KECS-CR-08-53

AhnLab Suhoshin Absolute v3.0 인증보고서

인증번호 : KECS-NISS-0136-2008

2008년 12월

IT보안인증사무국

제·개정 이력 현황

개정 번호	제·개정일	개정쪽	제·개정내용
00	2008.12.22	-	최초 작성

본 문서는 (주)안철수연구소의 AhnLab Suhoshin Absolute v3.0에 대한 인증보고서이다.

인증위원

행정안전부 장영환, 국가보안기술연구소 윤이중, 고려대학교 이희조,
광운대학교 유황빈, 성균관대학교 원동호, 숭실대학교 이경석,
한양대학교 송정환, 한국전자통신연구원 손승원, 한국정보보호학회 이홍섭

인증기관

IT보안인증사무국

평가기관

한국시스템보증(주)

목 차

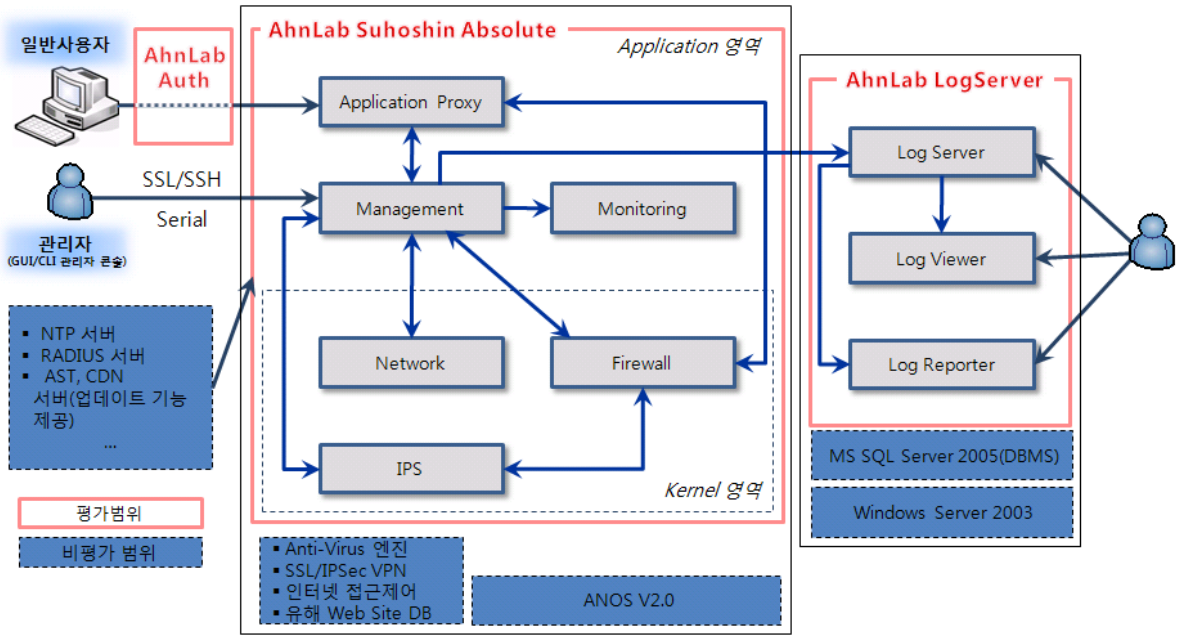
1. 요약

본 보고서는 AhnLab Suhoshin Absolute v3.0(이하 'TOE'라 한다)에 대한 정보보호시스템 공통평가기준(2008년 7월 16일 고시)(이하 '공통평가기준'이라 한다) EAL4 평가결과에 대한 인증기관의 인증결과를 서술한다. 본 보고서는 평가결과, 평가결과의 타당성 및 적합여부를 서술한다.

TOE에 대한 평가는 한국시스템보증(주)에서 수행되었으며, 2008년 12월 5일에 평가 완료되었다. 본 보고서의 내용은 한국시스템보증(주)에서 제출한 평가결과보고서의 내용에 기초하여 작성되었다. 평가는 제품이 공통평가기준 2부와 공통평가기준 3부의 요구사항을 만족하여, 공통평가기준 1부 245항에 따라 "적합"한 것으로 평가하였다.

TOE는 침입차단시스템(패킷필터링, 어플리케이션 필터링), 침입방지시스템, 안티스팸, 트래픽 제어, 시스템 격리, 안티 바이러스(anti-virus) 엔진과 연동을 통한 바이러스 차단기능 등의 네트워크 보안 기능을 수행하는 통합보안제품이다. TOE는 전용 하드웨어 플랫폼상에 구현된 네트워크 보안장비로 인터넷과 같은 외부망과 조직의 내부망을 연결하는 지점에 인라인(In-line)형태로 연결된다. 따라서, TOE는 내부 네트워크와 외부 네트워크 간에 전송되는 모든 정보를 처리한다.

TOE는 아래 [그림 1]과 같이 패킷 필터링(Packet Filtering), 어플리케이션 필터링(Application Filtering), 네트워크 주소 변환(NAT), 침입 방지(Intrusion Prevention), 악성 메일 차단, 안티 바이러스 (Anti-Virus) 엔진과의 연동 기능 등의 보안기능을 수행하는 AhnLab Suhoshin Absolute와 TOE의 감사 데이터 관리를 담당하는 AhnLab LogServer, 사용자 인증을 위한 AhnLab Auth로 구성된다.



[그림 1] TOE 구조

인증기관은 평가자의 평가활동 및 시험절차를 점검하고, 기술적인 문제점 및 평가절차에 대한 지침을 제공하고, 각 평가단위 및 평가보고서의 내용을 검토하였다.

인증기관은 평가결과가 평가제품이 보안목표명세서에 서술된 모든 보안기능 요구사항 및 보증요구사항을 만족한다는 것을 보증하고 있음을 확인하였다.

따라서, 인증기관은 평가자의 관찰사항, 평가결과가 정확하고 타당하며 평가결과가 정확하다고 인증하였다.

인증 효력범위 : 본 인증보고서에 포함된 정보는 AhnLab Suhoshin Absolute v3.0이 대한민국 정부기관에 의한 사용 승인 또는 품질보증을 의미하지 않는다.

2. 식별정보

다음 [표 1]은 평가제품 식별을 위한 정보를 나타낸다.

[표 1] 평가제품 식별정보

평가지침	정보보호시스템 평가인증지침 (2008. 7. 16.) 정보보호제품 평가인증 수행규정 (2008. 9. 1.)
평가제품	AhnLab Suhoshin Absolute v3.0
보호프로파일	침입차단시스템 보호프로파일 V2.0
보안목표명세서	AhnLab Suhoshin Absolute v3.0 보안목표명세서 Version 001 Revision 5(2008.10.17.)
평가보고서	AhnLab Suhoshin Absolute v3.0 평가결과보고서 V1.0
적합여부 평가결과	공통평가기준 2부 적합 공통평가기준 3부 적합
평가기준	정보보호시스템 공통평가기준 V3.1
평가방법론	정보보호시스템 공통평가방법론 V3.1
평가신청인	(주)안철수연구소
개발업체	(주)안철수연구소
평가자	한국시스템보증(주) 이현정, 최태경
인증담당자	IT보안인증사무국

TOE는 TOE 전용 하드웨어 플랫폼 상에서 운영된다. TOE가 운영되는 하드웨어 플랫폼 자체는 평가 대상에서 제외된다.

일반적으로, TOE가 탑재된 제품은 전용 하드웨어 플랫폼에 따라 식별된다. 각 제품별 전용 하드웨어 플랫폼의 세부사양은 다음 [표 2]와 같다.

[표 2] TOE 시스템 운영환경

TOE	모델명	요구사항
AhnLab Suhoshin Absolute	1000 R(0)	▪ CPU : Intel Pentium IV Xeon 2.8 GHz Dual ▪ RAM : 2 GB ▪ CF Memory : 2 GB ▪ NIC : 1000 Base-SX Gigabit Ethernet x 4 Ports 10/100 Ethernet x 4 Ports
	1000 R(1)	▪ CPU : Intel Pentium IV Xeon 3.4 GHz Dual ▪ RAM : 4 GB ▪ CF Memory : 2 GB ▪ NIC[기본형] : 1000 Base-SX Gigabit Ethernet x 4 Ports (Fiber) 10/100/1000 Ethernet x 4 Ports (Copper) 1000 Base-SX Gigabit Ethernet x 4 Ports (Fiber)(option) ▪ NIC[선택형] : 1000 Base-SX Gigabit Ethernet x 4 Ports (Fiber) 1000 Base-SX Gigabit Ethernet x 4 Ports (Fiber) 1000 Base-SX Gigabit Ethernet x 4 Ports (Fiber)(option)
	400 R(0)	▪ CPU : Intel Pentium IV Xeon 2.4 GHz ▪ RAM : 1 GB ▪ CF Memory : 2 GB ▪ NIC : 10/100 Ethernet x 4 ports (Copper)
	400 R(1)	▪ CPU : Intel Pentium IV Xeon 2.8 GHz ▪ RAM : 1 GB ▪ CF Memory : 2 GB ▪ NIC : 10/100/1000 Ethernet x 6 Ports (Copper) 1000 Base-SX Gigabit Ethernet x 2 Ports (Fiber)(option)
	400 R(2)	▪ CPU : Intel Pentium IV Xeon 2.8 GHz Dual ▪ RAM : 2 GB ▪ CF Memory : 2 GB ▪ NIC : 10/100/1000 Ethernet x 4 Ports 1000 Base-SX Gigabit Ethernet x 2 Ports (Fiber)(option)
	100 R(0)	▪ CPU : Intel Pentium 4 1.8 GHz ▪ RAM : 1 GB ▪ CF Memory : 2 GB ▪ NIC : 10/100 Ethernet x 4 Ports (Copper)
	100 R(1)	▪ CPU : Intel Mobile Celeron 1.2 GHz ▪ RAM : 1 GB ▪ CF Memory : 2 GB ▪ NIC : 10/100 Ethernet x 4 Ports (Copper)

TOE	항목	요구사항
AhnLab Log Server	CPU	Pentium IV 2.66 GHz 이상
	RAM	2 GB 이상
	HDD	100 GB 이상
	NIC	TCP/IP 기반 1개 이상
	운영체제	MS Windows Server 2003
	기타 소프트웨어	MS SQL 서버 2005
관리자 시스템	CPU	Pentium II 300 MHz 이상
	RAM	128 MB 이상
	HDD	2 GB 이상
	인터페이스	TCP/IP 기반 1개 이상 또는 RS-232C 시리얼 통신포트
	운영체제	MS Windows XP Service Pack 2 이상

3. 보안정책

평가제품은 아래와 같은 보안정책을 준수하여 운영된다.

P.감사 보안과 관련된 행동에 대한 책임을 추적하기 위해 보안관련 사건은 기록 및 유지되어야 하며, 기록된 데이터는 적절하게 검토되어야 한다.

P.안전한관리 TOE는 인가된 관리자가 안전한 방식으로 TOE를 관리할 수 있도록 관리 수단을 제공해야 한다.

4. 가정사항 및 범위

4.1 가정사항

평가제품은 아래와 같은 가정사항을 준수하여 설치 및 운용되어야 한다.

A.물리적보안 TOE는 인가된 관리자만이 접근 가능한 물리적으로 안전한 환경에 위치한다.

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.신뢰된관리자	TOE의 인가된 관리자는 악의가 없으며, TOE 관리 기능에 대하여 적절히 교육받았고, 관리자 지침에 따라 정확하게 의무를 수행한다.
A.운영체제보강	불필요한 운영체제상의 서비스나 수단 등을 모두 제거하는 작업과 운영체제상의 취약점에 대한 보강작업을 수행하여 운영체제에 대한 신뢰성과 안정성을 보장한다.
A.유일한연결점	모든 외부 네트워크와 내부 네트워크간의 통신은 TOE를 통해서만 이루어진다.

4.2 위협 대응범위

평가제품은 TOE가 요구하는 IT 환경에 적합한 수준의 보안위협에 대한 대처방법을 제공하고 있으며 강화된-기본 수준의 전문지식, 자원 동기를 가진 위협원에 의해 발생하는 논리적/물리적 공격에 대한 대처방법을 제공한다.

모든 보안목적 및 보안정책은 식별된 보안위협에 대한 대처방법을 제공할 수 있도록 서술되어 있다.

5. 제품정보

TOE의 물리적 범위에는 TOE가 운영되는 전용 하드웨어 플랫폼의CF 메모리 상에 펌웨어 형태로 저장된 'UTM 데몬 패키지', CD 형태로 제공되는 TOE 감사 데이터 관리 소프트웨어인 'AhnLab Suhoshin Absolute Log Server'와 TOE 운영 중 전용하드웨어에서 배포되는 'AhnLab Auth' S/W가 포함된다.

· UTM 데몬 패키지

UTM 데몬 패키지에는 패킷 필터링(Packet Filtering), 어플리케이션 필터링(Application Filtering), 네트워크 주소 변환(NAT), 침입 방지(Intrusion Prevention), 악성 메일 차단, 안티 바이러스 (Anti-Virus) 엔진과의 연동 기능을 수행하는 소프트웨어 모듈(AhnLab Suhoshin Absolute v3.0)이 포함되어 있다.

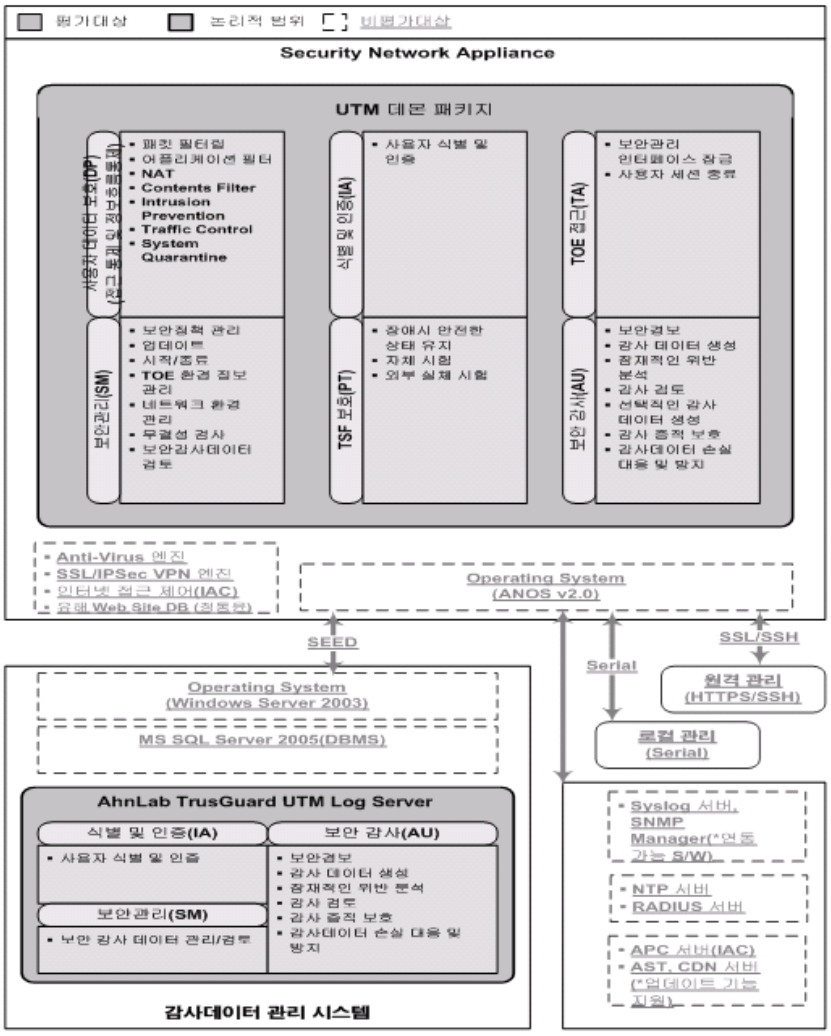
· AhnLab LogServer

AhnLab LogServer는 TOE 감사 데이터 관리 소프트웨어이다. AhnLab LogServer는Log Server 1.0.1.3(build20), Log Viewer 1.0.1.3(build20), Log Reporter 1.0.1.3(build20)의 3개 설치 파일로 구성되어 있다.

· AhnLab Auth 소프트웨어

인가된 관리자가 어플리케이션 필터링의 보안정책의 세부 정책으로 인증 정책을 강제한 경우 사용되는 AhnLab Auth 소프트웨어가 포함된다. AhnLab Auth는 ANOS와 함께 펌웨어 이미지에 포함된 형태로 배포되며, 사용자가 처음 인증 수행 시도 시 AhnLab Auth V1.0 소프트웨어를 TOE로부터 다운받아 설치/사용한다.

TOE의 논리적 평가범위는 [그림 2]와 같으며 다음과 같은 보안 기능을 제공한다.



[그림 2] TOE 논리적 범위

· 식별 및 인증

TOE는 자신에게 접근하는 모든 사용자를 식별한다. 사용자 식별이 이뤄지기 전에는 접근을 시도하는 모든 사용자는 TOE의 어떠한 기능도 사용할 수 없다. TOE는 관리자, 일반사용자, 로그관리자에 따라 식별 및 인증 기능을 제공한다.

TOE는 해당 계정의 인증 실패 횟수가 환경 설정에 정의된 횟수에 도달할 경우 ID 잠금 및 일정시간 동안 인증지연을 수행하여 악의적인사용자의 인증 시도로부터 TOE를 보호한다. 잠긴 계정은 인가된 관리자가 TOE의 보안관리 인터페이스를 통해서 해제 할 수 있다.

· 접근통제 및 정보흐름통제

TOE는 접근 통제 및 정보흐름통제 보안기능으로 Packet Filter(Dynamic & Stateful Packet Filtering), Application Filter(프록시), Network Address Translation(NAT), Contents Filter, Intrusion Prevention, 트래픽 제어(Traffic Control), 시스템 격리(Quarantine) 등을 제공한다.

· 보안관리

TOE는 TOE의 기능 및 동작을 관리할 수 있는 기능을 제공한다. TOE는 인가된 관리자가 설정한 보안정책에 따라 보안 기능과 TOE 운영환경설정 파일과 같은 TSF 데이터를 관리한다.

TOE는 기본적으로 네트워크, 서비스, 사용자, 보안 정책 객체를 관리 저장하고, 그에 따른 보안 정책을 방화벽 패킷 필터에 전달한다. 공유 메모리의 모든 내용은 환경 설정 파일에 저장되며, 파일의 내용은 암호화된다. 즉, 환경설정 파일의 내용은 TOE 구동 시 공유 메모리에 탑재되고, 설정 변경을 저장한다.

TOE는 기본적으로 HTTPS 프로토콜을 통한 웹 기반의 관리 인터페이스를 제공한다. TOE는 관리자가 지정한 보안정책에 따라 보안기능을 실행하고 TOE 운영환경설정 파일과 같은 TSF 데이터를 관리한다. 또한 TOE 관리 및 TOE 장애 발생시 이를 처리 하기 위해 CLI(Command Line Interface)를 통한 보안관리 기능도 제공한다.

또한, 물리적으로 분리된 TOE인 AhnLab LogServer를 통해 보안감사 데이터 관리/검토 할 수 있다.

· 보안감사

TOE는 운용 중 발생하는 감사데이터를 저장한다. TOE는 인가된 관리자가

지정한 보안 감사 대상 사건 발생시 감사데이터를 생성한다. 감사데이터에는 사건 일시, 사건 유형, 주체의 신원, 사건 결과(성공 또는 실패) 등의 내용이 포함된다. 또한 TOE는 인가된 관리자가 사건 유형에 따라 선택적으로 감사 데이터를 생성 여부를 결정할 수 있는 기능을 제공한다. 또한 TOE는 잠재적인 보안 위반 사건을 탐지한 경우, 인가된 관리자에게 실시간으로 통보하고 TOE 운영환경에 저장된 감사 증적(DB)의 감사 레코드에 인가된 관리자의 접근만을 허용한다. 따라서 TOE는 감사 레코드를 인가되지 않은 삭제 또는 변경으로부터 보호할 수 있다.

· TSF 보호

장애시 안전한 상태 유지 : TOE는 장애 발생시 재구동시켜야 할 중요 데몬과 동작 상태(예: start, stop, restart, reload)에 대한 리스트를 유지/관리한다. TOE는 관리 대상 데몬의 상태를 주기적 또는 인가된 관리자 요구시 검사하여, 비정상적으로 종료된 데몬이 발견되면 해당 데몬을 재구동시켜 보안 기능이 정상적으로 수행됨을 보장한다.

자체 시험 : TOE는 지정된 검사 주기마다 무결성 점검 대상들에 대한 해쉬값를 생성하여 최초 구동시 저장된 해쉬값(기준값)과 비교한다. 이때, 무결성이 위반 사항이 발견되면 TOE는 보안관리 인터페이스를 통해 인가된 관리자에게 통보하고 이에 대한 감사데이터를 생성한다.

· TOE 접근

TOE는 인가된 관리자의 비활동 경과 기간이 정의된 값(10분)을 초과하는 경우 상호작용하는 세션을 잠그는 기능을 제공한다. 잠긴 세션을 해제하기 전에 관리자를재인증한다.

TOE는 인증되지 않은 외부 실체가 TOE를 통해 세션을 형성한 후 비활동 경과 기간이 인가된 관리자가 지정한 세션 유지 기간을 초과한 경우 세션을 종료한다. 인가된 관리자가 사용자 인증을 강제한 서비스(예: 일반(General TCP) 프록시, HTTP 프록시, FTP 프록시) 에 대하여 인가된 사용자가 지정된 세션 유지 기간 동안 TOE를 통해 네트워크 트래픽을 송·수신하지 않은 경우, 인가된 사용자와 외부 실체간에 형성된 세션을 종료한다. 인가된 사용자가 서비스를 다시 요청하면 사용자 재인증을 성공적으로 완료한 경우에만 해당 외부 실체와 새로운 세션을 생성한다.

6. 설명서

평가제품이 제공하는 설명서는 아래와 같다:

- AhnLab Suhoshin Absolute v3.0 사용자운영설명서(UTM) v1.0 Revision 33

(2008. 10. 24.)
- AhnLab Suhoshin Absolute v3.0 사용자운영설명서(LogServer) v1.0 Revision 22 (2008. 12. 1.)
- AhnLab Suhoshin Absolute v3.0 사용자운영설명서(User) v1.0 Revision 1 (2008. 2. 26.)
- AhnLab Suhoshin Absolute v3.0 설치지침서 v1.0 Revision 5 (2008. 10. 24.)

7. 제품시험

7.1 개발자 시험

- **시험방법**

개발자는 제품의 보안기능을 고려하여 시험항목을 도출하였다. 각 시험항목은 시험서에 서술되어 있다. 시험서에 서술된 각 시험항목은 다음의 세부 항목을 포함하고 있다:

- 시험번호/시험자 : 시험항목 식별자 및 시험에 참여한 개발자
- 시험목적 : 시험 대상 보안기능 및 보안모듈을 포함하여 시험의 목적을 서술
- 시험환경 : 시험을 수행하기 위한 세부 시험환경
- 세부 시험절차 : 보안기능을 시험하기 위한 세부 절차
- 예상결과 : 시험절차를 수행하였을 때 나타날 것으로 예상되는 시험결과
- 실제결과 : 시험절차를 실제로 수행하였을 때 나타나는 시험결과
- 예상결과와 실제결과의 비교 : 예상결과 및 실제결과를 비교한 결과

평가자는 시험서의 시험환경, 시험절차, 시험범위 분석, 상세설계 시험 등 시험의 타당성을 평가하였다. 평가가는 개발자의 시험 및 시험결과가 평가환경에 적합함을 검증하였다.

- **시험환경**

시험서에 서술된 시험환경은 시험을 위한 네트워크 구성, 평가제품, PC 및 서버 등 세부환경을 포함하고 있다. 또한, 각 시험항목을 시험하기 위해 필요한 평가도구 등 세부적인 시험환경을 서술하고 있다.

- **시험범위 분석/상세설계 시험**

세부 평가결과는 ATE_COV 및 ATE_DPT 평가결과에 서술되어 있다.

- **시험결과**

시험서는 각 시험항목의 예상결과 및 실제결과를 서술하고 있다. 실제결과는 실제 제품의 동작화면 뿐만 아니라 감사기록을 통해서도 확인할 수 있다.

7.2 평가자 시험

평가자는 개발자 시험과 동일한 평가환경 및 평가도구를 사용하여 평가제품을 설치하고 개발자가 제공한 시험항목 전체를 시험하였다. 평가자는 모든 시험항목에서 실제결과가 예상결과와 일치함을 확인하였다.

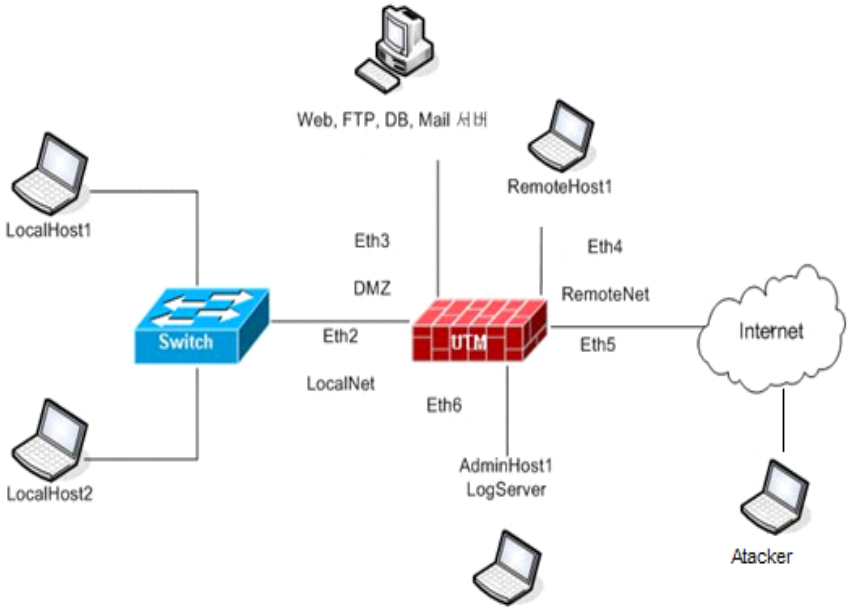
또한, 평가자는 개발자 시험에 기초하여 별도의 평가자 시험항목을 고안하여 시험한 결과, 실제결과가 예상결과와 일치함을 확인할 수 있었다.

평가자는 취약성 시험을 수행한 결과, 평가환경에서 어떠한 취약성도 악용 가능하지 않다는 점을 확인하였다.

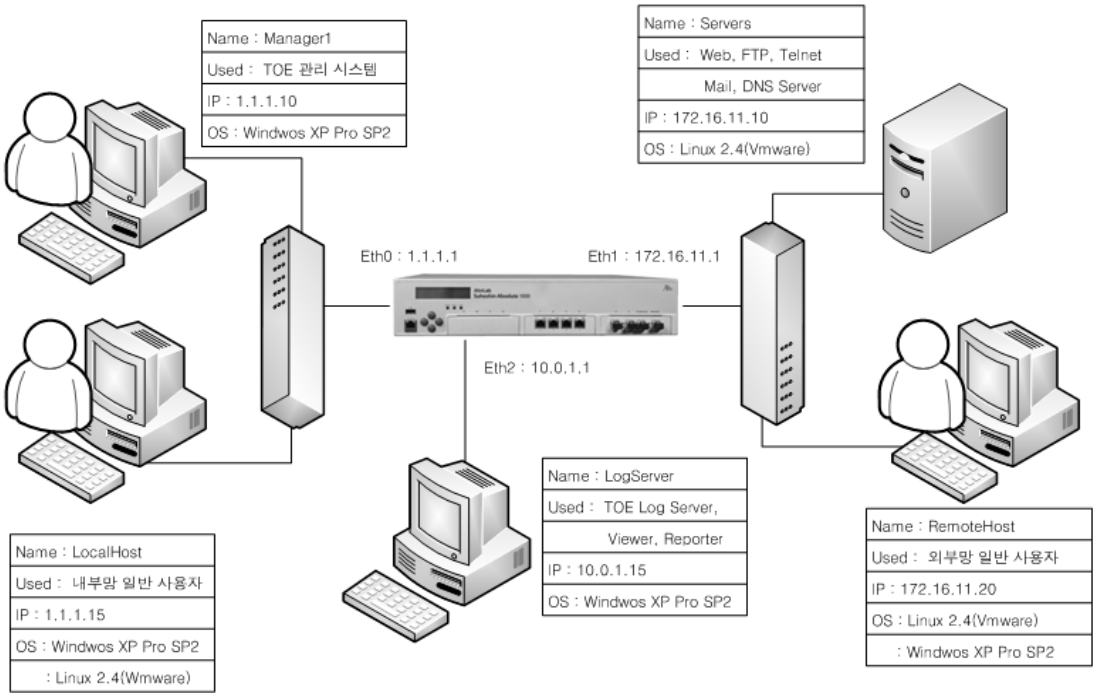
평가자의 시험결과는 평가제품이 설계문서에 서술된 대로 정상적으로 동작됨을 보증하였다.

8. 평가환경

평가환경은 개발자 시험을 검증하기 위한 환경과 평가자 독립시험을 위한 환경으로 나누어 구성하였다. [그림 3]은 개발자 시험환경을 [그림 4]는 평가자 독립시험 환경을 나타낸다.



[그림 3] 개발자 시험환경



[그림 4] 평가자 독립시험환경

9. 평가결과

평가는 공통평가기준, 공통평가방법론 V3.1을 적용하였다. 평가는 평가제품이 공통평가기준 2부, EAL4 평가보증등급의 3부에 적합하다고 평가하였다. 자세한 평가결과는 평가결과보고서에 서술되어 있다.

- **보안목표명세서 평가 (ASE)**

보안목표명세서 소개는 보안목표명세서 참조 및 TOE 참조를 유일하고 정확하게 식별하고 있으며, TOE 유형, TOE용도, 주요 보안 특징, TOE를 구성하는 물리적인 범위와 논리적 보안 특성을 충분히 이해 할 수 있을 정도로 서술하고 있다.

보안목표명세서 준수선언은 보안목표명세서 및 TOE가 준수할 공통평가기준의 버전, 보호프로파일 및 보안요구사항 패키지선언을 포함하고 있으며, TOE 유형, 보안 문제 정의 및 보안 목적과 일관성 있게 서술되어 있다.

보안목표명세서의 보안문제정의는 TOE 및 TOE의 운영환경에서 다루어져야 하는 보안문제 즉, 위협, 조직의 보안정책, 가정사항을 명확히 정의하고 있다.

보안목적은 식별된 위협을 만족시키며, 식별된 조직의 보안정책을 달성하고, 서술된 가정사항을 적절하고 완전하게 다루고 있으며, TOE 및 TOE 운영 환경에서의 보안 문제가 명확히 분류되어 정의되어 있다.

보안요구사항은 완전하고 일관성 있게 서술되어 있으며, 보안목적을 달성하기 위해 TOE의 개발에 알맞은 기반을 제공하고 있다.

TOE 요약명세는 모든 보안기능요구사항을 다루고 있으며, 보안목표명세서의 다른 부분과 일관성 있게 정의하고 있다.

따라서, 보안목표명세서는 완전하고, 일관성 있고, 기술적으로 타당하며, 결과적으로 TOE 평가의 기초자료로 사용하기에 적합하다.

- **개발 평가 (ADV)**

보안구조설명문서는 TSF 보안 수행이 손상되거나 우회되지 않는 방법, TSF가 제공하는 보안영역이 다른 영역과 어떻게 분리되는지 TSF의 구조 특성을 충분히 서술하고 있다.

기능명세는 TOE 보안기능을 적절히 서술하고 있으며, TOE 보안기능이 보안목표명세서의 보안기능요구사항을 만족시키기에 충분함을 설명하고 있다. 또한, TSF가 TSP을 어떻게 만족시킬 수 있는지 이해할 수 있을 정도로 TSFI(TSF Interface)를 적절하게 서술하고 있다.

TOE 설계는 TSF경계를 결정하기에 충분하도록 TOE에 대한 설명을 서브시스템 관점에서 서술하고 있으며, TSF 내부에 대한 설명은 모듈 관점으로 서술하고 있다. 또한 SFR이 완전하고 정확하게 구현되었음을 SFR-수행 모듈, SFR 지원 및 SFR 관점에서 충분히 설명하고 있다.

구현의 표현은 보안목표명세서의 보안기능요구사항을 만족하기에 충분하며, TOE설계를 정확하게 실현하고 있다.

따라서, TSF에 대한 인터페이스를 설명하는 기능명세, TOE 구조를 서브시스템 및 모듈로 설명하는 TOE 설계, 소스코드 수준의 설명인 구현의 표현, TSF 보안 수행이 손상되거나 우회되지 않는 방법을 설명하는 보안구조설명으로 구성된 개발문서는 TOE 보안기능을 제공하는 방법을 이해하기에 적절하다.

- **설명서 평가 (AGD)**

준비절차문서는 배포된 TOE를 보안목표명세서에 서술된 운영환경 내의 평가 받은 구성으로 변환시키기 위한 절차를 적절하게 서술하고 있으며, 그 결과 TOE가 안전하게 구성됨을 확인하였다.

사용자운영설명서는 TOE를 안전한 방식으로 관리하는 방법을 적절하게 서술하고 있다.

따라서, 설명서는 TOE 설치, 관리, 운영하는 자가 TOE를 안전하게 다룰 수 있는 방법을 적절하게 서술하고 있다.

- **생명주기 지원 평가 (ALC)**

형상관리 문서는 구현 표현의 변경사항들이 자동화 도구를 사용하여 통제되고 있음을 서술하고 있다. 또한, TOE 및 TOE와 관련된 형상항목을 명확하게 식별하고 있으며, 이러한 항목들을 변경하는 능력이 적절히 통제되고 있음을 서술하고 있다.

형상관리 문서로부터 개발자가 최소한 TOE 구현의 표현, ST의 보증 컴포넌트에서 요구하는 평가증거물, 보안 결함에 대하여 형상관리를 수행함을 확인하였다.

따라서, 형상관리 문서는 소비자가 평가된 TOE를 식별하도록 해주며, 형상항목이 유일하게 식별됨을 보장하고, 개발자가 TOE 변경을 통제 및 추적하기 위해 사용한 절차가 적절함을 보장한다.

배포 문서는 TOE를 사용자 측에 배포할 때 TOE의 보안을 유지하고 TOE의 변경 및 대체를 탐지하기 위한 모든 절차를 서술하고 있다.

따라서, 배포 문서는 개발자가 의도한 방식과 동일하게 TOE가 변경되지 않고 배포됨을 보장하기에 적절하다.

개발자의 개발환경에 대한 보안통제는 TOE를 안전하게 운영하기 위해 필요한 TOE 설계 및 구현의 비밀성 및 무결성을 제공하기에 적절함을 확인하였다.

개발자가 문서화된 TOE 생명주기 모델을 사용하고 있음을 확인하였다.

개발자가 일관성 있고 예측할 수 있는 결과를 낼 수 있는 잘 정의된 개발 도구를 사용했음을 확인하였다.

따라서, 생명주기 지원은 TOE 개발 전 과정에 사용된 보안절차 및 도구와 TOE를 개발하고 유지 보수하는 동안 개발자가 사용하는 절차를 적절하게 서술하고 있다.

- **시험 평가 (ATE)**

시험은 TOE 보안기능이 기능명세에 대하여 체계적으로 시험되었음을 확립하기에 충분하였다.

개발자는 TOE 설계에 대한 TOE 보안기능 시험을 수행하였음을 확인하였다.

개발자의 시험서는 보안기능이 명세된 대로 수행함을 입증하기에 충분하였다.

평가자는 TSF 일부에 대한 독립적인 시험을 수행하여 TOE가 명세된 대로 동작함을 확인하였고, 개발자 시험에 대한 전수시험을 통하여 개발자가 수행한 시험에 대한 신뢰를 얻었다.

따라서, 시험서를 통해 TOE 보안기능 보안목표명세서에 명시된 TOE 보안기능요구사항을 만족하고 설계 문서에 기술된 대로 동작함을 확인하였다.

- **취약성 평가 (AVA)**

취약성 분석서에는 TOE에 대해서 명백하게 알려진 취약성과 이에 대한 대응책을 기능 구현 또는 지침서나 설명서에 운용환경을 명시하는 등 대응책을 적절하게 서술하고 있으며, 평가자가 독립적인 취약성 분석을 수행하여 취약성 분석의 정확성을 확인하였다.

취약성 분석에서 TOE는 의도된 환경 내에서 강화된-기본 공격성공 가능성을 가진 공격자에 의해 악용 가능한 취약성을 가지지 않음을 확인하였다.

따라서, 평가자의 취약성 분석 및 평가자의 침투시험에 기반하여 의도한 환경 내에서 TOE에 악용 가능한 결함 및 약점이 존재하지 않음을 확인하였다.

10. 권고사항

평가 받은 TOE 운영환경에서만 TOE의 안전성을 보장할 수 있으므로 다음의 권고사항을 반드시 준수하여 TOE를 운영하여야 한다.

① TOE는 임의적 접근통제, 등급기반 접근통제, 침입방지정책, 어플리케이션 필터 정책, QoS 정책 등이 순차적으로 적용됨으로 TOE 보안관리자는 접근통제 특성을 숙지하여 접근통제 정책을 신중하게 적용해야 한다.

② 보안관리자는 AhnLab Suhoshin Absolute Logserver를 이용하여 여러 AhnLab Suhoshin Absolute로부터 생성되는 감사데이터를 관리할 수 있기 때문에 AhnLab Suhoshin Absolute 별로 생성되는 감사데이터의 시간이 상이한 경우 감사데이터의 신뢰성을 확보하기 어려우므로 각 AhnLab Suhoshin Absolute가 설치된 시스템의 시간을 정확하게 설정해야 한다.

③ TOE의 저장공간이 설정된 임계치에 도달하는 경우 관리자에게 알람(E-mail)로 통보하고 저장공간 소진 시 TOE의 보안기능을 중지하거나, 가장 오래된 감사데이터를 덮어쓰기 때문에 보안관리자는보안관련 사건 추적을 위하여 AhnLab Suhoshin Absolute와 AhnLab Suhoshin Absolute Logserver의 감사

기록 저장공간의 용량을 항시 확인하거나 E-mail 경고를 확인한 후 감사기록 저장공간이 포화되기 전에 백업받아 감사데이터를 유지해야 한다.

④ TOE는 임시 ID/PW가 설정된 상태로 배포된다. 임시 ID/PW를 사용할 경우 식별 및 인증에 대한 위협을 받을 수 있으므로 보안관리자는 TOE 설치/운영 시 임시로 설정된 ID/PW를 변경 후 TOE를 사용해야 한다. 또한 사용자에 대한 PW 변경을 TOE에서 자동으로 제공하고 있지 않으므로 TOE 사용 시 주기적인 ID/PW 변경을 권고한다.

⑤ 배포 시 설정된 TOE의 세션 시간 제한, 프록시 동시 연결 수, 침입탐지 시 처리 방법 등에 대한 설정은 각 운영 환경을 고려하지 않고 설정된 값이므로 보안관리자는TOE가 실제 설치되는 운영환경의 네트워크 상태와 보안상태를 확인하여 TOE의 설정 값을 적절하게 변경한 후 운영할 것을 권고한다.

⑥ TOE는 환경 설정 파일에 대한 백업 기능을 자동으로 제공하지 않으므로 보안관리자는 TOE의 설정 값을 변경한 경우 TOE에서 제공하는 백업기능을 이용하여 환경설정 파일을 주기적으로 백업하여 TOE에 장애가 발생할 경우를 사전에 대비할 것을 권고한다.

11. 용어 정의

아래의 약어가 본 보고서에서 사용되었다.

CR	Certification Report
EAL	Evaluation Assurance Level
IT	Information Technology
KECS	Korea IT security Evaluation and Certification Scheme
TOE	Target of Evaluation
ST	Security Target
TSF	TOE Security Functions

아래의 용어가 본 보고서에서 사용되었다.

TOE	평가의 대상인 IT제품이나 시스템 및 이와 관련된 설명서
감사기록	TOE의 보안에 관련된 사건의 기록을 저장하는 감사데이터
사용자	TOE 외부에서 TOE와 상호 동작하는 모든 실체, 사용자, 외부 IT 실체 등
인가된 관리자	TOE 보안정책에 따라 TOE를 안전하게 관리하는 인가된 사용자

인가된 사용자	TOE 보안정책에 따라 기능을 실행할 수 있는 사용자
외부 IT 실체	TOE 외부에서 TOE와 상호 작용하는 안전하거나 안전하지 않은 모든 IT 제품이나 시스템

12. 참고문헌

인증기관은 아래의 문서를 사용하여 본 인증보고서를 작성하였다:

[1] 정보보호시스템 공통평가기준 V3.1

[2] 정보보호시스템 공통평가방법론 V3.1

[3] 정보보호시스템 평가·인증 지침 (2008. 7. 16.)

[4] 정보보호제품 평가인증 수행규정 (2008. 9. 1.)

[5] AhnLab Suhoshin Absolute v3.0 보안목표명세서 Version 001 Revision 5 (2008.10.17.),(주)안철수연구소

[6] AhnLab Suhoshin Absolute v3.0 평가결과보고서 V1.0 (2008. 12. 5.)