국가용 보안요구사항 V3.0 기반의

# ITSCC V3.0 보안목표명세서 V1.0

2025. 4. 11.

과학기술정보통신부

IT보안인증사무국

• 제·개정 이력

| 버전 | 일 자 | 변경 내용 |
|---|---|---|
| 1.0 | 2025. 4. 11. | ㅇ 국가용 보안요구사항 V3.0 기반의 ITSCC V3.0 보안목표명세서 제정 |
| | | |
| | | |
| | | |

# 서 문

2024년 과학기술정보통신부는
정보보호제품 평가·인증 제도의 개선을 통해 기업의 참여 확대와 평가·인증 준비의 실효성을 제고하고자
다양한 정책적 노력을 추진하였습니다.

이에 발맞춰 IT보안인증사무국은
기업이 정보보호제품 평가를 준비하는 과정에서 겪는 어려움을 덜어주기 위해
제출문서에 대한 가이드와 템플릿을 제공하고, 작성 샘플을 마련하여 실질적인 지원을 제공하고자 합니다.

본 가이드는 정보보호제품 CC 평가 시 요구되는 중요 제출문서인 보안목표명세서 평가에서의
복잡한 절차와 기술적 요건을 명확히 이해할 수 있도록 구체적인 지침과 사례를 제시하여,
문서의 구성별(세부목차별) 작성 방향에 대한 안내와 함께 실무적인 작성 예시를 포함하고 있습니다.

본 가이드를 통해 기업이 평가를 준비하는 과정에서부터 체계적이고 효율적으로
평가·인증에 대한 사전 역량을 강화할 수 있을 것으로 기대합니다.

# CONTENTS


## 01 보안목표명세서 소개

1.1. 보안목표명세서 참조 ····· 9
1.2. TOE 참조 ····· 9
1.3. TOE 개요 ····· 9
1.4. TOE 설명 ····· 11

## 02 준수 선언

2.1. 공통평가기준 준수 선언 ····· 17
2.2. 보호프로파일(보안요구사항) 준수 선언 ····· 17
2.3. 준수 선언의 이론적 근거 ····· 17

## 03 보안문제정의

3.1. 위협 ····· 19
3.2. 조직의 보안정책 ····· 21
3.3. TOE 운영환경에 관한 가정사항 ····· 21

## 04 보안목적

4.1. TOE 보안목적 ····· 23
4.2. 운영환경에 대한 보안목적 ····· 24
4.3. 보안목적의 이론적 근거 ····· 25

## 05 확장 컴포넌트 정의

5.1. 암호지원(FCS, Cryptographic support) ····· 31
5.2. 보안관리(FMT, Security Management) ····· 32
5.3. TSF 보호(FPT, Protection of the TSF) ····· 33

## 06 보안요구사항

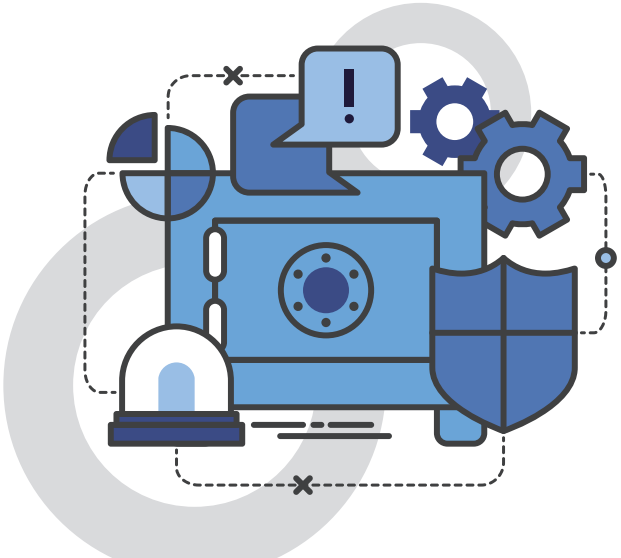
6.1. 보안기능요구사항 ····· 36
6.2. 보증요구사항 ····· 56
6.3. 보안요구사항의 이론적 근거 ····· 72
6.4. 종속관계에 대한 이론적 근거 ····· 78

## 07 TOE 요약명세

7.1. 침입차단시스템 기능 ····· 81
7.2. TOE 접근 ····· 87
7.3. 식별 및 인증 ····· 88
7.4. 보안관리 ····· 89
7.5. 보안감사 ····· 100
7.6. TSF 보호 ····· 102
7.7. 안전한 경로/채널 ····· 104
7.8. 암호지원 ····· 105

## 08 참고자료

## 09 용어 및 약어



01

# 보안목표명세서 소개

1.1. 보안목표명세서 참조
1.2. TOE 참조
1.3. TOE 개요
1.4. TOE 설명

# 1. 보안목표명세서 소개

## 1.1. 보안목표명세서 참조

| | |
|---|---|
| 제 목 | 국가용 보안요구사항 V3.0 기반의 ITSCC V3.0 보안목표명세서 |
| 버 전 | 1.0 |
| 작성자 | IT보안인증사무국 |
| 발간일 | 2025. 4. 11. |

## 1.2. TOE 참조

| | | |
|---|---|---|
| TOE 명칭 | | ITSCC |
| TOE 버전 | | V3.0 |
| TOE 구성요소 | HW | •ITSCCOS V3.0.0가 설치된 일체형 장비 |
| | SW (펌웨어) | •ITSCCOS V3.0.0(itsccos_v3.0.0.bin) |
| | 문서 | •ITSCC V3.0 설치매뉴얼 V1.1<br>•ITSCC V3.0 운영매뉴얼 V1.1 |

## 1.3. TOE 개요

TOE는 패킷 필터 및 상태 기반 감시 기능을 제공하는 침입차단시스템이다. 침입차단시스템은 외부 네트워크에서 내부 네트워크로 접근하는 트래픽을 제어하는 기능과 내부 네트워크와 외부 네트워크의 논리적 분리 및 물리적 분리를 통해 내부 자산에 대한 외부 사용자의 침입, 내부 사용자의 비인가된 정보유출 등을 방지하는 것이다. 침입차단시스템은 적용되는 네트워크 계층에 따라 패킷 필터, 상태 기반 감시, 어플리케이션, 어플리케이션-프록시 게이트웨이 등으로 분류된다. TOE는 패킷 필터링 및 상태기반 트래픽 필터링 기능을 제공하여 외부에서 내부로 유입되는 트래픽을 제어하고 외부 사용자의 침입을 차단한다. 또한 내부에서 외부로 나가는 트래픽을 제어하여 비인가된 정보 유출을 방지한다.

### 1.3.1. TOE의 용도 및 주요 보안 특성

TOE는 ITSCCOS V3.0.00이 실행되는 ITSCC 하드웨어 일체형(Appliance) 장비로 침입차단시스템 제품이다. ITSCC V3.0(TOE)는 TCP/IP 계층의 상태기반 트래픽 필터링 기능을 제공하는 침입차단시스템으로 동작한다. TOE는 IPv4 또는 ICMPv4의 패킷 헤더에 포함된 정보를 기반으로 네트워크 패킷을 필터링하는 기능 외에도 TCP/UDP 헤더에 포함된 정보를 기반으로 연결 상태를 추적하고 정상 상태에서 벗어난 패킷을 차단하는 기능을 제공한다. 즉, TOE는 패킷 필터 및 상태 기반 감시 침입차단시스템이다.

TOE는 정보흐름통제 규칙에 따라 네트워크 패킷의 헤더정보를 분석한 후 해당 패킷을 처리(허용, 거부, 차단 등) 한 후 각 연결의 상태를 추적하기 위해 상태 표에 출발지/목적지 IP주소, 출발지/목적지 포트번호, 프로토콜 및 연결 상태 정보 등을 기록한다. 상태 표에 기록된 패킷에 대해서는 정보흐름통제 규칙에 대한 모든 일치여부를 검사하는 대신 상태 표에 기록된 정보를 비교하여 일치하는 트래픽만 TOE를 통과할 수 있도록 허용한다.

TOE는 침입차단 주요 보안특징을 지원하기 위해 관리자 식별 및 인증, 보안관리, TOE 접근제한, TSF 보호, 보안감사 등의 기능도 제공한다. 또한 TLS, SSH 프로토콜을 통해 안전한 경로를 제공하고 이들 프로토콜을 처리하는 과정에서 암호키 관리 및 암호연산 기능을 수행한다.

### 1.3.2. TOE 유형

TOE는 네트워크 기반 침입차단 기능을 제공한다. TOE는 IPv4 네트워크간 전송되는 패킷을 정해진 규칙(트래픽 필터링 규칙, 상태 기반 감시 규칙)에 따라 차단하거나 통과시켜 공격자로부터 내부 네트워크 및 IT 자산을 보호하기 위한 목적으로 사용된다. TOE를 통과하여 외부 네트워크로부터 내부로 유입되는 트래픽을 제어하고 내부 IT 자산에 대한 외부 사용자의 침입을 차단한다. 또한, 내부 네트워크로부터 외부 네트워크로 나가는 트래픽을 제어하여 내부 사용자의 비인가된 정보 유출을 방지한다.

### 1.3.3. 비-TOE 식별(하드웨어/소프트웨어/펌웨어)

TOE는 감사기록을 외부 Syslog 서버로 전송할 수 있으며, 감사레코드의 시간정보에 대한 정확성을 보장하기 위해 외부 NTP 서버로부터 시간정보를 수신한다. 이를 위해 TLS 기반의 Syslog 프로토콜을 지원하는 Syslog 서버와 NTP 프로토콜을 지원하는 NTP 서버가 외부 IT실체로 필요하다.

### 1.3.4. TOE 범위 이외의 기타 기능

TOE는 하드웨어 일체형 장비이나 시스템 구성요소(CPU, RAM, 스토리지, 네트워크 인터페이스 등) 구동을 위한 펌웨어(BIOS, 드라이버)는 평가범위에서 제외된다. 다만, TOE 자체시험을 위한 BIOS 무결성 검증은 TOE 범위에 포함된다.

# 1.4. TOE 설명

## 1.4.1. TOE 물리적 범위

TOE는 감사기록을 외부 Syslog 서버로 전송할 수 있으며, 감사레코드의 시간정보에 대한 정확성을 보장하기 위해 외부 NTP 서버로부터 시간정보를 수신한다. 이를 위해 TLS 기반의 Syslog 프로토콜을 지원하는Syslog 서버와 NTP 프로토콜을 지원하는 NTP 서버가 외부 IT실체로 필요하다.

### 1.4.1.1. TOE 구성요소 및 배포 방법

TOE는 ITSCC 하드웨어 일체형 장비 및 문서(설치매뉴얼, 운영매뉴얼)로 구성된다. ITSCC 하드웨어 일체형장비에는 “TOE 논리적 범위”에 서술된 기능을 소프트웨어로 구현한 ITSCCOS V3.0.0이 설치되어 있다.
TOE는 다양한 하드웨어 플랫폼에 설치될 수 있으며 하드웨어 플랫폼 사양에 따라 제품의 모델명이 상이할 수 있다. 하지만 제품의 모델명이 상이하더라도 ITSCCOS V3.0.0 SW가 설치되어 동일한 보안기능을 제공하는 경우 동일 TOE로 간주한다.

| TOE 구성요소 | 버전정보 | 배포 형태 | 배포 방식 |
|---|---|---|---|
| ITSCC V3.0 | ITSCCOS 버전 : 3.0.0<br>(itsccos_v3.0.0.bin) | ITSCCOS가 설치된<br>하드웨어 일체형 장비 | 제조업체/판매업체를 통한<br>직접 배송 |
| ITSCC V3.0 설치매뉴얼 | 1.1 | PDF 파일 | 웹사이트 다운로드 |
| ITSCC V3.0 운영매뉴얼 | 1.1 | PDF 파일 | 웹사이트 다운로드 |

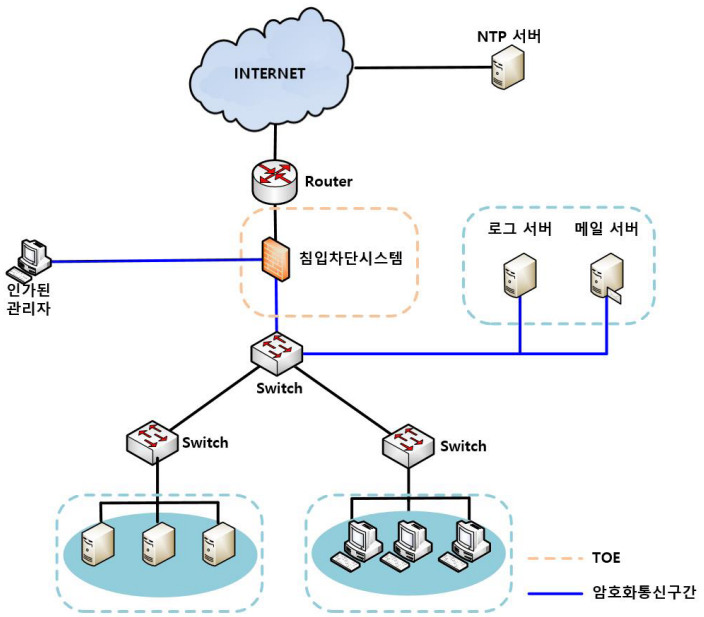
| 하드웨어 모델 | 구분 | | 시스템 사양 |
|---|---|---|---|
| ITSCCFW-1G | CPU | | Intel Xeon E3-1275 v5(4-Core 3.6 GHz) * 1 |
| | RAM | | 4 GB |
| | Storage | | 2TB HDD |
| | NIC | 기본구성 | 8 x 10/100/1000 Base-T RJ45 ports |
| | | 확장구성 | NIC 확장 슬롯은 1개이며, 아래와 같은 NIC 슬롯이 추가 장착 가능<br>- 8 x 10/100/1000 Base-T RJ45 ports<br>- 2 x 1000 Base-F SFP ports |
| | | 최대구성 | - 16 x 10/100/1000 Base-T RJ45 ports<br>또는<br>- 8 x 10/100/1000 Base-T RJ45 ports + 2 x 1000 Base-F SFP ports |
| ITSCCFW-10G | CPU | | Intel Xeon E3-1275 v5(4-Core 3.6 GHz) * 1 |
| | RAM | | 8 GB |
| | Storage | | 2TB HDD |

| | | | |
|---|---|---|---|
| ITSCCFW-10G | NIC | 기본구성 | - 슬롯에 장착 가능한 다음 NIC 종류 중 1개 택일<br>- 슬롯에 장착 가능한 NIC 종류<br>• 타입 1: 1G Fiber – 4 Ports<br>• 타입 2: 10G Fiber – 4 Ports<br>• 타입 3: 10G Fiber – 2 Ports<br>• 타입 4: 1G Copper – 8 Ports |
| | | 확장구성 | - NIC 확장 슬롯은 1개이며, 아래와 같은 NIC 슬롯이 추가 장착 가능<br>• 타입 1: 1G Fiber – 4 Ports<br>• 타입 2: 10G Fiber – 4 Ports<br>• 타입 3: 10G Fiber – 2 Ports<br>• 타입 4: 1G Copper – 8 Ports |
| | | 최대구성 | - 2개 슬롯(기본+확장 구성)에 장착 가능한 NIC 타입을 이용해 모두 장착한 형태<br>- 슬롯에 장착 가능한 NIC 종류<br>• 타입 1: 1G Fiber – 4 Ports<br>• 타입 2: 10G Fiber – 4 Ports<br>• 타입 3: 10G Fiber – 2 Ports<br>• 타입 4: 1G Copper – 8 Ports |

### 1.4.1.2. TOE 운영환경

TOE는 외부망 접점에 있는 WAN 인터페이스는 외부망에서 유입되는 트래픽을 수신하고 내부망 접점에 있는 LAN 인터페이스는 내부망에서 시작되는 트래픽을 처리한다. 따라서 내부망에서부터 시작된 트래픽은 LAN 인터페이스의 정보흐름통제규칙이 적용되어 필터링되고 외부망에서 흐름이 시작된 트래픽은 WAN 인터페이스의 정보흐름통제규칙이 적용되어 필터링된다. 패킷이 정보흐름 허용규칙에 일치하면 해당 세그먼트의 상태정보는 상태 표에 저장되고 이후 이와 관련된 트래픽은 정보흐름통제규칙 일치여부를 조사하지 않고 자동적으로 허용된다. 다만, 상태 표에 저장된 상태정보를 기반으로 허용/거부 여부가 최종 결정된다. 거부규칙에 일치하거나 일치하는 규칙이 없는 패킷에 대해서는 폐기(거부/차단)된다.

TOE 운영환경



## 1.4.2. TOE 논리적 범위

### 1.4.2.1. 보안감사

TOE는 TSF를 실행하는 주요 기능(침입차단, 암호연산, 보안관리, 잠재적 보안 위반 탐지)의 실행 결과와 감사기능 시동 및 종료에 대해 감사데이터를 생성한다. 감사데이터에는 사건 발생 일시, 사건 유형, 사건을 발생시킨 주체의 신원, 작업 내역 및 결과(성공/실패) 등이 포함된다. 외부 NTP 서버로부터 수신한 시각 정보를 동기화하여 이를 감사데이터의 사건 발생 일시로 기록한다.

생성된 감사데이터는 TOE 로컬디스크에 clog 파일형태로 1차 저장되고 감사 저장공간이 임계치에 도달하는 경우 감사기록을 원격 syslog 서버로 전송하며 감사 저장공간이 부족한 경우 관리자가 지정한 이메일로 경고메시지를 발송하고 자동백업을 수행한 후 감사기록을 덮어쓰기 한다.

관리자는 관리자 웹페이지(WebGUI)에 로그인하여 감사기록을 정렬 조회하거나 고급검색 기능을 이용하여 다양한 검색어(단어, 구문, 정규표현식 등)로 감사기록을 조회할 수 있다. CLI에 접속하여 감사기록이 저장된 clog 파일을 읽을 수는 있으나 다만, 트래픽 로그(정보흐름통제규칙에 적용된 패킷 처리결과)는 CLI로 접속하여 읽을 수는 있으나 사람이 이해할 수 없는 형태로 제공된다. 로컬 하드디스크에 저장된 clog 파일은 관리자라도 수정/삭제가 불가능하다. 또한, 감사된 사건에 대해 위반규칙에 따른 잠재적 보안 위반을 탐지하고 관리자가 지정한 이메일로 경고메시지를 발송한다.

### 1.4.2.2. 암호지원

TOE는 WebGUI 관리접속 시 HTTPS 연결을 위해 암호키 관리 및 암호연산을 수행하여 TLS Handshake 프로토콜과 TLS Record 프로토콜을 처리한다. 또한 CLI 관리접속 시 SSH 연결을 위해 암호키 관리 및 암호연산을 수행하여 SSH Transport 프로토콜과 사용자 인증 프로토콜을 처리한다. 환경파일에 저장하는 패스워드를 보호하기 위해 SHA-256 이상의 해시값을 계산하고 TSF 데이터 및 일부 중요한 TSF의 무결성 검증을 위해 SHA-256 이상의 해시값을 계산한다.

암호키 관리 및 암호연산은 연관된 ISO 표준, 인터넷 표준(RFC), 미국 연방표준(FIPS), 국내 표준(TTA)등에 적합하도록 진행된다. TOE는 암호연산 과정에서 메모리에 로드된 암호키는 덮어쓰기 방식을 통해 완전 삭제한다.

### 1.4.2.3. 사용자 데이터 보호

#### (가) 침입차단

TOE의 침입차단 기능은 TCP/IP 기반 네트워크 트래픽의 정보흐름를 통제하기 위해 IP주소 및 포트를 기반으로하는 패킷 필터링 메커니즘과 TCP/UDP 세그먼트의 Flag 값을 기반으로 트래픽 흐름을 통제하는 상태기반 감시 메커니즘으로 구성된다.

패킷 필터링 메커니즘은 내외부 네트워크간 IPv4 출발지/목적지 IP주소, 서비스(프로토콜, 포트) 정보에 기반하여 관리자가 설정한 정보흐름통제규칙에 따라 트래픽을 처리(거부/차단/허용)한다. 패킷 필터링 메커니즘은 TCP/UDP 덤프로부터 받은 네트워크 패킷에 대해 우선적용 거부규칙을 적용한 후 정보흐름통제규칙에서 정한 처리방식에 따라 정보흐름을 통제하고 일치하는 규칙이 존재하지 않는 패킷에 대해서는 무조건 차단하는 화이트리스트 방식을 적용한다.

상태기반 감시 메커니즘은 패킷 필터링 메커니즘을 통해 통과된 패킷의 상태 값을 상태 표에 기록하고 이후 동일 상태 값을 갖는 패킷에 대해 정보흐름통제규칙을 적용하지 않고 TOE를 통과시키게 된다. TCP/UDP 세그먼트의 Flag 값을 확인하여 해당 패킷에 대한 상태 값(State)을 상태 표에 기록하여 세션이 유지되는 동안 유지하며 패킷을 처리한다. 상태 표에 기록된 정보를 기반으로 조각난 패킷을 탐지하여 TTL이 만료되어도 조각난 패킷들이 모두 도착하지 못하면 이전에 수신한 관련 패킷들까지 모두 폐기한다. 또한 Half-open TCP 세션에 대해서도 임계치에 도달하면 세션을 종료하고 연결을 끊는다.

### 1.4.2.4. 식별 및 인증

TOE 사용자는 관리자이며 일반 사용자는 존재하지 않는다.

TOE는 관리자를 인증하기 위해 패스워드 기반 관리자 인증 메커니즘을 구현한다. 관리자 계정 생성 시에 관리자 패스워드를 등록할 때 인증 메커니즘에서 패스워드 검증규칙(4조합 9자리 이상)에 적합한지 검증을 수행한다. 관리자는 관리접속(HTTPS, SSH) 또는 로컬접속(콘솔 직접연결)을 통해 TOE 관리수단에 접속한 후 패스워드를 입력하여 관리자 식별 및 인증을 받는다. 3회 연속 인증실패 시 관리자가 설정한 인증지연 시간동안 잠금처리된다.

SSH 관리접속으로 CLI에 접속하는 경우 TOE는 SSH 인증 프로토콜에서 RSA 공개키 기반 인증방식을 적용하여 CLI 관리접속 관리자를 인증한다. 관리자 인증을 성공해야 SSH 보안채널이 형성되고 이후 패스워드 기반 관리자 인증 메커니즘이 관리자 패스워드 입력을 요청하여 패스워드 기반 관리자 인증을 수행한다.

### 1.4.2.5. 보안관리

TOE는 식별 및 인증 기능을 통해 인가된 관리자자가 TOE 보안기능 및 중요 데이터 등을 설정 및 관리할 수 있는 보안관리 기능을 제공한다. 보안관리 기능은 관리자 웹페이지(WebGUI) 및 콘솔(CLI) 등 2가지 형태의 관리수단을 통해 구현된다. WebGUI는 HTTPS 관리접속으로 TOE에 연결되고 콘솔(CLI)는 로컬접속(콘솔포트) 또는 SSH 관리접속으로 TOE에 연결된다.

WebGUI는 기본계정 패스워드 초기화, 웹서버 데몬 관리 등의 일부 기능을 제외하고 TOE의 모든 기능을 관리할 수 있는 수단을 제공하여 CLI는 제한적인 범위에서 관리수단을 제공한다.

### 1.4.2.6. TSF 보호

관리자 패스워드는 SHA 256으로 변환하여 환경설정 파일에 저장하고 환경설정 파일은 접근권한을 설정하여 접근을 제한한다. 감사데이터가 TOE 로컬 하드디스크에 저장되는 경우 관리수단을 통해서만 읽기가 가능하고 쓰기는 불가능하다.

감사기록 생성 시 정확한 시각정보를 기록할 수 있도록 외부 NTP 서버를 설정하여 이로부터 시각정보를 가져와 동기화한다.

TOE의 정상적인 운영을 위해 로그서버, NTP 서버 등 외부 IT실체에 대해 시동 시 또는 관리자 요구 시 정상 통신 여부를 확인하는 시험을 실행한다. 또한 난수 생성 기능, 암호연산 기능, CPU 및 메모리에 대해 시동 시 또는 주기적으로 자체 시험을 실행하며 환경설정 파일, 암호키 파일 등 일부 TSF 데이터와 원본 이미지, 부트로더 이미지 등 일부 TSF의 무결성을 검증한다.

TOE는 TOE 버전 정보를 조회할 수 있는 기능을 제공한다.

### 1.4.2.7. TOE 접근

관리자는 HTTPS 연결을 통해 WebGUI 관리접속을 하거나 SSH 연결을 통해 SSH 관리접속을 한다. HTTP 연결을 시도하는 경우 HTTPS로 강제 전환하고 SSH 공개키가 등록된 관리자에 대해서만 관리접속을 허용한다. 또한 TOE는 접속 가능 IP로 지정된 단말에서 관리접속을 허용하고 특히, SSH 관리접속의 경우 해당 관리자에 대해 허용된 범위에서만 명령어 실행을 허가한다. 동일 계정으로 이미 로그인 되어 있는 경우 나중에 요청한 관리접속에 대해 연결을 거부한다.

관리자 로그인 후 일정시간 활동이 없는 경우 세션을 잠그며 세션잠금을 해지하기 전에 재인증을 수행한다. 관리자가 로그아웃을 하는 경우 해당 세션 관련 정보를 모두 삭제하여 세션종료 처리를 한다.

### 1.4.2.8. 안전한 경로/채널

#### (가) 안전한 경로

TOE는 관리자가 관리접속 시 안전한 경로를 제공하기 위해 TLS 1.2 및 TLS 1.3을 구현하고 SSH v2를 구현한다.

WebGUI 관리접속 시 서버인증을 위해 TLS 1.2 및 TLS 1.3의 인증서 기반 인증방식을 적용하며 이때 인증서는 TOE 운영환경에 따라 관리자가 사설인증서 또는 공인인증서를 선택하여 등록할 수 있다. 관리자 웹 브라우저에서 인증서 체인검증 및 유효기간 검증을 수행한 후 최종적으로 전자서명을 검증하여 서버를 인증할 수 있도록 TOE에서 필요한 기능을 지원한다. 서버 인증서 유효기간이 경과한 경우 인증서 폐지목록에 등록하고 관리자에게 통보메일을 발송하는 등 서버 인증서를 관리할 수 있도록 관리자에게 관련 정보를 제공한다. TLS 핸드쉐이크 과정을 통해 세션 암호키가 생성되면 이를 사용하여 TLS Record 프로토콜을 통해 전송구간의 TSF 데이터 등을 보호한다.

CLI 관리접속 시 SSH 사용자 인증 프로토콜에서 상호인증을 수행하며 SSH 클라이언트 인증 시 RSA 공개키 기반 방식을 적용하고 상호인증 과정에서 교환한 정보를 토대로 세션 암호키를 생성한다. 이렇게 생성된 세션 암호키를 사용하여 SSH Transport 프로토콜을 통해 전송구간의 TSF 데이터 등을 보호한다.

02

# 준수 선언

2.1. 공통평가기준 준수 선언

2.2 보호프로파일(보안요구사항)
준수 선언

2.3. 준수 선언의 이론적 근거

# 2. 준수 선언

## 2.1. 공통평가기준 준수 선언

| | | |
|---|---|---|
| 공통평가기준 | | 정보보호시스템 공통평가기준 버전 3.1 개정 2판<br>•정보보호시스템 공통평가기준 1부 : 소개 및 일반모델, 버전 3.1r2 (CCMB-2007-09-001, 2007. 9)<br>•정보보호시스템 공통평가기준 2부 : 보안기능요구사항, 버전 3.1r2, (CCMB-2007-09-002, 2007. 9)<br>•정보보호시스템 공통평가기준 3부 : 보증요구사항, 버전 3.1r2, (CCMB-2007-09-003, 2007. 9) |
| 준수 형태 | 2부 보안기능요구사항 | 확장 : FCS_RBG.1, FMT_PWD.1, FPT_PST.1 |
| | 3부 보증요구사항 | 준수 |
| | 패키지 | EAL4 |

## 2.2. 보호프로파일(보안요구사항) 준수 선언

본 보안목표명세서에서는 보호프로파일을 준수선언하지 않았으므로 해당사항이 없다.

| | |
|---|---|
| 보호프로파일 (보안요구사항) | 서버 공통보안요구사항 V3.0 R1<br>침입차단시스템 보안요구사항 V3.0 |
| 보증등급 | - |
| TOE 유형 | 침입차단시스템 |

## 2.3. 준수 선언의 이론적 근거

본 보안목표명세서에서는 보호프로파일을 준수선언하지 않았으므로 해당사항이 없다.

03

# 보안문제정의

3.1. 위협
3.2. 조직의 보안정책
3.3. TOE 운영환경에 관한 가정사항
3.4. 국제용 평가·인증 FAQ

# 3. 보안문제정의

## 3.1. 위협

TOE에 의해 보호되는 기본 자산은 다음과 같다.

- 관리자가 관리수단을 통해 전송하는 TSF 데이터
- TOE 자체 및 TOE 운영에 관련하여 저장된 TSF 데이터

위협원은 보호하고자 하는 자산에 비인가 된 접근 또는 비정상적인 방법으로 위해를 가하는 IT실체 및 사용인이며, 다음과 같은 다양한 위협을 발생시킬 수 있다. 이때 TOE에 대한 위협원은 강화된-기본 수준의 전문지식, 자원, 동기를 가진다.

| T.REPLAY | (T.재사용) |
|---|---|

위협원은 인증정보 또는 세션정보를 알아내 복사하고 이를 재사용하여 TOE에 접속하거나 내부망에 접속할 수 있다.

| T.WEAK_PASSWORD | (T.취약한 패스워드) |
|---|---|

위협원은 패스워드의 디폴트값 이용 등 관리가 미흡한 패스워드를 획득하여 인가된 관리자로 위장한 후 TOE에 접근할 수 있고, 낮은 수준의 패스워드 규칙이 적용된 경우 인가된 관리자로 위장하여 TOE에 접근할 수 있다.

| T.ADMIN_SESSION_HIJACK | (T.관리자 세션 탈취) |
|---|---|

위협원은 로그인된 채로 방치된 관리자 화면에 접근하거나 로그아웃 상태에서 세션종료가 되지 않은 관리자 세션을 이용하여 관리자 권한을 탈취할 수 있다.

| T.RETRY_AUTH_ATTEMPT | (T.연속 인증시도) |
|---|---|

위협원은 연속적으로 인증을 시도하여 획득한 정보를 이용해 인증에 성공한 후 인가된 관리자로 위장하여 TOE에 접근할 수 있다.

| T.IMPERSONATION | (T.위장) |
|---|---|

위협원은 인가된 관리자나 통신상대로 가장하여 TOE 또는 내부망에 접근할 수 있다.

| T.UNTRUSTED_PATH | (T.안전하지 않은 통신경로) |
|---|---|

위협원은 관리자 관리접속 과정에서 발생된 트래픽을 스니핑하여 TOE 보안설정 등 미흡한 취약점을 발견하고 이를 악용하여 내부망에 불법접근하거나 중요정보를 유출시킬 수 있다.

| T.WEAK_CRYPTO_PROTOCOLS | (T.취약한 암호 프로토콜) |
|---|---|

위협원은 취약한 암호통신 프로토콜 또는 낮은 암호강도를 사용하는 트래픽을 분석하여 키정보를 유추하거나 통신암호문의 내용을 알아낼 수 있다.

| T.EXHAUSTED_RESOURCE | (T.네트워크자원고갈) |
|---|---|

위협원은 비표준 패킷 또는 비정상 크기의 패킷을 지속적으로 발송하여 네트워크 자원을 고갈시킴으로써 네트워크 장애를 일으킬 수 있다.

| T.ROUTING_LOOF | (T.경로무한루프) |
|---|---|

위협원은 출발지/목적지 주소를 공격대상 주소로 변경 및 조작하여 패킷을 외부로 전송하지 못하고 무한루프 상태로 빠지게 하여 네트워크 장애를 일으킬 수 있다.

| T.SERVICE_UNAVAILABLE | (T.서비스거부공격) |
|---|---|

위협원은 통신을 요청한 후 고의로 응답패킷을 보내지 않아 서버를 계속 기다리게 하거나 내부망 서버로 응답패킷을 대량으로 수신 또는 발송하게 하여 서버에 과부하를 유도할 수 있다.

| T.TSF_COMPROMISE | (T.TSF훼손) |
|---|---|

위협원은 비인가 된 접근 등을 통해 TSF를 훼손해서, TOE 기능의 오동작을 유발하거나 TOE 기능을 무력화 할 수 있다.

| T.TRAFFIC_CONTROL_BYPASS | (T.정보흐름통제우회) |
|---|---|

위협원은 외부망에서 전송되는 패킷의 출발지 정보를 내부망 IP주소로 조작하거나 비정상적인 패킷을 전송하여 정보흐름통제 규칙 우회시도를 수행할 수 있다.

## 3.2. 조직의 보안정책

| P.CORRECT_OPERATION | (P.안전한운영) |
|---|---|

관리자는 조직의 침입차단시스템 보안정책을 준수하도록 TOE를 안전하게 설정하고 TOE 운영매뉴얼에 따라 정확하게 운영할 수 있도록 관리 수단을 제공해야 한다.

| P.AUDIT | (P.감사) |
|---|---|

보안과 관련된 행동에 대한 책임을 추적하기 위해 보안관련 사건은 기록 및 유지되어야 하며, 기록된 데이터는 검토되어야 한다. 또한, 감사데이터 저장용 디스크의 사용 가능한 공간을 정기적으로 점검하여 감사데이터가 소실되는 것을 예방하고, 저장된 감사데이터에 대한 비인가된 변경 및 삭제가 발생하지 않도록 보호해야 한다.

| P.CRYPTO_STRENGTH | (P.암호강도) |
|---|---|

조직은 패스워드 등과 같은 중요정보의 저장 및 전송 구간에 대한 암호화 조치를 적용해야 하며 안전한 암호 알고리즘을 사용해야 한다.

## 3.3. TOE 운영환경에 관한 가정사항

| A.PHYSICAL_PROTECTION | (A.물리적보안) |
|---|---|

TOE는 인가된 관리자만이 접근 가능한 물리적으로 안전한 환경에 위치한다.

| A.TRUSTED_ADMIN | (A.신뢰된관리자) |
|---|---|

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

| A.SECURE_MAINTANANCE | (A.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 유지한다.

| A.SINGLE_POINT_OF_CONNECTION | (A.유일한연결점) |
|---|---|

모든 외부 네트워크와 내부 네트워크간의 통신은 TOE를 통해서만 이루어진다.

04

# 보안목적

4.1. TOE 보안목적
4.2. 운영환경에 대한 보안목적
4.3. 보안목적의 이론적 근거

# 4. 보안목적

TOE에 대한 보안목적은 TOE에 의해서 직접적으로 다루어지는 보안목적이고, 운영환경에 대한 보안목적은 TOE가 보안기능성을 정확히 제공할 수 있도록 운영환경에서 지원하는 기술적/절차적 수단에 의해 다루어야하는 보안목적이다.

## 4.1. TOE 보안목적

| | |
|---|---|
| O.TRAFFICE_CONTROL | O.정보흐름통제 |

TOE는 패킷의 출발지 정보와 목적지 정보를 식별하여 외부망과 내부망 사이의 트래픽 흐름을 통제하여야 한다. 패킷의 헤더 정보에는 출발지 및 목적지의 IP주소, 포트번호, 프로토콜, 상태정보 등이 포함된다.

| | |
|---|---|
| O.ABNORMAL_PACKET_BLOCK | O.비정상패킷차단 |

TOE는 TOE를 통과하는 패킷 중 비정상적인 구조를 가지는 패킷을 차단해야 한다.

| | |
|---|---|
| O.DoS_PROTECT | O.서비스거부공격차단 |

TOE는 네트워크 장애를 유발하는 공격에 대응해야 하며, 내부망의 IT 자원이 비정상적으로 사용되는 경우를 탐지하고 차단하여야 한다.

| | |
|---|---|
| O.I&A | O.식별및인증 |

TOE는 TOE에 접속하거나 인가된 관리자 역할을 수행하려는 경우 관리자를 유일하게 식별하고 안전하게 인증해야 한다.

| | |
|---|---|
| O.PASSWORD_MANAGEMENT | O.패스워드관리 |

TOE는 인가된 관리자의 패스워드를 보호하고 관리할 수 있는 수단을 제공해야 한다.

| | |
|---|---|
| O.SESSION_CONTROL | O.세션통제 |

TOE는 관리자 IP 등 보안 속성정보에 근거하여 세션을 통제 및 관리하고, 인가된 관리자 세션을 통해 전송되는 TSF 데이터를 노출, 변경으로부터 보호해야 한다.

| | |
|---|---|
| O.SECURITY_MANAGEMENT | O.보안관리 |

TOE는 TSF 및 TSF 데이터를 효율적으로 관리할 수 있는 안전한 수단을 제공해야 하고, 이러한 중요 관리기능 및 데이터에 대한 관리를 인가된 관리자로 제한해야 한다.

| O.AUDIT | O.감사 |
|---|---|

TOE는 보안과 관련된 모든 행동의 책임추적이 가능하도록 보안관련 사건을 기록 및 유지해야 하며, 기록된 데이터를 검토할 수 있는 수단을 제공해야 한다. 또한, 감사 데이터의 저장 공간이 임계치 초과 및 포화 상태에 도달했을 때 대응 기능을 제공하여 감사 기능을 유지시켜야 한다.

| O.SELF_PROTECTION | O.자체보호 |
|---|---|

TOE는 구동 시 주요 하드웨어 및 TSF(TOE 보안기능을 구성하는 주요 프로세스 등)에 대한 정상동작 여부를 시험해야 하고 인가된 관리자가 시험결과를 확인할 수 있도록 해야 한다. 또한, TOE 보안기능을 구성하는 주요 프로세스의 무결성을 검증해야 한다.

| O.SECURE_CRYPT | O.안전한암호 |
|---|---|

TOE는 중요정보를 암호화 하거나 전송데이터 암호화 시, 암호키를 안전하게 생성 및 관리하고 안전한 보안강도를 갖는 암호프로토콜을 사용해야 한다.

| O.STORED_DATA_PROTECTION | O.저장데이터보호 |
|---|---|

TOE는 저장된 TSF 데이터를 인가되지 않은 노출 및 변경으로부터 보호해야 한다.

## 4.2. 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_CONNECTION | OE.유일한 연결점 |
|---|---|

모든 외부 네트워크와 내부 네트워크간의 통신은 TOE를 통해서만 이루어져야 한다.

# 4.3. 보안목적의 이론적 근거

## 4.3.1. TOE 보안목적의 이론적 근거

| | O. 정보 흐름 통제 | O. 식별 및 인증 | O. 패스워드 관리 | O. 세션 통제 | O. 비정상 패킷차단 | O. 서비스 거부 공격 차단 | O. 자체 보호 | O. 감사 | O. 보안 관리 | O. 안전한 암호 | O. 저장 데이터 보호 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| T.재사용 | | | | X | | | | | | | |
| T.취약한패스워드 | | X | X | | | | | | | | |
| T.관리자세션탈취 | | | | X | | | | | | | |
| T.연속인증시도 | | X | | | | | | | | | |
| T.위장 | | X | | | | | | | | | |
| T.안전하지않은통신경로 | | | | X | | | | | | | |
| T.취약한암호프로토콜 | | | | | | | | | | X | |
| T.저장데이터훼손 | | | | | | | | | | | X |
| T.네트워크자원고갈 | | | | | X | X | | | | | |
| T.경로무한루프 | X | | | | | X | | | | | |
| T.서비스거부공격 | | | | | | X | | | | | |
| T.TSF훼손 | | X | | | | | X | | X | | X |
| T.정보흐름통제우회 | X | | | | | | | | | | |
| P.감사 | | | | | | | | X | | | |
| P.안전한운영 | | X | | | | | X | | X | | |
| P.암호강도 | | | | X | | | | | | X | X |

[TOE 보안문제정의와 TOE 보안목적 대응]

| T.REPLAY | O.세션통제 |
|---|---|

**T.재사용**은 **O.세션통제**에 의해 대응된다.

**O.세션통제**는 관리접속 시 인증데이터 재사용 공격에 방지할 수 있는 안전한 암호통신 프로토콜을 적용하고 관리자 로그아웃 시 세션종료를 통해 인증정보 또는 세션정보를 재사용한 인증우회에 대응한다.

| T.WEAK_PASSWORD | O.패스워드관리, O.식별및인증 |
|---|---|

**T.취약한패스워드**는 **O.패스워드관리, O.패스워드관리**에 의해 대응된다.

**O.패스워드관리**는 기본적으로 제공된 디폴트 패스워드가 있는 경우 관리자 최초 접속 시 강제 변경하는 기능을 제공하고, 패스워드 조합규칙 및 길이를 설정할 수 있도록 한다.

**O.패스워드관리**은 패스워드 허용기준(패스워드 길이 및 조합규칙 등)에 따라 패스워드를 검증하는 기능을 제공하도록 한다.

| T.ADMIN_SESSION_HIJACK | O.세션통제 |
|---|---|

**T.관리자세션탈취**는 **O.세션통제**에 의해 대응된다.

**O.세션통제**는 접속 IP 및 인가된 관리자가 설정한 속성정보를 기반으로 세션연결을 제한하고 인가된 관리자의 로그아웃 시 세션을 정상적으로 종료한다. 또한, 인가된 관리자 로그인 후 지정된 비활동 기간 초과 시 세션 잠금 또는 세션종료를 수행한다.

| T.RETRY_AUTH_ATTEMPT | O.식별및인증 |
|---|---|

**T.연속인증시도**는 **O.식별및인증**에 의해 대응된다.

**O.식별및인증**은 연속적인 인증실패를 탐지하여 해당 계정의 로그인을 일정시간 제한하는 등의 인증제한 조치를 수행한다.

| T.UNTRUSTED_PATH | O.세션통제 |
|---|---|

**T.안전하지않은통신경로**는 **O.세션통제**에 대응된다.

**O.세션통제**는 관리자 세션을 통해 전송되는 TSF 데이터를 노출, 변경으로부터 보호한다.

| T.WEAK_CRYPTO_PROTOCOLS | O.안전한암호 |
|---|---|

**T.취약한암호프로토콜**은 **O.안전한암호**에 대응된다.

**O.안전한암호**는 암호키를 안전하게 생성 및 관리하고 안전한 보안강도를 갖는 암호프로토콜을 사용하여 전송데이터를 보호한다.

| T.STORED_DATA_DAMAGE | O.저장데이터보호 |
|---|---|

**T.저장데이터훼손**은 **O.저장데이터보호**에 대응된다.

**O.저장데이터보호**는 TOE가 보호수단을 통하여 인가된 관리자 인증정보, 암호키 등과 같은 TSF 데이터를 인가되지 않은 노출, 변경으로부터 보호한다.

| | |
|---|---|
| T.EXHAUSTED_RESOURCE | O.비정상패킷차단, O.서비스거부공격차단 |

**T.네트워크자원고갈**은 **O.비정상패킷차단, O.서비스거부공격차단**에 의해 대응된다.
**O.비정상패킷차단**은 TOE를 통과하는 패킷 중 비정상적인 구조를 가지는 패킷을 차단한다.
**O.서비스거부공격차단**은 네트워크 장애를 유발하는 공격에 대응하며, 내부망의 IT 자원이 비정상적으로 사용되는 경우를 탐지하고 차단한다.

| | |
|---|---|
| T.ROUTING_LOOF | O.서비스거부공격차단, O.정보흐름통제 |

**T.경로무한루프**는 **O.서비스거부공격차단, O.정보흐름통제**에 의해 대응된다.
**O.서비스거부공격차단**은 네트워크 장애를 유발하는 공격에 대응한다.
**O.정보흐름통제**는 패킷의 출발지 정보와 목적지 정보를 식별하여 외부망과 내부망 사이의 트래픽 흐름을 통제한다.

| | |
|---|---|
| T.SERVICE_UNAVAILABLE | T.SERVICE_UNAVAILABLE |

**T.서비스거부공격**은 **O.서비스거부공격차단**에 의해 대응된다.
**O.서비스거부공격차단**은 내부망의 IT 자원이 비정상적으로 사용되는 경우를 탐지하고 차단한다.

| | |
|---|---|
| T.TSF_COMPROMISE | O.식별및인증, O.보안관리, O.자체보호, O.저장데이터보호 |

**T.TSF훼손**은 **O.식별및인증, O.보안관리, O.자체보호, O.저장데이터보호**에 의해 대응된다.
**O.식별및인증**은 관리자의 식별 및 인증이 성공한 후에만 TOE로의 접속이 가능하도록 하여 위협원의 우회 접속을 차단한다.
**O.보안관리**는 TOE 주요 관리기능 및 데이터에 대한 접근 및 설정을 인가된 관리자로 제한한다.
**O.자체보호**는 침입차단시스템 장비의 주요 프로세스 및 일부 하드웨어 요소에 대한 정상동작 여부 시험 기능을 제공한다. 또한 TSF 훼손여부를 식별하기 위해 무결성 검증 대상으로 설정된 파일(환경파일, 중요 기능을 수행하는 실행파일 등)에 대해 무결성 검증 수단을 제공한다.
**O.저장데이터보호**는 TOE에 저장된 TST데이터를 인가되지 않은 노출이나 변경으로부터 보호하는 기능을 제공한다.

| | |
|---|---|
| T.TRAFFIC_CONTROL_BYPASS | O.정보흐름통제 |

**T.정보흐름통제우회**는 **O.정보흐름통제**에 의해 대응된다.
**O.정보흐름통제**는 패킷의 출발지 정보와 목적지 정보를 식별하여 외부망과 내부망 사이의 트래픽 흐름을 통제한다.

| | |
|---|---|
| P.AUDIT | O.감사 |

**P.감사**는 **O.감사**에 의해 대응된다.
**O.감사**는 TOE는 보안과 관련된 모든 행동의 책임추적이 가능하도록 보안관련 사건을 기록 및 유지해야 하며, 기록된 데이터를 검토할 수 있는 수단을 제공한다. 또한, 감사 데이터의 저장 공간이 임계치 초과 및 포화 상태에 도달했을 때 대응 기능을 제공하여 감사 기능을 유지한다.

| P.CORRECT_OPERATION | O.보안관리, O.자체보호, O.식별및인증 |
|---|---|

**P.안전한운영**은 **O.보안관리, O.자체보호, O.식별및인증**에 의해 대응된다.

**O.보안관리**는 TOE 관리 기능에 대한 접근을 인가된 관리자로 제한하고 TOE를 안전하게 운영할 수 있는 수단을 제공한다.

**O.자체보호**는 TOE의 안전한 운영을 위해 TSF 및 외부실체에 대한 정상동작 여부를 시험할 수 있는 수단을 제공한다.

**O.식별및인증**은 TOE의 안전한 운영을 위해 인증에 성공한 인가된 관리자만이 TOE에 접속할 수 있는 수단을 제공한다.

| P.CRYPTO_STRENGTH | O.안전한암호, O.세션통제, O.저장데이터보호 |
|---|---|

**P.암호강도**는 **O.안전한암호, O.세션통제, O.저장데이터보호**에 의해 대응된다.

**O.안전한암호**는 중요정보를 암호화 하거나 전송데이터 암호화 시, 암호키를 안전하게 생성 및 관리하고 안전한 보안강도를 갖는 암호프로토콜을 사용한다.

**O.세션통제**는 관리자의 관리접속 구간에 안전한 암호 통신프로토콜 및 암호 알고리즘을 적용한다.

**O.저장데이터보호**는 TSF 데이터(인증정보, TOE 설정값 등) 암호화 저장 시 안전한 알고리즘을 적용한다.

## 4.3.2. TOE 보안목적의 이론적 근거

☞ 일치성 분석 표에서 매핑되지 않는 SPD 또는 운영환경에 대한 보안목적이 존재하는 경우 일치성이 결여된 것이므로 SPD 또는 운영환경에 대한 보안목적을 을 추가 식별하여 명세하거나 기존의 내용을 보완해야 함

| | OE.<br>물리적 보안 | OE.<br>보안유지 | OE.<br>신뢰된 관리자 | OE.<br>유일한 연결점 | OE.<br>로그백업 |
|---|---|---|---|---|---|
| P.안전한운영 | | | X | | |
| P.감사 | | | | | X |
| A.물리적보안 | X | | | | |
| A.보안유지 | | X | | | |
| A.신뢰된관리자 | | | X | | X |
| A.유일한연결점 | | | | X | |

[TOE 보안문제정의와 운영환경에 대한 보안목적 대응]

| P.CORRECT_OPERATION | OE.신뢰된 관리자 |
|---|---|

**P.안전한운영**은 **OE.신뢰된관리자**에 의해 이행된다.
**OE.신뢰된관리자**는 조직의 침입차단시스템 보안정책 및 운영매뉴얼에 따라 관리자가 TOE를 정확하게 운영하게 한다.

| P.AUDIT | OE.로그백업 |
|---|---|

**P.감사**는 **OE.로그백업**에 의해 이행된다.
**OE.로그백업**은 TOE의 기능뿐만 아니라 관리자에 의한 정기적인 감사데이터 저장 공간 점검이 이루어지며, 로그기록이 유실되지 않도록 정기적인 로그백업 또는 외부 로그서버로의 로그 전송 등을 수행한다.

| A.PHYSICAL_PROTECTION | OE.물리적 보안 |
|---|---|

**A.물리적보안**은 **OE.물리적 보안**에 의해 지원된다.
**OE.물리적보안**은 보호설비가 갖추어진 장소에 TOE를 배치하고, 인가된 관리자만이 접근하도록 출입을 통제한다.

| A.TRUSTED_ADMIN | OE.보안유지 |
|---|---|

**A.보안유지**는 **OE.보안유지**에 의해 지원된다.
**OE.보안유지**는 내부 네트워크 구성 변경, 호스트의 증감, 서비스의 증감 등으로 내부 네트워크 환경이 변화될 때, 변화된 환경과 보안정책을 즉시 TOE 운영정책에 반영하여 이전과 동일한 수준의 보안을 유지하도록 보장한다.

| A.TRUSTED_ADMIN | OE.신뢰된관리자, OE.로그백업 |
|---|---|

**A.신뢰된관리자**는 **OE.신뢰된 관리자, OE.로그백업**에 의해 지원된다.
**OE.신뢰된관리자**는 조직의 정보보호 교육 및 침입차단시스템 관리지침에 대한 훈련을 이수하여 조직의 네트워크를 안정적으로 운영할 수 있는 능력을 갖추고 있음을 보장한다. 또한, TOE의 안전한 운영 및 적절한 관리 방법에 따라 TOE를 안전하고 정확하게 운영함을 보장한다.
**OE.로그백업**은 인가된 관리자가 감사기록 유실에 대비하여 감사데이터 저장소의 여유 공간을 주기적으로 확인하고 감사기록이 소진되지 않도록 감사기록 백업(외부 로그서버, 별도 저장장치 등) 등을 수행하도록 보장한다.

| A.SINGLE_POINT_OF_CONNECTION | OE.유일한 연결점 |
|---|---|

**A.유일한연결점**은 **OE.유일한연결점**에 의해 지원된다.
**OE.유일한연결점**은 모든 외부 네트워크와 내부 네트워크간의 통신이 TOE를 통해서 이루어지도록 보장한다.

05

# 확장 컴포넌트 정의

5.1. 암호지원
(FCS, Cryptographic support)

5.2. 보안관리
(FMT, Security Management)

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

# 5. 확장 컴포넌트 정의

**본 보안목표명세서에서 확장한 컴포넌트의 정의는 다음과 같다.**

## 5.1. (FCS, Cryptographic support)

### 5.1.1. 난수 생성

**패밀리 개요**

난수 생성(FCS_RBG, Random Bit Generation ) 패밀리는 TOE 암호 연산 시 필요한 랜덤 값을 생성하는 기능을 요구하도록 정의한다.

**컴포넌트 계층관계 및 설명**

| | |
|---|---|
| FCS_RBG 난수 생성 | 1 |

FCS_RBG.1 난수 생성은 TSF가 TOE 암호 연산 시 필요한 랜덤 값을 생성하는 기능을 요구한다.

예상되는 관리 요구사항은 없다.

예상되는 감사 대상 행동은 없다.

#### 5.1.1.1. FCS_RBG.1 난수 생성

| | |
|---|---|
| 계층관계 | 없음 |
| 종속관계 | 없음 |
| FCS_RBG.1.1 | TSF는 다음의 [ 할당 : 표준 목록 ]에 부합하는 명세된 난수 발생기를 이용해서 암호 키 생성에 필요한 난수를 생성해야 한다. |

# 5.2. 보안관리(FMT, Security Management)

## 5.2.1. ID 및 패스워드

### 패밀리 개요

ID 및 패스워드(FMT_PWD, ID and 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

### 5.2.1.1. FMT_PWD.1 ID 및 패스워드 관리

| | |
|---|---|
| 계층관계 | 없음 |
| 종속관계 | FMT_SMF.1 관리기능 명세<br>FMT_SMR.1 보안 역할 |
| FMT_PWD.1.1 | TSF는 [할당 : 기능목록]의 패스워드를 다음과 같이 관리하는 능력을 [할당 : 인가된 역할]로 제한해야 한다.<br>1. [할당 : 패스워드 조합 규칙 및/또는 길이]<br>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.<br>1. [할당 : ID 조합 규칙 및/또는 길이]<br>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.

# 5.3. TSF 보호(FPT, Protection of the TSF)

## 5.3.1. 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.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

### 5.3.1.1. 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 비인가 된 [선택 : 노출, 변경]으로부터 보호해야 한다.

06

# 보안요구사항

6.1. 보안기능요구사항
6.2. 보증요구사항
6.3. 보안요구사항의 이론적 근거
6.4. 종속관계에 대한 이론적 근거

# 6. 보안요구사항

본 보안목표명세서는 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 보안목표명세서에서 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 이탤릭체*로 표시된다.

### 정교화

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

본 보안목표명세서는 요구사항의 의미를 명확히 하고, CC 컴포넌트 오퍼레이션 적용에 대한 ST 작성자의 의도를 전달하기 위해 “ST 작성자 **註**”가 제공된다.

## 6.1. 보안기능요구사항

TOE가 만족하는 보안기능요구사항은 다음과 같다. 비고란에 기재된 '정교화', '반복'의 경우 CC 컴포넌트의 오퍼레이션을 의미한다.

| 보안기능 클래스 | 보안기능 컴포넌트 | | 비고 |
|---|---|---|---|
| 보안감사 (FAU) | FAU_ARP.1 | 보안경보 | |
| | FAU_GEN.1 | 감사데이터 생성 | |
| | FAU_SAA.1 | 잠재적인 위반 분석 | |
| | FAU_SAR.1 | 감사검토 | 정교화 |
| | 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 데이터의 손실 방지 | |
| 암호지원 (FCS) | FCS_CKM.1 | 암호키 생성 | 반복 |
| | FCS_CKM.2 | 암호키 분배 | 반복 |
| | FCS_CKM.4 | 암호키 파기 | |
| | FCS_COP.1 | 암호 연산 | 반복 |
| | FCS_RBG.1(확장) | 난수 생성 | 반복 |
| 사용자 데이터보호 (FDP) | FDP_IFC.2 | 완전한 정보흐름 통제 | 반복 |
| | FDP_IFF.1 | 단일 계층 보안속성 | 반복 |
| 식별 및 인증 (FIA) | FIA_AFL.1 | 인증 실패 처리 | 반복 |
| | FIA_SOS.1 | 비밀정보의 검증 | |
| | FIA_UAU.1 | 인증 | 정교화 |
| | FIA_UAU.4 | 재사용 방지 인증메커니즘 | |
| | FIA_UAU.7 | 인증 피드백 보호 | 정교화 |
| | FIA_UID.1 | 사용자 식별 | 정교화 |
| 보안관리 (FMT) | FMT_MOF.1 | 보안기능 관리 | 정교화 |
| | FMT_MSA.1 | 보안속성 관리(침입차단) | 반복, 정교화 |
| | FMT_MSA.3 | 정적 속성 초기화 | 정교화 |
| | FMT_MTD.1(1) | TSF 데이터 관리(일반 TSF 데이터) | 반복, 정교화 |
| | FMT_MTD.1(2) | TSF 데이터 관리(암호관련 정보) | 반복, 정교화 |
| | FMT_PWD.1(확장) | ID 및 패스워드 관리 | 확장, 정교화 |
| | FMT_SMF.1 | 관리기능 명세 | |
| | FMT_SMR.1 | 보안 역할 | 정교화 |

| 보안기능 클래스 | 보안기능 컴포넌트 | | 비고 |
|---|---|---|---|
| TSF 보호 (FPT) | FPT_PST.1(확장) | 저장된 TSF 데이터 기본적인 보호 | 확장 |
| | FPT_STM.1 | 신뢰할 수 있는 타임스탬프 | |
| | FPT_TST.1 | TSF 자체 시험 | |
| TOE 접근 (FTA) | FTA_MCS.2 | 사용자 속성별 동시 세션 수의 제한 | 정교화 |
| | FTA_SSL.1 | TSF에 의한 세션 잠금 | |
| | FTA_SSL.3 | TSF에 의한 세션 종료 | |
| | FTA_TSE.1 | TOE 세션 설정 | 정교화 |
| 안전한 경로/채널 (FTP) | FTP_ITC.1 | 안전한 채널 | 정교화 |

[표 2] 도출된 SFR 목록

## 6.1.1. 보안감사(FAU)

### 6.1.1.1. FAU_ARP.1 보안 경보

| | |
|---|---|
| 계층관계 | 없음 |
| 종속관계 | FAU_SAA.1 잠재적인 위반 분석 |
| FAU_ARP.1.1 | TSF는 잠재적인 보안 위반을 탐지한 경우, [ 관리자가 설정한 이메일로 경고메시지 발송 ]을 취해야 한다. |

### 6.1.1.2. FAU_GEN.1 감사데이터 생성

| | |
|---|---|
| 계층관계 | 없음 |
| 종속관계 | FPT_STM.1 신뢰할 수 있는 타임스탬프 |
| FAU_ARP.1.1 | TSF는 다음 감사대상 사건에 대해 감사레코드를 생성할 수 있어야 한다.<br>a) 감사 기능의 시동(start-up)과 종료(shut-down)<br>b) *지정되지 않음* 감사 수준에 따른 모든 감사대상 사건<br>c) [ [표 3] 감사대상 사건의 "감사대상 사건" 참조 ] |
| FAU_ARP.1.2 | TSF는 최소한 다음 정보를 각 감사 레코드 내에 기록해야 한다.<br>a) 사건 일시, 사건 유형, 주체의 신원(가능한 경우), 사건 결과(성공 또는 실패)<br>b) 각 감사 사건 유형에 대하여, 보호프로파일/보안목표명세서에 포함된 기능 컴포넌트의 감사대상 사건 정의에 기반한 [ [표 3] 감사대상 사건의 "추가적인 감사기록 내용" 참조 ] |

| 보안기능 컴포넌트 | 감사대상 사건 | 추가적인 감사기록 내용 |
|---|---|---|
| FAU_ARP.1 | 잠재적인 보안 위반으로 인하여 취해지는 대응행동 | 적용된 위반 탐지 조건 |
| 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 | - |
| FCS_CKM.1<br>FC_CKM.2* | 암호키 생성/가져오기, 변경 등 | 키 용도, 키 명칭 |
| FCS_CKM.4 | 암호키 파기 | 키 용도, 키 명칭 |
| FCS_COP.1* | 암호 연산의 성공과 실패 | 암호 연산 유형 |
| FDP_IFF.1 | 요청된 정보흐름을 허용하는 결정<br>정보흐름 요청에 대한 모든 결정 | 상태정보(TCP 플래그 값)<br>상태 표 메모리 연관 정보 |
| FIA_AFL.1 | 패스워드 기반 인증에 실패한 인증 시도의 한계치 도달과 취해진 대응행동, 적절하다면 이어서 일어나는 정상 상태로의 회복 | 인증 연속실패 누적회수 |
| FIA_SOS.1 | 패스워드 허용기준 검증 실패 | - |
| FIA_UAU.1 | 인증 메커니즘의 모든 사용 | - |
| FIA_UAU.4 | 인증데이터의 재사용 시도 | - |
| FIA_UID.1 | 관리자 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<br>보안속성의 초기값에 대한 모든 변경 | - |
| FMT_MTD.1 | TSF 데이터 값에 대한 모든 변경 | 변경된 TSF 데이터 값 |
| FMT_PWD.1(확장) | 관리자 최초 로그인 시 패스워드 변경 | - |
| FMT_SMF.1 | 관리기능 사용 | 연관 메뉴명칭 |
| FMT_SMR.1 | 역할을 분담하는 관리자 그룹에 대한 변경 | 전후 변경내용 |
| FPT_TST.1 | TSF 자체 시험의 실행과 시험 결과 | 시험대상 프로세스/데몬 명칭<br>무결성 위반시 변경된 TSF 데이터 혹은 실행 코드 |
| FTA_MCS.2 | 동시 세션 수의 제한에 기반한 새로운 세션 거부 | 새로운 세션연결을 요청한 관리자 식별 정보 |
| FTA_SSL.1 | 관리접속 비활동 기간 경과 시 세션의 잠금 | 세션 잠금 원인 |
| FTA_SSL.3 | 관리접속 비활동 기간 경과 시 세션의 종료 | 세션 종료 원인 |
| FTA_TSE.1 | 세션 설정 메커니즘으로 인한 세션 설정 거부<br>사용자 세션을 설정하려는 모든 시도 | - |
| FTP_TRP.1 | 안전한 경로 기능의 장애<br>모든 안전한 경로 장애와 관련된 관리자 식별 | TLS 데몬에서 생성한 오류메시지 |

[표 3] 감사대상 사건

### 6.1.1.3. 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.<br>a) 잠재적인 보안 위반을 나타내는 알려진 [ 다음의 정의된 감사대상 사건 ]의 누적 또는 조합<br>•FIA_UAU.1의 감사대상 사건 중 동일 계정의 인증 실패<br>•FAU_STG.3의 감사 대상 사건 중 대응 행동 실패<br>•FAU_STG.4의 감사대상 사건 중 대응 행동 실패<br>•FDP_IFF.1의 감사대상 사건 중 상태 표 메모리 임계치 초과<br>•FDP_IFF.1의 감사대상 사건 중 관리자가 설정한 정보흐름통제규칙 적용결과<br>•FMT_MTD.1(1)의 감사대상 사건 중 SSH Authorized Key 설정 변경<br>•FMT_SMF.1의 감사대상 사건 중 관리자가 설정한 관리메뉴<br>•FPT_TST.1의 감사대상 사건 중 무결성 위반 감사 사건<br>b) [ 없음 ] |

### 6.1.1.4. FAU_SAR.1 감사 검토

| | |
|---|---|
| 계층관계 | 없음 |
| 종속관계 | FAU_GEN.1 감사 데이터 생성 |
| FAU_SAR.1.1 | TSF는 [ WebGUI-all 역할 또는 WebCfg-Dashboard 역할이 부여된 인가된 관리자 ]에게 감사 레코드로부터 [ 모든 감사 데이터 ]를 읽을 수 있는 기능을 제공해야 한다. |
| FAU_SAR.1.2 | TSF는 인가된 관리자가 정보를 해석하기에 적합하도록 감사 레코드를 제공해야 한다. |

### 6.1.1.5. FAU_SAR.3 선택 가능한 감사검토

| | |
|---|---|
| 계층관계 | 없음 |
| 종속관계 | FAU_SAR.1 감사 검토 |
| FAU_SAR.3.1 | TSF는 [ 사건유형별 검색어(단어, 구문, 정규표현식 등) 및 사건일시 기간을 AND한 조건 ]에 기초하여 감사 데이터에 대한 [ 오래된 순/최신순으로 정렬 ]을 적용할 수 있는 능력을 제공해야 한다. |

#### 6.1.1.6. 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. |

#### 6.1.1.7. 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 [ clog 파일크기의 80% ]를 초과할 경우 [ 관리자가 설정한 이메일로 경고메시지 통보, syslog 서버로 로그전송 기능 활성화 ] 을 취해야 한다. |

#### 6.1.1.8. FAU_STG.4 감사 데이터의 손실 방지

| | |
|---|---|
| 계층관계 | FAU_STG.4 |
| 종속관계 | FAU_STG.1 감사 증적 저장소 보호 |
| FAU_STG.4.1 | TSF는 감사 증적이 포화인 경우, TSF는 *가장 오래된 감사 레코드 덮어쓰기* 및 [ 자동백업 ]을 수행해야 한다. |

### 6.1.2. 암호지원(FCS)

#### 6.1.2.1. FCS_CKM.1 암호키 생성

| | |
|---|---|
| 계층관계 | 없음 |
| 종속관계 | [FCS_CKM.2 암호키 분배 또는 FCS_COP.1 암호 연산]<br>FCS_CKM.4 암호키 파기 |
| FCS_CKM.1.1 | TSF는 다음의 [ 다음 표준 ]에 부합하는 명세된 암호키 생성 알고리즘 [ 다음 암호키 생성 알고리즘 ]과 명세된 암호키 길이 [ 다음 암호키 길이 ]에 따라 암호키를 생성해야 한다. |

| 키생성 표준 | 암호키 생성 알고리즘 | 암호키 길이 |
|---|---|---|
| RFC 2898 | PBKDF2 | 256 비트 |
| RFC 4253 | SSHv2 Transport Layer Protocol의 HASH 함수 | AES용 128/256 비트 |

| | | |
|---|---|---|
| RFC 4253 | SSHv2 Transport Layer Protocol의 HASH 함수 | HMAC용 160 비트 |
| RFC 3526 | diffie-hellman-group14 | 2048 비트 |
| RFC 8268 | diffie-hellman-group14 | 2048 비트 |
| RFC 8268 | diffie-hellman-group15 | 3072 비트 |
| RFC5426<br>RFC8446 | TLS Record Protocol의 PRF 함수 (SAH256기반 의사난수생성) | AES용 128/256 비트 |
| RFC5426<br>RFC8446 | TLS Record Protocol의 PRF 함수 (SAH256기반 의사난수생성) | SEED용 128 비트 |
| RFC5426<br>RFC8446 | TLS Record Protocol의 PRF 함수 (SAH256기반 의사난수생성) | HMAC용 160/256비트 |
| RFC8422 | ECDH P-256 | 256비트 |
| RFC8422 | ECDH P-384 | 384비트 |
| RFC8422 | ECDH P-521 | 521비트 |
| RFC8017 (PKCS#1) | RSASP1(인증서 공개키쌍) | RSA 2048 비트 |
| RFC8017 (PKCS#1) | RSADP(인증서 공개키쌍) | RSA 2048 비트 |

**ST 작성자 註**

o 본 SFR은 저장 데이터 암호화 또는 관리자가 안전한 경로(SSH, HTTPS)로 TOE 관리수단(CLI, WebGUI)에 접속하여 데이터를 전송하는 경우 이들 데이터에 대한 암호화 및 MAC값 생성에 사용할 KEK, 세션키 생성에 관한 것이다.

o SSHv2(RFC4253)에서 정의한 Transport Layer Protocol에서 생하는 세션키(클라이언트의 초기벡터, AES 암호키, HMAC 키와 서버의 초기벡터, AES 암호키, HMAC 키)에 관한 사항을 정의한 것이며 키생성 알고리즘은 HASH 함수를 사용하되 RFC4253에서 특정하고 있지 않으므로 HASH 함수로 명세하였다.

o SSHv2(rfc4253)에서 정의한 Trasnport Layer Protocol에서 세션키 생성에 필요한 비밀정보 공유에 사용할 D-H 공개키 생성에 관한 것이다.

o SSHv2(rfc4253)에서 정의한 Trasnport Layer Protocol에서 서버인증을 위한 공개키는 TOE에서 생성하지 않고 외부에서 생성한 공개키를 TOE에 등록하는 방식을 적용하고 있으므로 본 요구사항에서는 비대칭키 생성에 관한 사항은 해당사항이 없다.

o TLS Record Protocol(RFC 5426, RFC8446)에서 사용할 세션키(클라이언트의 초기벡터, 암호키, HMAC 키와 서버의 초기벡터, AES 암호키, HMAC 키)에 관한 사항을 정의한 것이며 키생성 알고리즘은 PRF 함수로 정의하며 일반적으로 SHA256 함수를 사용한다.

o TLS Handshake Protocol(RFC 5426, RFC8446)에서 pre-master 비밀정보 공유에 사용할 D-H 공개키 생성에 관한 것이다.

o TLS Record Protocol(RFC 5426, RFC8446)에서 서버인증을 위한 공개키는 TOE에서 생성하지 않고 공인기관에서 발급한(예, 공인인증서)를 TOE에 등록하는 방식과 TOE 자체 인증서 생성 방식을 병행하고 있으므로 본 요구사항에서는 자체 인증서 생성 시에 필요한 비대칭키 생성에 관한 사항을 정의한다.

### 6.1.2.2. 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 [ 다음 표준 ]에 부합하는 명세된 암호키 분배 방법 [ 다음 암호키 분배 알고리즘 ] 에 따라 암호키를 분배해야 한다.

| 키교환 표준 | 암호키 분배 알고리즘 |
|---|---|
| RFC3526 | DHE_RSA |
| RFC 8268 | diffie-hellman-group14-256 |
| RFC8422 | ECDHE_ECDSA |
| RFC8422 | ECDHE_RSA |
| RFC8422 | ECDHE_ANON |

### 6.1.2.3. 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 [ 없음 ]에 부합하는 명세된 암호키 파기 방법 [ RAM 또는 Flash 메모리에 저장된 암호키 값을 “0” 또는 “난수”로 3회 덮어쓰기 후 해당 변수 삭제 ]에 따라 암호키를 파기해야 한다.

### 6.1.2.4. FCS_COP.1(1) 암호 연산(대칭키 암호연산)

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.4.1 TSF는 다음의 [ 다음 표준 ]에 부합하는 명세된 암호 알고리즘 [ 다음 대칭키 암호 알고리즘 ]과 명세된 암호키 길이 [ 다음 암호키 길이 ]에 따라 [ 다음 암호연산 ]을 수행해야 한다.

- ISO 10116에 부합하는 AES 128비트/192비트/256비트 암호키로 CBC 모드 및 GCM 모드 연산
- ISO 19772에 부합하는 AES 128비트/192비트/256비트 암호키로 GCM 모드 연산

### 6.1.2.5. FCS_COP.1(2) 암호 연산(HMAC)

| | |
|---|---|
| 계층관계 | 없음 |
| 종속관계 | [FDP_ITC.1 보안속성 없이 사용자 데이터 유입 또는<br>FDP_ITC.2 보안속성을 포함한 사용자 데이터 유입 또는<br>FCS_CKM.1 암호키 생성]<br>FCS_CKM.4 암호키 파기 |
| FCS_COP.1.1 | TSF는 다음의 [ 다음 표준 ]에 부합하는 명세된 암호 알고리즘 [ 다음 Keyed Hash 알고리즘 ]과 명세된 암호키 길이 [ 다음 암호키 길이 ]에 따라 [ 다음 암호연산 ]을 수행해야 한다.<br>•ISO/IEC 9797-2 에 부합하는 The Keyed-Hash Message Authentication Code (HMAC) SHA-256 알고리즘의 64바이트 암호키로 32바이트 길이로 메시지 축약 연산 |

### 6.1.2.6. FCS_COP.1(3) 암호 연산(해시)

| | |
|---|---|
| 계층관계 | 없음 |
| 종속관계 | [FDP_ITC.1 보안속성 없이 사용자 데이터 유입 또는<br>FDP_ITC.2 보안속성을 포함한 사용자 데이터 유입 또는<br>FCS_CKM.1 암호키 생성]<br>FCS_CKM.4 암호키 파기 |
| FCS_COP.1.1 | TSF는 다음의 [ 다음 표준 ]에 부합하는 명세된 암호 알고리즘 [ 다음 Hash 알고리즘 ]과 명세된 암호키 길이 [ 없음 ]에 따라 [ 다음 암호연산 ]을 수행해야 한다.<br>•IISO/IEC 10118-3:2004에 부합하는 SHA-256, SHA-512 알고리즘의 각 160비트, 256비트, 512비트 길이로 메시지 축약<br>•IISO/IEC 10118-3:2004에 부합하는 SHA-256 알고리즘의 256비트 길이로 TLS Handshake Protocol에서 사용하는 master secret 메시지 확장 |

### 6.1.2.7. FCS_COP.1(4) 암호 연산(전자서명)

| | |
|---|---|
| 계층관계 | 없음 |
| 종속관계 | [FDP_ITC.1 보안속성 없이 사용자 데이터 유입 또는<br>FDP_ITC.2 보안속성을 포함한 사용자 데이터 유입 또는<br>FCS_CKM.1 암호키 생성]<br>FCS_CKM.4 암호키 파기 |
| FCS_COP.1.1 | TSF는 다음의 [ 다음 표준 ]에 부합하는 명세된 암호 알고리즘 [ 다음 전자서명 알고리즘 ]과 명세된 암호키 길이 [ 다음 암호키 길이 ]에 따라 [ 다음 암호연산 ]을 수행해야 한다.<br>•ISO/IEC 9796-2에 명세된 전자서명 스킴 2 또는 전자서명 스킴 3 또는 FIPS PUB 186-4의 5.5절에 명세된 PKCS #1 v2.1이용한 RSASSA-PSS 및/또는 RSASSAPKCS2v1.5 전자서명 스킴에 부합하는 RSA 전자서명 알고리즘의 2048비트 전자서명 생성 및 검증 |

#### 6.1.2.8. FCS_RBG.1 난수 생성(확장)

| | |
|---|---|
| 계층관계 | 없음 |
| 종속관계 | 없음 |
| FCS_COP.1.1 | TSF는 다음의 [ 다음 난수발생기 표준 ]에 부합하는 명세된 난수발생기를 이용해서 암호키 생성에 필요한 난수를 생성해야 한다.<br>•TTAK.KO-12.0189 결정론적 난수발생기-제1부 블록 암호 기반 난수발생기<br>•TTAK.KO-12.0190 결정론적 난수발생기-제2부 해시 함수 기반 난수발생기<br>•TTAK.KO-12.0191 결정론적 난수발생기-제3부 HMAC 기반 난수발생기<br>•ISO/IEC 18031 Security techniques-Radom bit Generation |

### 6.1.3. 사용자 데이터 보호(FDP)

#### 6.1.3.1. FDP_IFC.2 완전한 정보흐름 통제

| | |
|---|---|
| 계층관계 | FDP_IFC.1 부분적인 정보흐름 통제 |
| 종속관계 | FDP_IFF.1 단일 계층 보안속성 |
| FDP_IFC.2.1 | TSF는 [ 다음의 주체 목록 및 정보 목록]과 SFP에 의하여 다루어지는 통제된 주체로/주체로부터의 정보흐름을 유발하는 모든 오퍼레이션에 대하여 [ 침입차단 SFP ]를 강제해야 한다. |

| 침입차단 방식 | 주체 | 정보 |
|---|---|---|
| 패킷 필터링 | 패킷 송신자 | 인터페이스를 통과하는 패킷 |
| | | 인터페이스가 목적지인 패킷 |
| NAT 전환 | 패킷 송신자 | Port Forward 패킷 |
| | | Outbound NAT 패킷 |
| 상태기반 트래픽 필터링 | 패킷 송신자 | 패킷 필터링에 의해 통과된 트래픽 |

| | |
|---|---|
| FDP_IFC.2.2 | TSF는 TOE 내의 모든 주체로/주체로부터 TOE내의 모든 정보흐름을 유발하는 모든 오퍼레이션들이 정보흐름통제 SFP에 의하여 다루어짐을 보장해야 한다. |

#### 6.1.3.2. FDP_IFF.1 단일 계층 보안속성

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

FDP_IFF.1.1 TSF는 적어도 [ 침입차단 SFP에서 통제되는 모든 주체 및 정보에 대한 각각의 다음 보안속성 ] 과 같은 주체 보안속성 및 정보 보안속성 유형에 기반하여 [ 침입차단 SFP ]를 강제해야 한다.

a) 주체 보안속성 : 출발지 IP주소

b) 정보 보안속성 : 출발지/목적지 IP주소, 출발지/목적지 포트(서비스), 네트워크 인터페이스, ICMPv4의 TYPE, ICMPv4의 CODE

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

a) IPv4 패킷의 IP주소가 NAT IP주소에 일치하면 Port InBound/OutBound NAT 또는 1:1 NAT 규칙에 따라 IP주소 전환 후 패킷 필터링 메커니즘으로 전달

b) IPv4 패킷의 출발지/목적지 정보가 정보흐름통제규칙(firewall rule)의 출발지/목적지 정보와 일치하고 해당 규칙의 action이 “pass”인 경우 게이트웨이로 전달

c) IPv4 패킷의 상태 정보가 상태 표에 정보와 일치하면 패킷 필터링 메커니즘을 통과하여 상태 기반 감시 메커니즘으로 전달

d) IPv4 패킷의 목적지 정보가 TOE 인터페이스 IP주소에 일치하고 action이 “pass”인 경우 해당 패킷을 TOE로 전달

FDP_IFF.1.3 TSF는 [ 침입차단 SFP의 다음과 같은 우선적용 거부규칙 ]을 강제해야 한다.

a) TSF는 유효하지 않은 플래그먼트 패킷을 차단해야 한다.

b) TSF는 완전히 재조립되지 않은 패킷을 차단해야 한다.

c) TSF는 네트워크 패킷의 출발지 주소가 브로드캐스트 네트워크인 경우 패킷을 차단해야 한다.

d) TSF는 네트워크 패킷의 출발지 주소가 멀티캐스트 네트워크/루프백주소인 경우 패킷을 차단해야 한다.

e) 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.

f) TSF는 다음 IP 옵션 패킷을 차단해야 한다. : Loose source 라우팅, Strict source라우팅, Record 라우트 지정

g) TSF는 내부/외부에서 들어오는 네트워크 패킷의 출발지 주소가 TOE 네트워크 인터페이스의 주소와 동일할 경우 패킷을 차단해야 한다.

h) TSF는 수신된 패킷의 출발지 주소가 TOE 네트워크 인터페이스 주소 대역과 관련이 없을 경우 패킷을 차단해야 한다.

i) TSF는 외부로부터 들어오는 네트워크 패킷의 출발지 주소가 내부 IP 주소인 경우 패킷을 차단해야 한다.

j) TSF는 내부에서 나가는 트래픽 중 외부 IP주소가 출발지인 트래픽의 경우 패킷을 차단해야 한다.

k) TSF는 외부로부터 들어오는 트래픽 중 SYN FLOODING 공격 트래픽의 경우 패킷을 차단해야 한다.

l) TSF는 외부로부터 들어오는 트래픽 중 UDP ECHO LOOP 공격 트래픽의 경우 패킷을 차단해야 한다.

m) TSF는 half-open된 [ 관리자가 설정한 Max number Connection TCP 접속 수 ]를 제한하고, 제한된 값에 도달하는 경우 새로운 연결시도를 차단해야 한다.

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

a) 유입된 패킷이 다음과 같은 프로토콜을 사용하며 세션테이블(상태 표)에 등록된 경우 이를 기반으로 동일 세션의 트래픽 흐름을 허용한다.

가. TCP : 출발지/목적지 주소, 출빌자/목적지 포트, 인터페이스

나. UDP : 출발지/목적지 주소, 출발지/목적지 포트, 인터페이스

다. ICMP : ICMP type

e) 출발지 IP주소가 LAN 인터페이스 주소이면 목적지를 제한하지 않고 모든 HTTP/HTTPS 연결 허용한다.

f) 출발지 IP주소가 메일서버의 주소이면 목적지를 제한하지 않고 모든 SMTP 연결을 허용한다.

g) 출발지 IP주소가 DNS서버의 주0소이면 목적지를 제한하지 않고 모든 DNS 서비스를 허용한다.

h) 패킷이 처리된 시간이 관리자가 설정한 정보흐름통제규칙(firewall rule)의 시간 대역에 포함하면 정보흐름통제규칙(firewall rule)을 적용하여 해당 규칙의 action이 “pass”이면 흐름을 허용한다.

i) 패킷의 정보에 NAT 처리가 필요한 경우 NAT 규칙을 적용하도록 NAT 데몬으로 전달한다.

FDP_IFF.1.5 TSF는 [ 다음과 같은 규칙 ]에 기반하여 정보흐름을 명시적으로 거부해야 한다.

a) 내부망에서 외부망으로 연결되는 Microsoft RPC 연결을 거부한다.

b) 내부망에서 외부망으로 연결되는 NetBIOS 연결을 거부한다.

c) 내부망에서 외부망으로 연결되는 SMB/CIFS 서비스를 차단한다.

d) 관리자가 설정한 Max state(수용할 수 있는 전체 최대 연결 개수)를 초과하는 경우 패킷을 거부하고 세션을 종료한다.

e) 관리자가 설정한 Max number hosts(동시 연결될 수 있는 호스트 최대 값)를 초과하는 경우 패킷을 거부하고 세션을 종료한다.

f) 관리자가 설정한 Max new connection(세션테이블에 할당된 메모리를 초과하지 않도록 자동 설정되는 TCP 연결 비율)을 초과하는 경우 패킷을 거부하고 세션을 종료한다.

g) 관리자가 설정한 state idle timeout(트래픽이 없어도 TCP/UDP 연결을 종료하지 않고 유지할 수 있는 최대 시간)을 초과하는 경우 세션을 종료한다.

h) 관리자가 설정한 State Timeouts(TCP/UDP 프로토콜 및 ICMP 프로토콜에서 상태 값을 갖는 연결을 기다리는 시간)을 초과한 경우 세션을 종료한다.

i) TCP 플래그 값을 기반으로 순서가 정상적이지 않은 경우 패킷을 거부하고 세션을 종료한다.

j) TCP 시퀀스 값을 기반으로 순서가 정상적이지 않은 경우 패킷을 거부하고 세션을 종료한다.

## 6.1.4. 식별 및 인증(FIA)

### 6.1.4.1. FIA_AFL.1 인증 실패 처리

| | |
|---|---|
| 계층관계 | 없음 |
| 종속관계 | FIA_UAU.1 인증 |
| FIA_AFL.1.1 | TSF는 [ WebGUI 로그인, SSH 접속을 통한 CLI 로그인, 로컬콘솔을 통한 CLI 로그인 ]에 관련된 [ 3 ]번의 실패한 인증 시도가 발생한 경우 이를 탐지해야 한다. |
| FIA_AFL.1.2 | 실패한 인증 시도가 정의된 횟수에 도달하면, TSF는 [ 5분 ~ 30분 범위에서 관리자가 설정한 인증지연 시간을 경과할 때 까지 관리접속 중단]을 수행해야 한다. |

### 6.1.4.2. FIA_SOS.1 비밀정보의 검증

| | |
|---|---|
| 계층관계 | 없음 |
| 종속관계 | 없음 |
| FIA_SOS.1.1 | TSF는 비밀정보가 [ 다음에 정의된 허용 기준 ]을 만족시킴을 검증하는 메커니즘을 제공해야 한다.<br>a) 관리자 패스워드의 경우 4조합 최소 9자리 이상 최대 20자리 이하<br>b) 사용자 계정(ID)과 동일한 패스워드 설정 금지<br>c) 동일한 문자•숫자의 연속적인 반복입력 금지<br>d) 키보드의 연속된 문자 또는 숫자의 순차적 입력 금지<br>e) 직전 사용된 패스워드 재사용 금지 |

**ST 작성자 註**

o 관리자는 SSH 관리접속을 위해 관리단말에 SSH 클라이언트 SW를 설치하고 SSH 개인키 접근을 위한 패스워드의 경우 4조합 9자리 이상으로 설정해야 한다. 다만, SSH 클라이언트 SW는 TOE 구성요소가 아니므로 운영환경에 대한 보안목적으로 대응한다.

### 6.1.4.3. FIA_UAU.1 인증

| | |
|---|---|
| 계층관계 | 없음 |
| 종속관계 | FIA_UID.1 식별 |
| FIA_UAU.1.1 | TSF는 **관리자**가 인증되기 전에 사용자를 대신하여 수행될 [ WebGUI 관리접속 시 인증서 기반 서버인증을 수반하는 HTTPS 연결, CLI 관리접속 시 공개키 기반 클라이언트 인증을 수반하는 SSH 채널 형성 ]을 허용해야 한다. |
| FIA_UAU.1.2 | TSF는 FIA_UAU.1.1에서 명시된 행동 이외의 **관리자**를 대신하여 TSF가 중재하는 다른 모든 행동을 허용하기 전에 관리자를 성공적으로 인증해야 한다. |

### 6.1.4.4. FIA_UAU.4 재사용 방지 인증 메커니즘

| | |
|---|---|
| 계층관계 | 없음 |
| 종속관계 | 없음 |
| FIA_SOS.1.1 | TSF는 [TLS Handshake Protocol, SSH Transport Protocol ]에 관련된 인증 데이터의 재사용을 방지해야 한다. |

**ST 작성자 註**

o TOE는 TLS Handshake Protocol 및 SSH Transport Protocol에서 세션연결이 중단되어 재연결 되는 경우 세션키를 갱신한다.

### 6.1.4.5. FIA_UAU.7 인증 피드백 보호

| | |
|---|---|
| 계층관계 | 없음 |
| 종속관계 | FIA_UID.1 인증 |
| FIA_UAU.7.1 | TSF는 인증이 진행되는 동안 **관리자**에게 [ 패스워드 입력 시 마스킹(****) 출력, 인증 실패 시 “인증에 실패하였습니다.” 오류메시지 출력 ]만을 제공해야 한다. |

### 6.1.4.6. FIA_UID.1 식별

| | |
|---|---|
| 계층관계 | 없음 |
| 종속관계 | 없음 |
| FIA_UID.1.1 | TSF는 사용자를 식별하기 전에 **관리자**를 대신하여 수행될 [ WebGUI 관리접속 시 인증서 기반 서버인증을 수반하는 HTTPS 연결, CLI 관리접속 시 공개키 기반 클라이언트 인증을 수반하는 SSH 채널 형성 ]을 허용해야 한다. |
| FIA_UID.1.2 | TSF는 FIA_UID.1.1에서 명시된 행동 이외의 **관리자**를 대신하여 TSF가 중재하는 다른 모든 행동을 허용하기 전에 각 **관리자**를 성공적으로 식별해야 한다. |

## 6.1.5. 보안 관리(FMT)

### 6.1.5.1. FMT_MOF.1 보안기능 관리

계층관계 없음

종속관계 FMT_SMF.1 관리기능 명세
FMT_SMR.1 보안 역할

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

| 관리 기능 | 연관 SFR |
|---|---|
| 경고메시지 메일발송 대상 사건 선택 | FAU_ARP.1 |
| 잠재적 보안위반 분석대상 사건의 누적 회수 설정<br>잠재적 보안위반 분석대상 사건의 조합규칙 설정<br>잠재적 보안위반으로 탐지할 중요 관리메뉴 선택 | FAU_SAA.1 |
| 감사 저장 실패가 예상되는 경우 대응행동 관리<br>1) 인가된 관리자에게 경고 메일을 발송할 이메일 설정<br>2) 로그 전송대상 syslog 메시지 발송/수신 서버 IP주소, 로그전송 대상 감사대상 사건 선택<br>3) 로그파일 삭제 및 재생성 | FAU_STG.3 |
| 감사 저장 실패경우를 대비한 감사 백업서버 및 syslog 전송서버 관리 | FAU_STG.4 |
| 상태 기반 감시 메커니즘 운영모드 관리<br>(Keep/Sloppy State/Synproxy/None) | FDP_IFF.1 |
| 관리자 패스워드 인증 실패인 경우 인증지연 시간 설정 | FIA_AFL.1 |
| NTP 서버 IP주소 설정 등 시간의 관리 | FPT_STM.1 |
| 동일 권한의 다중 관리자 계정 접속 차단 활성화,<br>Anti-lockout 활성화 등 관리접속 세션 설정 조건의 관리 | FTA_TSE.1 |
| TSF 데이터 전송 구간(웹페이지) 대상선정 관리 | FTP_TRP.1 |
| 로컬접속 시 포트 연결속도 제어, 주 콘솔 설정 | - |
| 물리/가상 네트워크 인터페이스, 라우터, NAT 등 네트워크 구성관리 | - |
| 기본계정 초기화, 웹서버 데몬 중지/재시작 등 TOE 운영 관리 | (CLI Only) |
| 백업 및 복원, 공장 초기화, 시동종료, 전원끄기 등 TOE 진단 관리 | - |
| WebGUI 관리접속 차단 해지 기능(Anti-lockout) 관리 | (WebGUI Only) |

[표 4] 보안관리 기능 목록

**ST 작성자 註**

○ 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.

### 6.1.5.2. FMT_MSA.1 보안속성 관리

계층관계 없음

종속관계 [FDTSFP_ACC.1 부분적인 접근통제 또는
FDP_IFC.1 부분적인 정보흐름통제]
FMT_SMF.1 관리기능 명세
FMT_SMR.1 보안 역할

FMT_MOF.1.1 TSF는 [ 다음 표 ]의 보안속성을 *변경, 삭제, [추가, 정보흐름통제규칙의 Action 선택, 적용순서 변경 및 활성화/비활성화]*하는 능력을 [ **WebCfg-All Pages 보안역할이 부여된 인가된 관리자** ]로 제한하도록 [ 침입차단 SFP]를 강제해야 한다.

| 보안속성 구분 | 보안속성 |
|---|---|
| 트래픽 필터링 규칙 | 프로토콜, ICMP type, 출발지 IP주소, 출발지 포트, 목적지 IP주소, 목적지 포트, 큐, 스케쥴 |
| 상태 기반 감시 규칙 | Max state, Max number hosts, Max number connections, Max new connection state idle timeout, TCP Flag, State Type, State Timeouts, Firewall Maximum States, Firewall Adaptive Timeouts, Gateway |
| NAT 규칙 | 출발지 IP주소 및 포트, 목적지 IP주소 및 포트, 변환될 IP주소 및 포트, 연관 정보통제흐름규칙, 프로토콜, 인터페이스 |

[표 4] 보안속성 목록

**ST 작성자 註**

○ 정보흐름통제규칙(firewall rule)은 IP주소 및 포트 기반으로 트래픽을 필터링하기 위한 트래픽 필터링 규칙, TCP/UDP 상태정보 기반으로 트래픽 흐름을 제어하기 위한 상태 기반 감시 규칙, 내부 사설 IP주소를 보호하기 위한 NAT 정책 적용 시 변환규칙을 정의한 NAT 규칙 등으로 구성된다.

### 6.1.5.3. 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 제한적인 디폴트값을 제공하도록 [ 침입차단 SFP]를 강제해야 한다.

FMT_MSA.3.2 TSF는 객체나 정보 생성 시 디폴트값을 대체하기 위하여 [ **WebCfg-All Pages 보안역할이 부여된 인가된 관리자** ]가 선택적인 초기값을 명세하도록 허용해야 한다.

### 6.1.5.4. FMT_MTD.1(1) TSF 데이터 관리(일반 TSF 데이터)

계층관계 없음

종속관계 FMT_SMF.1 관리기능 명세
FMT_SMR.1 보안 역할

FMT_MTD.1.1 TSF는 [ 다음 표에 명시된 TSF 데이터 ]을 ***관리***하는 능력을 [ **WebCfg-All Pages 보안역할이 부여된 인가된 관리자** ]로 제한해야 한다.

| 관리 대상 TSF 데이터 | 연관 SFR |
|---|---|
| WebGUI 웹서버 인증서 및 연관 개인키<br>SSH 클라이언트 인증 데이터(SSH 공개키쌍) | FIA_UAU.1 |
| 관리자 계정 및 연관 정보, 관리자 그룹 구성원 정보 | FIA_UID.1 |
| TOE 식별정보, 버전정보, 최근 부팅시간 등 시스템 기본 정보 | FPT_TUD.1 |
| 자체시험 대상별 시험 주기<br>게이트웨이, 인터페이스, 서비스 데몬 등 동작 상태정보 | FPT_TST.1 |
| 관리접속 세션에 대해서 세션 잠금이 발생하는 비활동 기간(기본값 : 10분, 10분 이내에서 설정) | FTA_SSL.1 |
| 관리접속이 허용되는 관리단말 IP주소 | FTA_TSE.1 |

[표 4] 관리대상 TSF 데이터 목록 및 연관 SFR

**ST 작성자 註**

○ 정교화 오퍼레이션을 적용한 “관리”의 의미는 디폴트값 변경(change_default), 질의(query), 변경(modify), 삭제(delete), 소거(clear), 기타 연산(other operation) 등을 포함한다.

### 6.1.5.5. FMT_MTD.1(2) TSF 데이터 관리(암호관련 정보)

계층관계 없음

종속관계 FMT_SMF.1 관리기능 명세
FMT_SMR.1 보안 역할

FMT_MTD.1.1 TSF는 [ 암호키 값, 암호키 관련 핵심보안 매개변수 ]을 ***변경***하는 능력을 [ **WebCfg-All Pages 보안역할이 부여된 인가된 관리자** ]로 제한해야 한다.

### 6.1.5.6. 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 [관리자 인증메커니즘]의 패스워드를 다음과 같이 관리하는 능력을 [ 인가된 관리자 ]로 제한해야 한다.
1. [ 없음 ]
2. [ 없음 ]

FMT_PWD.1.2 TSF는 [ 관리자 ]의 ID를 다음과 같이 관리하는 능력을 [ 인가된 관리자 ]로 제한해야 한다.
1. [ 없음 ]
2. [ 없음 ]

FMT_PWD.1.3 TSF는 *인가된 관리자가 최초 접속 시 ID 및 패스워드를 변경*하는 기능을 제공해야 한다.

**ST 작성자 註**

○ TOE에서 ID 및 패스워드 조합규칙 및 길이 등을 관리하는 기능을 제공하지 않고 패스워드 설정/변경 시 4조합, 9자리 이상 여부를 검증하도록 조합규칙 및 길이가 내장되어 있으므로, FMT_PWD.1.1, FMT_PWD.1.2 할당 오퍼레이션에 '없음'으로 명세하였다.

### 6.1.5.7. FMT_SMF.1 관리기능 명세

계층관계 없음

종속관계 없음

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

| 구분 | WebGUI | 콘솔(CLI) |
|---|---|---|
| System | Logout(GUI Log out) | 0) Logout (SSH Log out) |
| | Advanced(WebGUI/SSH/ Console Advaced option) | 14) Disable sshd |
| | User Manager | N/A |
| | User Setting | N/A |
| | Cert Manager | N/A |
| | Routing | N/A |
| Interface | WAN/LAN/OPTx Config | 1) Assign Interface |
| | | 2) Set interfaces(s) IP address |

| 구분 | WebGUI | 콘솔(CLI) |
|---|---|---|
| firewall | Aliases | N/A |
| | NAT | N/A |
| | Rules | N/A |
| | Schedules | N/A |
| Service | NTP | N/A |
| Diagnostics | Backup & Restore | 15) Restore recent configuration |
| | Command Prompt | 8) Shell<br>12) Developer Shell |
| | Factory defaults | 4) Reset to factory defaults |
| | Halt system | 6) Halt system |
| | Ping test | 7) Ping host |
| | Reboot system | 5) Reboot system |
| | States(activated firewall state) | N/A |
| | States Summary | N/A |
| | System Activity(memoty, process status) | N/A |
| | login threshold reach client Tables | N/A |
| Restart | N/A | 2) WebGUI account locked-out |
| | | 3) Reset webConfigurator password |
| | | 11) Restart webConfigurator |
| | | 16) Restart PHP-FPM |

### 6.1.5.8. FMT_SMR.1 보안 역할

계층관계 없음

종속관계 FIA_UID.1 식별

FMT_SMR.1.1 TSF는 [ 다음의 인가된 ] 역할을 유지해야 한다.

| 관리수단 | 역할 |
|---|---|
| WebGUI | WebCfg-All Pages |
| | WebCfg-Dashboard(all) |
| | WebCfg-System |
| CLI | User-System-Shell account access |
| | User-System-Copy files |
| | User-System-all |
| 환경설정 파일 | User-Config-Deny Config Write |

FMT_SMR.1.2 TSF는 **관리자**와 **FMT_SMR.1.1에 정의**된 역할을 연관 지을 수 있어야 한다.

## 6.1.6. TSF 보호(FPT)

### 6.1.6.1. FPT_PST.1 저장된 TSF 데이터 기본적인 보호(확장)

| | |
|---|---|
| 계층관계 | 없음 |
| 종속관계 | 없음 |
| FPT_PST.1.1 | TSF는 TSF에 의해 통제되는 저장소에 저장되는 [ 관리자 패스워드, 암호키, TOE 설정값, 감사 데이터 ]를 비인가된 노출로부터 보호해야 한다. |

### 6.1.6.2. FPT_STM.1 신뢰할 수 있는 타임스탬프

| | |
|---|---|
| 계층관계 | 없음 |
| 종속관계 | 없음 |
| FPT_STM.1.1 | TSF는 신뢰할 수 있는 타임스탬프를 제공할 수 있어야 한다. |

### 6.1.6.3. FPT_TST.1 TSF 자체 시험

| | |
|---|---|
| 계층관계 | 없음 |
| 종속관계 | 없음 |
| FPT_TST.1.1 | TSF는 [*난수 생성 기능, 암호연산 기능, CPU 및 메모리*]의 정확한 운영을 입증하기 위하여 *시동 시, 정규 운영 동안 주기적으로* 자체 시험을 실행해야 한다. |
| FPT_TST.1.2 | TSF는 인가된 사용자에게 [*환경설정 파일, 환경설정 해시값 파일, 암호키 파일*]의 무결성을 검증하는 기능을 제공해야 한다. |
| FPT_TST.1.3 | TSF는 인가된 사용자에게 [*원본 이미지, 부트로더 이미지*]의 무결성을 검증하는 기능을 제공해야 한다. |

## 6.1.7. TOE 접근(FTA)

### 6.1.7.1. 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 **관리자**에 대해 관리접속 세션과 로컬접속 세션의 동시 세션 연결금지 ] 규칙에 따라서 동일 **관리자**에 속하는 동시 세션의 최대 수를 제한해야 한다. |
| FTA_MCS.2.2 | TSF는 기본적으로 **관리자**별로 [ 1 ] 개의 세션 한계치를 강제해야 한다. |

#### 6.1.7.2. FTA_SSL.1 TSF에 의한 세션 잠금

| | |
|---|---|
| 계층관계 | 없음 |
| 종속관계 | FIA_UID.1 식별 |
| FTA_SSL.1.1 | TSF는 다음 방법에 의해 [**관리자** 로그아웃, 최대 10분 이내에서 관리자가 설정한 idle time] 후 상호작용 세션을 잠가야 한다.<br>a) 현재 내용을 읽을 수 없도록 화면표시 장치를 소거하거나 덮어쓰기 하기<br>b) 세션을 잠금해제하기 보다는 사용자의 데이터 접근/화면표시 장치의 모든 활동을 무력화하기 |
| FTA_SSL.1.2 | TSF는 세션을 잠금해제하기 전에 [ *관리자에 의한 세션 잠금 해제, 세션 잠금을 해제하기 전에 사용자 재인증* ]을 요구해야 한다. |

#### 6.1.7.3. FTA_SSL.3 TSF에 의한 세션 종료

| | |
|---|---|
| 계층관계 | 없음 |
| 종속관계 | 없음 |
| FTA_SSL.3.1 | TSF는 [**관리자** 로그아웃, 최대 10분 이내에서 관리자가 설정한 idle time] 후에 상호작용하는 세션을 종료해야 한다. |

#### 6.1.7.4. FTA_TSE.1 TOE 세션 설정

| | |
|---|---|
| 계층관계 | 없음 |
| 종속관계 | 없음 |
| FTA_SSL.3.1 | TSF는 [ 접속 IP, 동일 권한을 갖는 관리자 계정의 관리접속 세션 활성화 여부, SSH Authorized key에 따라 실행이 허용된 명령어, Anti-lockout 활성화 여부 ]에 기반하여 **관리자의 관리접속 세션** 설정을 거부할 수 있어야한다. |

### 6.1.8. 안전한 경로/채널(FTP)

#### 6.1.8.1. 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, [없음]*로부터 통신 데이터를 보호하는 통신 경로를 제공해야 한다. |
| FTP_TRP.1.2 | TSF는 ***관리접속 관리자***가 안전한 경로를 통하여 통신을 초기화하는 것을 허용해야 한다. |
| FTP_TRP.1.3 | TSF는 ***관리접속 관리자 인증***, *[TSF 데이터 전송]*에 대하여 안전한 경로의 사용을 요구해야 한다. |

## 6.2. 보증요구사항

본 보안목표명세서의 보증요구사항은 공통평가기준 3부의 보증 컴포넌트로 구성되었고, 평가보증등급은 국내용 EAL4이다. 다음 표는 CC Part 3에서 정의한 EAL4 보증 컴포넌트와 국내용 평가보증등급 EAL4를 요약하여 보여준다.

| 보증클래스 | CC Part3 보증 컴포넌트 | | 국내용 평가보증등급 |
|---|---|---|---|
| 보안목표 명세서 | ASE_INT.1 | 보안목표명세서 소개 | 좌동 |
| | ASE_CCL.1 | 준수 선언 | 좌동 |
| | ASE_SPD.1 | 보안문제 정의 | 좌동 |
| | ASE_OBJ.2 | 운영환경에 대한 보안목적 | 좌동 |
| | ASE_ECD.1 | 확장 컴포넌트 정의 | 좌동 |
| | ASE_REQ.2 | 도출된 보안요구사항 | 좌동 |
| | ASE_TSS.1 | TOE 요약명세 | 좌동 |
| 개발 | ADV_ARC.1 | 보안 아키텍처 설명 | 개발자 취약성 분석서로 대체 |
| | ADV_FSP.4 | 완전한 기능명세 | 생략 |
| | ADV_IMP.1 | TSF에 대한 구현의 표현 | 소스코드 취약점 분석서로 대체 |
| | ADV_TDS.3 | 기본적인 모듈화 설계 | 업체 자체 개발문서로 대체 |
| 설명서 | AGD_OPE.1 | 사용자 운영 설명서 | 좌동 |
| | AGD_PRE.1 | 준비 절차 | 좌동 |
| 생명주기지원 | ALC_CMC.4 | 생산지원, 수용절차 및 자동화 | 내규/지침으로 대체 가능 |
| | ALC_CMS.4 | 문제추적 형상관리 범위 | |
| | ALC_DEL.1 | 배포 절차 | |
| | ALC_DVS.1 | 보안대책의 식별 | |
| | ALC_LCD.1 | 개발자가 정의한 생명주기 모델 | |
| | ALC_TAT.1 | 잘 정의된 개발 도구 | |
| 시험 | ATE_COV.2 | 시험범위의 분석 | 개발자 전체 기능시험서로 대체 |
| | ATE_DPT.1 | 기본설계 시험 | |
| | ATE_FUN.1 | 기능 시험 | 좌동 |
| | ATE_IND.2 | 독립적인 시험 : 표본 시험 | 평가자 전체 기능시험 수행 |
| 취약성 평가 | AVA_VAN.3 | 집중화된 취약성 분석 | 좌동 |

[표 6] EAL4 보증패키지와 국내용 EAL4 평가보증등급

본 ST는 국내용 EAL4 평가보증등급 준수를 선언하였으며 이에 따른 보증요구사항은 다음과 같다.

## 6.2.1. 보안목표명세서 평가

### 6.2.1.1. 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. |

### 6.2.1.2. ASE_CCL.1 준수선언

| | |
|---|---|
| 종속관계 | ASE_INT.1 보안목표명세서 소개<br>ASE_ECD.1 확장 컴포넌트 정의<br>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 보안목표명세서가 준수하는 모든 보호프로파일 및 보안요구사항 패키지를 식별해야 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. |

### 6.2.1.3. ASE_SPD.1 보안문제정의

종속관계 없음

**개발자 요구사항**

| | |
|---|---|
| ASE_SPD.1.1D | 개발자는 보안문제정의를 제공해야 한다. |

**증거 요구사항**

| | |
|---|---|
| ASE_SPD.1.1C | 보안문제정의는 위협을 서술해야 한다. |
| ASE_SPD.1.2C | 모든 위협은 위협원, 자산, 악의적 행동의 관점에서 서술되어야 한다. |

ASE_SPD.1.3C 보안문제정의는 조직의 보안정책(OSP)을 서술해야 한다.

ASE_SPD.1.4C 보안문제정의는 TOE 운영환경에 관한 가정사항을 서술해야 한다.

**평가자 요구사항**

ASE_SPD.1.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

### 6.2.1.4. ASE_OBJ.2 보안목적

종속관계 ASE_SPD.1 보안문제정의

**개발자 요구사항**

ASE_OBJ.1.1D 개발자는 보안목적에 대한 설명을 제공해야 한다.

**증거 요구사항**

ASE_OBJ.2.1C 보안목적에 대한 설명은 TOE 보안목적과 운영환경에 대한 보안목적을 서술해야 한다.

ASE_OBJ.2.2C 보안목적의 이론적 근거는 TOE에 대한 각 보안목적을 보안목적에 의해 대응되는 위협과 보안목적에 의해 수행되는 조직의 보안으로 추적해야 한다.

ASE_OBJ.2.3C 보안목적의 이론적 근거는 운영환경에 대한 각 보안목적을 보안목적에 의해 대응되는 위협, 보안목적에 의해 수행되는 조직의 보안정책, 보안목적에 의해 지원되는 가정사항으로 추적해야 한다.

ASE_OBJ.2.4C 보안목적의 이론적 근거는 보안목적이 모든 위협에 대응함을 입증해야 한다.

ASE_OBJ.2.5C 보안목적의 이론적 근거는 보안목적이 모든 조직의 보안정책을 수행함을 입증해야 한다.

ASE_OBJ.2.6C 보안목적의 이론적 근거는 운영환경에 대한 보안목적이 모든 가정사항을 지원함을 입증해야 한다.

**평가자 요구사항**

ASE_OBJ.2.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

### 6.2.1.5. 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.

### 6.2.1.6. ASE_REQ.2 도출된 보안요구사항

종속관계 ASE_OBJ.2 보안목적
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.2.1C 보안요구사항에 대한 설명은 보안기능요구사항과 보증요구사항을 서술해야 한다.

ASE_REQ.2.2C 보안기능요구사항 및 보증요구사항에서 사용되는 모든 주체, 객체, 오퍼레이션, 보안 속성, 외부 실체, 기타 용어들은 정의되어야 한다.

ASE_REQ.2.3C 보안요구사항에 대한 설명은 보안요구사항에 대한 모든 오퍼레이션을 식별해야 한다.

ASE_REQ.2.4C 모든 오퍼레이션은 정확히 수행되어야 한다.

ASE_REQ.2.5C 보안요구사항의 각 종속관계는 만족되어야 하며, 그렇지 않을 경우에는 보안요구사항의 이론적 근거에 그에 대한 정당화가 제공되어야 한다.

ASE_REQ.2.6C 보안요구사항의 이론적 근거는 각 보안기능요구사항을 TOE에 대한 보안목적으로 추적해야 한다.

ASE_REQ.2.7C 보안요구사항의 이론적 근거는 보안기능요구사항이 TOE에 대한 모든 보안목적을 만족한다는 것을 입증해야 한다.

보안요구사항의 이론적 근거는 보증요구사항이 선택된 이유를 설명해야 한다.

ASE_REQ.2.8C 보안요구사항에 대한 설명은 내부적으로 일관성이 있어야 한다.

**평가자 요구사항**

ASE_REQ.2.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

### 6.2.1.7. 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.

## 6.2.2. 개발

### 6.2.2.1. ADV_ARC.1 기본적인 기능명세

| | |
|---|---|
| 종속관계 | ADV_FSP.1 기본적인 기능명세<br>ADV_TDS.1 기본적인 설계 |

**개발자 요구사항**

| | |
|---|---|
| ADV_ARC.1.1D | 개발자는 TSF의 보안특성이 우회되지 않도록 TOE를 설계하고 구현해야 한다. |
| ADV_ARC.1.2D | 개발자는 신뢰되지 않은 능동적 실체에 의한 침해로부터 TSF 자체를 보호할 수 있도록 TSF를 설계하고 구현해야 한다. |
| ADV_ARC.1.3D | 개발자는 TSF의 보안 아키텍쳐 설명을 제공해야 한다. |

**증거 요구사항**

| | |
|---|---|
| ADV_ARC.1.1C | 보안 아키텍쳐 설명은 TOE 설계문서에 서술된 SFR-수행 추상화 설명에 알맞은 상세 수준으로 서술되어야 한다. |
| ADV_ARC.1.2C | 보안 아키텍쳐 설명은 TSF에 의해서 SFR과 일관성 있게 유지되어야 하는 보안영영을 서술해야 한다. |
| ADV_ARC.1.3C | 보안 아키텍쳐 설명은 TSF 초기화 과정이 어떻게 안전한지 서술해야 한다. |
| ADV_ARC.1.4C | 보안 아키텍쳐 설명은 TSF가 침해로부터 자신을 보호함을 입증해야 한다. |
| ADV_ARC.1.5C | 보안 아키텍쳐 설명은 TSF가 SFR-수행 기능성의 우회를 방지함을 입증해야 한다. |

**평가자 요구사항**

| | |
|---|---|
| ADV_ARC.1.1E | 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다. |

### 6.2.2.2. ADV_FSP.4 완전한 기능명세

| | |
|---|---|
| 종속관계 | 없음 |

**개발자 요구사항**

| | |
|---|---|
| ADV_FSP.4.1D | 개발자는 기능명세를 제공해야 한다. |
| ADV_FSP.4.2D | 개발자는 기능명세에서 SFR로의 추적성을 제공해야 한다. |

**증거 요구사항**

| | |
|---|---|
| ADV_FSP.4.1C | 기능명세는 TSF를 완전하게 표현해야 한다. |
| ADV_FSP.4.2C | 기능명세는 모든 TSFI에 대한 목적과 사용 방법을 서술해야 한다. |

ADV_FSP.4.3C 기능명세는 각 TSFI와 관련된 모든 매개변수를 식별 및 서술해야 한다.

ADV_FSP.4.4C 기능명세는 각 TSFI에 관련된 모든 행동을 서술해야 한다.

ADV_FSP.4.5C 기능명세는 각 TSFI 호출 결과로 발생하는 모든 직접적인 오류메시지를 서술해야 한다.

ADV_FSP.4.6C 추적성은 SFR이 기능명세 내의 TSFI로 추적됨을 입증해야 한다.

**평가자 요구사항**

ADV_FSP.4.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

ADV_FSP.4.2E 평가자는 기능명세가 SFR을 정확하고 완전하게 실체화하는지 결정해야 한다.

### 6.2.2.3. ADV_IMP.1 TSF에 대한 구현의 표현

종속관계 ADV_TDS.3 기본적인 모듈화 설계
ALC_TAT.1 잘 정의된 개발 도구

**개발자 요구사항**

ADV_IMP.1.1D 개발자는 전체 TSF에 대한 구현의 표현을 가용하게 해야 한다.

ADV_IMP.1.2D 개발자는 TOE 설계 설명과 구현의 표현 표본간의 대응관계를 제공해야 한다.

**증거 요구사항**

ADV_IMP.1.1C 구현의 표현은 더 이상의 설계과정 없이 TSF가 생성될 수 있는 상세수준으로 TSF를 정의해야 한다.

ADV_IMP.1.2C 구현의 표현은 개발 인력이 사용한 형태이어야 한다.

ADV_IMP.1.3C TOE 설계 설명과 구현의 표현 표본간의 대응관계는 이들의 일치성을 입증해야 한다.

**평가자 요구사항**

ADV_IMP.1.1E 평가자는 선택된 구현의 표현 표본에 대해 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

### 6.2.2.4. ADV_TDS.3 기본적인 모듈화 설계

종속관계 ADV_FSP.4 완전한 기능명세

**개발자 요구사항**

ADV_TDS.3.1D 개발자는 TOE 설계를 제공해야 한다.

ADV_TDS.3.2D 개발자는 기능명세의 TSFI와 TOE 설계에 사용 가능한 가장 상세수준 분해간의 대응관계를 제공해야 한다.

**증거 요구사항**

| | |
|---|---|
| ADV_TDS.3.1C | 설계는 TOE의 구조를 서브시스템 측명에서 서술해야 한다. |
| ADV_TDS.3.2C | 설계는 TSF를 모듈 측면에서 서술해야 한다. |
| ADV_TDS.3.3C | 설계는 TSF의 모든 서브시스템을 식별해야 한다. |
| ADV_TDS.3.4C | 설계는 TSF의 각 서브시스템에 대한 설명을 제공해야 한다. |
| ADV_TDS.3.5C | 설계는 TSF의 모든 서브시스템들 간의 상호작용에 대한 설명을 제공해야 한다. |
| ADV_TDS.3.6C | 설계는 TSF 서브시스템과 TSF 모듈간의 대응관계를 제공해야 한다. |
| ADV_TDS.3.7C | 설계는 각 SFR-수행 모듈을 그 목적 및 다른 모듈 간의 상관관계 측명에서 서술해야 한다. |
| ADV_TDS.3.8C | 설계는 각 SFR-수행 모듈을 SFR-관련 인터페이스, 인터페이스로부터의 반환 값, 다른 모듈과의 상호작용 및 다른 SFR-수행 모듈에서 호출된 SFR-관련 인터페이스 측면에서 서술해야 한다. |
| ADV_TDS.3.9C | 설계는 각 SFR-지원 또는 SFR-비-간섭 모듈을 목적 및 다른 모듈과의 상호작용 측면에서 서술해야 한다. |
| ADV_TDS.3.10C | 대응관계는 모든 TSFI가 자신이 호출하는 TOE 설계 내에 서술된 행동으로 추적됨을 입증해야 한다. |

**평가자 요구사항**

| | |
|---|---|
| ADV_TDS.31E | 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다. |
| ADV_TDS.32E | 평가자는 설계가 모든 보안기능요구사항을 정확하고 완전하게 실체화하는지 결정해야 한다. |

## 6.2.3. 설명서

### 6.2.3.1. 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 관련사항들을 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.

### 6.2.3.2. 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.

## 6.2.4. 생명주기 지원

### 6.2.4.1. ALC_CMC.4 생산지원, 수용절차 및 자동화

종속관계 ALC_CMS.1 TOE 형상관리 범위
ALC_DVS.1 보안대책의 식별
ALC_LCD.1 개발자가 정의한 생명주기 모델

**개발자 요구사항**

ALC_CMC.4.1D 개발자는 TOE 및 그에 대한 참조를 제공해야 한다.

ALC_CMC.4.2D 개발자는 형상관리 문서를 제공해야 한다.

ALC_CMC.4.3D 개발자는 형상관리 시스템을 사용해야 한다.

**증거 요구사항**

ALC_CMC.4.1C TOE는 유일한 참조를 위한 레이블을 붙여야 한다.

ALC_CMC.4.2C 형상관리 문서는 형상항목을 유일하게 식별하는 데 사용된 방법을 서술해야 한다.

ALC_CMC.4.3C 형상관리 시스템은 모든 형상항목을 유일하게 식별해야 한다.

ALC_CMC.4.4C 형상관리 시스템은 형상항목에 인가된 변경만을 허용하는 자동화된 수단을 제공해야 한다.

ALC_CMC.4.5C 형상관리 시스템은 자동화된 수단을 이용하여 TOE의 생산을 지원해야 한다.

ALC_CMC.4.6C 형상관리 문서는 형상관리 계획을 포함해야 한다.

ALC_CMC.4.7C 형상관리 계획은 형상관리 시스템이 TOE 개발에 사용되는 방법을 서술해야 한다.

ALC_CMC.4.8C 형상관리 계획은 변경되거나 새로 생성된 형상항목을 TOE의 일부로 수용하는데 사용된 절차를 서술해야 한다.

ALC_CMC.4.9C 증거는 모든 형상항목이 형상관리 시스템 하에 유지되고 있음을 입증해야 한다.

ALC_CMC.4.10C 증거는 형상관리 시스템이 형상관리 계획에 따라 운영되고 있음을 입증해야 한다.

**평가자 요구사항**

ALC_CMC.4.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

### 6.2.4.2. ALC_CMS.4 문제추적 형상관리 범위

종속관계 없음

**개발자 요구사항**

ALC_CMS.4.1D 개발자는 TOE에 대한 형상목록을 제공해야 한다.

**증거 요구사항**

ALC_CMS.4.1C 형상목록은 TOE, 보증요구사항에서 요구하는 평가증거, TOE를 구성하는 부분, 구현 표현, 보안 결함 보고서 및 해결 상태를 포함해야 한다.

ALC_CMS.4.2C 형상목록은 형상항목을 유일하게 식별해야 한다.

ALC_CMS.4.3C 형상목록은 각 TSF 관련 형상항목의 개발자를 표시해야 한다.

**평가자 요구사항**

ALC_CMS.4.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

### 6.2.4.3. ALC_DEL.1 배포 절차

종속관계 없음

**개발자 요구사항**

ALC_DEL.1.1D 개발자는 소비자에게 TOE나 TOE 일부를 배포하는 절차를 문서화하여 제공해야 한다.

ALC_DEL.1.2D 개발자는 배포 절차를 사용해야 한다.

**증거 요구사항**

ALC_DEL.1.1C 배포 문서는 TOE를 소비자에게 배포할 때 보안을 유지하기 위해 필요한 모든 절차를 서술해야 한다.

**평가자 요구사항**

ALC_DEL.1.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

### 6.2.4.4. ALC_DVS.1 보안대책의 식별

종속관계 없음

**개발자 요구사항**

ALC_DVS.1.1D 개발자는 개발보안 문서를 작성하여 제공해야 한다.

**증거 요구사항**

ALC_DVS.1.1C 개발보안 문서는 개발환경 내에서 TOE 설계 및 구현 과정의 비밀성과 무결성을 보호하기 위하여 필요한 물리적, 절차적, 기술적 및 기타 보안대책을 서술해야 한다.

**평가자 요구사항**

ALC_DVS.1.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

ALC_DVS.1.2E 평가자는 보안대책이 적용되고 있는지 확인해야 한다.

### 6.2.4.5. ALC_LCD.1 개발자가 정의한 생명주기 모델

종속관계 없음

**개발자 요구사항**

ALC_LCD.1.1D 개발자는 TOE의 개발과 유지에 사용되는 생명주기 모델을 수립해야 한다.

ALC_LCD.1.2D 개발자는 생명주기 정의 문서를 제공해야 한다.

**증거 요구사항**

ALC_LCD.1.1C 생명주기 정의 문서는 TOE의 개발과 유지에 사용되는 모델을 서술해야 한다.

ALC_LCD.1.2C 생명주기 모델은 TOE의 개발과 유지에 필요한 통제를 제공해야 한다.

**평가자 요구사항**

ALC_LCD.1.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

### 6.2.4.6. ALC_TAT.1 잘 정의된 개발 도구

종속관계 ADV_IMP.1 TSF에 대한 구현의 표현

**개발자 요구사항**

ALC_TAT.1.1D 개발자는 TOE에 사용된 각 개발 도구를 식별한 문서를 제공해야 한다.

ALC_TAT.1.2D 개발자는 각 개발 도구에 대해 구현-종속적인 선택사항을 문서화하여 제공해야 한다.

**증거 요구사항**

ALC_TAT.1.1C 구현에 사용된 각 개발 도구는 잘 정의된 것이어야 한다.

ALC_TAT.1.2C 각 개발 도구 문서는 구현에 사용된 모든 규정과 지시어 뿐만 아니라 모든 명령문의 의미를 모호하지 않게 정의해야 한다.

ALC_TAT.1.3C 각 개발 도구 문서는 모든 구현-종속적인 선택사항의 의미를 모호하지 않게 정의해야 한다.

**평가자 요구사항**

ALC_TAT.1.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

## 6.2.5. 시험

### 6.2.5.1. ATE_COV.2 시험범위의 분석

종속관계 ADV_FSP.2 보안-수행 기능명세
ATE_FUN.1 기능 시험

**개발자 요구사항**

ATE_COV.2.1D 개발자는 시험범위의 분석을 제공해야 한다.

**증거 요구사항**

ATE_COV.2.1C 시험범위의 분석은 시험 문서 내의 시험항목과 기능명세 내의 TSFI간의 일치성을 입증해야 한다.

ATE_COV.2.2C 시험범위의 분석은 기능명세 내의 모든 TSFI가 시험되었음을 입증해야 한다.

**평가자 요구사항**

ATE_COV.2.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

### 6.2.5.2. ATE_DPT.1 기본설계 시험

종속관계 ADV_ARC.1 보안 아키텍쳐 설명
ADV_TDS.2 아키텍쳐 설계
ATE_FUN.1 기능 시험

**개발자 요구사항**

ATE_DPT.1.1D 개발자는 시험의 상세수준 분석을 제공해야 한다.

**증거 요구사항**

ATE_DPT.1.1C 시험의 상세수준 분석은 시험 문서 내의 시험항목과 TOE 설계 내의 TSF 서브시스템 간의 일치성을 입증해야 한다.

ATE_DPT.1.2C 시험의 상세수준 분석은 TOE 설계 내의 모든 TSF 서브시스템이 시험되었음을 입증해야 한다.

**평가자 요구사항**

ATE_DPT.1.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

### 6.2.5.3. 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.

### 6.2.5.4. ATE_IND.2 독립적인 시험 : 표본 시험

종속관계 ADV_FSP.2 보안-수행 기능명세 기능명세
AGD_OPE.1 사용자 운영 설명서
AGD_PRE.1 준비 절차
ATE_COV.1 시험범위의 증거
ATE_FUN.1 기능 시험

**개발자 요구사항**

ATE_IND.2.1D 개발자는 시험할 TOE를 제공해야 한다.

**증거 요구사항**

ATE_IND.2.1C TOE는 시험하기에 적합해야 한다.

ATE_IND.2.2C 개발자는 개발자의 TSF 기능 시험에 사용된 자원과 동등한 자원을 제공해야 한다.

**평가자 요구사항**

ATE_IND.2.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

| | |
|---|---|
| ATE_IND.2.2E | 평가자는 개발자 시험 결과를 검증하기 위하여 시험문서 내의 시험항목에 대한 표본 시험을 수행해야 한다. |
| ATE_IND.2.3E | 평가자는 TSF가 명세된대로 동작함을 확인하기 위하여 TSF의 일부를 시험해야 한다. |

## 6.2.6. 취약성 평가

### 6.2.6.1. AVA_VAN.3 집중화된 취약성 분석

종속관계

ADV_ARC.1 보안 아키텍쳐 설명
ADV_FSP.4 완전한 기능명세
ADV_TDS.3 기본적인 모듈화 설계
ADV_IMP.1 TSF에 대한 구현의 표현
AGD_OPE.1 사용자 운영 설명서
AGD_PRE.1 준비 절차
ATE_DPT.1 기본설계 시험

**개발자 요구사항**

| | |
|---|---|
| AVA_VAN.3.1D | 개발자는 시험할 TOE를 제공해야 한다. |

**증거 요구사항**

| | |
|---|---|
| AVA_VAN.3.1C | TOE는 시험하기에 적합해야 한다. |

**평가자 요구사항**

| | |
|---|---|
| AVA_VAN.3.1E | 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다. |
| AVA_VAN.3.2E | 평가자는 TOE의 잠재적 취약성을 식별하기 위해 공개 영역에 대한 조사를 수행해야 한다. |
| AVA_VAN.3.3E | 평가자는 TOE의 잠재적 취약성을 식별하기 위해 설명서, 기능명세, TOE 설계 및 보안 아키텍쳐 설명, 구현의 표현을 이용하여 집중화된 독립적인 취약성 분석을 수행해야 한다. |
| AVA_VAN.3.4E | 평가자는 TOE가 강화된-기본 공격 성공 가능성을 가진 공격자에 의해 행해지는 공격에 내성이 있음을 결정하기 위해, 식별된 잠재적 취약성에 근거하여 침투시험을 수행해야 한다. |

# 6.3. 보안요구사항의 이론적 근거

## 6.3.1. 보안기능요구사항의 이론적 근거

보안기능요구사항의 이론적 근거는 다음을 입증한다.

▷ 각 TOE 보안목적은 적어도 하나의 TOE 보안기능요구사항에 의해 다루어진다.

▷ 각 보안기능요구사항은 적어도 하나의 TOE 보안목적을 다룬다.

| 보안기능 요구사항 | O. 정보 흐름 통제 | O. 비정상 패킷 차단 | O. 서비스 거부공격 차단 | O. 식별 및 인증 | O. 패스워드 관리 | O. 세션 통제 | O. 보안 관리 | O. 감사 | O. 자체 보호 | O. 안전한 암호 | O. 저장 데이터 보호 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| FAU_ARP.1 | | | | | | | | X | | | |
| FAU_GEN.1 | | | | | | | | X | | | |
| FAU_SAA.1 | | | | | | | | X | | | |
| FAU_SAR.1 | | | | | | | | X | | | |
| FAU_SAR.3 | | | | | | | | X | | | |
| FAU_STG.1 | | | | | | | | X | | | |
| FAU_STG.3 | | | | | | | | X | | | |
| FAU_STG.4 | | | | | | | | X | | | |
| FCS_CKM.1 | | | | | | X | | | | X | |
| FCS_CKM.2 | | | | | | X | | | | X | |
| FCS_CKM.4 | | | | | | X | | | | X | |
| FCS_COP.1(1) | | | | | | X | | | | X | |
| FCS_COP.1(2) | | | | | | X | | | | X | |
| FCS_COP.1(3) | | | | | | X | | | | X | |
| FCS_COP.1(4) | | | | | | X | | | | X | |
| FCS_RBG.1 | | | | | | | | | | X | |
| FDP_IFC.2 | X | X | X | | | | | | | | |
| FDP_IFF.1 | X | X | X | | | | | | | | |
| FIA_AFL.1 | | | | X | | | | | | | |
| FIA_SOS.1 | | | | X | | | | | | | |
| FIA_UAU.1 | | | | X | | | | | | | |
| FIA_UAU.4 | | | | X | | | | | | | |
| FIA_UAU.7 | | | | | X | | | | | | |
| FIA_UID.1 | | | | X | | | | | | | |
| FMT_MOF.1 | | | | | | | X | | | | |

| 보안기능 요구사항 | O. 정보 흐름 통제 | O. 비정상 패킷 차단 | O. 서비스 거부공격 차단 | O. 식별 및 인증 | O. 패스 워드 관리 | O. 세션 통제 | O. 보안 관리 | O. 감사 | O. 자체 보호 | O. 안전한 암호 | O. 저장 데이터 보호 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| FMT_MSA.1 | | | | | | | X | | | | |
| FMT_MSA.3 | | | | | | | X | | | | |
| FMT_MTD.1(1) | | | | | | | X | | | | |
| FMT_MTD.1(2) | | | | | | | X | | | | |
| FMT_PWD.1 | | | | | X | | X | | | | |
| FMT_SMF.1 | | | | | | | X | | | | |
| FMT_SMR.1 | | | | | | | X | | | | |
| FPT_PST.1 | | | | | | | | | | | X |
| FPT_STM.1 | | | | | | | | X | | | |
| FPT_TST.1 | | | | | | | | | X | | |
| FTA_MCS.2 | | | | | | X | | | | | |
| FTA_SSL.1 | | | | | | | | | | | |
| FTA_SSL.3 | | | | | | X | | | | | |
| FTA_TSE.1 | | | | | | X | | | | | |
| FTP_TRP.1 | | | | | | X | | | | | |

[보안목적과 보안기능요구사항 대응]

| O.정보흐름통제 | FDP_IFC.2, FDP_IFF.1, FMT_MSA.1, FMT_MSA.3 |
|---|---|

FDP_IFC.2 및 FDP_IFF.1은 네트워크 패킷 및 세그먼트에 적용되는 정보흐름통제규칙을 정의함으로써 트래픽에 대한 TOE 통과여부를 결정할 수 있는 능력을 보장하므로 보안목적을 만족시킨다.

FMT_MSA.1은 인가된 관리자가 정보흐름통제규칙을 관리할 수 있는 능력을 제공하도록 정의함으로써 조직의 운영환경에 맞는 트래픽 흐름을 통제할 수 있도록 보장하므로 보안목적을 만족시킨다.

FMT_MSA.3은 제한적인 디폴트 값을 제공하고 관리자가 선택한 초기값으로 디폴트 값을 변경하도록 정의함으로써 트래픽 흐름을 통제하는 기본정책을 적용하도록 보장하므로 보안목적을 만족시킨다.

| O.비정상패킷차단 | FDP_IFC.2, FDP_IFF.1, FDP_MSA.1 |
|---|---|

FDP_IFC.2 및 FDP_IFF.1은 상태 값을 기반으로 비정상적인 구조를 갖는 네트워크 패킷을 차단하도록 통제범위 및 정보흐름통제규칙을 정의하고 이에 따라 TOE 통과여부를 결정할 수 있는 능력을 보장하므로 보안목적을 만족시킨다.

FMT_MSA.1은 정보흐름통제정책에 적용되는 보안속성을 관리하도록 관리자에게 관리수단을 제공함을 보장하므로 보안목적을 만족시킨다.

| O.서비스거부공격차단 | FDP_IFC.2, FDP_IFF.1, FDP_MSA.1 |
|---|---|

TOE는 네트워크 장애를 유발하는 공격에 대응해야 하며, 내부망의 IT 자원이 비정상적으로 사용되는 경우를 탐지하고 차단하여야 한다.

FDP_IFC.2 및 FDP_IFF.1은 상태 값을 기반으로 비정상적인 구조를 갖는 네트워크 패킷을 차단하도록 통제범위 및 정보흐름통제규칙을 정의하고 이에 따라 TOE 통과여부를 결정할 수 있는 능력을 보장하므로 보안목적을 만족시킨다.

FMT_MSA.1은 정보흐름통제정책에 적용되는 보안속성을 관리하도록 관리자에게 관리수단을 제공함을 보장하므로 보안목적을 만족시킨다.

| O.식별및인증 | FIA_AFL.1, FIA_UAU.1, FIA_UAU.4, FIA_UID.1, FIA_SOS.1 |
|---|---|

FIA_AFL.1은 관리자 로그인 시 연속 3번의 인증을 실패하면 관리자가 지정한 인증지연 시간동안 인증 시도를 차단하여 안전한 인증을 지원하므로 본 보안목적을 만족시킨다.

FIA_UID.1 및 FIA_UAU.1은 관리자가 WebGUI에 접속하는 경우 로그인(식별 및 인증)하기 전에 HTTPS 연결을 먼저 수행하고, CLI에 접속하는 로그인(식별 및 인증)전에 SSH 연결을 먼저 수행하여 안전한 경로를 먼저 형성하도록 허용한 후 관리자 식별 및 인증을 수행한다. 이와 같이 관리자를 유일하게 식별하고 안전하게 인증하므로 본 보안목적을 만족시킨다.

FIA_UAU.4는 인증 데이터의 재사용을 방지하는 능력을 보장하므로 본 보안목적을 만족시킨다.

FIA_SOS.1은 관리자 등록 시 패스워드(관리자 패스워드, SSH 개인키 접근용 패스워드)를 입력하는 경우 TOE에 내장된 패스워드 복잡도 규칙(4조합 9자리 이상, 20자리 이하)을 만족시킴을 검증함으로써 안전한 인증을 지원하므로 본 보안목적을 만족시킨다.

| O.패스워드관리 | FIA_UAU.7, FMT_PWD.1 |
|---|---|

FIA_UAU.7은 패스워드 입력이 진행되는 동안 마스킹 처리된 값(*)만 출력됨을 보장하고, 인증 실패 시 실패 이유에 대한 피드백을 제공하지 않음을 보장하므로 본 보안목적을 만족시킨다.

FMT_PWD.1은 초기 패스워드를 강제변경하는 기능을 지원하여 패스워드를 안전하게 생성 및 관리하는 능력을 보장하므로 본 보안목적을 만족시킨다. 패스워드 조합규칙 및 길이는 TOE에 내장되어 있으므로 관리수단을 제공하지 않는다.

| O.세션통제 | FCS_CKM.1, FCS_CKM.2, FCS_CKM.4, FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4), FTA_MCS.2, FTA_SSL.1, FTA_SSL.3 FTA_TSE.1, FTP_TRP.1 |
|---|---|

FCS_CKM.1 및 FCS_CKM.2는 SSH, HTTPS 관리접속 시 SSH, TLS 통신에 필요한 암호키를 표준에 적합한 키길이로 생성하고 이를 기반으로 RFC 8268에 따라 통신용 세션키를 관리자의 SSH 클라이언트, 웹 브라우저와 분배하므로 관리자가 원격에서 전송하는 TSF 데이터를 보호하기 위한 SSH, TLS 프로토콜 구현을 지원함으로써 본 보안목적을 만족시킨다.

FCS_CKM.4는 휘발성 저장장치에 존재하는 경우 “0”으로 1회 덮어쓰기 및 비휘발성 저장장치에 존재하는 경우 “0” 또는 “난수”로 3회 덮어쓰기로 암호키가 파기됨을 보장하므로 본 보안목적을 만족시킨다.

FCS_COP.1(1)은 SSH 및 HTTPS 프로토콜 처리 과정에서 필요한 대칭키 암호연산을 표준에 부합하도록 수행함으로써 SSH 관리접속 및 HTTPS 관리접속 시 전송구간 TSF 데이터 암호화를 지원하므로 본 보안목적을 만족시킨다.

FCS_COP.1(2)은 SSH 및 HTTPS 프로토콜 처리 과정에서 필요한 HMAC 암호연산을 표준에 부합하도록 수행함으로써 SSH 관리접속 및 HTTPS 관리접속 시 전송구간 TSF 데이터 암호화를 지원하므로 본 보안목적을 만족시킨다.

FCS_COP.1(3)은 SSH 및 HTTPS 프로토콜 처리 과정에서 필요한 해시연산을 표준에 부합하도록 수행함으로써 SSH 관리접속 및 HTTPS 관리접속 시 전송구간 TSF 데이터 암호화를 지원하므로 본 보안목적을 만족시킨다.

FCS_COP.1(3)은 SSH 및 HTTPS 프로토콜 처리 과정에서 필요한 전자서명 연산을 표준에 부합하도록 수행함으로써 SSH 관리접속 및 HTTPS 관리접속 시 전송구간 TSF 데이터 암호화를 지원하므로 본 보안목적을 만족시킨다.

FTA_MCS.2는 관리자 관리접속에 대해 동시 세션을 차단하고 동일 관리자에 대해 관리접속 세션과 로컬접속 세션의 동시 세션연결을 차단하여 관리자별 최대 1개 세션만을 유지함으로써 관리자 IP에 근거한 세션통제를 보장하므로 본 보안목적을 만족시킨다.

FTA_SSL.1, FTA_SSL.3은 관리자가 설정한 비활동 기간이 경과하면 세션을 잠그고 세션잠금을 해제하지 전에 인증메커니즘에서 재인증을 수행함으로써 관리자 세션을 관리하므로 본 보안목적을 만족시킨다.

FTA_TSE.1은 접속 IP, 동일 권한을 갖는 관리자 계정의 관리접속 세션, SSH Authorize key에 따라 실행이 허용된 명령어, anti-lockout 활성화 등에 기반하여 관리자 관리접속 세션 설정 여부를 결정함을 보장하므로 본 보안목적을 만족시킨다.

FTP_TRP.1은 관리자가 접속하는 경우 암호통신 프로토콜(TLS 기반 HTTPS, SSH)을 적용하여 안전한 경로를 제공함을 보장하므로 본 보안목적을 만족시킨다.

| | |
|---|---|
| **O.보안관리** | **FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1(1), FMT_MTD.1(2), FMT_PWD.1, FMT_SMF.1, FMT_SMR.1** |

FMT_MOF.1은 인가된 관리자가 감사기능 설정, TLS 버전 선택, 로컬접속 콘솔 관리, 관리자 세션관리, 상태 기반 감시 메커니즘 운영모드 관리, 외부 실체 관리 등 TSF 및 TSF 데이터를 관리할 수 있는 안전한 수단을 제공함을 보장하므로 본 보안목적을 만족시킨다.

FMT_MSA.1은 인가된 관리자가 트래픽 필터링 규칙, 상태 기반 감시 규칙, NAT 규칙을 관리할 수 있는 수단을 제공함을 보장하므로 본 보안목적을 만족시킨다.

FMT_MSA.3은 인가된 침입차단 SFP에서 적용하는 보안속성에 대해 제한적인 기본 값을 제공하고 초기값을 설정하는 관리수단을 제공함을 보장하므로 본 보안목적을 만족시킨다.

FMT_MTD.1(1) 및 FMT_MTD.1(2)은 인가된 관리자가 TSF 데이터를 관리하도록 관리수단을 제공하고 특히 암호키 및 암호관련 매개변수를 안전하게 관리하는 수단을 제공함을 보장하므로 본 보안목적을 만족시킨다.

FMT_PWD.1은 관리자가 최초 접속 시 ID 및 패스워드를 강제변경하는 기능을 제공함을 보장하므로 안전한 수단을 제공하여야 하는 본 보안목적을 만족시킨다.

FMT_SMF.1은 TSF가 수행해야 하는 보안기능, 보안속성, TSF 데이터 등의 관리기능을 제공하도록 보장하므로 TSF 및 TSF 데이터를 효율적으로 관리하여야 하는 보안목적을 만족시킨다.

FMT_SMR.1은 WebGUI 및 CLI 등 관리수단 유형에 따른 역할을 정의하고 관리자에게 역할을 할당하는 기능을 제공하도록 보장하므로 관리기능을 인가된 사용자로 제한하여야 하는 본 보안목적을 만족시킨다.

| O.감사 | FAU_GEN.1, FPT_STM.1, FAU_SAA.1, FAU_ARP.1, FAU_SAR.1, FAU_SAR.3, FAU_STG.1, FAU_STG.3, FAU_STG.4 |
|---|---|

FAU_GEN.1은 보안과 관련된 모든 행동에 대해 책임추적이 가능하도록 감사정보를 감사레코드에 기록하여 생성하는 기능을 제공함을 보장하므로 책임추적이 가능한 보안관련 사건 기록 및 유지에 대한 본 보안목적을 만족시킨다.

FPT_STM.1은 감사정보에 저장될 사건 일시를 신뢰된 NTP 서버로부터 수신한 시간정보로 기록함을 보장하므로 책임추적이 가능한 사건 기록을 요구하는 본 보안목적을 만족시킨다.

FAU_SAA.1 및 FAU_ARP.1은 검사 규칙에 따라 감사된 사건을 분석하여 잠재적 보안 위반으로 탐지하는 경우 관리자가 설정한 이메일로 관련 내용을 통보하는 기능을 제공하도록 보장하므로 보안관련 모든 행동의 책임추적을 요구하는 본 보안목적을 만족시킨다.

FAU_SAR.1 및 FAU_SAR.3은 감사레코드 조회기능을 제공하고 특히 검색어 기준으로 특정 사건을 검색하여 정렬할 수 있는 감사기능 제공을 보장하므로 감사데이터 검토 수단 제공을 요구하는 본 보안목적을 만족시킨다.

FAU_STG.1은 인가되지 않은 삭제로부터 감사레코드를 보호하고 비인가된 변경을 방지하도록 보장하므로 감사데이터 위·변조 방지를 요구하는 본 보안목적을 만족시킨다.

FAU_STG.3 및 FAU_STG.4는 감사 증적이 clog 파일 크기의 80%를 초과하는 경우 관리자가 설정한 메일로 통보하고 syslog 서버 로그전송 기능 자동 활성화를 보장하며, 감사 증적이 포화인 경우 자동 백업을 수행한 후 오래된 감사 레코드 덮어쓰기를 수행함을 보장하므로 감사저장 공간 초과시 적절한 대응행동을 요구하는 본 보안목적을 만족시킨다.

| O.자체보호 | FPT_TST.1 |
|---|---|

FPT_TST.1은 주요 TSF(난수생성 기능, 암호연산 기능) 및 주요 하드웨어 (CPU 및 메모리)의 정확한 운영을 위한 자체 시험을 보장하고, 일부 TSF 데이터 및 원본 이미지, 부트로더 이미지의 무결성을 검증하는 기능을 보장하므로 본 보안목적을 만족시킨다.

| O.안전한 암호 | FCS_RBG.1, FCS_CKM.4, FCS_CKM.1, FCS_CKM.2, FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4) |
|---|---|

FCS_RBG.1은 키 생성 자료 및 암호키 생성에 필요한 안전한 난수 생성을 보장하므로 안전한 보안강도를 갖는 암호키를 생성해야 하는 본 보안목적을 만족시킨다.

FCS_CKM.1은 SSH 및 HTTPS 연결 시 서버 인증 및 통신 암호화에 필요한 키 생성 자료 및 암호키를 안전하게 생성하도록 보장하므로 안전한 보안강도를 갖는 암호키를 생성해야 하는 본 보안목적을 만족시킨다.

FCS_CKM.2는 SSH 및 HTTPS 연결 시 세션키 생성에 필요한 암호키를 안전하게 분배하도록 보장하므로 관리접속을 통해 전송되는 TSF 데이터의 비밀성과 무결성을 보장해야 하는 본 보안목적을 만족시킨다.

FCS_CKM.4는 휘발성 저장장치에 존재하는 암호키를 “0” 또는 “난수”로 3회 덮어쓰기를 통해 암호키가 파기됨을 보장하므로 암호키를 안전하게 관리하여야 하는 본 보안목적을 만족시킨다.

FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4)은 관리접속을 위한 SSH 및 HTTPS 연결 시 암호알고리즘에 따른 암호연산을 지원하므로 암호키 또는 평문을 알아낼 수 없도록 안전한 암호알고리즘을 적용해야 하는 본 보안목적을 만족시킨다.

| O.저장데이터보호 | FPT_PST.1 |
|---|---|

FPT_PST.1은 TOE에 저장되는 TSF 데이터에 대한 인가되지 않은 변경 또는 노출로부터 보호하기 위해 패스워드는 해시값을 저장하고 환경설정 파일은 저장 시 파일 퍼미션을 700으로 강제 변경므로 본 보안목적을 만족시킨다.

## 6.3.2. 보증요구사항의 이론적 근거

본 보안목표명세서의 평가보증등급은 국내용 평가보증등급 EAL4로 선정하였다.

EAL4는 기존의 생산공정을 변경하지 않고 일반적으로 사용되고 있는 개발 방법론을 적용하여 얻을 수 있는 최대한의 보증 수준이다. 따라서 완전한 인터페이스 명세, 기본적인 모듈 설계, 일부 TSF 구현명세서 등 일부 개발과정에서 추가적인 문서화 작업이 요구된다. 또한 개발환경 보안, TOE 형상관리 자동화, TOE 배포절차 등 일부 개발프로세스 개선이 요구된다. 생산공정을 변경하지 않는 범위 내애서 개발프로세스를 개선하여 이에 따라 추가적인 개발문서를 작성하고 이를 토대로 본 보안목표명세서에서 정의한 보안기능요구사항을 분석함으로써 제한적 범위에서 최대 수준의 보증을 제공한다.

보안기능요구사항의 분석에 대한 정확성, 객관성 확보를 위해 개발자시험 표본결과 확인, 설계문서(기능명세, TOE 모듈설계)에 기반한 평가자 독립시험, 강화된-기본 공격 성공 가능성을 가진 공격자의 침투 공격에 대한 내성을 입증하는 취약성 분석과 침투시험이 수행되며 이는 평가기관에서 수행된다.

# 6.4. 종속관계에 대한 이론적 근거

## 6.4.1. 보안기능요구사항의 종속관계

다음 표는 보안기능요구사항의 종속관계를 보여준다.

| 번호 | ST 보안기능 요구사항 | CC 제2부 보안기능요구사항 종속관계 | 본 표에서 SFR 식별을 위해 부여한 번호 |
|---|---|---|---|
| 1 | FAU_ARP.1 | FAU_SAA.1 | 3 |
| 2 | FAU_GEN.1 | FPT.STM.1 | 33 |
| 3 | FAU_SAA.1 | FAU_GEN.1 | 2 |
| 4 | FAU_SAR.1 | FAU_GEN.1 | 2 |
| 5 | FAU_SAR.3 | FAU_SAR.1 | 5 |
| 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] | 10, 12 |
| | | FCS_CKM.4 | 11 |
| 10 | FCS_CKM.4 | [FCS_CKM.2 또는 FCS_COP.1] | 10, 12 |
| | | FCS_COP.1 | 11 |
| 11 | FCS_RGB.1(확장) | [FDP_ITC.1 또는 FDP_ITC.2 또는 FCS_CKM.1] | 9 |
| 12 | FDP_IFC.2 | [FDP_ITC.1 또는 FDP_ITC.2 또는 FCS_CKM.1] | 9 |
| | | FCS_CKM.4M.4 | 11 |
| 14 | FDP_IFF.1 | - | - |
| 17 | FIA_AFL.1 | FDP_IFF.1 | 18 |
| 18 | FIA_SOS.1 | FDP_IFC.1 | 17 |
| | | FMT_MSA.3 | 27 |
| 19 | FIA_UAU.1 | FIA_UAU.1 | 21 |
| 20 | FIA_UAU.4 | - | - |
| 21 | FIA_UAU.7 | FIA_UID.1 | 24 |
| 22 | FIA_UID.1 | - | - |
| 23 | FMT_MOF.1 | FIA_UAU.1 | 21 |
| 24 | FMT_MSA.1 | - | - |
| 25 | FMT_MSA.3 | FMT_SMF.1 | 30 |
| | | FMT_SMR.1 | 31 |

| 번호 | ST 보안기능 요구사항 | CC 제2부 보안기능요구사항 종속관계 | 본 표에서 SFR 식별을 위해 부여한 번호 |
|---|---|---|---|
| 26 | FMT_MTD.1(1) | [FDP_ACC.1 또는 FDP_IFC.1] | 17 |
| | | FMT_SMF.1 | 30 |
| | | FMT_SMR.1 | 31 |
| 27 | FMT_MTD.1(2) | FMT_MSA.1 | 26 |
| | | FMT_SMR.1 | 31 |
| 28 | FMT_PWD.1(확장) | FMT_SMF.1 | 30 |
| | | FMT_SMR.1 | 31 |
| 29 | FMT_SMF.1 | - | 확장 컴포넌트 정의 30, 31 |
| 30 | FMT_SMR.1 | - | - |
| 31 | FPT_PST.1(확장) | FIA_UID.1 | 24 |
| 32 | FPT_STM.1 | - | - |
| 33 | FPT_TST.1 | - | - |
| 35 | FTA_MCS.2 | - | - |
| 37 | FTA_SSL.1 | FIA_UID.1 | 24 |
| 38 | FTA_SSL.3 | - | 21 |
| 39 | FTA_TSE.1 | | |
| 40 | FTP_TRP.1 | - | - |
| 41 | FTP_TRP.1 | - | - |

[표 7] 종속관계 이론적 근거

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

FMT_PWD.1은 본 보안목표명세서에서 확장 컴포넌트로 정의된 것이므로 CC 제2부에서 정의된 종속관계는 없다. 하지만 확장 컴포넌트 정의에 따라 FMT_SMF.1 및 FMT_SMR.1에 종속관계를 가지므로 이를 식별하였다.

## 6.4.2. 보증요구사항의 종속관계

정보보호시스템 공통평가기준에서 제공하는 EAL4 보증 패키지의 종속관계는 이미 만족되어 있으므로 이에 대한 이론적 근거는 생략한다.

07

# TOE 요약명세

7.1. 침입차단시스템 기능
7.2. TOE 접근
7.3. 식별 및 인증
7.4. 안전한 경로/채널
7.5. 보안감사
7.6. 보안관리
7.7. TSF 보호
7.8. 암호지원

# 7. TOE 요약명세

## 7.1. 침입차단시스템 기능

### 7.1.1. 패킷 필터링 메커니즘

패킷 필터링 메커니즘은 정해진 규칙에 따라 트래픽을 통과시키거나 차단(Block)/거부(reject) 시킬 수 있다. 차단(Block)은 트래픽을 폐기만하고 트래픽 발신자에게 응답 메시지를 전송하지 않는 것이다. 이 경우 발신자는 시간종료가 되기 전까지는 계속하여 연결을 시도하게 된다. 거부(reject)는 거부된 TCP/UDP 트래픽에 대해 응답 메시지를 발신자에게 전송하는 처리방식이다. 거부된 TCP 트래픽에 대해 발신자는 TCP RST(reset) 응답 메시지를 수신하게 되고 거부된 UDP 트래픽에 대해 발신자는 ICMP Unreachable 메시지를 수신되게 된다.

#### 7.1.1.1. 외부망에서 내부망으로 유입되는 트래픽 필터링

TOE는 여러 개의 네트워크 인터페이스를 가지고 있으므로 외부망(예, 인터넷 망)과의 접점을 여러 개로 설정할 수 있다. 트래픽은 WAN 인터페이스를 통해 외부망에서 내부망으로 유입된다. DMZ 영역이 구성되어 있는 경우 외부에서 DMZ 영역으로 유입되는 트래픽과 외부에서 내부망으로 유입되는 트래픽에 대해 정호흐름통제 규칙을 구분하여 설정 및 적용할 수 있다.

외부망 접점에서 트래픽을 처리하는 WAN 인터페이스에 적용되는 패킷 필터링 기본 정책은 정보흐름통제규칙(firewall rule)에 일치하는 경우에만 해당 규칙의 Action에 따라 패킷 처리방식(허용/차단/거부)을 결정하고 일치하는 규칙이 존재하지 않는 경우 모든 패킷을 차단하는 화이트리스트 방식이다. TOE를 설치하면 기본 허용규칙은 없으며 모든 트래픽을 차단하는 기본 차단규칙만이 존재하는 제한적인 기본정책이다. 관리자는 모든 트래픽을 차단하는 규칙이 기본규칙으로 설정되어 있으므로 관리자는 “7.2.5 보안관리조직”에서 명세한 보안관리 수단(WebGUI)을 통해 조직의 정책에 부합하는 정보흐름통제규칙(firewall rule)을 추가, 변경, 삭제 등의 관리행동을 수행한다.

#### 7.1.1.2. 내부망에서 외부망으로 나가는 트래픽 필터링

TOE는 여러 개의 인터페이스를 지원하므로 DMZ 영역을 구분하고 내부망을 다중 영역으로 분할하여 설정하여 이들에 대한 정보흐름통제규칙을 구분하여 적용할 수 있다. 내부망 LAN 인터페이스에서 외부망 WAN 인터페이스 또는 다른 내부망 LAN 인터페이스로 나가는 아웃바운드 트래픽에 대해 HTTP/HTTPS, 이메일, DNS 서비스 등을 모두 허용하도록 TOE 설치 시 다음과 같이 기본 허용규칙이 설정되어 있다.

| 규칙 설명 | 출발지 IP주소 | 목적지 IP주소 | 목적지 포트 |
|---|---|---|---|
| 모든 호스트의 HTTP 및 HTTPS 접속 허용 | LAN Network | Any | TCP 80<br>TCP 443 |
| 메일서버의 SMTP 접속 허용 | Mail Server | Any | TCP 25 |
| 내부 DNS 서버의 DNS 질의 요청 허용 | DNS Server | Any | TCP 53<br>UDP 53 |

다만, 출발지 IP주소가 분명히 잘못되어 있는 경우 해당 트래픽을 외부망으로 보내지 않고 차단한다. 또한 내부망에 대한 정보가 인터넷 등과 같은 외부망으로 새어나가지 못하도록 다음과 같은 특정 프로토콜의 동작을 중지시킬 수 있다.

•TCP 포트 135번을 사용하는 Microsoft RPC
• TCP 및 UDP 포트 137번 ~ 139번을 사용하는 NetBIOS
• TCP 및 UDP 포트 445번을 사용하는 SMB/CIFS(Server Message Block/Common Interent File System)

이외에도 네트워크 장비 설정오류로 인해 로그 정보가 외부망으로 유출되는 것을 차단할 수 있도록 SNMP, SNMP 트랩, syslog 등과 같은 프로토콜 동작을 제한시킬 수도 있다.

### 7.1.1.3. 자동 추가 규칙

관리자가 "7.2.5 보안관리"에서 명세한 WebGUI에서 정보흐름통제규칙 자동생성 기능을 활성화시키고 자동생성 규칙에 관련된 TOE 보안기능이 활성화되어 있으면 다음과 같은 규칙이 자동으로 생성된다.

| 자동추가 규칙 | 설명 |
|---|---|
| anti-lockout rule | 관리자가 실수로 관리 웹인터페이스 접근을 차단하지 못하도록 내부망 출발지 IP주소에서 목적지 TOE LAN IP주소의 침입차단시스템 관리 프로토콜로 향하는 트래픽을 허용하는 규칙 |
| anti-spoofing rules | 스푸핑된 트래픽(uRPF, Unicast Reverse Path Forwarding)을 기본적으로 차단하는 규칙 예를 들어 WAN 인터페이스로 유입되는 패킷의 출발지 주소가 내부망 대역인 경우이거나 내부망 대역에 포함되지 않은 출발지 IP주소를 갖고 외부로 나가는 패킷에 대해 폐기 |
| Block Private Networks | WAN 인터페이스에서 RFC 1918에 정의된 서브네트워크에 대한 차단 규칙 |
| Block Bogon Networks | 예약되어 있거나 할당되지 않은 IP주소 대역을 가지고 있어 인터넷에서는 결코 보여지지 않는 패킷을 차단하는 규칙 |

TOE를 처음 설치하는 경우 WAN 인터페이스에 대해 자동생성되는 기본규칙은 없다. 하지만 관리자가 WebGUI에서 "Block Private Networks" 옵션을 활성화한 경우 외부망에서 유입되는 패킷의 출발지 주소가 내부 사설망 대역(10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16)에 포함되면 무조건 해당 패킷을 차단하는 기본 차단규칙이 WAN 인터페이스의 정보흐름통제규칙에 자동 추가된다.

마찬가지로 TOE를 처음 설치하는 경우 LAN 인터페이에 대해 기본적으로 모든 아웃바운드 패킷은 허용이므로 정보흐름통제규칙은 없다. 다만, 관리자가 WebGUI에서 "Anti-Lockout Rule" 옵션을 활성화하면 관리자가 실수로 WebGUI 로그인 페이지가 잠김처리되지 않도록 하는 규칙이 자동 추가된다.

### 7.1.1.4. 시간기반 정보흐름통제규칙

정보흐름통제규칙을 관리자가 지정한1 시간동안에만 활성화하여 일시적으로 적용할 수 있다. 지정된 시간 대역에만 적용되고 이외에는 해당 규칙이 존재하지 않는 것처럼 동작한다는 점을 제외하면 일반 정보흐름통제규칙과 동일하다. 예를 들어 특정 허용규칙이 활성화되는 기간을 토요일로 설정한 경우 토요일에는 해당 트래픽이 TOE를 통과하게 되지만 토요일 이외에는 해당 트래픽은 차단된다. 시간기반 정보흐름통제규칙도 일반 정보흐름통제규칙과 같이 Top-Down 순서대로 적용된다.

### 7.1.1.5. 정보흐름통제규칙 적용 순서

다음과 같이 3가지로 분류하여 정보흐름통제규칙을 순차적으로 적용하여 처리한다. 패킷의 보안속성을 토대로 정보흐름통제규칙과 순차적으로 비교하여 일치하는 규칙이 존재하면 해당 규칙을 적용하여 패킷을 처리(허용/차단/거부)하고 이후 규칙에는 적용을 받지 않는다.

| 규칙 분류 | 설명 | 규칙 적용 순서 |
|---|---|---|
| Floating Rules | 인바운드 트래픽, 아웃바운드 트래픽, 기타 방향성을 갖는 트래픽을 처리하는 다양한 네트워크 인터페이스 대상으로 복잡한 규칙적용이 필요할 때 생성하는 규칙<br>"match" 행동(Action)이 정의된 규칙은 패킷을 허용하거나 차단하지 않고 트래픽을 큐에 일시 저장하거나 트래픽 성형(shaping)을 위해 제한함 | Floating Rules<br>⇩<br>Interface Gourp Rules<br>⇩<br>Interface Rules |
| Interface Gourp Rules | 인바운드 트래픽을 처리하는 네트워크 인터페이스에 대해 그룹핑하여 동일 규칙을 그룹핑된 인터페이스에 동시 적용 | |
| Interface Rules | 네트워크 인터페이스 마다 적용되는 특정 규칙이 필요할 때 개별 생성하는 규칙 | |

## 7.1.2. 상태기반 감시 메커니즘

상태기반 감시 메커니즘은 패킷 필터링 메커니즘을 통해 통과된 트래픽에 대해서만 상태 표에 기록한다. 패킷 필터링 메커니즘에서 통과된 패킷에 대한 연결정보를 상태 표에 기록하고 있다가 이에 일치하는 트래픽에 대해서는 자동으로 통과시킨다. 상태 표에 기록되는 연결정보에는 출발지 정보, 목적지 정보, 프로토콜, 포트 및 TCP/UDP 패킷의 상태정보, ICMP 메시지 정보 등이 있다. 상태 표에 기록된 연결정보에 일치하는 트래픽은 패킷 필터링 메커니즘을 거치지 않고 바로 상태기반 감시 메커니즘으로 들어와 처리된다.

상태기반 감시 메커니즘의 운영모드는 다음과 같다.

---

* "관리자가 지정한"이란 구문은 본 문서에서 "관리자가 "7.2.5 보안관리"에서 명세한 관리수단(WebGUI 및/또는 CLI)에서 TOE를 관리하는 행위"를 의미하는 것으로, 해당 관리행위에 대해서는 "7.2.5 보안관리"절에서 서술하고 있다.

| State Type | 설명 |
|---|---|
| Keep(기본 값) | 패킷 필터링 메커니즘에서 허용된 패킷에 대한 상태정보를 상태 표에 기록하여 유지하고 이를 기반으로 트래픽의 정보흐름을 결정하는 기본 운영모드 |
| Sloppy State | Keep 상태보다는 엄격하지 않게 정책을 적용하는 운영모드<br>- 패킷 필터링 메커니즘에서 트래픽 연결을 반만 볼 수 있어 상태정보 유효성 검사를 실패하는 경우에만 해당 트래픽을 차단 |
| Synproxy | DoS 공격, SYN flooding 공격 등에 대처할 수 있도록 WAN 인터페이스로 유입되는 TCP 연결(SYN → SYNACK → ACK)처리를 위한 프록시 기능을 수행하는 운영모드 |
| None | 상태기반 감시 메커니즘을 적용하지 않는 운영모드 |

사용자 세션에 대해 인바운드 트래픽과 아웃바운드 트래픽에 대한 상태정보를 유지하여야 하므로 상태 표의 최대 크기가 1,000,000이라 하면 사용자 세션은 500,000까지 처리할 수 있다. 이러한 임계치를 초과하면 추가적인 연결은 차단된다. 메모리 소진 공격에 대처할 수 있도록 상태 표의 최대 크기(기본값 : RAM 사이즈의 10%)를 관리자가 설정할 수 있으며 이러한 관리기능에 대한 상세내용은 “7.2.5 보안관리”를 참조한다.

정보흐름통제규칙에 일치하여 TCP/UDP 연결에 성공한 트래픽에 대해 다음과 같은 상태 값을 상태 표에 유지하여 상태기반 패킷 감시 기능을 수행하게 된다.

| 상태 값(State) | 설명 |
|---|---|
| SYN_SENT | TCP 핸드쉐이크 시작을 시도하기 위해 TCP SYN 패킷을 보낸 상태 |
| CLOSED | 한 쪽에서 연결 종료를 고려하고 있는 상태 또는 어떠한 트래픽도 받지 못한 상태 |
| ESTABLISHED | TCP 연결이 완전히 성립된 상태 |
| TIE_WAIT/FIN_WAIT | TCP 연결을 종료하거나 끊는 과정에 있는 상태 |
| NO_TRAFFIC | 상태에 일치하는 패킷을 수신하지 못한 상태 |
| SINGLE | 단일 패킷이 관찰된 상태 |
| MULTIPLE | 다중 패킷이 관찰된 상태 |
| ESTABLISHED:ESTABLISHED | 양방향 TCP 연결이 완전히 성립된 상태 |
| SYN_SENT:CLOSED | 한 쪽에서 TCP SYN 패킷을 보내서 SYN_SENT 상태이나 다른 쪽에서 이에 상응하는 응답을 받지 못한 상태로 패킷이 목적지에 도달하지 못했거나 패킷이 차단된 경우 발생하는 상태 |
| SINGLE:NO_TRAFFIC | 한 쪽에서 UDP 패킷을 보냈으나 다른 쪽에서 이에 상응하는 응답을 받지 못한 상태 |
| SINGLE:MULTIPLE | UDP 프로토콜 등에서 클라이언트가 1개 패킷을 보내고 응답 측에서는 여러 개의 패킷을 전송하고 있는 상태 |
| MULTIPLE:MULTIPLE | UDP 프로토콜 등에서 양방향에서 다중 패킷을 보내고 있는 상태 |
| 0:0 | ICMP 프로토콜이 동작 중일 때 나타나는 상태 |

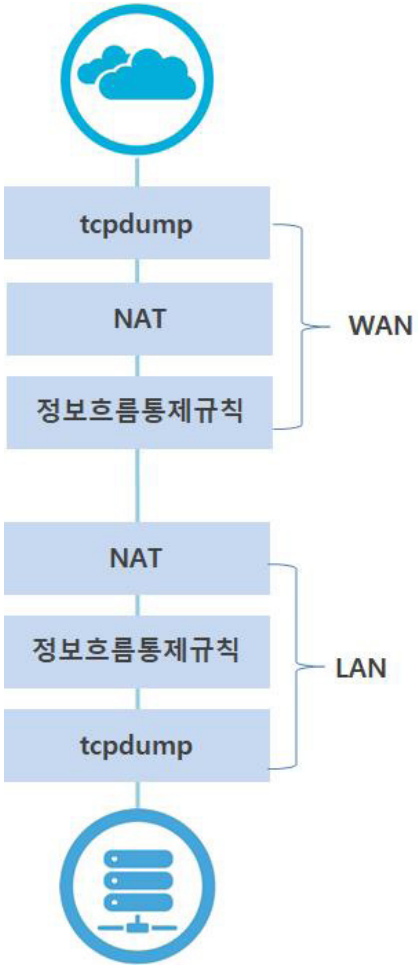
TOE는 상태 표에 기록된 정보를 기반으로 조각난 패킷을 탐지할 수 있다. 조각난 패킷이 목적지로 도착하는 경우 TOE는 조각나 패킷들을 모아서 재조립하여 완성된 패킷으로 만든다. 조각들이 모두 도착하지 못한 경우 TOE는 조각 패킷들이 도착할 때 까지 기다린다. TTL이 만료되기 전까지 조각난 모든 패킷이 도착하기를 기다렸다가 모든 패킷이 도착하면 재조립한다. TTL이 만료되어도 조각난 패킷들이 모두 도착하지 못한 경우 나머지 패킷들을 모두 폐기(drop)한다.

TOE는 half-open TCP 세션에 대해서도 full TCP 세션을 유지하는 방식과 동일하게 임계치에 도달하는 경우 세션을 종료하고 연결을 끊는다.

### 7.1.3. 패킷 처리 절차

TOE는 정보흐름통제규칙을 적용하기 전에 패킷이 다음에 해당하는 지 여부를 먼저 검사하고 해당하는 경우 자동 폐기한다.

•유효하지 않은 조각을 가진 패킷
- 완전히 재조립할 수 없는 조각 패킷
- 출발지 주소가 브로드캐스트 네트워크로 정의된 패킷
- 출발지 주소가 멀티캐스트 네트워크로 정의된 패킷
- 출발지 주소가 루프백 주소로 정의된 패킷
- 출발지 또는 목적지 주소가 0.0.0.0으로 정의되었거나 240.0.0./24로 정의된 패캣
- Loose Source Routing, Stric Source Routing 또는 Record Route 등 IP 옵션을 가진 패킷
- 출발지 주소가 네트워크를 수신한 인터페이스 주소와 동일한 패킷
- 출발지 또는 목적지 주소가 링크로컬 주소인 패킷
- 출발지 주소가 패킷을 수신한 네트워크 인터페이스에서 연관시킬 수 없는 대역의 주소를 가진 패킷

| WAN □ LAN | 트래픽 흐름 |
| --- | --- |
| WAN 인터페이스에서 NAT 처리<br>(Port Forward 또는 1:1 NAT)<br>□<br>WAN 인터페이스의 정보흐름통제규칙 적용<br>□<br>LAN 인터페이스에서 NAT 처리<br>(1:1 NAT 또는 Outbound NAT)<br>□<br>LAN 인터페이스에서<br>아웃바운트 트래픽에 대한 Floating rules 적용 |  |
| **LAN □ WAN** | |
| LAN 인터페이스에서 NAT 처리<br>(Port Forward 또는 1:1 NAT)<br>□<br>LAN 인터페이스의 정보흐름통제규칙 적용<br>(인바운드 Floating rules → 그룹 rules → 인터페이스 rules)<br>□<br>WAN 인터페이스에서 NAT 처리<br>(1:1 NAT 또는 Outbound NAT)<br>□<br>WAN 인터페이스에서 아웃바운드 트래픽에 대한 Floating rules 적용 | |

인터넷 등과 같은 외부망에서 유입되는 트래픽은 WAN 인터페이스의 정보흐름통제규칙을 적용하여 처리하고 LAN에 연결되어 있는 호스트 또는 단말에서 외부망이나 다른 내부망으로 내보내는 트래픽은 LAN 인터페이스의 정보흐름통제규칙을 적용하여 처리된다. 또한 NAT가 적용되어 있는 경우 정보흐름통제규칙이 적용되기 이전에 NAT 규칙이 먼저 적용된다.

NAT가 적용되어 있는 경우 인터페이스로 들어가는 트래픽에 대해 정보흐름통제규칙(firewall rule) 보다 NAT(Inbound NAT)가 먼저 처리되므로 목적지 주소가 변화된 패킷에 대해 규칙이 적용된다. 일반적으로 WAN에서 Port Forward는 목적지가 사설 IP주소 대역으로 변환된 후에 규칙이 적용된다. 인터페이스에서 나가는 트래픽에 대해서도 정보흐름통제규칙(firewall rule) 보다 NAT(Outbound NAT)가 적용되므로 출발지 주소가 변환된 후에 규칙이 적용된다. Port Forward는 목적지 주소/포트를 변환하므로 Inbound NAT 또는 Destination NAT라고 하며 Outbound NAT는 출발지 주소/포트를 변환하므로 Source NAT라고 하기도 한다.

## 7.2. TOE 접근

### 7.2.1. 관리자 접속

관리자는 콘솔(CLI)에 로컬접속(직렬포트, IO 장치)하거나 SSH 관리접속을 할 수 있으며 관리자 웹페이지(WebGUI)에 HTTPS로 관리접속을 할 수 있다. 동일 관리자 계정에 대해 1개의 세션만 가능하며 관리접속 세션과 로컬접속 세션을 동시에 허용하지 않고 먼저 로그인한 세션을 유지하고 나중에 로그인을 시도한 세션을 차단한다.

#### 7.2.1.1. 관리자 웹페이지(WebGUI)

관리자 웹페이지(WebGUI)에 관리접속 시 HTTPS가 연결된다. HTTPS 연결을 위해 인증서 기반의 서버인증을 수행하는 TLS 프로토콜이 수행된다. 인증서는 자체 생성하여 사용할 수도 있고 외부 공인인증기관에서 발급한 인증서를 등록하여 사용할 수 있다. HTTP 연결을 시도하여도 HTTPS로 자동 전환될 수 있도록 80포트 접속 시 443포트로 리다이렉트된다.

#### 7.2.1.2. 관리자 콘솔(CLI)

로컬 접속하는 경우 단말기를 직렬포트로 연결하거나 IO 장치(키보드, 마우스)를 TOE에 연결시켜 콘솔에 접근한다. 이에 대해 TOE가 논리적으로 제공할 수 있는 보안기능은 없으므로 물리적 출입통제 보호대책이 적용되는 안전한 장소에 설치 및 운영되어야 한다는 가정사항이 유지되어야 한다.
내부 관리전용망 등 원격에서 콘솔에 접속하고자하는 경우 관리자가 “7.2.5 보안관리”에서 명세된 WebGUI 또는 CLI 수단을 이용하여 SSH 데몬 기능을 활성화하고 SSH Authorized Key를 등록하여야 SSH를 통한 CLI 관리접속이 허용된다.

### 7.2.2. 관리접속 제한

“7.2.5 보안관리”에서 명세한 바와 같이 SSH Authorized Key를 TOE에 등록할 때 접속단말의 IP주소를 지정하고 실행 가능한 명령어를 특정할 수 있으므로 관리자가 설정한 값에 따라 SSH Authorized Key로 접속할 수 있는 단말 및 명령어를 제한한다.

동일 권한을 갖는 관리자 계정의 관리접속이 동시에 연결되면 관리기능 설정에 상충이 발생하므로 이를 제한한다. 따라서 동일 권한을 갖는 관리자 계정의 관리접속 세션이 이미 연결되어 있는 경우 동일 권한을 갖는 다른 관리자 계정으로 로그인 시 세션연결이 거부된다.

Anti-lockout이 활성화되어 있는 경우 내부망 대역에서는 TOE 관리인터페이스에 접근이 허용되는 규칙이 자동생성되어 추가되므로 기본적으로 모든 내부망 대역에서 TOE 관리인터페이스의 관리포트(443, 22) 접속이 허용된다. 관리자가 지정한 단말에서만 관리인터페이스에 접속하도록 TOE LAN 인터페이스에 대한 정보흐름통제규칙을 통해 접근을 통제한다.

### 7.2.3. 세션 관리

#### 7.2.3.1. 관리접속 세션

WebGUI 또는 CLI 관리자 로그인 세션에 대해 idle 시간이 관리자가 설정한 세션 타임아웃 시간(기본 값: 10분)을 경과하면 세션잠기며 세션잠금을 해제하기 전에 사용자 재인증을 수행해야 한다.

## 7.3. 식별 및 인증

### 7.3.1. 패스워드 기반 관리자 인증

관리자가 TLS기반의 HTTPS 기반 웹페이지(WebGUI)에 관리접속하거나 SSH 기반 CLI에 관리접속하는 경우 패스워드 기반 관리자 인증을 수행한다. 또한 로컬접속(콘솔연결)을 하는 경우에도 동일한 패스워드 기반 관리자 인증을 수행한다. SSH 기반 CLI에 관리접속하는 경우 패스워드 기반 관리자 인증은 SSHv2 사용자 인증 프로토콜에서 수행하는 SSH 클라이언트 인증과는 별도로 수행된다. 즉 SSH 클라이언트 인증에 성공하여 SSH 채널이 형성된 이후에 패스워드 기반 관리자 인증이 수행된다.

패스워드 입력 시 화면에는 '*"로 치환되어 입력된 자리 수만 표시하고 ID 및 패스워드 자동완성 기능은 지원하지 않는다. 관리자가 원격에서 입력한 ID 및 패스워드는 HTTPS또는 SSH 프로토콜를 통해 암호화되어 TOE로 전송된다. TOE는 암호화된 ID 및 패스워드를 복호화한 후에 패스워드에 대한 SHA 256 해시값을 계산하고 TOE에 저장되어 있는 관리자 패스워드 해시값과 비교한다. 해시값이 일치하지 않은 경우 인증실패에 대한 상세 메시지 없이 인증에 실패하였다는 메시지만 전송한다. 연속인증실패 임계치(3회)를 초과하는 경우 해당 계정은 관리자가 설정한 인증지연 시간동안 잠금처리된다.

### 7.3.2. SSH 공개키 기반 관리자 인증

TOE는 SSHv2(RFC 4251, RFC 4252, RFC 4523)의 사용자 인증 프로토콜에서 RSA 공개키 기반 인증방식으로 CLI 관리접속 관리자를 인증한다. TOE는 SSH 사용자 인증 프로토콜를 수행하는 과정에서 관리자 계정 생성 시에 등록된 관리자의 RSA 공개키를 이용하여 관리자를 인증한다. 관리자 계정 및 SSH 공개키 등록에 관한 사항은 "7.2.5 보안관리"절을 참조한다.

### 7.3.3. 패스워드 검증

TOE는 관리자가 다음과 같은 패스워드를 등록하는 경우 패스워드 조합규칙 및 최소길이에 부합하는지를 검증한다.

•패스워드 기반 관리자 인증메커니즘에서 사용되는 패스워드에 대해 4조합 9자리 이상
•사용자 계정(ID)과 동일한 패스워드 설정 금지
- 동일한 문자.•숫자의 연속적인 반복입력 금지
- 키보드의 연속된 문자 또는 숫자의 순차적 입력 금지
- 직전 사용된 패스워드 재사용 금지

# 7.4. 보안관리

## 7.4.1. 보안관리 수단

TOE는 관리자 웹페이지(WebGUI) 및 콘솔(CLI) 등 2가지 형태의 관리수단을 제공한다. WebGUI을 사용하기 위해서는 HTTPS 세션을 연결하고, 콘솔(CLI)을 사용하기 위해서는 SSH 관리접속 또는 로컬접속(직렬포트, IO장치 등을 이용한 콘솔포트 연결)을 한다. 콘솔을 통해 제공되는 수단은 제한적이며 일부 메뉴는 WebGUI에서는 지원되지 않고 콘솔에서만 단독으로 제공되는 관리수단이 있다. WebGUI 및 콘솔을 통해 제공되는 관리기능은 다음과 같다.

| 구분 | WebGUI | 콘솔(CLI) |
|---|---|---|
| System | Logout(GUI Log out) | 0) Logout (SSH Only) |
| | Update(최신 버전 패치) | 13) Update from console |
| | Advanced<br>(WebGUI 옵션 설정 : HTTP 연결 시 HTTPS 강제전환, Anti-lockout 활성화)<br>(SSH 옵션 설정 : SSH 활성화, SSH 키 생성, SSH 인증방법 선택, SSH 포트 변경 등)<br>(콘솔 옵션 설정 : 직렬포트 허용 직렬포트 연결 시 속도 제한, 주 콘솔 설정 등) | 14) Disable sshd |
| | User Manager(관리자 계정 및 그룹 관리) | N/A |
| | User Setting(자신의 계정에 대해 기본 값 변경) | N/A |
| | Cert Manager(인증서 및 인증서 폐지목록 관리) | N/A |
| | Routing(게이트웨이 관리, 고정 라우팅 관리 등) | N/A |
| Interface | WAN(외부망 접점 인터페이스 관리)<br>LAN(내부망 접점 인터페이스 관리)<br>OPTx(DMZ 등 영역별 인터페이스 관리) | 1) Assign Interface |
| | WAN(외부망 접점 인터페이스 관리)<br>LAN(내부망 접점 인터페이스 관리)<br>OPTx(DMZ 등 영역별 인터페이스 관리) | 2) Set interfaces(s) IP address<br>- 네트워크 인터페이스에 IP주소 할당<br>- anti-lockout rule 적용으로 잠금 처리된 WebGUI 계정에 대해 잠금해제 |
| 침입차단 | Aliases(IP주소/네트워크/포트 그룹핑 및 별칭 부여) | N/A |
| | NAT(port forwards, Outbound NAT 관리) | N/A |
| | Rules(정보흐름통제규칙) | N/A |
| | Schedules(정보흐름통제규칙 적용 시간대 관리) | N/A |
| Service | NTP<br>(시각정보 동기화를 위한 NTP 프로토콜 설정관리) | N/A |
| | SNMP(SNMP 프로토콜 설정 관리) | N/A |

| 구분 | WebGUI | 콘솔(CLI) |
|---|---|---|
| Status | Dashbord<br>(정보흐름통제규칙 적용 현황, 시스템 기본정보 표시) | N/A |
| | Gateways(게이트웨이 상태정보 표시) | N/A |
| | Monitoring<br>(CPU 및 메모리 사용량, 네트워크 사용량, firewall states 등 정보 표시) | N/A |
| | NTP(NTP 데몬 상태 표시) | N/A |
| | Services(시스템 데몬 상태 표시) | N/A |
| | System logs<br>(firewall 등 서비스 로그, 시스템 로그 표시) | 10) Filter Logs<br>(WebGUI 보다 상세 정보를 포함하고 있으나 가공하지 않은 firewall log 화면출력) |
| Diagnostics | Backup & Restore<br>(환경설정 파일 백업 및 복원) | 15) Restore recent configuration |
| | Comman Prompt<br>(쉘 명령어/PHP 코드 실행, 파일 업로드/다운로드) | 8) Shell<br>12) Developer Shell |
| | Factory defaults<br>(초기 설치 시 기본 환경설정 값으로 리셋) | 4) Reset to factory defaults |
| | Halt system<br>(firewall 시동종료, 전원 끄기) | 6) Halt system |
| | pfInfo<br>(패킷 관련 통계정보 표시) | N/A |
| | pfTop<br>(정보흐름통제규칙 적용률, 허가된 데이터 크기, 트래픽 처리속도, 상태 표 및 관련 통계정보 표시) | 9) pfTop |
| | Ping<br>(목표 IP주소로 ICMP echo 요청) | 7) Ping host |
| | Reboot system<br>(firewall 재부팅) | 5) Reboot system |
| | States<br>(현재 활성화된 firewall states 표시) | N/A |
| | States Summary<br>(상태 표에 대한 정보 표시) | N/A |
| | System Activity<br>(메모리 사용량, 실행중인 프로세스 목록 표시) | N/A |
| | Tables<br>(WebGUI 로그인 시도횟수를 초과한 클라이언트, SSH 로그인 시도횟수를 초과한 클라이언트) | N/A |
| | Test Port<br>(TCP 연결 테스트) | N/A |

| 구분 | WebGUI | 콘솔(CLI) |
|---|---|---|
| | N/A | 3) Reset webConfigurator password<br>- admin 기본계정 재생성 또는 재활성화<br>- admin 기본계정 패스워드 초기화 |
| | | 11) Restart webConfigurator<br>(웹서버 데몬 재시작) |
| | | 16) Restart PHP-FPM<br>(웹 서버 데몬을 위한 PHP 프로세스 중지/재시작) |

## 7.4.2. 관리자 계정 및 보안역할 관리

### 7.4.2.1. 관리자 계정 및 그룹 관리

TOE는 계정을 관리하도록 다음과 같은 정보를 갖는 관리자 계정 또는 그룹을 추가/수정/비활성화/활성화하는 관리수단을 제공한다.

| 구분 | 계정 연관정보 | 설명 |
|---|---|---|
| 관리자 계정 | Disabled 체크박스 | ◆ 관리자 계정 활성화/비활성화 여부 |
| | Username | ◆ 관리자 식별정보(로그인 시 ID)<br>◆ 16자 이하 설정(문자, 숫자, 일부 특수문자(“.”, “-”, “_”) 만 허용) |
| | 패스워드 | ◆ 관리자 인증데이터(로그인 시 패스워드) |
| | Full name(선택 사항) | ◆ 관리자 계정에 대한 설명 등 보충설명 |
| | Expiration Date | ◆ 계정 유효기간(기간 경과 시 자동으로 비활성화 처리) |
| | Group Memberships | ◆ 해당 관리자 계정이 소속된 그룹명 |
| | Effective Privileges | ◆ 해당 관리자 계정에 부여할 보안역할 |
| | Certificate | ◆ 인증서 생성/등록(인증서 이름, 인증기관, 키길이, 유효기간 등) |
| | Authorized Keys | ◆ SSH 접속 시 필요한 SSH 공개 키 |
| | 관리단말 IP주소 | ◆ SSH 접속 시 허용되는 단말 IP주소(최대 2개. 단, 주소 범위로 설정 불가능) |
| 관리자 그룹 | Group name | ◆ 관리자 그룹 식별정보<br>◆ 16자 이하 설정(문자, 숫자, 일부 특수문자(“.”, “-”, “_”) 만 허용) |
| | Scope | ◆ 로컬그룹/관리접속 그룹 |
| | Description(선택 사항) | ◆ 그룹 설명 |
| | Group Memberships | ◆ 그룹 구성원(관리자 계정) |
| | Assigned Privileges | ◆ 할당되어 있는 보안역할(특권) |

관리자가 접속할 수 있는 IP주소 등록은 관리자 계정 생성 시 SSH Authorized Key를 등록하는 과정에서 함께 설정하며 이에 대한 값은 SSH 환경설정 파일에 저장된다.

### 7.4.2.2. 관리자 패스워드 관리

TOE 설치 시 기본 값으로 설정된 관리자 패스워드 값을 관리자 WEB-GUI 또는 SSH-CLI 관리수단을 활용하여 인가된 관리자는 관리자 패스워드를 변경할 수 있다. 신규 입력된 패스워드가 최소 4조합 9자리 이상인지 여부를 검증하고, 기존 패스워드와 동일하거나 추측하기 쉬운 패스워드인지 여부를 검증한다. 패스워드 검증조건에 만족하는 경우 패스워드는 SHA 256 해시 값으로 변환되어 환경설정 파일에 저장된다.

### 7.4.2.3. 인증서 및 CRL 관리

WebGUI에서 HTTPS 세션연결 시 관리자 패스워드 인증방식 외에 TLS 상호인증을 추가적으로 수행하고자 하는 경우 관리자 계정 생성에서 인증서를 생성한다. 또한 이미 생성된 관리자 계정에 대해서도 TLS 상호인증 방식을 추가할 수 있으며 관리자 계정 수정 메뉴에서 기 생성된 인증서를 선택하거나 인증서를 생성할 수 있다.

TOE는 WebGUI의 HTTPS 연결 시에 사용하는 인증서를 관리할 수 있도록 인증서 추가, 수정, 내보내기 또는 삭제 등 인증서 관리 기능을 인가된 관리자에게 제공한다.

| 인증서 관리 | 설명 |
|---|---|
| 인증서 추가 | 다음 3가지 중에서 한가지 방법을 선택<br>◆ 기 발급된 인증서 가져오기 : 인증서 발급일, *.crt, *.key 파일 가져오기<br>◆ 내부 자체 인증서 생성 : CA, 키길이(기본 값 : 2048), 메시지 축약 알고리즘(기본 값 SHA 256), 인증서 유형(HTTPS Server 등 서버 인증서, 인증기관 루트 인증서), 유효기간(기본 값 : 3650일), DN<br>◆ 인증서 서명 요청서 생성 : 자체 생성한 인증서에 대해 외부 인증기관에게 서명 요청 |
| 인증서 내보내기 | PKCS#12 파일 또는 *.crt 파일 및 *.key 파일 쌍 형태로 파일 다운로드 |
| 인증서 제거 | 인증서 목록에서 인증서 삭제 및 관련 데이터 삭제 |

인증서 유효성을 검증하는 과정에서 인증서 유효기간 경과여부와 함께 인증서취소목록(CRL)에 등록된 인증서 인지 여부를 확인하여야 하므로 TOE는 WebGUI에서 CRL 관리 기능을 인가된 관리자에게 제공한다. 인증서취소목록 관리 기능은 인증서 관리 기능(CRL 생성, 내보내기, 가져오기, 폐기)과 유사하다. 인증서가 더 이상 유효하지 않으면 관리자는 해당 인증서를 CRL에 등록하여 인증서를 폐기한다.

#### 7.4.2.4. 보안역할(특권) 관리

관리자 계정 생성 시에 다음과 같은 미리 정의된 보안역할(특권)을 할당하며 관리가 계정 관리 기능을 통해 보안역할(특권)을 추가/삭제 및 관리자 계정 비활성화를 할 수 있다.

| 관리수단 | 특권(Privilege) | 설명 |
|---|---|---|
| WebGUI | WebCfg-All Pages | ◆ WebGUI에서 제공하는 모든 메뉴에 대한 접근권한 |
| | WebCfg-Dashboard(all) | ◆ TOE 대시보드에 대한 접근권한 |
| | WebCfg-System | ◆ 패스워드 관리 페이지에 대한 접근권한을 가짐<br>(계정 소유자 자신의 패스워드만 변경) |
| CLI | User-System-Shell account access | ◆ SSH을 통한 CLI 로그인 권한 |
| | User-System-Copy files | ◆ SSH을 통한 CLI 로그인 후 CLI 파일전송 명령어 접근권한 |
| | User-System-all | ◆ “root” 기본계정이 가진 모든 권한 |
| 환경설정 파일 | User-Config-Deny Config Write | ◆ 환경설정 파일(config.xml) 접근이 거부되어 있는 권한 |

CLI 관련 특권은 관리자 계정 생성 시 SSH Authorized Key를 등록하는 과정에서 함께 설정하며 이에 대한 값은 SSH 환경설정 파일에 저장된다.

### 7.4.3. TSF 보안관리

#### 7.4.3.1. SSH 데몬 관리

원격에서 CLI에 접속하기 위해서는 SSH 데몬을 활성화하여야 하며 관리자는 WebGUI 또는 CLI에서 SSH 데몬을 활성화/비활성화시킬 수 있다. SSH 데몬 동작과 관련하여 관리자가 설정할 수 있는 값은 다음과 같다.

| 관리행위 | 설명 |
|---|---|
| 활성화/비활성화 선택 | ◆ SSH 데몬 활성화/비활성화 여부 |
| SSH-CLI 로그인 허용 계정 관리 | ◆ 관리자 계정 중에서 SSH를 이용한 CLI 로그인을 허용할 계정을 선택 |
| SSH 포트 | ◆ 22번 포트번호를 다른 포트번호로 변경 |

#### 7.4.3.2. WebGUI 관리접속 차단 해지 기능(Anti-lockout) 관리

인가된 관리자는 Anti-lockout 기능을 활성화할 수 있다. Anti-lockout 기능이 활성화되면 외부망이 아닌 내부망에서 관리인터페이스에 접속하는 경우 모든 접속을 허용하게 된다. 외부망에서 접속을 차단하고 내부망에서도 일부 대역(관리전용 내부망)의 특정 단말에서만 접속을 허용하게 하려면 인가된 관리자는 TOE LAN 인터페이스에 대한 정보흐름통제규칙을 추가할 수 있다. 내부 관리망이 아닌 다른 내부망에서 관리인터페이

스에 접속하지 못하도록 하려면 관리포트(443, 22) 별칭 및 관리호스트 별칭을 생성하고 이를 활용하여 TOE LAN 인터페이스에 대한 규칙을 추가함으로써 관리인터페이스 접근을 제한할 수 있다. 즉, SSH 및 HTTPS 접속 시에만 관리 인터페이스에 대한 접근을 허용하도록 하고 이외의 경우 모두 차단하도록 관리포트 Alias를 생성하고 관리 인터페이스에 접속할 수 있는 내부 관리호스트 Alias를 생성한다. 출발지를 내부 관리호스트 Alias하고 목적지 LAN 인터페이스 IP주소에 목적지 포트를 관리포트 Alias로 지정한 인바운드 허용규칙을 추가한다. 또한 ANY 출발지에서 목적 LAN 인터페이스 IP주소에 목적지 포트를 관리포트 Alias로 지정한 인바운드 거부규칙을 추가한다. 거부규칙 보다 허용규칙이 먼저 적용되도록 규칙 순서를 조정한다. 이렇게 Alias 생성과 LAN 인터페이스에 대한 인바운드 규칙을 추가하여 관리자 관리접속 IP주소를 관리할 수 있다. 이 경우에는 관리접속 IP주소를 특정 주소로 지정해야 하며 범위로 설정할 수 없다.

### 7.4.3.3. 감사기능 관리

관리자는 WebGUI에서 모든 이벤트에 대해 공통으로 적용되는 다음과 같은 로그 기능을 관리할 수 있다. 다만, 이벤트 종류별로 별도 설정 값이 존재하는 경우 공통설정 부분은 무시되고 별도 설정된 값이 적용된다. 예를 들어 일반 공통 설정 부분에서 Forward Display를 설정하더라도 firewall 기능 설정에서 로그 관련하여 Reverse Display로 설정하면 실제 firewall 관련 감사기록 조회 시 최근 사건부터 화면에 표시된다.

| 구분 | 로그 기능 관리 | 설정 값/관리 행위 |
|---|---|---|
| 일반 공통 | Forward/Reverse Display | ◆ 로그조회 시 오래된 사건부터 화면에 표시(기본 값)<br>◆ 로그조회 시 최근 사건부터 화면에 표시 |
| | GUI Log Entries | ◆ 화면에 표시되는 감사기록 건 수(기본 값 : 50) |
| | log filtering | ◆ 검색어 등에 따른 고급 검색기능(기본 값 : 비활성화) |
| | Log File Size(Bytes) | ◆ clog 파일 크기(기본 값 : 500KB으로 약 2500건의 감사기록 저장) |
| | Log Packets from Default Block Rules | ◆ 정보흐름통제규칙에 일치하지 않아 차단된 패킷에 대한 감사기록 여부 (기본 값 : 활성화) |
| | Log Packets from Default Pass Rules | ◆ 정보흐름통제규칙에 일치하여 허용된 패킷에 대한 감사기록 여부 (기본 값 : 비활성화) |
| | Web Server Log | ◆ 관리 WEB GUI 수행 등 웹서비스 수행 결과 기록 여부 |
| | Potential violation detection condition | ◆ 잠재적 보안 위반으로 탐지하기 위한 감사대상 사건 누적 회수 설정<br>◆ 잠재적 보안 위반으로 탐지하기 위한 정보흐름통제규칙 적용 결과 조합<br>◆ 잠재적 보안 위반으로 탐지하기 위한 관리접속을 통해 접근한 중요 관리메뉴 선택 및 조합 |
| | Warning Message e-mail send | ◆ 경고메시지 수신 이메일 주소<br>◆ 경고메일 발송 대상 사건 선택 |
| | Reset Log File | ◆ 로그파일에 기록된 감사기록 내용 삭제 |

관리자는 WebGUI에서 syslog 전송 기능의 동작과 관련하여 다음과 같은 값을 설정할 수 있다.

| syslog 관련 설정 값 | 설명 |
|---|---|
| 출발지 주소 | syslog 데몬이 메시지를 내보내는 콘솔이 설치되어 있는 주소<br>(기본 값 : any) |
| IP 프로토콜 | syslog 파일 전송에 사용되는 인터넷 프로토콜(IPv4) |
| 원격 로그서버 | ◆ 원격 로그서버의 IP주소 또는 호스트 명과 포트번호(옵션)<br>- 최대 3대 서버 주소까지 설정 가능<br>- 포트번호를 생략하는 경우 514 포트 적용 |
| 로그 전송 대상 | ◆ Everything<br>◆ System Event<br>◆ Firewall Event<br>◆ Captive Portal Event<br>◆ Gateway Monitor Event<br>◆ Network Time Protocol Event |

## 7.4.4. TSF 데이터 관리

### 7.4.4.1. 동작 상태정보 조회

인가된 관리자는 TOE의 정상동작 상태를 파악하기 위해 네트워크 인터페이스 및 데몬의 상태정보를 조회할 수 있다.

| 상태정보 종류 | 설명 |
|---|---|
| Gateways | TOE에 설정된 게이트웨이 상태 정보<br>◆ 게이트웨이 IP주소<br>◆ 게이트웨이 RTT(지연시간)<br>◆ 패킷 손실율<br>◆ 동작 상태(온라인, 경고, Down, 정보 수집 중 등) |
| Interface Statistics | TOE의 네트워크 인터페이스 통계정보<br>◆ 인터페이스별 유입/송출 패킷, 바이트, 오류 횟수 |
| Interfaces | TOE의 네트워크 인터페이스 정보<br>◆ 인터페이스별 유형 및 이름, IP주소, 인터페이스 활성화 상태(UP/DOWN), 속도 |
| Service Status | ◆ 각 데몬의 동작 상태(실행/중지) |
| System Information | ◆ Name : TOE 명칭<br>◆ Version : TOE 현재 버전 정보(버전 및 하부 플랫폼 버전, 설치 시간)<br>◆ Platform : TOE 실행에 필요한 SW<br>◆ Uptime : 최근 부팅 시간<br>◆ Current date/time : time zone, 현재 날짜 및 시간<br>◆ Last config change : 최근 환경설정 변경 일<br>◆ State tabl size : 상태기반 필터링을 위한 상태 표 최대 크기<br>◆ CPU/Memory/Disk 사용량 |
| NTP Status | ◆ NTP 서버 및 시간 |

## 7.4.5. 보안속성 관리

### 7.4.5.1. 정보흐름통제규칙(firewall rule) 관리

관리자는 WebGUI에서 인터페이스에 적용되는 정보흐름통제규칙(firewall rule)을 추가, 수정, 삭제, 활성화/비활성화할 수 있으며 적용 순서를 변경할 수도 있다. 관리자가 추가 또는 수정할 수 있는 보안속성은 다음과 같다. 정보흐름통제규칙은 제한적인 기본 값을 가지며 관리자는 이러한 기본 값을 초기 값으로 명시하여 기본 값을 대체할 수 있다. 제한적인 기본 값이란 출발지/목적지 주소 및 포트를 특정하고 일치하는 경우에만 해당 규칙을 허용/차단/거부 시킨다.

| 기본 보안속성 | 설명 |
|---|---|
| 프로토콜 | IPv4 TCP/UDP, IPv4 ICMP 등 네트워크 프로토콜 구분 |
| ICMP type | 프로토콜이 ICMP인 경우 ICMP type 값(any, ping) |
| 출발지 | 호스트 IP주소, 별칭 이름, 네트워크 대역, 인터페이스 주소, 인터페이스 명칭 등 |
| 출발지 포트 | 프로토콜이 TCP/UDP인 경우 서비스를 의미하는 포트 번호(1~1024, 1024~65535) |
| 목적지 | 호스트 IP주소, 별칭 이름, 네트워크 대역, 인터페이스 주소, 인터페이스 명칭 등 |
| 목적지 포트 | 프로토콜이 TCP/UDP인 경우 서비스를 의미하는 포트 번호(1~1024, 1024~65535) |
| 큐 | 유입되는 트래픽에 대해 floating rule의 ‘match’ action이 적용되면 허용/거부/차단을 일시 보류하고 큐에 저장 |
| 스케쥴 | 날짜, 요일, 시간(분단위)에 따라 해당 규칙을 자동 적용하도록 설정 |
| Action | 허용(Pass)/차단(Block)/거부(reject) 등 패킷을 처리하는 방식 |

트래픽이 발현된 인터페이스에서만 트래픽을 필터링할 수 있다. 정보흐름통제규칙에서 명세하는 인터페이스는 해당 규칙으로 통제하려는 트래픽을 수신하는 인터페이스를 의미한다. 따라서 정보흐름통제규칙(firewall rule)은 인터페이스별로 구성된다. 예를 들어 WAN에 적용되는 정보흐름통제규칙과 LAN에 적용되는 정보흐름통제규칙은 구분되어 있으므로 관리자는 먼저 어떤 인터페이스에서 처리되는 트래픽에 적용하는 규칙을 관리할지를 결정해야 한다. 다만, 출발지 및 목적지 보안속성 값이 물리적 네트워크 인터페이스(WAN, LAN), 가상 네트워크 인터페이스, 인터페이스 그룹 등인 경우 TOE를 통과하는 패킷이 아니라 TOE가 목적지이거나 출발지인 패킷을 의미한다.

관리자는 WebGUI에서 정보흐름통제규칙이 적용되는 시간대를 날짜, 요일, 시분 단위로 지정할 수 있다. 예를 들어 게임사이트 등과 같이 업무에 관계없는 사이트에 대해 근무시간에서 접속을 차단하고 근무시간 외에는 접속을 허용하도록 규칙을 정해진 시간대에 따라 적용여부를 자동으로 변경할 수 있다.

관리자는 WebGUI에서 정보흐름규칙마다 감사기록 생성 여부를 설정하고 생성된 감사기록을 원격 로그 서버로 즉시 전송할지 여부도 설정할 수 있다. 감사레코드에 기록될 정보는 관리자가 조정할 수 있다. 정보흐름통제규칙(firewall rule)의 변경이력이 기록되며 조회 가능하다. 변경이력에 기록되는 정보는 변경 일시(년월일 및 시분초), 변경한 주체 식별정보, 변경작업을 요청한 호스트 IP주소, Action(생성/갱신/삭제)이다.

관리자는 WebGUI에서 상태기반 감시 메커니즘의 운영모드 및 고급 보안속성을 설정할 수 있다. 상태기반 감시 메커니즘의 운영모드에 대한 상세내용은 “7.2.1.2 상태기반 감시 메커니즘”을 참조한다. 고급 보안속성은 규칙을 신규로 생성하는 것이 아니라 기존의 패킷 필터링 정보흐름통제규칙에 대해 규칙 마다 추가 설정할 수 있는 값이다.

| 고급 보안속성 | 설명 |
|---|---|
| Max state | 해당 규칙에서 수용할 수 있는 전체 최대 연결 개수 |
| Max number hosts | 해당 규칙으로 동시 연결될 수 있는 전체 출발지 IP주소 개수 |
| Max number connections | 호스트 하나에 Fully TCP 연결을 허용하는 최대 개수 |
| Max new connections | 상태 표가 허용된 메모리 용량을 초과하지 않도록 TCP 연결 비율을 제한 |
| state idle timeout | 트래픽이 없어도 TCP/UDP 연결을 종료하지 않고 유지할 수 있는 최대 시간 |
| TCP Flag | 정상 TCP 연결상태를 체크하기 위한 TCP 플래그 값<br>(Any/SYN/ACT/FIN/RST/PSH/URG) |
| State Type | 상태정보 추적 옵션(Keep/Sloppy State/Synproxy/None) |
| Satte Timeouts | TCP/UDP 프로토콜 및 ICMP 프로토콜에서 상태 값을 갖는 연결을 기다리는 시간을 초단위로 조정<br>- TCP First, TC Opening, TCP Established, TCP Closing, TCP FIN Wait, TCP Closed<br>- UDP First, UDP Single, UDP Multiple<br>- ICMP First, ICMP Error |
| Firewall Maximum States | 상태 표에서 상태정보를 유지할 수 있는 최대 연결 개수(기본 값 : RAM 크기의 10%, RAM 1MB 크기에 1,000개 연결 상태가 유지될 수 있으며 RAM의 최대 50%까지 설정 가능함) |
| Firewall Adaptive Timeouts | 상태 표에 할당된 메모리가 임계치(Firewall Maximum States)에 가까워 졌을 때 State 처리량을 적정수준까지 감소시켜 통제하는 방법으로 적정수준을 자동계산하여 결정<br>- Adaptive Start : adaptive 스케일링을 시작하게 되는 임계치 (기본 값: Firewall Maximum States의 60%)<br>- Adaptive End : 상태 표에 기록된 모든 상태들을 즉시 purge시키는 상태 표 임계치 (기본 값: Firewall Maximum States의 120%)<br>- 계산 식 : {(Firewall Maximum States*Adaptive End) - 현재 상태 표 크기}/ {(Firewall Maximum States*Adaptive Start) - 현재 상태 표 크기} * 100 |
| Gateway | 해당 규칙에 일치하는 트래픽에 적용될 게이트웨이 또는 게이트웨이 그룹 설정 |

관리자가 WebGUI의 대시보드에서 침입차단 기능의 상태정보를 종합적으로 모니터링할 수 있다.

| 상태정보 종류 | 설명 |
|---|---|
| Firewall States | ◆ 정보흐름통제규칙이 적용되는 패킷이 유입되고 나가는 인터페이스<br>◆ TCP/UDP/ICMP/ESP 등과 같은 프로토콜 종류<br>◆ 출발지 및 목적지 주소 및 포트번호<br>◆ SYN, SYN+ACK, ACK 등과 같은 TCP 프로토콜 상태 값<br>◆ 규칙에 적용되어 처리되고 있는 패킷 수<br>◆ 규칙에 적용되어 처리되고 있는 전체 패킷 용량 |
| State table | ◆ SYN_SENT : TCP 핸드쉐이크에서 TCP SYN 패킷이 보내진 상태<br>◆ CLOSED : 연결종료 또는 트래픽이 발생하지 않는 상태<br>◆ ESTABLISHED : 한쪽 TCP 연결이 성립되어 있는 상태<br>◆ TIME_WAIT/FIN_WAIT : TCP 연결을 종료하고 있는 상태<br>◆ NO_TRAFFIC : 수신되는 패킷이 없는 상태<br>◆ SIGNLE : 단일 패킷만 관찰된 상태<br>◆ MULTIPLE : 다중 패킷들이 관찰되고 있는 상태<br>◆ ESTABLSIHED:ESTABLISHED : TCP 양방향 연결이 모두 성립된 상태<br>◆ SYN_SENT:CLOSED : TCP SYN 패킷을 보냈으나 응답을 받지 못한 상태<br>◆ SINGLE:NO_TRAFFIC : UDP 프로토콜 등에서 응답을 받지 못한 상태<br>◆ SINGLE:MUTIPLE : UDP 프로토콜 등에서 1개 전송 패킷에 대해 다중 패킷을 수신하는 상태(예, DNS 질의 응답)<br>◆ MULTIPLE:MULTIPLE : UDP 프로토콜 등에서 다중 패킷이 송수신되고 있는 상태<br>◆ 0:0 : ICMP 프로토콜의 패킷이 처리되는 상태 |

### 7.4.5.2. NAT 규칙관리

관리자는 WebGUI에서 Port Forward NAT 규칙, OutBound NAT 규칙, 1:1 NAT 규칙을 다음과 같이 관리할 수 있다.

| NAT 종류 | 관리 행동 |
|---|---|
| Port Foward (Inbound NAT/ Destination NAT) | ◆ Disabled : 활성화/비활성화<br>◆ No RDR : 해당 규칙에 일치하는 경우 어떠한 리다렉션도 수행하지 않음<br>◆ Interface : Port Forward가 활성화되는 인터페이스<br>◆ Protocol : TCP/UDP<br>◆ Source : 해당 규칙에 접근할 수 있는 출발지 IP주소 및 포트를 제한(일반적인 경우 외부 인터넷으로부터 들어오는 모든 트래픽에 대해 Port Forward를 적용하므로 “any” 값이 설정됨)<br>◆ Destination : 전달될 트래픽이 초기에 설정되었던 목적지(일반적인 경우 WAN 주소가 설정됨)<br>◆ Destination port range : 원래 목적지 포트<br>◆ Redirect target IP : 변환 주소지<br>◆ Redirect target port : 변환 포트번호<br>◆ Filter Rule Association : 정보흐름통제규칙(firewall rule)에 연관 규칙 자동 추가여부를 설정 |

| NAT 종류 | 관리 행동 |
| --- | --- |
| Outbound NAT (Source NAT) | ◆ Disabled : 활성화/비활성화<br>◆ Do not NAT : 해당 규칙에 일치하는 경우 해당 패킷이 나갈 때 NAT가 적용되지 않음(일반적으로 예외 적용이 필요한 경우 설정)<br>◆ Interface : 트래픽이 인터페이스를 나갈 때 NAT 규칙이 적용되는 인터페이스(일반적으로 “WAN”으로 설정됨)<br>◆ Protocol : NAT를 적용할 프로토콜을 지정(일반적으로 모든 트래픽에 적용하므로 “anu”으로 설정됨)<br>◆ Source : 인터페이스를 나갈 때 변환될 로컬 네트워크(일반적으로 LAN, DMZ 설정됨)<br>◆ Destination : 인터페이스를 나가는 트래픽은 어디든 갈 수 있으므로 일반적으로 “any”로 설정됨<br>◆ Translation : 해당 규칙에 일치하면 변환될 출발지 주소(일반적으로 WAN IP주소로 변환됨)<br>◆ Port : 변환될 포트번호를 설정(일반적으로 공란으로 남겨 둠)<br>◆ Static Port : 출발지 주소가 변환된 이후에도 포트번호는 유지해야 하는 경우 원래 포트 번호 지정 |
| 1:1 NAT | ◆ Disabled : 활성화/비활성화<br>◆ Interface : 1:1 NAT 변환이 발생하게 되는 인터페이스<br>◆ External subnet IP : 인터페이스로 들어오거나 나갈 때 변환될 공인 IP주소(일반적인 경우 WAN 인터페이스 주소가 됨)<br>◆ Internal IP : External subnet IP주소로 변화될 방화벽 뒤에 있는 내부 사설 IP주소<br>◆ Destination(선택) : 내부 IP주소에서 특정한 주소로 나갈때에만 1:1 NAT를 적용하거나 목적지에서 External subnet IP주소로 나갈때에만 1:1 NAT를 적용하고자 할 때 목적지 IP주소를 지정<br>◆ Filter Rule Association : 정보흐름통제규칙(firewall rule)에 연관 규칙 자동 추가 여부를 설정 |

# 7.5. 보안감사

## 7.5.1. 로그생성 및 보존

일반적으로 다음과 같은 감사대상 사건에 대해 로그가 생성되며 SFR에 관련된 감사대상 사건은 “6.2.1.2 FAU_GEN.1 감사데이터 생성”에 열거한 바와 같다. 로그 생성 시 기록되는 정보는 기본적으로 사건발생 시각(년, 월, 일, 시분초), 주체 식별자, IP주소, 사건유형, 성공/실패 등이며 다음과 같이 사건유형에 따라 추가 기록되는 정보들이 있다.

| 사건 유형 | 감사대상 사건 | 추가기록 감사레코드 |
|---|---|---|
| system | 감사기능 시동 및 종료 | ◆ 없음 |
| | 감사 저장소 관련 대응 행동 | ◆ 없음 |
| | 잠재적 보안위반 탐지시 대응 행동 | ◆ 적용된 위반탐지 조건 |
| | 관리자 로그인 및 로그아웃 | ◆ 관리자 계정명 |
| | 관리자 인증 연속실패 시 대응 행동 | ◆ 실패 누적 횟수 |
| | 관리자 비활동 기간 경과 시 대응 행동 | ◆ 세션 잠금 원인 |
| | 보안관리 기능을 이용한 기능 관리 행동 | ◆ 변경 이전 값, 변경된 값<br>◆ 관리자가 접근한 관리 메뉴 명칭 |
| | 암호키 생성/가져오기, 변경, 삭제 등 | ◆ 키 용도, 키 명칭 |
| | 암호 연산의 성공과 실패 | ◆ 암호 연산 유형 |
| | 패스워드 재설정 | ◆ 변경한 관리자 계정명, 변경대상 계정명 |
| | HTTPS 관리접속 시 통신보안 프로토콜 성공과 실패 | ◆ TLS 버전 |
| | NTP 서버, Syslog 서버 등과 정상 연동 검사 | ◆ 시험대상 외부 실체 식별 정보 |
| | 프로세스/데몬 시작 및 종료 | ◆ 프로세스/데몬 명칭 |
| firewall | 정보흐름통제규칙에 설정된 값에 따라 해당 규칙에 매칭되는 경우 | ◆ 출발지 IP주소 및 포트<br>◆ 목적지 IP주소 및 포트<br>◆ 프로토콜 |
| | 상태 기반 감시 필터링에 따라 폐기된 트래픽 | ◆ 상태정보(TCP 플래그 값) |
| | 상태 표 메모리 임계치 초과 | ◆ RAM 크기<br>◆ Firewall Adaptive Timeouts<br>◆ Firewall Maximum States |

생성된 감사기록은 파일시스템에 clog 파일 형식으로 저장되며 clog 파일 크기는 고정이므로 파일 용량을 초과하는 경우 해당 파일을 관리자가 지정한 경로에 자동백업한 후 오래된 감사기록을 덮어쓰기 한다. 따라서 감사기록을 일정기간 보존해야 하는 조직의 정책을 유지할 수 있도록 원격 로그서버로 감사기록을 전송할 수 있는 TLS 기반 syslog 전송기능을 지원한다. clog 파일 용량이 80%를 초과하는 경우 관리자 이메일로 경고메시지를 발송하고 syslog 서버로 로그전송을 시작한다.

로컬 하드디스크에 저장된 감사기록 파일은 관리자라도 수정/삭제가 불가능하다..

## 7.5.2. 로그 조회

관리자는 WebGUI에서 사건 유형별로 감사기록 조회가 가능하다. 조회 시 사건발생일시(오래된 순서/최신 순서)를 기준으로 정렬이 가능하며 고급검색 조건에서 사건 유형별로 지원되는 검색어 종류가 다음과 같다. 검색어는 단어, 구문 형태로 입력 가능하며 감사레코드 기록 형식을 고려한 정규표현식을 입력하여도 조회 가능하다.

| 사건 유형 | 정렬 기준 | 검색어 |
|---|---|---|
| system log | 사건발생일시<br>(월일 및 시분초) | ◆ 시간(월단위 선택)<br>◆ 프로세스/데몬 이름<br>◆ 프로세스 ID(PID)<br>◆ 검색결과 표시 건수 |
| firewall log | 사건발생일시<br>(월일 및 시분초) | ◆ 출발지 IP주소<br>◆ 목적지 IP주소<br>◆ 허용<br>◆ 차단<br>◆ 인터페이스<br>◆ 출발지 포트<br>◆ 목적지 포트<br>◆ 프로토콜<br>◆ 프로토콜 플래그(예, SYN+ACK, FIN+ACK 등) |

정보흐름통제규칙에 적용되어 생성된 로그에 대해서는 CLI에서 조회 가능하나 이해할 수 없는 형태의 law 데이터 형식으로 저장되므로 이러한 기능에 대해서는 보안요구사항으로 도출하지 않았다.

## 7.5.3. 로그 분석 및 보안경고

다음 사건의 경우 1건이라도 발생하는 경우 관리자에게 경고메일을 발송한다.

- 감사기록 저장소의 임계치 초과 시 대응행동 실패
- 감사기록 저장소 공간 부족에 따른 대응행동 실패
- 상태 표 메모리 임계치 초과
- TSF 및 TSF 데이터 무결성 검증 실패
- SSH Authorized Key 설정 변경

다음의 감사대상 사건 발생 횟수가 관리자가 지정한 누적 횟수를 초과하는 경우 잠재적 위반사건으로 탐지하고 이에 대해 관리자에게 사건 유형 및 해당 로그기록을 이메일 본문에 담아 경고메일을 발송한다.

- 동일 ID에 대해 누적된 인증 실패 회수가 관리자가 지정한 누적 회수 이상인 경우
- TLS Cipher Suite 변경 회수가 관리자가 지정한 누적 회수 이상인 경우
- 관리자가 지정한 관리메뉴 접근이 관리자가 지정한 누적 회수 이상인 경우

다음의 감사대상 사건들을 관리자가 지정한 조합 규칙에 의해 연관 분석한 경우 잠재적 위반사건으로 탐지하고 이에 대해 관리자에게 사건 유형 및 해당 로그기록을 이메일 본문에 담아 경고메일을 발송한다.

- 관리자가 지정한 정보흐름통제규칙에 적용되어 통과된 패킷들에 대해 관리자가 지정한 조합 규칙에 일치하는 경우

# 7.6. TSF 보호

## 7.6.1. TSF 데이터 보호

### 7.6.1.1. 관리자 패스워드 보호

TOE는 관리자 계정 생성 시 등록된 패스워드를 SHA 256으로 변환하여 환경설정 파일에 저장하고 입력받은 평문 패스워드는 변환 즉시 완전파기 한다. 따라서 패스워드는 TOE에 하드코딩되거나 평문(단순 인코딩 포함)으로 저장되지 않는다.

### 7.6.1.2. 암호키 보호

통신보안 프로토콜(SSH, HTTPS)에서 세션마다 생성되는 세션키는 메모리에 상주하며 유효기간이 경과하면 메모리에서 완전파기 된다. 또한 세션키에 접근할 수 있는 외부 인터페이스가 존재하지 않으므로 외부에서 접근이 불가능하다.

### 7.6.1.3. TOE 설정값(환경설정 파일) 보호

정보흐름통제규칙을 포함하여 인가된 관리자가 보안관리 수단(WebGUI, CLI)으로 설정한 TOE 설정값, 패스워드 해시값 등은 파일 형태로 TOE의 로컬 하드디스크에 저장된다. 환경설정 파일 변경 시 마다 해시 값을 생성하여 파일명, 파일변경 일시, 파일을 변경한 ID와 함께 별도 환경설정 해시값 파일에 저장한다. 환경설정 파일 및 환경설정 해시값 파일은 User-System-all 보안역할을 가진 인가된 관리자만이 읽기 및 쓰기가 가능하고 그룹권한은 제거된다.

### 7.6.1.4. 감사 데이터

감사 데이터가 TOE의 로컬 하드디스크에 저장되는 경우 WebGUI 또는 CLI 등 관리수단을 이용한 조회만 가능하고 파일시스템을 통해 파일에 직접 접근하여 읽기/쓰기하는 것은 제한된다.

## 7.6.2. 타임스탬프

관리자가 설정한 NTP 서버에서 NTP 프로토콜을 통해 시각정보를 가져와 동기화한다. NTP 서버는 최대 3개까지 설정 가능하다. 이때 같이 설정된 TimeZone을 고려하여 감사기록 생성 시에 타임스탬프가 기록된다.

## 7.6.3. TSF 자체 시험

### 7.6.3.1. 난수 생성 및 암호연산 기능 시험

난수 생성 및 암호연산 기능이 필수적인 TSF의 부분이므로 이들의 정확한 운영을 입증하기 위해 시동시, 정규 운영 동안 주기적(월 1회)으로 자체시험을 실행한다.
난수 생성 모듈에서 생성한 난수에 대해 NIST SP 800-90B 난수성 테스트를 실시한다. 또한 난수성 테스트를 통과한 난수를 이용하여 용도별 암호키를 생성하고 HMAC 연산, 대칭키 암호화 연산을 실행하여 정상동작 여부를 시험한다. 또한 난수성 테스트를 통과한 난수를 이용하여 인증서의 서명값을 생성 및 검증하는 연산을 실행하여 정상동작 여부를 시험한다.

### 7.6.3.2. 환경설정 파일 등 중요파일 무결성 검증 시험

TOE 설정 값, 패스워드 해시 값 등 중요 TSF 데이터가 저장되어 있는 환경설정 파일, 환경설정 파일의 해시값이 저장되어 있는 환경설정 해시값 파일, 암호키 파일 등 중요파일에 대해 생성 및 변경 시마다 HMAC 연산을 통한 해시값을 계산하여 부가한다. 시동 시와 관리자 요구 시 요구 시점에서의 파일에 대한 해시값을 계산하고 원본 해시값과 비교하여 무결성을 검증한다. HMAC 연산은 “7.2.9 암호지원”절에 명세한 바와 같이 암호모듈에서 표준에 적합한 암호연산을 수행한다.

### 7.6.3.3. BIOS 자체 시험 및 Boot loader 이미지 검증

시동 시와 정규 운영 동안 주기적(분기 1회)으로 CPU 및 메모리에 대해 known answer tests를 수행함으로써 CPU 및 메모리를 초기화하고 BIOS는 원본 이미지 체크섬과 비교하여 무결성을 검증 한다. 또한 부트 로더 이미지에 대해서도 무결성을 검증 한다. 무결성 검증은 “7.2.9 암호지원”절에 명세한 바와 같이 암호모듈에서 표준에 적합한 암호연산(해시 또는 HMAC)을 수행한다.

# 7.7. 안전한 경로/채널

## 7.7.1. 안전한 경로

TOE는 관리자가 사용하는 관리단말과 TOE 사이에 전송되는 TSF 데이터 등 중요데이터의 기밀성과 무결성을 보장하기 위해 WebGUI 연결시 TLS 1.2(RFC 5246) 및 TLS 1.3(RFC 8446)기반의 HTTPS (RFC 2818) 프로토콜을 적용하고 원격에서 CLI 연결시 SSHv2 프로토콜을 적용한다.

### 7.7.1.1. HTTPS

TOE는 TLSv1.2(RFC 5246), TLSv1.3(RFC8446) 및 HTTPS(RFC 2818)을 구현한다. TLS 클라이언트에서 SSL 3.0 이하 및 TLS v1.1 연결을 요청하는 경우 TOE는 이에 대한 연결요청을 거부한다. TLS 연결시 TOE가 지원하는 Cipher suits는 다음과 같다.

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA(RFC 3268)
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA(RFC 3268)
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256(RFC 5246)
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256(RFC 5246)
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA(RFC 4492)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA(RFC 4492)
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256(RFC 5289)
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256(RFC 5289)

관리단말에서 WebGUI에 관리접속을 하는 경우 TLS 기반 HTTPS를 이용하여 안전한 경로를 제공한다. 이에 따라 X.509 인증서(RFC 5280) 기반 서버인증을 하도록 관리자가 WebGUI에서 인증서를 생성하거나 등록할 수 있다. TOE는 HTTPS 세션연결을 위한 핸드쉐이크 과정에서 TOE가 가지고 있는 서버 인증서를 TLS 클라이언트가 실행중인 관리단말로 전송하여 서버 인증서의 유효성을 검증할 수 있게 지원한다. 인증서 체인 검증과 인증서 유효기간 확인을 모두 성공해야 HTTPS 세션연결이 성공되며 인증서 폐지 목록을 사용할 수 없거나 인증서 체인 검증에 실패하면 HTTPS 세션연결을 위한 핸드쉐이크 과정을 종료하고 TCP 연결을 끊는다. 인증서 유효기관 경과 시 인증서 폐지목록에 등록하고 관리자에게 경고메시지를 발송한다. 5회 이상 인증서 체인 검증 누적 실패 시에도 관리자에게 경고메시지를 발송한다.

### 7.7.1.2. SSH

TOE는 관리자가 원격에서 CLI에 접속할 때 안전한 경로를 제공할 수 있도록 SSH v2(RFC 4521, 4252, 4253, 4254, 5647, 5656, 6187, 6668)을 구현한다.

SSH 프로토콜은 전형적인 클라이언트/서버 구조이므로 SSH 클라이언트 프로그램이 설치되어 있는 관리단말에서 SSH 통신채널을 개시한다. 관리단말에서의 SSH 통신채널 개시 요청을 받은 TOE는 SSH 키교환 프로토콜을 통해 세션키를 설정하여 암호 통신채널을 형성한 후 SSH 사용자 인증 프로토콜을 통해 SSH 클라

이언트(CLI 접속을 요청한 관리자)를 인증한다. SSH 클라이언트 인증(사용자 인증)에 성공해야 SSH 채널이 형성된다. SSH v2는 패스워드 기반 인증, 호스트 기반 인증, 커버러스 인증, 공개키 기반 인증 등 다양한 클라이언트 인증방식을 정의하고 있으나 TOE는 공개키 기반 인증방식만 지원한다. SSH 클라이언트인증을 위한 SSH Authorized Key는 "7.2.5 보안관리"절에서 명세한 바와 같이 관리자 계정 생성 시에 관리자에 의해 등록된다.

# 7.8. 암호지원

## 7.8.1. 암호 키관리 및 암호연산

TOE는 안전한 경로를 제공하기 위해 WebGUI 연결 및 syslog 전송 시 지원되는 TLS 1.2 및 1.3은 OpenSSL 라이브러리를 이용하며 원격 CLI 연결 시 지원되는 SSH는 OpenSSH 라이브러리을 이용한다. OepnSSH 및 OpenSSL에서 처리되는 키생성 및 암호연산은 다음 표준을 준수하여 구현된 것이다.

| 기능 | 키길이 | 표준 | |
|---|---|---|---|
| FCS_CKM.1 | | | |
| RSA 키생성 | 2048 bits | FIPS PUB 186-4 | |
| DH 키생성 | Group 14 2048 bits | RFC 3526 | |
| 암호키 생성(TLS 통신용 암호키) | | | |
| AES 키생성 | 128/256 bits | RFC 5246 | |
| SEED 키생성 | 128 bits | RFC 5246 | |
| KeyedHash 키생성 | 256 bits | RFC 5246 | |
| FCS_CKM.4 암호키 파기 | | | |
| "0" 덮어쓰기 | 없음 | 없음 | |
| "난수" 덮어쓰기 | 없음 | 없음 | |
| FCS_COP.1(1) 암호 연산(대칭키 암호연산) | | | |
| AES CBC 모드 및 GCM 모드 | 128/192/256 bits | ISO 10116 | |
| AES GCM 모드 | 128/192/256 bits | ISO 19772 | |
| FCS_COP.1(2) 암호 연산(HMAC) | | | |
| HMAC-SHA-256 | 256 bits | ISO/IEC 9797-2 | |
| FCS_COP.1(3) 암호 연산(해시) | | | |
| SHA-256, SHA-512 메시지 축약 | 256/512 bits | ISO 10118-3:2004 | |
| SHA-256 메시지 확장 | 256 bits | ISO 10118-3:2004 | |
| FCS_COP.1(4) 암호 연산(전자서명 검증) | | | |
| RSA-PSS 전자서명 생성 및 검증 | 2048 bits | ISO/IEC 9796-2<br>FIPS PUB 186-4 | |
| FCS_RGB.1 난수 생성(확장) | | | |
| HASH_DRBG(SHA-256) | - | ISO/IEC 18031 | |

### 7.8.2. 암호키 파기

안전한 경로 및 안전한 채널을 제공하는 과정에서 적용되는 암호프로토콜에서 사용하는 암호키는 다음과 같으며 이들 키는 RAM 또는 Flash 메모리에만 저장되며 이들 암호키는 '0'이나 난수로 3회 덮어쓰기한다.

| 암호프로토콜 | 암호키 용도 |
|---|---|
| TLS 1.2 및 1.3 프로토콜 | SSL D-H Keys |
| | HTTPS/TLS Session encryption key |
| | HTTPS/TLS Authentication Key |
| | HTTPS/TLS Session key |
| | HTTPS/TLS Encryption Key |
| SSHv2 프로토콜 | SSH Session Authentication Key |
| | SSH Session Encryption Key |

TOE는 전용 하드웨어 잡음원 생성기를 이용하여 256비트 엔트로피를 생성하여 암호연산에 필요한 난수생성 기능을 지원한다. TOE는 암호키 및 인증서를 TOE 밖으로 내보내기 할 수 있으며 이들 암호키 및 인증서가 더 이상 필요하지 않은 경우 관리자가 WebGUI 또는 CLI에서 삭제할 수 있다. 이 경우 해당 키 파일의 내용을 "0"으로 덮어쓰기 한 후에 해당 파일을 삭제한다.

08

# 참고자료

# 8. 참고자료


| 자료 명 | 저 자 | 비 고 |
|---|---|---|
| **정보보호시스템 공통평가기준 버전 3.1 개정 2판**<br>•정보보호시스템 공통평가기준 1부 : 소개 및 일반모델, 버전 3.1r1 (CCMB-2007-09-001)<br>•정보보호시스템 공통평가기준 2부: 보안기능요구사항, 버전 3.1r2 (CCMB-2007-09-002)<br>•정보보호시스템 공통평가기준 3부: 보증요구사항, 버전 3.1r2 (CCMB-2007-09-003) | CCMB | 2007. 9 |
| 서버 공통보안요구사항 V3.0 R1 | 국가정보원 | 2023.12.5. |
| 침입차단시스템 보안요구사항 V3.0 | 국가정보원 | 2023.12.5. |
| 국가용 침입차단시스템 보호프로파일 V3.0(KECS-PP-1312-2024) | IT보안인증사무국 | 2024.6.28 |

09

# 용어 및 약어

# 9. 용어 및 약어

| | |
|---|---|
| CC | Common Criteria |
| CCMB | Common Criteria Maintenance Board |
| EAL | Evaluation Assurance Level |
| HTTPS | Hypertext Transfer Protocol over Secure Socket Layer |
| IP | Internet Protocol |
| IT | Information Technology |
| NTP | Network Time Protocol |
| SFP | Security Function Policy |
| SFR | Security Functional Requirement |
| SSH | Secure Shell |
| SSL | Secure Socket Layer |
| ST | Security Target |
| TLS | Transport Layer Security |
| TOE | Target of Evaluation |
| TSF | TOE Security Functionality |