐츠/URL 필터링 등 어플리케이션 트래픽 필터링 기능을 제공할 수 있다.

TOE는 보안 기능 및 관리 기능 구동 시 주요 사건을 감사데이터로 기록하여 관리하는 보안감사 기능, 방화벽 관리자의 신원 검증, 연속 인증 실패 처리 등의 식별 및 인증 기능, TSF가 통제하는 저장소 내에 저장된 데이터를 보호하는 기능, TSF 자체시험 및 외부실체 시험 등의 TSF 보호 기능을 제공한다. 또한, IPSec, TLS, SSH, HTTPS와 같은 암호통신 지원 등을 위한 암호키 생성, 파기, 연산을 수행하는 암호 지원 기능, 보안 기능 및 관리자 역할 정의, 환경설정 등을 위한 보안관리 기능, 인가된 관리자의 접속 세션 관리를 위한 TOE 접근 기능, TOE와 관리접속 관리자 간의 안전한 통신을 제공하는 안전한 경로/채널 기능을 포함한다.

1.2.4. 비-TOE 및 TOE 운영환경

다음 [그림 1]은 TOE가 동작하는 운영환경을 나타낸다.



[그림 1] TOE 운영환경

TOE는 자신을 통과하지 않는 트래픽에 대해서는 공격 탐지 및 차단이 불가능하기 때문에, 일반적으로 다음 그림과 같이 외부 네트워크와 보호하고자 하는 내부 자산 사이에 인라인 방식으로 설치하여 자산에 대한 모든 접근 시도가 반드시 침입차단시스템을 통과하도록 구성한다. 침입차단시스템은 운영환경에 따라 IPv4/IPv6, 고가용성을 위한 HA(High Availability) 모드 등 다양한 환경으로 구성할 수 있다.

인가된 관리자는 웹브라우저나 Serial 통신, 관리프로그램을 통해 TOE에 접속할 수 있으며, SSH나 SSL등 안전한 통신을 이용하여 보안관리를 수행할 수 있다.

TOE를 운영하기 위해 필요한 외부 IT실체로는 시간 동기화를 위한 NTP 서버, 감사데이터의 외부 저장 및 관리를 위한 로그서버, 감사데이터 손실 예측 시 인가된 관리자 알림을 위한 메일서버 등 다양한 외부 IT실체가 사용될 수 있다.

TOE(침입차단시스템)를 제외한 NTP 서버, 로그서버, 메일서버는 TOE 운영환경에 해당한다. 또한, 보안기능요구사항(이하 "SFR"이라 함)으로 도출되지 않은 부분(예: 침입차단시스템 보안기능 구동과 무관한 기능)은 TOE 물리적 구성요소 등을 고려하여 'TOE 범위에서 제외' 또는 'TOE 범위에 포함시키되 non-TSF로 분류' 가능하다.

본 보호프로파일은 다양한 형태로 구현된 TOE를 반영하기 위해 개발되었으며, 보안목표명세서 작성자가 본 보호프로파일을 수용할 경우 TOE 실행을 위해 필요하지만 TOE가 아닌 모든 하드웨어, 펌웨어 또는 소프트웨어를 기술해야 한다.

1.3. 작성규칙

본 보호프로파일은 일부 약어 및 명확한 의미 전달을 위해 영어를 혼용한다. 사용된 표기법, 형태, 작성 규칙은 공통평가기준을 따른다.

공통평가기준은 보안기능요구사항에서 수행될 수 있는 반복, 할당, 선택, 정교화 오퍼레이션을 허용한다. 각 오퍼레이션은 본 보호프로파일에서 사용된다.

반복

오퍼레이션을 다양하게 적용하여 하나의 컴포넌트를 여러 번 반복할 경우 사용된다. 반복 오퍼레이션의 결과는 컴포넌트 식별자 뒤에 괄호 안의 반복번호, 즉. (반복 번호)로 표시한다.

할당

명세되지 않은 매개변수에 특정 값을 할당하는데 사용된다(예 : 패스워드 길이). 할당 오퍼레이션의 결과는 대괄호, 즉. [할당 값]으로 표시된다.

선택

요구사항 서술시 정보보호시스템 공통평가기준에서 제공되는 선택사항 중 하나 이상을 선택하는데 사용된다. 선택 오퍼레이션의 결과는 *밑줄 그은 이탤릭*체로 표시된다.

정교화

요구사항에 상세사항을 추가함으로써 요구사항을 더욱 제한하는데 사용된다. 정교화 오퍼레이션의 결과는 **굵은 글씨**로 표시된다.

보안목표명세서 작성자

속성의 최종 결정이 보안목표명세서 작성자에 의해 이루어짐을 나타내는데 사용된다. 보안목표명세서 작성자 오퍼레이션은 중괄호 안의 { 보안목표명세서 작성자에 의해 결정(된) }으로 표시된다. 또한, 보호프로파일에서 완벽하게 수행되지 않은 보안기능요구사항의 오퍼레이션은 보안목표명세서 작성자에 의해 완벽하게 수행되어야 한다.

본 보호프로파일은 요구사항의 의미를 명확히 하고, 구현 시 선택사항에 대한 정보를 제공하며, 요구사항에 대한 "적합/부적합" 기준을 정의하기 위해 "응용 시 주의사항"이 제공된다. 응용 시 주의사항은 필요한 경우 해당 요구사항과 함께 제공된다.

1.4. 용어정의

본 보호프로파일에 사용된 용어 중 공통평가기준에 사용된 용어와 동일한 것은 공통평가기준을 따른다.

객체(Object)

주체의 오퍼레이션 대상이며 정보를 포함하거나 수신하는 TOE 내의 수동적인 실체

공격 성공 가능성(Attack potential)

공격자의 전문지식, 자원, 동기 등의 측면에서 파악된 TOE 공격에 소요되는 노력의 정도

반복(Iteration)

둘 이상의 서로 다른 요구사항을 표현하는데 동일한 컴포넌트를 사용하는 것

보안목표명세서(ST, Security Target)

특정 TOE에 적합한 구현-종속적인 보안요구 명세서

보호프로파일(PP, Protection Profile)

TOE 유형에 적합한 구현-독립적인 보안요구 명세서

사용자(User)

"외부 실체"를 참조하되, 침입차단시스템에서 사용자는 인가된 관리자를 의미함

선택(Selection)

컴포넌트에 서술된 목록에서 하나 이상의 항목을 명세하는 것

신원(Identity)

인가된 사용자를 식별하는 유일한 표현. 그 사용자의 본명이나, 약칭 혹은 가명일 수 있다.

엘리먼트(Element)

분할할 수 없는 보안 요구(사항)의 최소 단위

역할(Role)

사용자와 TOE 사이에 허용되는 상호작용을 설정하는 미리 정의된 규칙의 집합

(CC 컴포넌트의) 오퍼레이션(Operation(on a component of the CC))

컴포넌트를 수정하거나 반복하는 것. 컴포넌트에 허용된 오퍼레이션은 할당, 반복, 정교화, 선택이 있다.

(객체의) 오퍼레이션(Operation(on a subject))

주체가 객체에 대해 수행하는 특정 행동

외부 실체(External Entity)

TOE의 외부에서 TOE와 상호작용하는(또는 상호 작용할 수 있는) 실체(사람 또는 IT)

위협원(Threat Agent)

자산에 불법적인 접근, 변경, 삭제 등 위협을 일으키는 인가되지 않은 외부 실체

인가된 관리자(Authorized Administrator)

TOE를 안전하게 운영 및 관리하는 인가된 사용자

인가된 사용자(Authorized User)

SFR(보안기능요구사항)에 따라서 기능을 실행할 수 있는 사용자

인증 데이터(Authentication Data)

사용자의 신원을 증명하기 위하여 사용되는 정보

자산(Assets)

TOE의 소유자가 가치를 부여하는 실체

정교화(Refinement)

컴포넌트에 세부사항을 추가하여 명세하는 것

조직의 보안정책(Organizational Security Policies)

실제 또는 가상적인 조직에 의해 운영환경에 현재 부여되고/거나 앞으로 부여될 것으로 여겨지는 보안 규칙, 절차, 관행, 지침의 집합

종속관계(Dependency)

컴포넌트 간의 관계로, 종속하는 컴포넌트에 근거한 요구사항이 보호프로파일, 보안목표명세서, 또는 패키지에 포함되어 있는 경우, (그 컴포넌트에) 종속되는 컴포넌트에 근거한 요구사항도 보호프로파일, 보안목표명세서, 또는 패키지에 포함 되어야 하는 관계

주체(Subject)

객체에 대한 오퍼레이션을 수행하는 TOE 내의 능동적인 실체

추가(Augmentation)

패키지에 하나 이상의 요구사항을 추가하는 것

컴포넌트(Component)

엘리먼트의 집합으로서 요구사항의 기초를 형성하는데 사용될 수 있는 가장 작은 선택 단위

클래스(Class)

같은 보안목적을 가지는 공통평가기준 패밀리의 모음

평가대상(TOE, Target of Evaluation)

가능한 설명서가 수반되는 소프트웨어, 펌웨어 및/또는 하드웨어 집합

평가보증등급(EAL, Evaluation Assurance Level)

공통평가기준에서 미리 정의된 보증 수준을 가지는 3부의 보증요구사항으로 이루어진 보증 패키지

패밀리(Family)

유사한 목적을 가지지만 강조점이나 엄격함이 서로 다른 컴포넌트의 모음

할당(Assignment)

(공통평가기준의) 컴포넌트 또는 요구사항 내에서 식별된 매개변수를 구체적으로 명세하는 것

TOE 보안기능성(TSF, TOE Security Functionality)

SFR(보안기능요구사항)들의 정확한 수행에 기여하는 TOE의 모든 하드웨어, 소프트웨어, 펌웨어로 구성된 집합

TSF 데이터(TSF Data)

TOE의 오퍼레이션에 영향을 줄 수 있는, TOE에 의해서 TOE를 위하여 생성된 데이터

관리접속(Management access)

TOE 관리를 목적으로 관리자가 HTTPS, SSH, TLS, IPSec 등을 이용하여 접속을 시도하는 행위

로컬접속(Local access)

TOE 관리를 목적으로 관리자가 장비에 콘솔포트를 통하여 직접 접속을 시도하는 행위

패킷(Packet)

인터넷망에서 데이터의 전송에서 사용되는 데이터의 묶음

IPSec (Internet Protocol Security protocol)

네트워크나 네트워크 통신의 패킷 처리 계층에서의 보안을 위해 사용하는 프로토콜

SSL(Secure Sockets Layer)
컴퓨터 네트워크 망에서 기밀성, 무결성과 같은 보안성을 제공하기 위해 넷스케이프에서 제안한 보안 프로토콜

TLS(Transport Layer Security)
SSL에 기반을 둔 서버와 클라이언트간의 암호화 인증통신 프로토콜로써 RFC 2246에 기술

해야 한다/하여야 한다(Shall/must)

응용 시 주의사항에 제시된 '해야 한다' 또는 '하여야 한다' 등은 TOE에 필수로 적용되어야 할 요구사항임

할 수 있다/될 수 있다(Can/could)

응용 시 주의사항에 제시된 '할 수 있다' 또는 '될 수 있다' 등은 보안목표명세서 작성자의 선택에 따라 TOE에 적용될 수 있는 요구사항임

권고한다/권고된다(Recommend/be recommended)

응용 시 주의사항에 제시된 '권고한다' 또는 '권고된다' 등은 TOE에 필수로 적용하기를 요구하지는 않으나 TOE의 안전한 운영을 위하여 적용할 것을 권하는 요구사항임

1.5. 보호프로파일의 구성

1장은 보호프로파일 소개로 보호프로파일 참조 및 TOE 개요 정보를 제공한다.

2장은 준수선언으로 공통평가기준, 보호프로파일, 패키지에 대한 준수를 선언하고 준수 선언의 이론적 근거 및 보호프로파일 준수 방법에 대해 서술한다.

3장은 TOE 보안기능성을 정확히 제공할 수 있도록 운영환경에서 지원하는 운영환경에 대한 보안목적을 정의한다.

4장은 침입차단시스템 특성에 따라 추가적으로 필요한 확장 컴포넌트를 정의한다.

5장은 보안요구사항으로 보안기능요구사항 및 보증요구사항을 서술한다. 필요한 경우, 보안요구사항의 의미를 명확히 하고 보안목표명세서 작성자가 오퍼레이션을 정확하게 적용하도록 세부 지침을 설명하기 위해 응용 시 주의사항을 서술한다.

참고자료는 본 보호프로파일에 관심이 있는 사용자가 본 보호프로파일에서 언급된 내용 이상의 관련 정보가 필요한 경우를 위하여 참고한 자료들을 서술한다.

약어표는 본 PP에서 사용되는 약어를 제시한다.

2. 준수 선언

2.1. 공통평가기준 준수 선언

공통평가기준		정보보호시스템 공통평가기준 버전 3.1 개정4판 • 정보보호시스템 공통평가기준 1부 : 소개 및 일반모델, 버전 3.1r4 (CCMB-2012-09-001, 2012. 9) • 정보보호시스템 공통평가기준 2부: 보안기능요구사항, 버전 3.1r4 (CCMB-2012-09-002, 2012. 9) • 정보보호시스템 공통평가기준 3부: 보증요구사항, 버전 3.1r4 (CCMB-2012-09-003, 2012. 9)
준수 형태	2부 보안기능요구사항	확장 : FMT_PWD.1, FPT_PST.1, FPT_TUD.1, FTA_SSL.5
	3부 보증요구사항	준수
	패키지	추가 : EAL1 추가(ATE_FUN.1)

2.2. 보호프로파일 준수 선언

본 보호프로파일이 준수하는 다른 보호프로파일은 없다.

2.3. 패키지 준수 선언

본 보호프로파일이 준수하는 보증요구사항 패키지는 EAL1이며, 일부 보증요구사항을 추가 정의한다.

- 보증패키지 : EAL1 추가(ATE_FUN.1)

2.4. 준수 선언의 이론적 근거

본 보호프로파일은 다른 보호프로파일에 대한 준수를 선언하지 않았으므로, 준수선언의 이론적 근거 기술은 필요하지 않다.

2.5. 보호프로파일 준수 방법

본 보호프로파일을 준수하려는 보호프로파일 또는 보안목표명세서는 "엄격한 보호프로파일 준수"를 해야 한다.

3. 보안목적

다음의 운영환경에 대한 보안목적은 TOE가 보안기능성을 정확히 제공할 수 있도록 운영환경에서 지원하는 기술적/절차적 수단에 의해 다루어야하는 보안목적이다.

3.1. 운영환경에 대한 보안목적

OE.PHYSICAL_CONTROL	OE.물리적보안

TOE는 인가된 관리자만이 접근하도록 출입을 통제하며 보호설비가 갖추어진 장소에 위치해야 한다.

OE.SECURITY_MAINTANANCE	OE.보안유지

네트워크 구성 변경, 호스트의 증감, 서비스의 증감 등으로 내부 네트워크 환경이 변화될 때, 변화된 환경과 보안정책을 즉시 TOE 운영정책에 반영하여, 이전과 동일한 수준의 보안을 유지해야 한다.

OE.TRUSTED_ADMIN	OE.신뢰된관리자

TOE의 인가된 관리자는 악의가 없으며, TOE 관리 기능에 대하여 적절히 교육받았고, 인가된 관리자 지침에 따라 정확하게 의무를 수행해야 한다.

OE.SINGLE_POINT_OF_CONNECTION	OE.유일한연결점

모든 외부 네트워크와 내부 네트워크간의 통신은 TOE를 통해서만 이루어져야 한다.

OE.LOG_BACKUP	OE.로그백업

관리자는 감사기록 유실에 대비하여 감사데이터 저장소의 여유 공간을 주기적으로 확인하고 감사기록이 소진되지 않도록 감사기록 백업(외부 로그서버, 별도 저장장치 등) 등을 수행해야 한다.

4. 확장 컴포넌트 정의

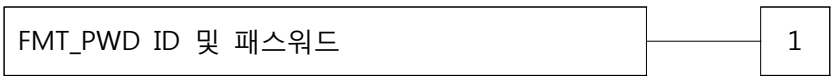
4.1. 보안관리(FMT, Security Management)

4.1.1. ID 및 패스워드

패밀리 개요

ID 및 패스워드(FMT_PWD, ID & PassWord) 패밀리는 인가된 사용자가 TOE에서 사용하는 ID 및 패스워드 관리를 통제하고, ID 및/또는 패스워드를 설정 또는 변경하는 기능을 요구하도록 정의한다.

컴포넌트 계층관계 및 설명



FMT_PWD.1 ID 및 패스워드 관리는 TSF가 ID 및 패스워드 관리기능을 제공할 것을 요구한다.

관리 : FMT_PWD.1

FMT에서 다음과 같은 관리 기능이 고려될 수 있다.

a) ID, 패스워드 설정 규칙의 관리

감사 : FMT_PWD.1

FAU_GEN 보안감사 생성 데이터 생성 패밀리가 보호프로파일/보안목표명세서에 포함되면 다음 행동을 감사기록할 것을 권고한다.

a) 최소 : ID, 패스워드에 대한 모든 변경

4.1.1.1. FMT_PWD.1 ID 및 패스워드 관리

계층관계	없음
종속관계	FMT_SMF.1 관리기능 명세 FMT_SMR.1 보안 역할
FMT_PWD.1.1	TSF는 [할당 : *기능목록*]의 패스워드를 다음과 같이 관리하는 능력을 [할당 : *인가된 역할*]로 제한해야 한다.

1. [할당 : *패스워드 조합 규칙 및/또는 길이*]
2. [할당 : *패스워드에 제외할 특수 문자 관리 등 기타 관리*]

FMT_PWD.1.2 TSF는 [할당 : *기능목록*]의 ID를 다음과 같이 관리하는 능력을 [할당 : *인가된 역할*]로 제한해야 한다.

1. [할당 : *ID 조합 규칙 및/또는 길이*]
2. [할당 : *ID에 제외할 특수 문자 관리 등 기타 관리*]

FMT_PWD.1.3 TSF는 [선택 : *설치 과정에서 ID 및 패스워드를 설정, 설치 과정에서 패스워드를 설정, 인가된 관리자가 최초 접속 시 ID 및 패스워드를 변경, 인가된 관리자가 최초 접속 시 패스워드를 변경 중 하나를 선택*]하는 기능을 제공해야 한다.

응용 시 주의사항

- o TOE에서 인가된 역할이 ID 및 패스워드 조합규칙 등을 관리하는 기능을 제공하지 않을 경우, FMT_PWD.1.1, FMT_PWD.1.2 할당 오퍼레이션에 '없음'을 명세하면 된다.
- o 인가된 역할이 설정할 수 있는 ID 및/또는 패스워드 조합규칙에는 최소 길이 및 최대 길이 설정, 영문 대문자/영문 소문자/숫자/특수문자 등 혼합 규칙 설정을 포함할 수 있다.

4.2. TSF 보호(FPT, Protection of the TSF)

4.2.1. 저장된 TSF 데이터 보호

패밀리 개요

저장된 TSF 데이터 보호(FPT_PST, Protection of Stored TSF data) 패밀리는 TSF가 통제하는 저장소에 저장되는 TSF 데이터를 인가되지 않은 변경 또는 노출로부터 보호하기 위한 규칙을 정의한다.

컴포넌트 계층관계 및 설명

FPT_PST 저장된 TSF 데이터 보호	1

FPT_PST.1 저장된 TSF 데이터의 기본적인 보호는 TSF에 의해 통제되는 저장소 내에 저장된 TSF 데이터가 보호될 것을 요구한다.

관리 : FPT_PST.1

예상되는 관리 요구사항 없음

감사 : FPT_PST.1

예상되는 감사 대상 행동 없음

4.2.1.1. FPT_PST.1 저장된 TSF 데이터의 기본적인 보호

계층관계 없음

종속관계 없음

FPT_PST.1.1 TSF는 TSF에 의해 통제되는 저장소에 저장되는 [할당 : *TSF 데이터*]를 비인가된 [선택 : *노출, 변경*]으로부터 보호해야 한다.

응용 시 주의사항

- o TSF에 의해 통제되는 저장소는 TOE 내부 또는 TOE와 상호작용하는 외부 실체(DBMS 등)를 의미한다.
- o 보호대상 TSF 데이터 예
  - 사용자 패스워드, 암호키(사전 공유키, 대칭키, 개인키), TOE 설정값(보안 정책, 환경설정 매개변수), 감사 데이터 등
- o 비인가된 노출 또는 변경으로부터 보호하기 위한 방법으로 TSF 데이터를 암호화해서 저장하거나 접근통제 및 숨김 등을 적용할 수 있다.

4.2.2. TSF 업데이트

패밀리 개요

TSF 업데이트(FPT_TUD, Trusted UpDate) 패밀리는 TOE 펌웨어/소프트웨어 업데이트 요구사항을 정의한다.

컴포넌트 계층관계 및 설명

FPT_TUD TSF 업데이트	1

FPT_TUD.1 TSF 보안패치 업데이트는 업데이트를 설치하기 전에 업데이트 파일에 대한 유효성을 검증하는 기능을 포함하여 TOE 펌웨어/소프트웨어의 신뢰된 업데이트를 보장할 것을 요구한다.

관리 : FPT_TUD.1

FMT에서 다음과 같은 관리 기능이 고려될 수 있다.

a) 업데이트 파일 검증 메커니즘 관리

감사 : FPT_TUD.1

FAU_GEN 보안감사 생성 데이터 생성 패밀리가 보호프로파일/보안목표명세서에 포함되면 다음 행동을 감사기록할 것을 권고한다.

a) 최소 : 업데이트 파일 무결성 검증 결과(성공, 실패)

4.2.2.1. FPT_TUD.1 TSF 보안패치 업데이트

계층관계	없음
종속관계	없음
FPT_TUD.1.1	TSF는 [할당 : *인가된 역할*]에게 TOE의 버전 정보를 조회할 수 있는 기능을 제공해야 한다.
FPT_TUD.1.2	TSF는 업데이트를 설치하기 전에 [선택 : *해쉬값 비교, 전자서명 검증*]을 이용하여 업데이트 파일에 대한 유효성 검증을 수행해야 한다.

응용 시 주의사항

- o TSF는 인가된 역할이 가장 최근에 설치되어 실행된 TOE의 현재버전을 확인할 수 있는 기능을 제공해야 한다.
- o 최신 업데이트 및 보안패치는 보안 취약점을 제거하기 위해 꼭 필요하지만, 업데이트 파일에 대한 검증없이 적용할 경우 시스템 오작동, 서비스 장애 등이 발생할 수 있으므로, 업데이트 파일에 대한 유효성 검증이 요구된다.

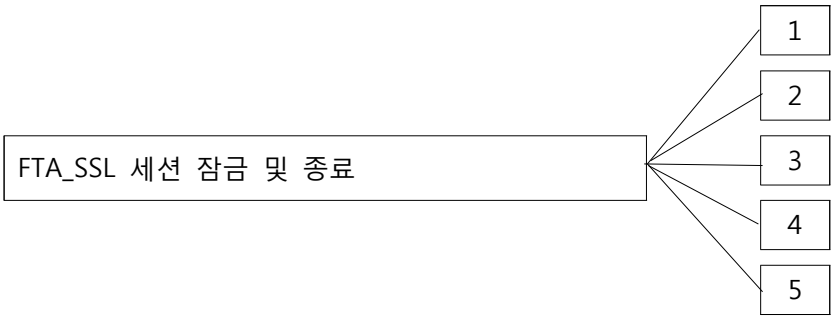
4.3. TOE 접근(FTA, TOE Access)

4.3.1. 세션 잠금 및 종료

패밀리 개요

세션 잠금 및 종료(FTA_SSL, Session Locking and termination) 패밀리는 TSF가 TSF에 의한 세션과 사용자에 의한 세션을 잠금, 잠금 해제 및 종료하는 능력을 제공하는 요구사항을 정의한다.

컴포넌트 계층관계 및 설명



CC 2부에서 세션 잠금 및 종료 패밀리는 4개의 컴포넌트로 구성된다. 본 PP에서, 다음과 같이 1개 컴포넌트를 추가 확장함에 따라, 5개의 컴포넌트로 구성된다.

※ CC 2부에 포함된 4개 컴포넌트 관련 서술은 생략한다.

FTA_SSL.5 TSF에 의한 세션 관리는 TSF가 명세된 사용자 비활동 기간 후 세션을 잠금 또는 종료하는 요구사항을 제공한다.

관리 : FTA_SSL.5

FMT에서 다음과 같은 관리 기능이 고려될 수 있다.

a) 각 사용자에 대해서 세션 잠금 또는 종료가 발생하는 사용자 비활동 기간의 명세

b) 세션 잠금 또는 종료가 발생하는 디폴트 사용자 비활동 시간의 명세

감사 : FTA_SSL.5

FAU_GEN 보안감사 생성 데이터 생성 패밀리가 보호프로파일/보안목표명세서에 포함되면 다음 행동을 감사기록할 것을 권고한다.

a) 최소 : 상호작용 세션의 잠금 또는 종료

4.3.1.1. FTA_SSL.5 TSF에 의한 세션 관리

계층관계	없음
종속관계	[FIA_UAU.1 인증 또는 없음]
FTA_SSL.5.1	TSF는 [할당 : *사용자 비활동 기간*] 후 상호작용 세션을 [선택 : • *세션 잠금 및/또는 세션잠금을 해제하기 전에 사용자 재인증,* • *세션 종료*] 해야 한다.

응용 시 주의사항

o 본 사항은 사용자 로컬접속 및 관리접속(SSH, HTTPS 등)에 모두 적용할 수 있다.

5. 보안요구사항

보안요구사항은 본 보호프로파일을 수용하는 TOE에서 만족되어야 하는 기능 및 보증요구사항을 서술한다.

본 보호프로파일에서 정의된 보안기능요구사항은 공통평가기준 2부 및 4장 확장 컴포넌트 정의로부터 관련 보안기능 컴포넌트를 선정하여 표현하였다.

또한, 본 보호프로파일에서는 보안기능요구사항을 다음과 같이 필수 SFR과 선택 SFR로 구분하였다.

- 필수 SFR : 침입차단시스템에서 필수로 구현하도록 요구되는 항목
- 선택 SFR : 침입차단시스템에서 필수로 구현하도록 요구되지 않으나 TOE에서 관련 기능을 추가로 제공할 경우, 보안목표명세서 작성자는 해당 SFR을 보안목표명세서에 포함해야 한다.

다음 표는 본 보호프로파일에서 사용하는 보안기능요구사항을 요약하여 보여준다.

보안기능 클래스	보안기능 컴포넌트		필수 SFR / 선택 SFR
보안감사 (FAU)	FAU_ARP.1	보안경보	필수 SFR
	FAU_GEN.1	감사데이터 생성	필수 SFR
	FAU_SAA.1	잠재적인 위반 분석	필수 SFR
	FAU_SAR.1	감사검토	필수 SFR
	FAU_SAR.3	선택 가능한 감사검토	필수 SFR
	FAU_SEL.1	선택적인 감사	선택 SFR
	FAU_STG.1	감사 증적 저장소 보호	필수 SFR
	FAU_STG.3	감사 데이터 손실 예측 시 대응 행동	필수 SFR
	FAU_STG.4	감사 데이터 손실 방지	필수 SFR
암호 지원 (FCS)	FCS_CKM.1	암호키 생성	필수 SFR
	FCS_CKM.2	암호키 분배	선택 SFR
	FCS_CKM.4	암호키 파기	필수 SFR
	FCS_COP.1	암호 연산	필수 SFR
사용자 데이터 보호 (FDP)	FDP_IFC.1	부분적인 정보흐름 통제(어플리케이션 트래픽 필터링)	선택 SFR
	FDP_IFC.2	완전한 정보흐름 통제(상태기반 트래픽 필터링)	필수 SFR
	FDP_IFF.1	단일 계층 보안속성(상태기반 트래픽 필터링)	필수 SFR
	FDP_IFF.1	단일 계층 보안속성(어플리케이션 트래픽 필터링)	선택 SFR
식별 및 인증 (FIA)	FIA_AFL.1	인증 실패 처리	필수 SFR
	FIA_SOS.1	비밀정보의 검증	필수 SFR
	FIA_UAU.1	인증	필수 SFR
	FIA_UAU.4	재사용 방지 인증 메커니즘	필수 SFR
	FIA_UAU.7	인증 피드백 보호	필수 SFR

보안기능 클래스	보안기능 컴포넌트		필수 SFR / 선택 SFR
	FIA_UID.1	사용자 식별	필수 SFR
보안 관리 (FMT)	FMT_MOF.1	보안기능 관리	필수 SFR
	FMT_MSA.1	보안속성 관리	필수 SFR
	FMT_MSA.3	정적 속성 초기화	필수 SFR
	FMT_MTD.1	TSF 데이터 관리	필수 SFR
	FMT_PWD.1(확장)	ID 및 패스워드 관리	필수 SFR
	FMT_SMF.1	관리기능 명세	필수 SFR
	FMT_SMR.1	보안 역할	필수 SFR
TSF 보호 (FPT)	FPT_ITT.1	내부전송 TSF 데이터의 기본적인 보호	선택 SFR
	FPT_PST.1(확장)	저장된 TSF 데이터 기본적인 보호	필수 SFR
	FPT_STM.1	신뢰할 수 있는 타임스탬프	필수 SFR
	FPT_TEE.1	외부 실체 시험	필수 SFR
	FPT_TST.1	TSF 자체 시험	필수 SFR
	FPT_TUD.1(확장)	TSF 보안패치 업데이트	선택 SFR
TOE 접근 (FTA)	FTA_MCS.2	사용자 속성별 동시 세션 수의 제한	필수 SFR
	FTA_SSL.5(확장)	TSF에 의한 세션 관리	필수 SFR
	FTA_TSE.1	TOE 세션 설정	필수 SFR
안전한 경로/채널 (FTP)	FTP_ITC.1	TSF 간 안전한 채널	선택 SFR
	FTP_TRP.1	안전한 경로	필수 SFR

[표 1] 보안기능요구사항

5.1. 보안기능요구사항(필수 SFR)

본 보호프로파일을 준수하는 침입차단시스템은 다음 표와 같은 '필수 SFR'을 만족해야 한다. 비고란에 기재된 '정교화', '반복'의 경우 CC 컴포넌트의 오퍼레이션을 의미한다.

보안기능 클래스	보안기능 컴포넌트		비 고
보안감사 (FAU)	FAU_ARP.1	보안경보	
	FAU_GEN.1	감사데이터 생성	
	FAU_SAA.1	잠재적인 위반 분석	
	FAU_SAR.1	감사검토	
	FAU_SAR.3	선택 가능한 감사검토	
	FAU_STG.1	감사 증적 저장소 보호	
	FAU_STG.3	감사 데이터 손실 예측 시 대응 행동	
	FAU_STG.4	감사 데이터 손실 방지	
암호 지원 (FCS)	FCS_CKM.1	암호키 생성	
	FCS_CKM.4	암호키 파기	
	FCS_COP.1	암호 연산	

보안기능 클래스	보안기능 컴포넌트		비 고
사용자 데이터 보호 (FDP)	FDP_IFC.2	완전한 정보흐름 통제	
	FDP_IFF.1	단일 계층 보안속성	
식별 및 인증 (FIA)	FIA_AFL.1	인증 실패 처리	
	FIA_SOS.1	비밀정보의 검증	
	FIA_UAU.1	인증	
	FIA_UAU.4	재사용 방지 인증 메커니즘	
	FIA_UAU.7	인증 피드백 보호	
	FIA_UID.1	사용자 식별	
보안 관리 (FMT)	FMT_MOF.1	보안기능 관리	정교화
	FMT_MSA.1	보안속성 관리	정교화
	FMT_MSA.3	정적 속성 초기화	정교화
	FMT_MTD.1	TSF 데이터 관리	정교화
	FMT_PWD.1(확장)	ID 및 패스워드 관리	확장
	FMT_SMF.1	관리기능 명세	
	FMT_SMR.1	보안 역할	정교화
TSF 보호 (FPT)	FPT_PST.1(확장)	저장된 TSF 데이터 기본적인 보호	확장
	FPT_STM.1	신뢰할 수 있는 타임스탬프	
	FPT_TEE.1	외부 실체 시험	정교화
	FPT_TST.1	TSF 자체 시험	정교화
TOE 접근 (FTA)	FTA_MCS.2	사용자 속성별 동시 세션 수의 제한	
	FTA_SSL.5(확장)	TSF에 의한 세션 관리	확장, 정교화
	FTA_TSE.1	TOE 세션 설정	정교화
안전한 경로/채널 (FTP)	FTP_TRP.1	안전한 경로	정교화

[표 2] 필수 SFR

5.1.1. 보안감사(FAU)

5.1.1.1. FAU_ARP.1 보안 경보

계층관계 없음

종속관계 FAU_SAA.1 잠재적인 위반 분석

FAU_ARP.1.1 TSF는 잠재적인 보안 위반을 탐지한 경우, [할당 : *행동 목록*]을 취해야 한다.

5.1.1.2. FAU_GEN.1 감사데이터 생성

계층관계 없음

종속관계 FPT_STM.1 신뢰할 수 있는 타임스탬프

FAU_GEN.1.1 TSF는 다음과 같은 감사대상 사건들의 감사레코드를 생성할 수 있어야 한다.

a) 감사 기능의 시동(start-up)과 종료(shut-down)

b) *지정되지 않음* 감사 수준에 따른 모든 감사대상 사건

c) [[표 3] 감사대상 사건의 "감사대상 사건" 참조, [할당 : *기타 특별히 정의된 감사대상 사건*]]

FAU_GEN.1.2 TSF는 최소한 다음 정보를 각 감사 레코드 내에 기록해야 한다.

a) 사건 일시, 사건 유형, 주체의 신원(가능한 경우), 사건 결과(성공 또는 실패)

b) 각 감사 사건 유형에 대하여, 보호프로파일/보안목표명세서에 포함된 기능 컴포넌트의 감사대상 사건 정의에 기반한 [[표 3] 감사대상 사건의 "추가적인 감사기록 내용" 참조, [할당 : *기타 감사 관련 정보*]]

응용 시 주의사항

- o 보안목표명세서 작성자는 TOE에서 지원해야 하는 감사기록을 아래 표를 참조하여 FAU_GEN.1.1 할당 오퍼레이션을 적용해야 한다. 단, TOE의 보안기능 구동과 관련된 주요 사건은 반드시 감사대상 사건에 포함하여 감사기록을 남기도록 권고된다.
- o 감사기능이 TOE의 주요 프로세스에 포함되어 동작하는 경우, 감사기능의 '시동(start-up)'은 TOE 초기 시동 후 주요 프로세스의 시동에 대한 감사기록으로 판단하여도 무방하다. 감사기능의 '종료'는 '시동'과 유사한 수준(예: 프로세스 종료 감사기록 등) 또는 하위 수준 사건(예: 장비 종료 감사기록 등)의 감사기록으로 대체할 수 있다.
- o 감사데이터에는 사건 발생 일시, 사건 유형, 사건을 발생시킨 주체의 신원(예: 계정, IP 등), 사건의 결과(성공 또는 실패)를 포함해야 한다.

보안기능 컴포넌트	감사대상 사건	추가적인 감사기록 내용
FAU_ARP.1	잠재적인 보안 위반으로 인하여 취해지는 대응행동	
FAU_SAA.1	분석 메커니즘의 동작개시와 동작정지, 도구에 의한 자동대응	
FAU_STG.3	임계치를 초과했을 경우의 대응행동	
FAU_STG.4	감사 저장이 실패했을 경우의 대응행동	
FDP_IFF.1	요청된 정보흐름을 허용하는 결정 정보흐름 요청에 대한 모든 결정	객체의 식별 정보
FIA_AFL.1	실패한 인증 시도의 한계치 도달과 취해진 대응행동, 적절하다면 이어서 일어나는 정상 상태로의 회복	
FIA_UAU.1	인증 메커니즘의 모든 사용	

보안기능 컴포넌트	감사대상 사건	추가적인 감사기록 내용
FIA_UAU.4	인증데이터의 재사용 시도	
FIA_UID.1	제공된 사용자 신원을 포함하여 사용자 식별 메커니즘의 모든 사용	
FMT_MOF.1	TSF 기능에 대한 모든 변경	
FMT_MSA.1	보안속성 값 대한 모든 변경	
FMT_MSA.3	허가 규칙이나 제한 규칙의 기본 설정에 대한 변경 보안속성의 초기값에 대한 모든 변경	
FMT_MTD.1	TSF 데이터 값에 대한 모든 변경	변경된 TSF 데이터 값
FMT_PWD.1	패스워드에 대한 모든 변경	
FMT_SMF.1	관리기능 사용	
FMT_SMR.1	역할을 분담하는 사용자 그룹에 대한 변경	
FPT_STM.1	시간의 변경	
FPT_TEE.1	외부 실체 시험의 실행과 시험 결과	
FPT_TST.1	TSF 자체 시험의 실행과 시험 결과	무결성 위반시 변경된 TSF 데이터 혹은 실행 코드
FTA_MCS.2	동시 세션 수의 제한에 기반한 새로운 세션 거부	
FTA_SSL.5	상호작용 세션의 잠금 또는 종료	
FTA_TSE.1	세션 설정 메커니즘으로 인한 세션 설정 거부 사용자 세션을 설정하려는 모든 시도	
FTP_TRP.1	안전한 경로 기능의 장애 모든 안전한 경로 장애와 관련된 사용자 식별	

[표 3] 감사대상 사건

5.1.1.3. FAU_SAA.1 잠재적인 위반 분석

계층관계 없음

종속관계 FAU_GEN.1 감사 데이터 생성

FAU_SAA.1.1 TSF는 감사된 사건을 검사하는 경우에 규칙 집합을 적용할 수 있어야 하고, 이 규칙에 기반하여 SFR의 수행에 대한 잠재적 위반을 지적할 수 있어야 한다.

FAU_SAA.1.2 TSF는 감사된 사건을 검사하는 경우에 다음과 같은 규칙을 적용해야 한다.

a) 잠재적인 보안 위반을 나타내는 알려진 [할당 : *정의된 감사대상 사건의 부분집합*]의 누적 또는 조합

b) [할당 : *기타 규칙*]

응용 시 주의사항

o FAU_SAA..1.2에서 [할당 : 정의된 감사대상 사건의 부분집합]의 예는 다음과 같다.

- FIA_UAU.1의 감사대상 사건 중 인증실패 감사 사건
- FDP_IFF의 감사대상 사건 중 통제규칙 위반 감사 사건
- FPT_TST.1의 감사대상 사건 중 무결성 위반 감사 사건 등

5.1.1.4. FAU_SAR.1 감사검토

계층관계	없음
종속관계	FAU_GEN.1
FAU_SAR.1.1	TSF는 [할당 : *인가된 사용자*]에게 감사 레코드로부터 [모든 감사 데이터]를 읽을 수 있는 기능을 제공해야 한다.
FAU_SAR.1.2	TSF는 사용자가 정보를 해석하기에 적합하도록 감사 레코드를 제공해야 한다.

5.1.1.5. FAU_SAR.3 선택 가능한 감사검토

계층관계	없음
종속관계	FAU_SAR.1 감사 검토
FAU_SAR.3.1	TSF는 [할당 : *논리 관계를 갖는 기준*]에 기초하여 감사 데이터에 대한 [할당 : *선택 및/또는 순서화 방법*]을 적용할 수 있는 능력을 제공해야 한다.

응용 시 주의사항

- o AND, OR 등의 논리적 관계 기준에 따른 선택적인 감사 검토가 가능해야 한다.
- o 검색결과에 대한 정렬 또는 순서화 방법을 적용하여 감사데이터를 조회할 수 있다.

5.1.1.6. FAU_STG.1 감사 증적 저장소 보호

계층관계	없음
종속관계	FAU_GEN.1 감사 데이터 생성
FAU_STG.1.1	TSF는 인가되지 않은 삭제로부터 감사 증적 내에 저장된 감사레코드를 보호해야 한다.
FAU_STG.1.2	TSF는 감사 증적 내에 저장된 감사 레코드에 대한 비인가된 변경을 *방지*해야 한다.

응용 시 주의사항

- o 인가된 관리자라 할지라도 감사데이터를 삭제 및 변경할 수 없도록, 관련 유저인터페이스(UI) 및 CLI 명령어가 제공되지 않아야 한다.
- o 본 보안기능 요구사항은 TOE 보안기능요구사항으로 완전히 구현할 수 없는 경우, TOE 운영환경에서 감사 증적 저장소 보호를 지원할 수 있다.

5.1.1.7. FAU_STG.3 감사 데이터 손실 예측 시 대응 행동

계층관계	없음
종속관계	FAU_STG.1 감사 증적 저장소 보호

FAU_STG.3.1 TSF는 감사 증적이 [할당 : *미리 정의된 한도*]를 초과할 경우 [인가된 관리자에게 통보, [할당: *기타 감사 저장 실패가 예상되는 경우에 취해야 할 대응행동*]]을 취해야 한다.

응용 시 주의사항

- o 감사증적 크기가 디스크 용량의 일정 기준(예: 90% 이상) 초과시 관리자가 알 수 있는 기능
  - 제공 방법(예시: 알람, 관리자 이메일 발송, LED 표시 등)
  - 임계치 정보 제공(예시: 90%, 100% 등)
- o 감사데이터 손실 예측 시 관리자의 대응행동으로 감사데이터를 외부 로그서버 또는 백업서버로 전송하는 기능을 제공할 수 있다. 감사데이터를 안전한 통신을 통하여 외부 로그서버 또는 백업서버로 전달하는 경우, '선택 SFR'인 FTP_ITC.1을 참조한다.
- o 본 SFR은 TOE 보안기능요구사항으로 완전히 구현할 수 없는 경우, TOE 운영환경에서 감사 데이터 손실 예측에 따른 대응행동을 지원할 수 있다.

5.1.1.8. FAU_STG.4 감사 데이터의 손실 방지

계층관계	FAU_STG.3 감사 데이터 손실 예측 시 대응 행동
종속관계	FAU_STG.1 감사 증적 저장소 보호

FAU_STG.4.1 TSF는 감사 증적이 포화인 경우, TSF는 [선택 : *'감사된 사건을 무시', '특별 권한을 갖는 인가된 사용자에 의해 취해진 행동을 제외한 감사된 사건의 방지', ' 가장 오래된 감사 레코드 덮어쓰기' 중 하나를 선택*] 및 [할당 : *감사 저장 실패의 경우에 취해야 할 그 밖의 행동*]을 수행해야 한다.

응용 시 주의사항

- o 실제로 감사 저장소가 포화인 경우, 감사 데이터의 손실을 방지하기 위한 대응행동을 취해야 한다. 또한, 본 SFR은 TOE 보안기능요구사항으로 완전히 구현할 수 없는 경우, TOE 운영환경에서 감사 데이터 손실 방지를 지원할 수 있다.

5.1.2. 암호지원(FCS)

5.1.2.1. FCS_CKM.1 암호키 생성

계층관계	없음
종속관계	[FCS_CKM.2 암호키 분배 또는 FCS_COP.1 암호 연산] FCS_CKM.4 암호키 파기

FCS_CKM.1.1	TSF는 다음의 [할당 : *표준 목록*]에 부합하는 명세된 암호키 생성 알고리즘 [할당 : *암호키 생성 알고리즘*]과 명세된 암호키 길이 [할당 : *암호키 길이*]에 따라 암호키를 생성해야 한다.

응용 시 주의사항

- o 본 SFR은 관리접속 시 비밀성, 무결성을 지원하기 위해 사용하는 TLS, SSH, HTTPS 등 암호통신 프로토콜 또는 중요 데이터 저장 시 암호화에 필요한 암호키 생성과 관련된 요구사항으로 보안목표명세서 작성자는 TOE가 제공하는 암호 알고리즘 등에 따라 반복 오퍼레이션을 수행하도록 권고된다.
- o TLS, SSH, HTTPS 등 암호통신 프로토콜에서 암호통신에 사용할 키를 통신 개체 간에 설정하기 위해 통신 개체들은 비대칭 암호키를 생성하게 되며 FCS_CKM.1에서는 이러한 요구사항을 정의한다. 키 설정 프로토콜은 '선택 SFR'인 FCS_CKM.2에서 정의한다. 만약 키 설정과정에서 TOE는 비대칭 키를 수신하는 역할이면 키를 생성할 필요가 없다.
- o 암호 알고리즘 및 암호키 길이는 암호비도 112비트 이상을 만족하도록 권고한다. 또한, 암호모듈 검증제도(KCMVP)에서 검증된 안전한 암호 알고리즘의 사용을 권고한다.

5.1.2.2. FCS_CKM.4 암호키 파기

계층관계	없음
종속관계	[FDP_ITC.1 보안속성 없이 사용자 데이터 유입 또는 FDP_ITC.2 보안속성을 포함한 사용자 데이터 유입 또는 FCS_CKM.1 암호키 생성]
FCS_CKM.4.1	TSF는 다음의 [할당 : *표준 목록*]에 부합하는 명세된 암호키 파기 방법 [할당 : *암호키 파기 방법*]에 따라 암호키를 파기해야 한다.

5.1.2.3. FCS_COP.1 암호 연산

계층관계	없음
종속관계	[FDP_ITC.1 보안속성 없이 사용자 데이터 유입 또는 FDP_ITC.2 보안속성을 포함한 사용자 데이터 유입 또는 FCS_CKM.1 암호키 생성] FCS_CKM.4 암호키 파기
FCS_COP.1.1	TSF는 다음의 [할당 : *표준 목록*] 에 부합하는 명세된 암호 알고리즘 [할당 : *암호 알고리즘*]과 명세된 암호키 길이 [할당 : *암호키 길이*]에 따라 [할당 : *암호 연산 목록*]을 수행해야 한다.

응용 시 주의사항

- o 본 SFR은 관리접속, TOE 구성요소 간 통신 시 비밀성, 무결성을 지원하기 위해 사용하는 TLS, SSH, HTTPS 등 암호통신 프로토콜 또는 중요 데이터 저장 시 암호화 관련 요구사항이다.

o 암호연산 시 사용하는 암호알고리즘 종류(대칭키, 비대칭키, 해시, Keyed 해시 등) 마다 FCS_COP.1을 반복하여 정의하도록 권고된다.
예: FCS_COP.1(1) 암호 연산 (대칭키 암호연산)
FCS_COP.1(2) 암호 연산 (MAC)
FCS_COP.1(3) 암호 연산 (해시)
FCS_COP.1(4) 암호 연산 (전자서명 생성)
FCS_COP.1(5) 암호 연산 (전자서명 검증)

o 암호 알고리즘에서 사용하는 암호 키 길이는 FCS_COP.1.1의 암호키 길이를 정의해야 한다. 단, 암호화 및 해시 알고리즘 보안강도는 112 bit급 이상 사용을 권고한다.
- 해시: SHA-224/256/384/512 등
- 대칭키 암호: SEED, ARIA-128/192/256 등
- 공개키 암호: RSA 2048 등
- 전자서명: RSA-PSS-2048/3072, ECDSA/KCDSA/EC-KCDSA 등

o 암호모듈검증제도(KCMVP)에서 검증된 안전한 암호 알고리즘의 사용을 권고한다.

5.1.3. 사용자 데이터 보호(FDP)

5.1.3.1. FDP_IFC.2 완전한 정보흐름 통제(상태기반 트래픽 필터링)

계층관계	FDP_IFC.1 부분적인 정보흐름통제
종속관계	FDP_IFF.1 단일 계층 보안속성
FDP_IFC.2.1	TSF는 [할당 : *주체 목록 및 정보 목록*]과 SFP에 의하여 다루어지는 통제된 주체로/주체로부터의 정보흐름을 유발하는 모든 오퍼레이션에 대하여 [상태기반 트래픽 필터링 SFP]을 강제해야 한다.
FDP_IFC.2.2	TSF는 TOE 내의 모든 주체로/주체로부터 TOE내의 모든 정보흐름을 유발하는 모든 오퍼레이션들이 정보흐름통제 SFP에 의하여 다루어짐을 보장해야 한다.

응용 시 주의사항

o 네트워크나 전송계층(L3, L4 Layer)에서 동작하는 상태기반 트래픽 필터링 기능의 경우 IP, 포트, 프로토콜 정보를 기반으로 정보흐름을 통제한다.
o 세션 계층(L5, L6, L7 Layer) 이상에서 동작하는 어플리케이션 트래픽 필터링 기능의 경우 패킷 헤더 정보를 이용하여 정보흐름을 통제한다.
o 어플리케이션 트래픽 필터링이 제공되는 경우, "선택 SFR" 부분을 참조하여 SFR을 작성해야 한다.

5.1.3.2. FDP_IFF.1 단일 계층 보안속성(상태기반 트래픽 필터링)

계층관계	없음
종속관계	FDP_IFC.1 부분적인 정보흐름 통제 FMT_MSA.3 정적 속성 초기화

FDP_IFF.1.1 TSF는 적어도 [할당 : *다음의 SFP에서 통제되는 주체와 정보의 목록, 주체와 정보 각각에 대한 보안속성*]과 같은 주체 보안속성 및 정보 보안속성 유형에 기반하여 [상태기반 트래픽 필터링 SFP]를 강제해야 한다.

FDP_IFF.1.2 TSF는 다음과 같은 규칙이 유지되면 통제된 오퍼레이션을 통하여 통제된 주체와 통제된 정보 간의 정보흐름을 허용해야 한다 :

[할당 : *각 오퍼레이션에 대하여 주체와 정보 보안속성 간에서 유지되어야 하는 보안속성에 기반한 관계*]

FDP_IFF.1.3 TSF는 [다음의 정보흐름통제 SFP]을 강제해야 한다.

1. TSF는 유효하지 않은 플래그먼트 패킷을 차단해야 한다.
2. TSF는 완전히 재조립되지 않은 패킷을 차단해야 한다.
3. TSF는 네트워크 패킷의 출발지 주소가 브로드캐스트 네트워크인 경우 패킷을 차단해야 한다.
4. TSF는 네트워크 패킷의 출발지 주소가 멀티캐스트 네트워크/루프백주소인 경우 패킷을 차단해야 한다.
5. TSF는 IPv4를 위한 RFC 5735에서 명세한 예약된 주소(240.0.0.0/4), 지정되지 않은 주소(예 0.0.0.0)가 네트워크 패킷의 출발지/목적지 주소인 경우 패킷을 차단해야 한다.
6. TSF는 다음 IP 옵션 패킷을 차단해야 한다 : Loose source 라우팅, Strict source 라우팅, Record 라우트 지정
7. TSF는 내부/외부에서 들어오는 네트워크 패킷의 출발지 주소가 TOE 네트워크 인터페이스의 주소와 동일할 경우 패킷을 차단해야 한다.
8. TSF는 수신된 패킷의 출발지 주소가 TOE 네트워크 인터페이스 주소 대역과 관련이 없을 경우 패킷을 차단해야 한다.
9. TSF는 외부로부터 들어오는 네트워크 패킷의 출발지 주소가 내부 IP 주소인 경우 패킷을 차단해야 한다.
10. TSF는 내부에서 나가는 트래픽 중 외부 IP 주소가 출발지인 트래픽의 경우 패킷을 차단해야 한다.
11. TSF는 외부로부터 들어오는 트래픽 중 SYN FLOODING 공격 트래픽의 경우 패킷을 차단해야 한다.
12. TSF는 외부로부터 들어오는 트래픽 중 UDP ECHO LOOP 공격 트래픽의 경우 패킷을 차단해야 한다.
13. TSF는 half-open된 [할당 : *지원하는 TCP 접속 수*]를 제한하고, 제한된 값에 도달할 경우 새로운 연결시도를 차단해야 한다.
14. [선택 : *TSF는 IPv6를 위한 RFC 3513에서 명세한 예약된 주소(2000::/3 범위가 아닌 유니캐스트 주소), 또는 명세되지 않은 주소가 네트워크 패킷의 출발지/목적지 주소인 경우 패킷을 차단해야 한다*, *없음 중 하나를 선택*]

15. [선택 : *TSF는 출발지/목적지 주소가 링크로컬 주소인 경우 패킷을 차단해야 한다, 없음 중 하나를 선택*]
16. { 보안목표명세서 작성자에 의해 결정 } 된 기타 규칙

FDP_IFF.1.4 TSF는 [다음과 같은 규칙]에 기반하여 정보흐름을 명시적으로 인가해야 한다.

1. 유입된 패킷이 다음과 같은 프로토콜을 사용하며 세션테이블에 등록된 경우
   가. TCP : 출발지/목적지 주소, 출발지/목적지 포트, { 보안목표명세서 작성자에 의해 결정 }된 정보

   나. UDP : 출발지/목적지 주소, 출발지/목적지 포트

   다. ICMP : [선택 : *출발지/목적지 주소, 타입,* [선택*: 코드*], [할당 *: 속성 목록*], *다른 프로토콜 없음*]
2. 유입된 패킷의 프로토콜이 다음과 같으며, 동적규칙에서 사용하는 경우
   가. 프로토콜 : [선택 : *FTP, SIP, H.323,* [할당 : *기타 프로토콜*], *없음*]

FDP_IFF.1.5 TSF는 [할당 : *보안속성에 기반하여 명시적으로 정보흐름을 거부하는 규칙*]에 기반하여 정보흐름을 명시적으로 거부해야 한다.

응용 시 주의사항

o 정보흐름통제 규칙은 개별 또는 특정 대역의 출발지/목적지 주소 및 포트 등 다양한 정보에 의해 구성될 수 있다.

o 기본적으로 모든 트래픽을 차단한 뒤, 규칙에 따라 허용된 트래픽만 통과시키는 화이트리스트 방식을 적용해야 하며, 장애 시 모든 트래픽을 통과(Bypass) 시킬 수 있는 기능은 제공되지 않아야 한다.

o FDP_IFF.1.1에서 주체의 보안속성은 출발지 IP주소가 될 수 있으며, 정보의 보안속성은 다음과 같은 내용이 될 수 있다.

가. 출발지 ip
나. 목적지 ip
다. 포트번호
라. 네트워크 인터페이스
마. 프로토콜

프로토콜	필드
ICMPv4	Type
	Code
ICMPv6	Type
	Code
IPv4	출발지 주소
	목적지 주소
	전송계층 프로토콜
IPv6	출발지 주소
	목적지 주소
	전송계층 프로토콜
	IPv6 확장헤더 필드
TCP	출발지 포트
	목적지 포트
UDP	출발지 포트
	목적지 포트

※ IPv6 확장헤더 필드는 Hop-by-Hop Options Header, Routing Header 등이 존재한다.
o FDP_IFF.1.3에서 다수의 네트워크 인터페이스가 존재하는 경우, 각각의 인터페이스에 하나의 규칙이나 다수의 규칙이 적용될 수 있어야 한다. 또한 각각의 규칙은 우선순위에 따라 적용되어야 한다.
o TSF에서 IPv6를 제공하지 않을 경우, FDP_IFF.1.3 선택 오퍼레이션에 '없음'을 명세할 수 있다.
o FDP_IFF.1.3에서 링크로컬주소는 IPv6 주소에서 단일 링크/네트워크(이더넷) 내로 범위가 제한되게 하는 주소체계를 의미한다.

5.1.4. 식별 및 인증(FIA)

5.1.4.1. FIA_AFL.1 인증 실패 처리

계층관계	없음
종속관계	FIA_UAU.1 인증
FIA_AFL.1.1	TSF는 [할당 : *인증 사건의 목록*]에 관련된 [선택 : [할당 : *양수*], *"관리자가 구성가능한* [할당 : *허용할 수 있는 수의 범위*]*안의 양수"*] 번의 실패한 인증 시도가 발생한 경우 이를 탐지해야 한다.
FIA_AFL.1.2	실패한 인증 시도가 정의된 횟수에 *도달*하면, TSF는 [할당 : *대응행동 목록*]을 수행해야 한다.

응용 시 주의사항

o 보안목표명세서 작성자는 인증실패 횟수 및 대응행동을 설정할 수 있으나, TOE에서 제공하는 디폴트값은 다음과 같이 설정되어야 한다.
  - 인증 실패 횟수 : 디폴트값 5회 이하
  - 대응행동 목록 : 식별 및 인증 기능 비활성화(디폴트값 5분 이상)
o 인증사건의 목록 예제 : 관리자, 사용자 인증시도
o TOE와 서비스(SSH 등)에 따라 인증실패 횟수와 대응행동 등을 다르게 설정하는 경우 보안목표명세서 작성자는 반복 오퍼레이션을 적용한다.

5.1.4.2. FIA_SOS.1 비밀정보의 검증

계층관계	없음
종속관계	없음
FIA_SOS.1.1	TSF는 비밀정보가 [할당 : *정의된 허용 기준*]을 만족시킴을 검증하는 메커니즘을 제공해야 한다.

응용 시 주의사항

o 비밀정보의 검증은 관리자가 새로운 관리자의 패스워드 생성 시, 패스워드 변경 시, 관리자가 최초 접속할 경우의 패스워드 변경 시와 같이 모든 패스워드 생성 · 변경 시에 적용될 수 있다.

o 패스워드 복잡도 기준을 만족해야 하는 비밀정보는 다음과 같은 인증데이터가 될 수 있다.

- 인가된 관리자 패스워드

o 보안목표명세서 작성자는 FIA_SOS.1.1 [할당: *정의된 허용 기준*]에 패스워드 조합규칙 및 길이 등을 명세할 수 있으나, 패스워드를 영문자/숫자/특수문자 중 3가지 이상의 조합규칙 및 9자리 이상으로 설정하는 기준이 포함되어야 한다.

o 관리자가 정의한 허용 기준으로 패스워드 복잡도 검증 동작 방식을 결정하는 경우 할당 오퍼레이션에서 *"FMT_PWD.1 에서 관리자가 정의한 허용 기준"*을 정의해야 한다.

5.1.4.3. FIA_UAU.1 인증

계층관계	없음
종속관계	FIA_UID.1 식별
FIA_UAU.1.1	TSF는 사용자가 인증되기 전에 사용자를 대신하여 수행될 [할당 : *TSF가 중재하는 행동의 목록*]을 허용해야 한다.
FIA_UAU.1.2	TSF는 FIA_UAU.1.1에서 명시된 행동 이외의 사용자를 대신하여 TSF가 중재하는 다른 모든 행동을 허용하기 전에 사용자를 성공적으로 인증해야 한다.

응용 시 주의사항

o TOE에서 사용자는 TOE 관리기능을 수행하는 관리자이며, 관리기능 접근권한에 따라 관리자 역할을 세분화하여 정의할 수 있다. 관리자 역할을 세분화하는 경우 FMT_SMR.1에서 요구사항을 정의한다. 본 요구사항은 TOE가 지원하는 로컬접속(콘솔포트) 및 관리접속(SSH 등)에 적용해야 한다.

o 패스워드 인증방식의 경우 식별 및 인증이 한 번에 이루어지므로 일반적으로 FIA_UID.1에서 정의한 'TSF가 중재하는 행동의 목록'과 동일하다. 인증서 기반 인증방식의 경우 식별 및 인증 이전에 인증서 저장위치/매체 선택 및 인증서 목록을 열거해주는 기능을 허용해야 한다. 따라서 보안목표명세서 작성자는 TOE에서 지원하는 인증방식에 따라 관리자 식별 및 인증 이전에 실행되어야 할 기능목록을 고려하여 할당 오퍼레이션을 수행한다.

o FIA_UAU.1.1 할당 오퍼레이션에 명세할 행동 목록이 없는 경우, FIA_UAU.1과 계층관계에 있는 FIA_UAU.2를 사용하는 것이 권고된다.

5.1.4.4. FIA_UAU.4 재사용 방지 인증 메커니즘

계층관계	없음
종속관계	없음
FIA_UAU.4.1	TSF는 [할당 : *식별된 인증 메커니즘(들)*]에 관련된 인증 데이터의 재사용을 방지해야 한다.

응용 시 주의사항

o 패스워드 인증방식과 같이 관리자 세션마다 인증 데이터가 동일한 경우 관리자 세션정보를 탈취하여 관리자 인증을 우회할 수 있으므로 세션ID를 암호화하거나 세션마다 세션ID의 유일성

을 보장(예, 패스워드 기반 암호인증 프로토콜, 타임스탬프, 난수값 포함 등)하여 인증 데이터의 재사용을 방지할 수 있다. 다중 인증메커니즘을 지원하는 경우 인증 데이터 재사용 방지가 필요한 인증 메커니즘(예, OTP 방식 등)을 식별하여 할당 오퍼레이션에 적용한다. 예를 들어 SMS 인증번호 방식의 경우 재사용 방지를 위해 시간제한, 인증번호 길이, 난수성 등 SMS 인증번호 보안속성을 추가로 설정할 수 있다.

5.1.4.5. FIA_UAU.7 인증 피드백 보호

계층관계	없음
종속관계	FIA_UAU.1 인증

FIA_UAU.7.1	TSF는 인증이 진행되는 동안 사용자에게 [할당 : *피드백 목록*]만을 제공해야 한다.

응용 시 주의사항

- o 입력되는 패스워드 등을 화면에서 볼 수 없도록 마스킹(예: "****" 등)해야 하고, 마스킹 처리해야 하는 대상은 다음과 같다. 패스워드 입력값 노출을 방지하기 위한 방법으로 사용자가 입력한 문자를 화면에 표시하지 않는 방법도 허용된다. 본 사항은 TOE의 로컬접속(콘솔포트) 및 관리접속(SSH 등)에 적용해야 한다.
  - 관리자 패스워드 생성, 변경 및 관리자 인증 시
- o 식별 및 인증 실패 시, 실패 이유에 대한 피드백(예: 잘못된 계정을 입력하였습니다, 잘못된 패스워드를 입력 하였습니다 등)을 제공하지 않아야 하며, TOE가 지원하는 로컬접속(콘솔포트) 및 관리접속(SSH 등)에 적용할 수 있다.

5.1.4.6. FIA_UID.1 사용자 식별

계층관계	없음
종속관계	없음

FIA_UID.1.1	TSF는 사용자를 식별하기 전에 사용자를 대신하여 수행될 [할당 : *TSF가 중재하는 행동의 목록*]을 허용해야 한다.
FIA_UID.1.2	TSF는 FIA_UID.1.1에서 명시된 행동 이외의 사용자를 대신하여 TSF가 중재하는 다른 모든 행동을 허용하기 전에 각 사용자를 성공적으로 식별해야 한다.

응용 시 주의사항

- o TOE에서 사용자는 TOE 장비 관리기능을 수행하는 관리자이며, 관리기능 접근권한에 따라 관리자 역할을 세분화하여 정의할 수 있다. 관리자 역할을 세분화하는 경우 FMT_SMR.1에서 요구사항을 정의한다. 본 사항은 TOE가 지원하는 로컬접속(콘솔포트) 및 관리접속(SSH 등)에 적용해야 한다.
- o FIA_UID.1.1 할당 오퍼레이션에 명세할 행동 목록이 없는 경우, FIA_UID.1과 계층관계에 있는 FIA_UID.2를 사용하는 것이 권고된다.

5.1.5. 보안 관리(FMT)

보안기능 컴포넌트	관리 기능	관리 유형
FAU_ARP.1	대응행동의 관리(추가, 제거 변경)	보안기능 관리
FAU_SAA.1	규칙의 유지(규칙 집합에서 규칙을 추가, 변경, 삭제)	보안기능 관리
FAU_SAR.1	감사 레코드 읽기 권한을 갖는 사용자 그룹의 유지(추가, 변경, 삭제)	보안역할 관리
FAU_STG.3	임계치의 유지	TSF 데이터 한계치 관리
	감사 저장 실패가 예상되는 경우에 취해야 할 대응 행동의 유지	보안기능 관리
FAU_STG.4	감사 저장 실패의 경우에 취해야 할 대응행동의 유지	보안기능 관리
FDP_IFF.1	명시적인 접근 결정에 사용된 속성의 관리	보안속성 관리
FIA_AFL.1	실패한 인증 시도의 한계치 관리	TSF 데이터 한계치 관리
	인증 실패인 경우 취해질 대응행동의 관리	보안기능 관리
FIA_SOS.1	비밀정보를 검증하기 위하여 사용된 허용 기준의 관리	TSF 데이터 관리
FIA_UAU.1	관리자에 의한 인증 데이터의 관리 관련 사용자에 의한 인증 데이터의 관리	TSF 데이터 관리
	사용자가 인증되기 전에 수행할 수 있는 행동 목록의 관리	보안기능 관리
FIA_UID.1	사용자 신원의 관리	TSF 데이터 관리
	인가된 관리자가 식별 전에 허용되는 행동을 변경할 수 있는 경우, 그러한 행동 목록의 관리	보안기능 관리
FMT_MOF.1	TSF 기능과 상호작용할 수 있는 역할 그룹의 관리	보안 역할 관리
FMT_MSA.1	보안속성과 상호작용할 수 있는 역할 그룹의 관리	보안속성 관리
	보안속성에 의해 명세된 값을 상속하는 규칙의 관리	
FMT_MSA.3	초기값을 명세할 수 있는 역할 그룹의 관리	보안 역할 관리
	주어진 접근통제 SFP에 따라 디폴트값을 허가하거나 제한하도록 설정하는 것에 대한 관리 보안속성에 의해 명세된 값을 상속하는 규칙의 관리	보안속성 관리
FMT_MTD.1	TSF 데이터와 상호작용할 수 있는 역할 그룹의 관리	보안 역할 관리
FMT_PWD.1	ID, 패스워드 설정 규칙의 관리	보안기능 관리
FMT_SMR.1	역할을 분담하는 사용자 그룹의 관리	보안 역할 관리
FPT_STM.1	시간 관리	보안기능 관리
FPT_TEE.1	'초기 시동 시', '주기적으로', 또는 '명세된 조건에서'와 같이, 외부 실체 시험이 발생되는 조건의 관리 (적절한 경우) 시간 간격의 관리	TSF 데이터 관리
FPT_TST.1	'초기 시동 시', '주기적으로', 또는 '명세된 조건에서'와 같이, TSF 자체 시험이 발생되는 조건의 관리 (적절한 경우) 시간 간격의 관리	TSF 데이터 관리

보안기능 컴포넌트	관리 기능	관리 유형
FTA_MCS.2	관리자에 의한 동시 사용자 세션 수 최대 허용치를 관리하기 위한 규칙의 관리	TSF 데이터 한계치 관리
FTA_SSL.5	각 사용자에 대해서 세션 잠금 또는 종료가 발생하는 사용자 비활동 기간의 명세 세션 잠금 또는 종료가 발생하는 디폴트 사용자 비활동 시간의 명세	TSF 데이터 관리
FTA_TSE.1	인가된 관리자에 의한 세션 설정 조건의 관리	TSF 데이터 관리
FTP_TRP.1	안전한 경로를 요구하는 행동의 구성(지원되는 경우에 한함)	보안기능 관리

[표 4] 컴포넌트별 보안관리 행동 및 관리 유형

5.1.5.1. FMT_MOF.1 보안기능 관리

계층관계 없음

종속관계 FMT_SMF.1 관리기능 명세

FMT_SMR.1 보안 역할

FMT_MOF.1.1 TSF는 [할당 : *기능목록*]의 기능에 대해 ***관리 행동***을 하는 능력을 [인가된 관리자]로 제한해야 한다.

응용 시 주의사항

- o 정교화 오퍼레이션을 적용한 "관리 행동"은 일부 TSF 기능에 대해 행동을 결정(determine the behavior), 중지(disable), 개시(enable), 행동을 변경(modify the behaviour of)하는 능력을 모두 포함한다. 본 사항은 TOE가 지원하는 로컬접속(콘솔포트) 및 관리접속(SSH 등)에 적용해야 한다.
- o 보안기능 행동을 결정할 수 있는 조건 또는 규칙을 추가, 삭제, 변경하는 활동은 보안기능 관리 행동에 해당하고 조건 또는 규칙에 따라 TSF가 대응해야 할 행동을 추가, 제거, 변경하는 활동도 보안기능 관리 행동에 해당한다. 또한 동일한 목적을 위해 제공하는 메커니즘, 프로토콜 등이 다양할 경우 이를 선택하는 활동은 행동 변경에 해당하므로 보안기능 관리 행동이다.
- o 보안목표명세서 작성자는 [표 4] 컴포넌트별 보안관리 행동 및 관리 유형을 참고하여 TOE에서 관리기능을 지원하는 경우 FMT_MOF.1.1 할당 오퍼레이션을 수행할 수 있다.
- o 보안목표명세서 작성자는 각 컴포넌트에 대하여 [표 4] 컴포넌트별 보안관리 행동 및 관리 유형에 제시된 관리 기능 이외에도 추가적인 보안기능 관리 행동을 정의 할 수 있고, 본 문서에 정의된 보안기능 요구사항 이외의 추가 혹은 확장된 요구사항에 대한 보안기능 관리 행동을 제시할 수 있다.

5.1.5.2. FMT_MSA.1 보안속성 관리

계층관계 없음

종속관계 [FDP_ACC.1 부분적인 접근통제 또는

FDP_IFC.1 부분적인 정보흐름통제]

	FMT_SMF.1 관리기능 명세 FMT_SMR.1 보안 역할
FMT_MSA.1.1	TSF는 [할당 : *보안속성 목록*]의 보안속성을 [선택 : *디폴트값 변경, 질의, 변경, 삭제,* [할당 : *기타 연산*]]하는 능력을 [인가된 관리자]로 제한하도록 [할당 : ***상태기반 트래픽필터링 SFP,*** *정보흐름통제 SFP*]를 강제해야 한다.

응용 시 주의사항

- o 보안목표명세서 작성자는 [표 4] 컴포넌트별 보안관리 행동 및 관리 유형을 참고하여 TOE에서 보안속성 관리 기능을 지원하는 경우 FMT_MSA.1.1에 할당 오퍼레이션을 정의한다.
- o 보안목표명세서 작성자는 각 컴포넌트에 대하여 [표 4] 컴포넌트별 보안관리 행동 및 관리 유형에 제시된 관리 기능 이외에도 추가적인 보안속성 관리 행동을 정의 할 수 있고, 본 문서에 정의된 보안기능 요구사항 이외의 추가 혹은 확장된 요구사항에 대한 보안속성 관리 행동을 제시할 수 있다.

5.1.5.3. FMT_MSA.3 정적 속성 초기화

계층관계	없음
종속관계	FMT_MSA.1 보안속성 관리 FMT_SMR.1 보안 역할
FMT_MSA.3.1	TSF는 SFP를 강제하기 위하여 사용되는 보안속성의 [선택 : *제한적인, 허가하는,* [할당 : *기타 속성의*] *중 하나를 선택*] 디폴트값을 제공하도록 [할당 : ***상태기반 트래픽필터링 SFP,*** *정보흐름통제 SFP*]를 강제해야 한다.
FMT_MSA.3.2	TSF는 객체나 정보 생성 시 디폴트값을 대체하기 위하여 [인가된 관리자]가 선택적인 초기값을 명세하도록 허용해야 한다.

5.1.5.4. FMT_MTD.1 TSF 데이터 관리

계층관계	없음
종속관계	FMT_SMF.1 관리기능 명세 FMT_SMR.1 보안 역할
FMT_MTD.1.1	TSF는 [할당 : *TSF 데이터 목록*]을 ***관리***하는 능력을 [인가된 관리자]로 제한해야 한다.

응용 시 주의사항

- o 정교화 오퍼레이션을 적용한 "관리"의 의미는 디폴트값 변경(change_default), 질의(query), 변경(modify), 삭제(delete), 소거(clear), 기타 연산(other operation) 등을 포함한다.
- o 보안목표명세서 작성자는 [표 4] 컴포넌트별 보안관리 행동 및 관리 유형을 참고하여 TOE에서 TSF 데이터 관리 기능을 지원하는 경우 FMT_MTD.1.1에 할당 오퍼레이션을 수행할 수 있다.
- o 보안목표명세서 작성자는 각 컴포넌트에 대하여 [표 4] 컴포넌트별 보안관리 행동 및 관리 유

형에 제시된 관리 기능 이외에도 추가적인 TSF 데이터 관리 행동을 정의 할 수 있고, 본 문서에 정의된 보안기능 요구사항 이외의 추가 혹은 확장된 요구사항에 대한 TSF 데이터 관리 행동을 제시할 수 있다. 예를 들어, 연속인증 실패 시 TOE 접속 제한 시간 설정 등과 같은 관리 행동이 제시될 수 있다.

5.1.5.5. FMT_PWD.1 ID 및 패스워드 관리(확장)

계층관계	없음
종속관계	FMT_SMF.1 관리기능 명세 FMT_SMR.1 보안 역할
FMT_PWD.1.1	TSF는 [할당: *기능목록*]의 패스워드를 다음과 같이 관리하는 능력을 [인가된 관리자]로 제한해야 한다. 1. [할당 : *패스워드 조합 규칙 및/또는 길이*] 2. [할당 : *패스워드에 제외할 특수 문자 관리 등 기타 관리*]
FMT_PWD.1.2	TSF는 [할당: *기능목록*]의 ID를 다음과 같이 관리하는 능력을 [인가된 관리자]로 제한해야 한다. 1. [할당 : *ID 조합 규칙* 및/또는 길이] 2. [할당 : *ID에 제외할 특수 문자 관리 등 기타 관리*]
FMT_PWD.1.3	TSF는 [선택 : *설치 과정에서 ID 및 패스워드를 설정, 설치 과정에서 패스워드를 설정, 인가된 관리자가 최초 접속 시 ID 및 패스워드를 변경, 인가된 관리자가 최초 접속 시 패스워드를 변경 중 하나를 선택*]하는 기능을 제공해야 한다.

응용 시 주의사항

- o TOE에서 관리자가 ID 및 패스워드 조합규칙과 길이 등을 관리하는 기능을 제공하지 않을 경우, FMT_PWD.1.1, FMT_PWD.1.2 할당 오퍼레이션에 '없음'을 명세할 수 있다.
- o 보안목표명세서 작성자는 FMT_PWD.1.1 [할당 : *기능목록*]에 관리자 패스워드 생성 및 변경을 포함하여 패스워드 관리가 필요한 기능에 대해 정의해야 한다.
- o 본 사항은 TOE가 지원하는 로컬접속(콘솔포트) 및 관리접속(SSH 등)에 적용해야 한다.
- o FMT_PWD.1.1에서 관리자가 설정할 수 있는 패스워드 조합규칙에는 영문자/숫자/특수문자 중 3가지 이상의 조합 규칙 및 9자리 이상으로 구성하는 설정을 포함해야 한다.
- o FMT_PWD.1.3에 제시된 '설치 과정에서 ID 및 패스워드를 설정, 설치 과정에서 패스워드를 설정'의 경우에는 관리자 최초 접속 시 패스워드 강제 변경 기능을 요구하지 않는다.

5.1.5.6. FMT_SMF.1 관리기능 명세

계층관계	없음
종속관계	없음

FMT_SMF.1.1	TSF는 다음의 관리 기능을 수행할 수 있어야 한다: [할당 : *TSF가 제공하는 관리 기능 목록*]

응용 시 주의사항

o 보안목표명세서 작성자는 관리 행동을 지원하는 모든 기능을 열거한다. FMT_SMF.1에 열거된 관리기능 목록은 FMT_MOF.1, FMT_MTD.1, FMT_MSA.1, FMT_PWD.1 등에서 오퍼레이션으로 정의한 TSF 기능관리 및 TSF 데이터, 보안속성 관리 행동에 일관성을 보장해야 한다.

5.1.5.7. FMT_SMR.1 보안 역할

계층관계	없음
종속관계	FIA_UID.1 식별
FMT_SMR.1.1	TSF는 [할당 : *인가된 역할*] 역할을 유지해야 한다.
FMT_SMR.1.2	TSF는 사용자와 **FMT_SMR.1.1에 정의된** 역할을 연관 지을 수 있어야 한다.

5.1.6. TSF 보호(FPT)

5.1.6.1. FPT_PST.1 저장된 TSF 데이터 기본적인 보호(확장)

계층관계	없음
종속관계	없음
FPT_PST.1.1	TSF는 TSF에 의해 통제되는 저장소에 저장되는 [할당 : *TSF 데이터*]를 비인가된 *노출*로부터 보호해야 한다.

응용 시 주의사항

o TSF에 의해 통제되는 저장소는 TOE 내부 또는 TOE와 상호작용하는 외부 실체(DBMS 등)를 의미한다.

o 보호대상 TSF 데이터 예

- 관리자 패스워드, 암호키(사전 공유키, 대칭키, 개인키), TOE 설정값(보안정책, 환경설정 매개변수), 감사 데이터 등

o 비인가된 노출로부터 보호하기 위한 방법으로 TSF 데이터를 암호화해서 저장하거나 접근통제 및 숨김 등을 적용할 수 있다.

o 관리자의 패스워드가 TOE에 하드코딩 되거나 평문(단순 인코딩 포함)으로 저장되지 않아야 한다.

o 암호와 관련된 부분은 암호지원(FCS) 클래스를 참고한다.

5.1.6.2. FPT_STM.1 신뢰할 수 있는 타임스탬프

계층관계	없음
종속관계	없음

FPT_STM.1.1 TSF는 신뢰할 수 있는 타임스탬프를 제공할 수 있어야 한다.

응용 시 주의사항

o TSF에서 신뢰할 수 있는 타임스탬프 기능을 모두 제공하거나, TSF는 외부 실체(예: 신뢰할 수 있는 NTP 서버)의 신뢰된 시간정보를 동기화해서 타임스탬프 기능을 수행할 수 있다.

5.1.6.3. FPT_TEE.1 외부 실체 시험

계층관계 없음

종속관계 없음

FPT_TEE.1.1 TSF는 [할당: *외부 실체의 속성 목록*] 만족되는지 검사하기 위해 [선택 : *초기 시동 시, 정규 운영 중 주기적으로, 인가된* ***관리자*** *요구 시,* [할당 *: 기타 조건들*]] 일련의 시험을 실행해야 한다.

FPT_TEE.1.2 시험이 실패할 경우, TSF는 [할당 : *대응행동*]을 수행해야 한다.

응용 시 주의사항

o 외부 실체 시험 대상은 보안목표명세서 작성자에 의하여 선택 가능하나, 시험 대상이 되는 실체의 비정상상태(예: 오류, 정지 등) 등으로 인하여 TOE의 주요 기능 및 보안기능에 영향을 미치는 경우 해당 실체는 외부 실체 시험의 대상으로 반드시 포함하여야 한다.

o 외부 실체 시험이 실패할 경우 대응행동으로 시험대상 실체에 맞는 적절한 대응행동이 제시될 수 있다. 예를 들어, TOE의 주요 기능 및 보안기능에 영향을 미치는 외부 실체의 경우 하드웨어 외벽의 LED 또는 알람 등을 이용하여 관리자가 장비의 비정상 상태를 즉시 인지하도록 기능을 제공할 수 있다.

o 외부 실체 시험은 동일한 시점에 전체 시험대상이 모두 한꺼번에 시험되어야 함을 요구하지는 않으나, 시험대상별로 필수적으로 시험되어야 할 시점에는 반드시 시험되도록 해야 한다. 시험대상별로 필수적으로 시험되어야 할 시점에는 반드시 시험되도록 해야 한다. 예를 들어, 초기 시동 시에 TOE의 주요 기능 및 보안기능에 영향을 미치는 외부 실체는 모두 시험되어야 함을 의미한다.

o 운영 중 수행하는 외부 실체 시험의 주기(예: *정규 운영 중 1시간 단위, 인가된 관리자 요구 시 등)* 는 보안목표명세서 작성자에 의하여 선택 가능하나, TOE의 비정상상태 발생시 피해를 주지 않는 범위 내에서 시험주기를 결정하여야 한다.

o 관리자가 외부 실체 시험을 직접 실행하는 기능을 제공할 수 있고, 직접 실행하는 시험의 대상은 전체 또는 일부로 보안목표명세서 작성자에 의하여 지정 될 수 있다.

o NTP서버, 인증서버, 로그서버, DBMS 등 TOE와 연동하는 TOE 외부의 모든 실체가 추가적인 시험의 대상이 될 수 있고, TOE의 안전하고 정확한 운영을 위하여 필요한 외부 실체는 시험대상에 포함시키도록 권고된다.

5.1.6.4. FPT_TST.1 TSF 자체시험

계층관계	없음
종속관계	없음

FPT_TST.1.1	TSF는 [선택 : [할당 : *TSF의 부분들*], *TSF*]의 정확한 운영을 입증하기 위하여 *시동 시, 정규 운영 동안 주기적으로* 자체 시험을 실행해야 한다.
FPT_TST.1.2	TSF는 **인가된 관리자**에게 [선택 : [할당 : *TSF 데이터의 부분들*], *TSF 데이터*]의 무결성을 검증하는 기능을 제공해야 한다.
FPT_TST.1.3	TSF는 **인가된 관리자**에게 [선택 : [할당 : *TSF의 부분들*], *TSF*]의 무결성을 검증하는 기능을 제공해야 한다.

응용 시 주의사항

- o TSF 자체시험은 식별 및 인증 프로세스, 정보흐름통제 프로세스, 보안관리 프로세스 등의 보안기능 구동과 관련된 주요 프로세스 등에 적용하도록 권고한다.
- o TSF 자체시험 대상은 보안목표명세서 작성자에 의하여 선택 가능하나, 시험 대상이 되는 실체의 비정상상태(예: 오류, 정지 등) 등으로 인하여 주요 기능 및 보안기능에 영향을 미치는 경우 해당 실체는 자체시험의 대상으로 반드시 포함하여야 한다.
- o TOE의 설정값(예: 환경설정 매개변수), TSF 등이 무결성 검증 대상이 될 수 있다.
- o TSF 자체시험은 동일한 시점에 전체 시험대상이 모두 한꺼번에 시험되어야 함을 요구하지는 않으나, 시험대상별로 필수적으로 시험되어야 할 시점에는 반드시 시험되도록 해야 한다. 예를 들어, 초기 시동 시에 TOE의 보안 기능에 영향을 미치는 TSF는 모두 시험되어야 함을 의미한다.
- o 운영 중 수행하는 TSF 자체시험의 주기는 보안목표명세서 작성자에 의하여 선택 가능하나, TOE의 비정상상태 발생시 피해를 주지 않는 범위 내에서 시험주기를 결정하여야 한다.

5.1.7. TOE 접근(FTA)

5.1.7.1. FTA_MCS.2 사용자 속성별 동시 세션 수의 제한

계층관계	FTA_MCS.1 기본적인 동시 세션 수의 제한
종속관계	FIA_UID.1 식별

FTA_MCS.2.1	TSF는 [관리자 관리접속 세션의 경우 동시 세션의 최대 수는 1로 제한, 동일 사용자에 대해 관리접속 세션과 로컬접속 세션의 동시 세션 연결금지, { 보안목표명세서 작성자에 의해 결정 }된 동시 세션의 최대 수에 대한 규칙] 규칙에 따라서 동일 사용자에 속하는 동시 세션의 최대 수를 제한해야 한다.
FTA_MCS.2.2	TSF는 기본적으로 사용자별로 [1] 개의 세션 한계치를 강제해야 한다.

응용 시 주의사항

- o FMT_MCS.2에 제시된 세션이라 함은 '관리자의 접속'을 의미하므로 세션수는 '관리자의 접속수'로 적용해야 한다.
- o TOE에 접속하는 인가된 관리자의 관리접속에 대하여 서비스별(예: SSH, HTTPS, TLS, IPSec)로 세션수를 제한하는 경우, FTA_MCS.2.1 할당 오퍼레이션으로 정의한다.
- o 한 단말에서 관리자의 관리접속 후 다른 단말에서 동일 계정 또는 동일 권한으로 관리접속을 다시 수행하는 경우, 신규 접속을 차단하거나 이전 접속을 종료해야 한다.
- o TOE의 인가된 관리자 권한에 따라 높은 권한을 가진 사용자가 먼저 관리접속 중인 경우, 그보다 낮은 권한을 갖는 사용자의 관리접속은 제한될 수 있다.
- o TOE 운영상황에 대한 모니터링만 수행하는 인가된 관리자에 대해서는 중복로그인을 허용할 수 있다.
- o 동일 권한으로 로그인 한 경우라도, 정책이 충돌하지 않음을 입증하면 중복 로그인을 허용할 수 있다.

5.1.7.2. FTA_SSL.5 TSF에 의한 세션 관리(확장)

계층관계	없음
종속관계	FIA_UAU.1 인증 또는 없음

FTA_SSL.5.1 TSF는 [할당 : **관리자** 비활동 기간] 후 **관리자의** 상호작용 세션을 [선택 :

- *세션 잠금 및/또는 세션잠금을 해제하기 전에* ***관리자*** *재인증,*
- *세션 종료*] 해야 한다.

응용 시 주의사항

- o 본 SFR은 일정시간 관리자 활동이 없는 경우 세션을 잠그거나 종료하는 기능을 요구하고, TOE가 지원하는 로컬접속(콘솔포트) 및 관리접속(SSH 등)에 적용해야 한다.
- o 인가된 관리자자 비활동 시간은 TOE에서 고정된 값(10분 이내)을 사용하거나, 인가된 관리자가 설정하는 기능을 제공할 수 있다. 단, 디폴트값은 10분 이내로 설정되어야 한다.
- o 단, 모니터링만 수행하는 관리자 계정에 대해서는 세션 잠금 또는 종료를 적용하지 않을 수 있다.
- o TOE와 서비스(SSH 등)에 따라 비활동 시간과 대응행동(세션 잠금 또는 세션 종료)을 다르게 제공할 경우 보안목표명세서 작성자는 반복 오퍼레이션을 적용한다.
- o 세션잠금의 경우 세션잠금을 해제하기 이전에는 관리자의 데이터 접근 등의 모든 활동을 무력화 해야 하며, TOE 설정값 등 현재 내용을 읽을 수 없도록 화면표시 장치를 소거하거나 덮어쓰기를 수행하도록 요구된다.

5.1.7.3. FTA_TSE.1 TOE 세션 설정

계층관계	없음
종속관계	없음

FTA_TSE.1.1	TSF는 [접속 IP, [선택: *접속 시간, 동일 계정의 관리접속 세션 활성화 여부, 동일 권한을 갖는 관리자 계정의 관리접속 세션 활성화 여부,* [할당: *중요 관리기능 속성*], *없음*]]에 기반하여 **관리자의 관리접속 세션** 설정을 거부할 수 있어야 한다.

응용 시 주의사항

- o 관리자의 접속 가능 IP로 지정된 단말에서만 관리자의 관리접속을 세션을 허용해야 한다.
- o 보안목표명세서 작성자는 접속 가능 IP 수를 설정할 수 있으나, TOE에서 제공하는 디폴트값은 2개 이하로 설정되어야 한다.
- o 관리자의 접속 가능 IP 설정 시, 192.168.10.2 ~ 253 등과 같이 IP주소 범위를 지정하여 추가하는 방식은 허용하지 않으며, 개별적으로 IP주소를 1개씩 추가하도록 구현해야 한다. 또한, IP 주소 지정 시 네트워크 전체 범위를 의미하는 0.0.0.0, 192.168.10.*, any 등에 대한 설정은 허용하지 않는다.
- o 보안목표명세서 작성자는 접속 IP 외 추가적으로 관리자 접속시간, 동일 계정 관리접속 세션 활성화 여부 등을 추가할 수 있다.

5.1.8. 안전한 경로/채널(FTP)

5.1.8.1. FTP_TRP.1 안전한 경로

계층관계	없음
종속관계	없음

FTP_TRP.1.1	TSF는 자신과 ***관리접속*** **관리자** 간에 다른 통신 경로와 논리적으로 구별되고, 단말의 보증된 식별을 제공하며, *변경, 노출,* [할당: *무결성 또는 비밀성 위반의 다른 유형*]로부터 통신 데이터를 보호하는 통신 경로를 제공해야 한다.
FTP_TRP.1.2	TSF는 [선택 : *TSF,* ***관리접속 관리자***]가 안전한 경로를 통하여 통신을 초기화하는 것을 허용해야 한다.
FTP_TRP.1.3	TSF는 [선택 : ***관리접속 관리자 인증***, [할당: *안전한 경로가 요구되는 기타 서비스*]]에 대하여 안전한 경로의 사용을 요구해야 한다.

응용 시 주의사항

- o TOE는 관리자의 관리접속 시 암호통신 프로토콜을 이용한 신뢰된 채널을 제공해야 한다. SSH, TLS, HTTPS, IPSec이 제시될 수 있고, 암호와 관련된 부분은 FCS 클래스를 참고한다.
- o 관리자의 관리접속 시 TLS 프로토콜을 지원하는 경우 TLS 1.2(RFC 5246) 이상을 지원해야 하고, SSH 프로토콜을 지원하는 경우 SSH v2(RFC 4251 ~ 4254) 이상을 지원해야 한다. 암호와 관련된 부분은 FCS 클래스를 참고하되 사용하는 프로토콜에서 공개된 취약점은 모두 보완하여 안전하게 사용하도록 권고된다.

o HTTPS는 HTTP에 TLS를 적용한 것이다. HTTPS는 소켓 통신에서 평문을 이용하는 대신에 TLS를 통해 세션 데이터를 암호화한다. TLS는 취약점 패치가 되고 안정성이 검증된 최신버전을 적용하도록 권고된다.

5.2. 보안기능요구사항(선택 SFR)

본 보호프로파일에서의 '선택 SFR'은 다음과 같다. '선택 SFR'은 필수로 구현하도록 요구되지 않으나 TOE에서 관련 기능을 추가로 제공할 경우, 보안목표명세서 작성자는 해당 SFR을 보안목표명세서에 포함해야 한다.

보안기능 클래스	보안기능 컴포넌트		비고
보안감사 (FAU)	FAU_SEL.1	선택적인 감사	
암호지원 (FCS)	FCS_CKM.2	암호키 분배	정교화
사용자 데이터보호 (FDP)	FDP_IFC.1	부분적인 정보흐름 통제	
	FDP_IFF.1	단일 계층 보안속성(어플리케이션 트래픽 필터링)	
TSF 보호 (FPT)	FPT_ITT.1	내부전송 TSF데이터의 기본적인 보호	
	FPT_TUD.1(확장)	TSF 보안패치 업데이트	
안전한 경로/채널 (FTP)	FTP_ITC.1	TSF 간 안전한 채널	

[표 5] 선택 SFR

5.2.1. 보안감사(FAU)

5.2.1.1. FAU_SEL.1 선택적인 감사

계층관계	없음
종속관계	FAU_GEN.1 감사 데이터 생성
	FMT_MTD.1 TSF 데이터 관리
FAU_SEL.1.1	TSF는 다음 속성에 기반하여 모든 감사대상 사건 집합으로부터 감사되어야 할 사건의 집합을 선택할 수 있어야 한다. a) [선택 : *객체 신원, 사용자 신원, 주체 신원, 호스트 신원, 사건 유형*] b) [할당 : *감사 선택의 기초가 되는 추가 속성 목록*]

응용 시 주의사항

- o FAU_SEL.1 선택적인 감사는 선택적으로 구현 가능한 기능 요구사항('선택 SFR')으로 TOE에서 위 기능을 추가로 제공할 경우, 보안목표명세서 작성자는 본 요구사항을 SFR에 포함해야 한다.
- o 보안목표명세서 작성자가 본 SFR을 포함할 경우, 필요 시 보안문제정의 및 보안목적 등을 추가적으로 도출해야 한다.
- o 보안목표명세서 작성자는 감사되어야 할 사건의 집합을 선택할 수 있으나, TOE에서 제공하는 디폴트값은 FAU_GEN.1에서 정의한 모든 감사대상 사건을 포함하도록 설정되어야 한다.

5.2.2. 암호지원(FCS)

5.2.2.1. FCS_CKM.2 암호키 분배

계층관계	없음
종속관계	[FDP_ITC.1 보안속성 없이 사용자 데이터 유입 또는 FDP_ITC.2 보안속성을 포함한 사용자 데이터 유입 또는 FCS_CKM.1 암호키 생성] FCS_CKM.4 암호키 파기
FCS_CKM.2.1	TSF는 다음의 [할당 : *표준 목록*]에 부합하는 명세된 암호키 분배 방법 [할당 : *암호키 분배 방법*] 에 따라 암호키를 분배해야 한다.

응용 시 주의사항

- o FCS_CKM.2 암호키 분배는 선택적으로 구현 가능한 기능 요구사항('선택 SFR')으로 TOE에서 위 기능을 추가로 제공할 경우, 보안목표명세서 작성자는 본 요구사항을 SFR에 포함해야 한다.
- o 보안목표명세서 작성자가 본 SFR을 포함할 경우, 필요 시 보안문제정의 및 보안목적 등을 추가적으로 도출해야 한다.
- o FCS_CKM.2.1에서 정의한 암호키 설정 방법에서 사용하는 키는 FCS_CKM.1.1에서 생성한 키와 연관되어야 한다.

5.2.3. 사용자 데이터 보호(FDP)

5.2.3.1. FDP_IFC.1 부분적인 정보흐름 통제(어플리케이션 트래픽 필터링)

계층관계	없음
종속관계	FDP_IFF.1 단일 계층 보안속성
FDP_IFC.1.1	TSF는 [할당 : *주체 목록, 정보 목록, SFP에 의하여 다루어지는 통제된 주체로/주체로부터의 통제된 정보흐름을 유발하는 오퍼레이션의 목록*]에 대하여 [어플리케이션 트래픽 필터링 SFP]를 강제해야 한다.

응용 시 주의사항

- o FDP_IFF.1 부분적인 정보흐름 통제(어플리케이션 트래픽 필터링)는 선택적으로 구현 가능한 기능 요구사항('선택 SFR')으로, TOE에서 위 기능을 추가로 제공할 경우, 보안목표명세서 작성자는 본 요구사항을 SFR에 포함해야 한다.
- o 보안목표명세서 작성자가 본 SFR을 포함할 경우, 필요 시 보안문제정의 및 보안목적 등을 추가적으로 도출해야 한다.

5.2.3.2. FDP_IFF.1 단일 계층 보안속성(어플리케이션 트래픽 필터링)

계층관계	없음
종속관계	FDP_IFC.1 부분적인 정보흐름통제 FMT_MSA.3 정적 속성 초기화
FDP_IFF.1.1	TSF는 적어도 [할당 : *다음의 SFP에서 통제되는 주체와 정보의 목록, 주체와 정보 각각에 대한 보안속성*]과 같은 주체 보안속성 및 정보 보안속성 유형에 기반하여 [어플리케이션 트래픽 필터링 SFP]를 강제해야 한다.
FDP_IFF.1.2	TSF는 다음과 같은 규칙이 유지되면 통제된 오퍼레이션을 통하여 통제된 주체와 통제된 정보 간의 정보흐름을 허용해야 한다. [*할당 : 각 오퍼레이션에 대하여 주체와 정보 보안속성 간에서 유지되어야 하는 보안속성에 기반한 관계*]
FDP_IFF.1.3	TSF는 [할당 : *추가 정보흐름통제 SFP 규칙*]을 강제해야 한다.
FDP_IFF.1.4	TSF는 [할당 : *보안속성에 기반하여 명시적으로 정보흐름을 인가하는 규칙*]에 기반하여 정보흐름을 명시적으로 인가해야 한다.
FDP_IFF.1.5	TSF는 [할당 : *보안속성에 기반하여 명시적으로 정보흐름을 거부하는 규칙*]에 기반하여 정보흐름을 명시적으로 거부해야 한다.

응용 시 주의사항

- o FDP_IFF.1 부분적인 정보흐름 통제(어플리케이션 트래픽 필터링)는 선택적으로 구현 가능한 기능 요구사항('선택 SFR')으로, TOE에서 위 기능을 추가로 제공할 경우, 보안목표명세서 작성자는 본 요구사항을 SFR에 포함해야 한다.
- o 보안목표명세서 작성자가 본 SFR을 포함할 경우, 필요 시 보안문제정의 및 보안목적 등을 추가적으로 도출해야 한다.
- o 어플리케이션 트래픽 필터링 보안속성: IP주소(출발지, 목적지), 포트(출발지, 목적지), 서비스(SMTP, POP3, HTTP), 프로토콜(TCP, UDP) 등

5.2.4. TSF 보호

5.2.4.1. FPT_ITT.1 내부전송 TSF 데이터의 기본적인 보호

계층관계	없음
종속관계	없음
FPT_ITT.1.1	TSF는 TOE의 분리된 부분 간에 TSF 데이터가 전송될 때 *노출, 변경*으로부터 TSF 데이터를 보호해야 한다.

응용 시 주의사항

- o FPT_ITT.1 TSF 간 안전한 채널은 선택적으로 구현 가능한 기능 요구사항('선택 SFR')으로 TOE

에서 위 기능을 추가로 제공할 경우, 보안목표명세서 작성자는 본 요구사항을 SFR에 포함해야 한다.

- o 보안목표명세서 작성자가 본 SFR을 포함할 경우, 필요 시 보안문제정의 및 보안목적 등을 추가적으로 도출해야 한다.
- o 암호와 관련된 부분은 암호지원(FCS) 클래스를 참고한다.

5.2.4.2. FPT_TUD.1 TSF 보안패치 업데이트(확장)

계층관계	없음
종속관계	없음
FPT_TUD.1.1	TSF는 [할당 : *인가된 역할*]에게 TOE의 버전 정보를 조회할 수 있는 기능을 제공해야 한다.
FPT_TUD.1.2	TSF는 업데이트를 설치하기 전에 [선택 : *해쉬값 비교, 전자서명 검증*]을 이용하여 업데이트 파일에 대한 유효성 검증을 수행해야 한다.

응용 시 주의사항

- o FPT_TUD.1 TSF 보안패치 업데이트는 선택적으로 구현 가능한 기능 요구사항('선택 SFR')으로 TOE에서 위 기능을 추가로 제공할 경우, 보안목표명세서 작성자는 본 요구사항을 SFR에 포함해야 한다.
- o 보안목표명세서 작성자가 본 SFR을 포함할 경우, 필요 시 보안문제정의 및 보안목적 등을 추가적으로 도출해야 한다.
- o TSF는 인가된 역할이 가장 최근에 설치되어 실행된 TOE의 현재 버전을 확인할 수 있는 기능을 제공해야 한다.
- o 업데이트는 자동 또는 수동 업데이트 형태로 제공될 수 있다. online 업데이트를 제공할 경우, 전송되는 업데이트 파일 보호를 위해 안전한 통신채널을 통해 업데이트 파일을 배포해야 한다. 관련 내용은 '선택 SFR' FTP_ITC.1을 참고한다.
- o TOE의 펌웨어 설치 실패 및 업데이트 파일의 검증 실패 시 기존 펌웨어 버전을 이용하여 안전하게 부팅하여 구동될 수 있도록 해야 한다.

5.2.5. 안전한 경로/채널(FTP)

5.2.5.1. FTP_ITC.1 TSF 간 안전한 채널

계층관계	없음
종속관계	없음
FTP_ITC.1.1	TSF는 자신과 다른 신뢰된 IT 제품 간에 다른 통신 채널과 논리적으로 구별되고, 단말의 보증된 식별을 제공하며, 변경이나 노출로부터 채널 데이터를 보호하는 통신 채널을 제공해야 한다.

FTP_ITC.1.2 TSF는 [선택 : *TSF, 신뢰된 IT 제품*]이 안전한 채널을 통하여 통신을 초기화하는 것을 허용해야 한다.

FTP_ITC.1.3 TSF는 [할당 : *안전한 채널이 요구되는 기능 목록*]에 대하여 안전한 채널을 통하여 통신을 초기화해야 한다.

응용 시 주의사항

- o FTP_ITC.1 TSF 간 안전한 채널은 선택적으로 구현 가능한 기능 요구사항('선택 SFR')으로 TOE에서 위 기능을 추가로 제공할 경우, 보안목표명세서 작성자는 본 요구사항을 SFR에 포함해야 한다.
- o 보안목표명세서 작성자가 본 SFR을 포함할 경우, 필요 시 보안문제정의 및 보안목적 등을 추가적으로 도출해야 한다.
- o FTP_ITC.1에 제시된 신뢰된 IT 제품의 예로는 외부 로그서버 또는 인증서버, 업데이트 서버 등이 있다.
- o TOE가 업데이트 서버와 연동하는 경우, TSF 업데이트 요구사항인 '선택 SFR' FPT_TUD.1을 참고한다.
- o TSF가 외부 로그서버 또는 인증서버 등과 연동하는 경우, TSF와 각 서버는 암호통신 프로토콜을 이용한 신뢰된 채널을 제공하여 감사데이터, 인증데이터, TOE 설정파일 등의 TSF 데이터를 보호해야 한다. 암호와 관련된 부분은 FCS 클래스를 참고한다.
- o TSF와 신뢰된 IT 제품 간의 통신 시 TLS 프로토콜을 지원하는 경우 TLS 1.2(RFC 5246) 이상을 지원해야 하고, SSH 프로토콜을 지원하는 경우 SSH v2(RFC 4251 ~ 4254) 이상을 지원해야 한다. 암호와 관련된 부분은 FCS 클래스를 참고하되 사용하는 프로토콜에서 공개된 취약점은 모두 보완하여 안전하게 사용하도록 권고된다.

5.3. 보증요구사항

본 보호프로파일의 보증요구사항은 공통평가기준 3부의 보증 컴포넌트로 구성되었고, 평가보증등급은 EAL1+이다. 다음 표는 보증 컴포넌트를 요약하여 보여준다.

보증클래스	보증 컴포넌트	
보안목표명세서	ASE_INT.1	보안목표명세서 소개
	ASE_CCL.1	준수 선언
	ASE_OBJ.1	운영환경에 대한 보안목적
	ASE_ECD.1	확장 컴포넌트 정의
	ASE_REQ.1	명시된 보안요구사항
	ASE_TSS.1	TOE 요약명세
개발	ADV_FSP1	기본적인 기능명세
설명서	AGD_OPE.1	사용자 운영 설명서
	AGD_PRE.1	준비 절차
생명주기지원	ALC_CMC.1	TOE 레이블링
	ALC_CMS.1	TOE 형상관리 범위
시험	ATE_FUN.1	기능 시험
	ATE_IND.1	독립적인 시험 : 기능 확인
취약성 평가	AVA_VAN.1	취약성 조사

[표 6] 보증요구사항

5.3.1. 보안목표명세서 평가

5.3.1.1. ASE_INT.1 보안목표명세서 소개

종속관계 없음

개발자 요구사항

ASE_INT.1.1D 개발자는 보안목표명세서 소개를 제공해야 한다.

증거 요구사항

ASE_INT.1.1C 보안목표명세서 소개는 보안목표명세서 참조, TOE 참조, TOE 개요, TOE 설명을 포함해야 한다.

ASE_INT.1.2C 보안목표명세서 참조는 유일하게 보안목표명세서를 식별해야 한다.

ASE_INT.1.3C TOE 참조는 TOE를 식별해야 한다.

ASE_INT.1.4C	TOE 개요는 TOE의 용도와 주요 보안 특성을 요약해야 한다.
ASE_INT.1.5C	TOE 개요는 TOE 유형을 식별해야 한다.
ASE_INT.1.6C	TOE 개요는 TOE에서 요구되는 비-TOE에 해당하는 하드웨어/소프트웨어/펌웨어를 식별해야 한다.
ASE_INT.1.7C	TOE 설명은 TOE의 물리적인 범위를 서술해야 한다.
ASE_INT.1.8C	TOE 설명은 TOE의 논리적인 범위를 서술해야 한다.
평가자 요구사항	
ASE_INT.1.1E	평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.
ASE_INT.1.2E	평가자는 TOE 참조, TOE 개요, TOE 설명이 서로 일관성이 있음을 확인해야 한다.

5.3.1.2. ASE_CCL.1 준수선언

종속관계	ASE_INT.1 보안목표명세서 소개 ASE_ECD.1 확장 컴포넌트 정의 ASE_REQ.1 명시된 보안요구사항
개발자 요구사항	
ASE_CCL.1.1D	개발자는 준수 선언을 제공해야 한다.
ASE_CCL.1.2D	개발자는 준수 선언의 이론적 근거를 제공해야 한다.
증거 요구사항	
ASE_CCL.1.1C	준수 선언은 보안목표명세서 및 TOE가 준수하는 공통평가기준의 버전을 식별하기 위해 공통평가기준 준수 선언을 포함해야 한다.
ASE_CCL.1.2C	공통평가기준 준수 선언은 보안목표명세서의 공통평가기준 2부에 대한 준수 선언을 "2부 준수" 또는 "2부 확장"으로 서술해야 한다.
ASE_CCL.1.3C	공통평가기준 준수 선언은 보안목표명세서의 공통평가기준 3부에 대한 준수 선언을 "3부 준수" 또는 "3부 확장"으로 서술해야 한다.
ASE_CCL.1.4C	공통평가기준 준수 선언은 확장 컴포넌트 정의와 일관성이 있어야 한다.
ASE_CCL.1.5C	준수 선언은 보안목표명세서가 준수하는 모든 보호프로파일 및 보안요구사항 패키지를 식별해야 한다.
ASE_CCL.1.6C	준수 선언은 보안목표명세서의 패키지에 대한 준수 선언을 '패키지 준수' 또는 '패키지 추가'로 서술해야 한다.
ASE_CCL.1.7C	준수 선언의 이론적 근거는 보안목표명세서의 TOE 유형이 그 보안목표명세서가 준수하는 보호프로파일의 TOE 유형과 일관성이 있음을 입증해야 한다.
ASE_CCL.1.8C	준수 선언의 이론적 근거는 보안목표명세서의 보안문제정의에 대한 설명이 그 보안목표명세서가 준수하는 보호프로파일의 보안문제정의 설명과 일관성이 있음을 입증해야 한다.

ASE_CCL.1.9C	준수 선언의 이론적 근거는 보안목표명세서의 보안목적에 대한 설명이 그 보안목표명세서가 준수하는 보호프로파일의 보안목적 설명과 일관성이 있음을 입증해야 한다.
ASE_CCL.1.10C	준수 선언의 이론적 근거는 보안목표명세서의 보안요구사항에 대한 설명이 그 보안목표명세서가 준수하는 보호프로파일의 보안요구사항 설명과 일관성이 있음을 입증해야 한다.
평가자 요구사항	
ASE_CCL.1.1E	평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

5.3.1.3. ASE_OBJ.1 운영환경에 대한 보안목적

종속관계	없음
개발자 요구사항	
ASE_OBJ.1.1D	개발자는 보안목적에 대한 설명을 제공해야 한다.
증거 요구사항	
ASE_OBJ.1.1C	보안목적에 대한 설명은 운영환경에 대한 보안목적을 서술해야 한다.
평가자 요구사항	
ASE_OBJ.1.1E	평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

5.3.1.4. ASE_ECD.1 확장 컴포넌트 정의

종속관계	없음
개발자 요구사항	
ASE_ECD.1.1D	개발자는 보안요구사항에 대한 설명을 제공해야 한다.
ASE_ECD.1.2D	개발자는 확장 컴포넌트 정의를 제공해야 한다.
증거 요구사항	
ASE_ECD.1.1C	보안요구사항에 대한 설명은 확장된 모든 보안요구사항을 식별해야 한다.
ASE_ECD.1.2C	확장 컴포넌트 정의는 각각 확장된 보안요구사항에 대한 확장 컴포넌트를 정의해야 한다.
ASE_ECD.1.3C	확장 컴포넌트 정의는 각 확장 컴포넌트가 기존의 공통평가기준 컴포넌트, 패밀리, 클래스와 어떻게 연관되는지를 서술해야 한다.
ASE_ECD.1.4C	확장 컴포넌트 정의는 기존의 공통평가기준 컴포넌트, 패밀리, 클래스와 방법론을 모델로 하여 표현해야 한다.
ASE_ECD.1.5C	확장 컴포넌트는 각 엘리먼트에 대한 준수 여부를 입증할 수 있도록 측정 가능하고 객관적인 엘리먼트로 구성되어야 한다.

평가자 요구사항	
ASE_ECD.1.1E	평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.
ASE_ECD.1.2E	평가자는 확장된 컴포넌트가 기존의 컴포넌트를 이용하여 명확히 표현할 수 없음을 확인해야 한다.

5.3.1.5. ASE_REQ.1 명시된 보안요구사항

종속관계	ASE_ECD.1 확장 컴포넌트 정의
개발자 요구사항	
ASE_REQ.1.1D	개발자는 보안요구사항에 대한 설명을 제공해야 한다.
ASE_REQ.1.2D	개발자는 보안요구사항의 이론적 근거를 제공해야 한다.
증거 요구사항	
ASE_REQ.1.1C	보안요구사항에 대한 설명은 보안기능요구사항과 보증요구사항을 서술해야 한다.
ASE_REQ.1.2C	보안기능요구사항 및 보증요구사항에서 사용되는 모든 주체, 객체, 오퍼레이션, 보안 속성, 외부 실체, 기타 조건들은 정의되어야 한다.
ASE_REQ.1.3C	보안요구사항에 대한 설명은 보안요구사항에 대한 모든 오퍼레이션을 식별해야 한다.
ASE_REQ.1.4C	모든 오퍼레이션은 정확히 수행되어야 한다.
ASE_REQ.1.5C	보안요구사항의 각 종속관계는 만족되어야 하며, 그렇지 않을 경우에는 보안요구사항의 이론적 근거에 그에 대한 정당화가 제공되어야 한다.
ASE_REQ.1.6C	보안요구사항에 대한 설명은 내부적으로 일관성이 있어야 한다.
평가자 요구사항	
ASE_REQ.1.1E	평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

5.3.1.6. ASE_TSS.1 TOE 요약명세

종속관계	ASE_INT.1 보안목표명세서 소개 ASE_REQ.1 명시된 보안요구사항 ADV_FSP.1 기본적인 기능명세
개발자 요구사항	
ASE_TSS.1.1D	개발자는 TOE 요약명세를 제공해야 한다.
증거 요구사항	
ASE_TSS.1.1C	TOE 요약명세는 TOE가 어떻게 각각의 보안기능요구사항을 만족시키는지 서술해야 한다.

평가자 요구사항	
ASE_TSS.1.1E	평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.
ASE_TSS.1.2E	평가자는 TOE 요약명세가 TOE 개요 및 TOE 설명과 일관성이 있음을 확인해야 한다.

5.3.2. 개발

5.3.2.1. ADV_FSP.1 기본적인 기능명세

종속관계	없음
개발자 요구사항	
ADV_FSP.1.1D	개발자는 기능명세를 제공해야 한다.
ADV_FSP.1.2D	개발자는 기능명세에서 SFR로의 추적성을 제공해야 한다.
증거 요구사항	
ADV_FSP.1.1C	기능명세는 각 SFR-수행 및 SFR-지원 TSFI에 대한 목적과 사용 방법을 서술해야 한다.
ADV_FSP.1.2C	기능명세는 각 SFR-수행 및 SFR-지원 TSFI와 관련된 모든 매개변수를 식별해야 한다.
ADV_FSP.1.3C	기능명세는 인터페이스를 SFR-비-간섭으로 분류한 것에 대한 이론적 근거를 제공해야 한다.
ADV_FSP.1.4C	추적성은 SFR이 기능명세 내의 TSFI로 추적됨을 입증해야 한다.
평가자 요구사항	
ADV_FSP.1.1E	평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.
ADV_FSP.1.2E	평가자는 기능명세가 SFR을 정확하고 완전하게 실체화하는지 결정해야 한다.

5.3.3. 설명서

5.3.3.1. AGD_OPE.1 사용자 운영 설명서

종속관계	ADV_FSP.1 기본적인 기능명세
개발자 요구사항	
AGD_OPE.1.1D	개발자는 사용자 운영 설명서를 제공해야 한다.
증거 요구사항	

AGD_OPE.1.1C	사용자 운영 설명서는 각각의 사용자 역할에 대해 안전한 처리환경 내에서 통제되어야 하는 사용자가 접근 가능한 기능 및 특권에 대해 적절한 경고를 포함해서 서술해야 한다.
AGD_OPE.1.2C	사용자 운영 설명서는 각각의 사용자 역할에 대해 TOE에 의해 안전한 방식으로 제공되는 인터페이스의 사용 방법을 서술해야 한다.
AGD_OPE.1.3C	사용자 운영 설명서는 각각의 사용자 역할에 대해 사용 가능한 기능 및 인터페이스를 서술해야 한다. 특히 사용자의 통제 하에 있는 모든 보안 매개변수에 대해 안전한 값을 적절하게 표시해야 한다.
AGD_OPE.1.4C	사용자 운영 설명서는 각각의 사용자 역할에 대해, 수행되어야 할 사용자가 접근할 수 있는 기능과 연관된 보안-관련 사건의 각 유형을 명확히 제시해야 한다. 여기에는 TSF의 통제 하에 있는 실체에 대한 보안 특성의 변경도 포함되어야 한다.
AGD_OPE.1.5C	사용자 운영 설명서는 (장애 후의 운영 또는 운영상의 오류 후의 운영을 포함한) TOE의 모든 가능한 운영 모드, 그 영향 및 안전한 운영 유지를 위한 관련 사항들을 식별해야 한다.
AGD_OPE.1.6C	사용자 운영 설명서는 각각의 사용자 역할에 대해 보안목표명세서에 기술된 대로 운영환경에 대한 보안목적을 만족시키기 위해 준수해야 하는 보안대책을 서술해야 한다.
AGD_OPE.1.7C	사용자 운영 설명서는 명확하고 타당해야 한다.
평가자 요구사항	
AGD_OPE.1.1E	평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

5.3.3.2. AGD_PRE.1 준비 절차

종속관계	없음
개발자 요구사항	
AGD_PRE.1.1D	개발자는 준비 절차를 포함하여 TOE를 제공해야 한다.
증거 요구사항	
AGD_PRE1.1C	준비 절차는 배포된 TOE의 안전한 인수를 위해 필요한 모든 단계를 개발자의 배포 절차와 일관되게 서술해야 한다.
AGD_PRE1.2C	준비 절차는 TOE의 안전한 설치 및 운영환경의 안전한 준비를 위해 필요한 모든 단계를 보안목표명세서에 기술된 운영환경에 대한 보안목적과 일관되게 서술해야 한다.
평가자 요구사항	
AGD_PRE.1.1E	평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.
AGD_PRE.1.2E	평가자는 TOE가 운영을 위해 안전하게 준비될 수 있음을 확인하기 위해 준비 절차를 적용해야 한다.

5.3.4. 생명주기 지원

5.3.4.1. ALC_CMC.1 TOE 레이블링

종속관계	ALC_CMS.1 TOE 형상관리 범위
개발자 요구사항	
ALC_CMC.1.1D	개발자는 TOE 및 그에 대한 참조를 제공해야 한다.
증거 요구사항	
ALC_CMC.1.1C	TOE는 유일한 참조를 위한 레이블을 붙여야 한다.
평가자 요구사항	
ALC_CMC.1.1E	평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

5.3.4.2. ALC_CMS.1 TOE 형상관리 범위

종속관계	없음
개발자 요구사항	
ALC_CMS.1.1D	개발자는 TOE에 대한 형상목록을 제공해야 한다.
증거 요구사항	
ALC_CMS.1.1C	형상목록은 TOE 및 보증요구사항에서 요구하는 평가증거를 포함해야 한다.
ALC_CMS.1.2C	형상목록은 형상항목을 유일하게 식별해야 한다.
평가자 요구사항	
ALC_CMS.1.1E	평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

5.3.5. 시험

5.3.5.1. ATE_FUN.1 기능 시험

종속관계	ATE_COV.1 시험범위의 증거
개발자 요구사항	
ATE_FUN.1.1D	개발자는 TSF를 시험하고 그 결과를 문서화해야 한다.
ATE_FUN.1.2D	개발자는 시험 문서를 제공해야 한다.
증거 요구사항	

ATE_FUN.1.1C	시험 문서는 시험계획, 예상 시험결과, 실제 시험결과로 구성되어야 한다.
ATE_FUN.1.2C	시험계획은 수행되어야 할 시험항목을 식별하고 각 시험 수행의 시나리오를 서술해야 한다. 이러한 시나리오는 다른 시험결과에 대한 순서 종속관계를 포함해야 한다.
ATE_FUN.1.3C	예상 시험결과는 시험의 성공적인 수행으로 기대되는 결과를 제시해야 한다.
ATE_FUN.1.4C	실제 시험결과는 예상 시험결과와 일관성이 있어야 한다.
평가자 요구사항	
ATE_FUN.1.1E	평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

5.3.5.2. ATE_IND.1 독립적인 시험 : 기능 확인

종속관계	ADV_FSP.1 기본적인 기능명세 AGD_OPE.1 사용자 운영 설명서 AGD_PRE.1 준비 절차
개발자 요구사항	
ATE_IND.1.1D	개발자는 시험할 TOE를 제공해야 한다.
증거 요구사항	
ATE_IND.1.1C	TOE는 시험하기에 적합해야 한다.
평가자 요구사항	
ATE_IND.1.1E	평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.
ATE_IND.1.2E	평가자는 TSF가 명세된 대로 동작함을 확인하기 위하여 TSF의 일부를 시험해야 한다.

5.3.6. 취약성 평가

5.3.6.1. AVA_VAN.1 취약성 조사

종속관계	ADV_FSP.1 기본적인 기능명세 AGD_OPE.1 사용자 운영 설명서 AGD_PRE.1 준비 절차
개발자 요구사항	
AVA_VAN.1.1D	개발자는 시험할 TOE를 제공해야 한다.
증거 요구사항	
AVA_VAN.1.1C	TOE는 시험하기에 적합해야 한다.

평가자 요구사항	
AVA_VAN.1.1E	평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.
AVA_VAN.1.2E	평가자는 TOE의 잠재적 취약성을 식별하기 위해 공개 영역에 대한 조사를 수행해야 한다.
AVA_VAN.1.3E	평가자는 TOE가 기본 공격 성공 가능성을 가진 공격자에 의해 행해지는 공격에 내성이 있음을 결정하기 위해, 식별된 잠재적 취약성에 근거하여 침투시험을 수행해야 한다.

5.4. 보안요구사항의 이론적 근거

5.4.1. 보안기능요구사항의 종속관계

다음 표는 보안기능요구사항의 종속관계를 보여준다.

번호	보안기능요구사항	종속관계	참조번호
1	FAU_ARP.1	FAU_SAA.1	3
2	FAU_GEN.1	FPT_STM.1	27
3	FAU_SAA.1	FAU_GEN.1	2
4	FAU_SAR.1	FAU_GEN.1	2
5	FAU_SAR.3	FAU_SAR.1	4
6	FAU_STG.1	FAU_GEN.1	2
7	FAU_STG.3	FAU_STG.1	6
8	FAU_STG.4	FAU_STG.1	6
9	FCS_CKM.1	[FCS_CKM.2 또는 FCS_COP.1]	11
		FCS_CKM.4	10
10	FCS_CKM.4	[FDP_ITC.1 또는 FDP_ITC.2 또는 FCS_CKM.1]	9
11	FCS_COP.1	[FDP_ITC.1 또는 FDP_ITC.2 또는 FCS_CKM.1]	9
		FCS_CKM.4	10
12	FDP_IFC.2	FDP_IFF.1	13
13	FDP_IFF.1	FDP_IFC.1	12
		FMT_MSA.3	22
14	FIA_AFL.1	FIA_UAU.1	16
15	FIA_SOS.1	-	-
16	FIA_UAU.1	FIA_UID.1	19
17	FIA_UAU.4	-	-
18	FIA_UAU.7	FIA_UAU.1	16
19	FIA_UID.1	-	-
20	FMT_MOF.1	FMT_SMF.1	24
		FMT_SMR.1	25
21	FMT_MSA.1	[FDP_ACC.1 또는 FDP_IFC.1]	12
		FMT_SMF.1	24
		FMT_SMR.1	25

번호	보안기능요구사항	종속관계	참조번호
22	FMT_MSA.3	FMT_MSA.1	21
		FMT_SMR.1	25
23	FMT_MTD.1	FMT_SMF.1	24
		FMT_SMR.1	25
24	FMT_SMF.1	-	-
25	FMT_SMR.1	FIA_UID.1	19
26	FMT_PWD.1	FMT_SMF.1	24
		FMT_SMR.1	25
27	FPT_STM.1	-	
28	FPT_TEE.1	-	
29	FPT_TST.1	-	
30	FPT_PST.1	-	
31	FTA_MCS.2	FIA_UID.1	19
32	FTA_SSL.5	[FIA_UAU.1 또는 없음]	16
33	FTA_TSE.1	-	-
34	FTP_TRP.1	-	-

[표 7] 종속관계 이론적 근거

FDP_IFF.1, FMT_MSA.1은 FDP_IFC.1에 종속관계를 가지며, 이는 FDP_IFC.1과 계층관계에 있는 FDP_IFC.2에 의해 만족된다.

5.4.2. 보증요구사항의 종속관계

정보보호시스템 공통평가기준에서 제공하는 EAL1 보증 패키지의 종속관계는 이미 만족되어 있으므로 이에 대한 이론적 근거는 생략한다.

추가된 보증요구사항인 ATE_FUN.1은 종속관계로 ATE_COV.1을 포함한다. ATE_FUN.1은 개발자가 시험항목에 대한 시험을 정확하게 수행하고 시험서에 기록했는지 확인하기 위해 추가되었으며, 시험항목과 TSFI간의 일치성을 제시하는 ATE_COV.1이 반드시 필요한 것은 아니라고 판단되어 본 보호프로파일에서는 추가하지 않았다.

참고자료

자 료 명	저 자	비 고
정보보호시스템 공통평가기준 버전 3.1 개정4판 • 정보보호시스템 공통평가기준 1부 : 소개 및 일반모델, 버전 3.1r4 (CCMB-2012-09-001) • 정보보호시스템 공통평가기준 2부: 보안기능요구사항, 버전 3.1r4 (CCMB-2012-09-002) • 정보보호시스템 공통평가기준 3부: 보증요구사항, 버전 3.1r4 (CCMB-2012-09-003)	CCMB	2012. 9
국가용 정보보호제품 보안요구사항 - 침입차단시스템 보안요구사항	국가사이버안전센터, IT보안인증사무국	2012. 2

약 어 표

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
NTP	Network Time Protocol
OSI	Open Systems Interconnection
OTP	One Time Password
SFP	Security Function Policy
SFR	Security Functional Requirement
SMS	Short Message Service
SSH	Secure Shell
SSL	Secure Socket Layer
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality