KECS-CR-07-09

SECUINXG V1.6 인증보고서

인증번호 : KECS-NISS-0068-2007

2007년 12월

IT보안인증사무국

제·개정 이력 현황

개정 번호	제·개정일	개정쪽	제·개정내용
00	2007. 6.21	-	최초 작성
01	2007. 9.21	18p	인증효력유지(변경승인) 내역 추가
02	2007.12.12	19p	인증효력유지(변경승인) 내역 추가

본 문서는 (주)시큐아이닷컴의 SECUINXG V1.6에 대한 인증 보고서이다.

인증위원

정보통신부 조규조, 국가보안기술연구소 박종욱,
고려대학교 임종인, 이화여자대학교 채기준, 성균관대학교 김승주,
순천향대학교 염흥렬, 충남대학교 류재철, 한남대학교 이강수,
한국전자통신연구원 손승원

인증기관

IT보안인증사무국

평가기관

한국정보보호진흥원

목 차

1. 요약

본 보고서는 SECUINXG V1.6에 대한 정보보호시스템 공통평가기준(2005년 5월 21일 고시)(이하 '공통평가기준'이 한다) EAL 4 평가결과에 대한 인증기관의 인증결과를 서술한다. 본 보고서는 평가결과, 평가결과의 타당성 및 적합여부를 서술한다.

SECUINXG V1.6에 대한 평가는 한국정보보호진흥원에서 수행되었으며, 2007년 6월 4일에 평가 완료되었다. 본 보고서의 내용은 한국정보보호진흥원에서 제출한 평가보고서의 내용에 기초하여 작성되었다. 평가는 제품이 공통평가기준 2부와 3부의 EAL 4 평가보증등급을 만족하여, 공통평가기준 1부 191항에 따라 "적합"한 것으로 평가하였다.

SECUINXG V1.6은 네트워크의 내부 네트워크, 서버 및 서비스를 외부로부터 보호하고 외부 네트워크로 전송되거나 내부 네트워크로 들어오는 정보 및 서비스 정보를 보호하기 위해 개발된 '침입방지시스템(IPS)' 제품으로 (주)시큐아이닷컴에서 개발되었다.

제품은 크게 시스템의 기본적인 운영환경을 제공하는 SecuiOS, 시스템 자원을 제공하는 하드웨어, 그리고 침입방지시스템 보안기능을 제공하는 보안 소프트웨어로 구성된다. 평가제품은 아래와 같은 주요 보안기능을 제공한다:

- 보안 감사 및 감사 데이터의 생성 및 보호(Audit)
- 보안 관리 (SEC_MAN)
- 불법적인 접근으로부터 내부 자산 및 내부 정보 보호 (Firewall)
- 불법적인 접근 및 공격의 방지 (IPS)
- TOE 사용자의 식별 및 인증 (UI&AD)
- TSF 안정성 (TSF_SAFER)
- 네트워크 트래픽 제어 (Traffic_Control)
- 프로세스 감시(Mon_Process)

인증기관은 평가자의 평가활동 및 시험절차를 점검하고, 기술적인 문제점 및 평가절차에 대한 지침을 제공하고, 각 평가단위 및 평가보고서의 내용을 검토하였다. 인증기관은 평가제품이 보안목표명세서에 서술된 모든 보안기능 요구사항 및 보증요구사항을 만족함을 평가결과가 보증함을 확인하였다. 따라서, 인증기관은 평가자의 관찰사항과 평가결과가 정확하고 타당하며, 적합여부 평가결과가 정확하다고 인증하였다.

인증 효력범위 : 본 인증보고서에 포함된 정보는 SECUINXG V1.6이 대한민국 정부기관에 의한 사용 승인 또는 SECUINXG V1.6에 대한 품질보증을 의미하지 않는다.

2. 식별정보

다음 [표 1]은 평가제품 식별을 위한 정보를 나타낸다.

[표 1] 평가제품 식별정보

평가지침	정보보호시스템 평가·인증지침 (2007.5.30, 정보통신부고시 제2007-19호) 정보보호제품 평가인증 수행규정 (2007.4.15)
평가제품	SECUINXG V1.6
보호프로파일	네트워크 침입방지시스템 보호프로파일 V1.1
보안목표명세서	SECUINXG V1.6 보안목표명세서 version 1.11, 2007-05-29
평가보고서	SECUINXG V1.6 평가보고서 V1.0, 2007-06-04
적합여부 평가결과	공통평가기준 2부 적합 공통평가기준 3부 적합
평가기준	정보보호시스템 공통평가기준 (2005.5.21, 정보통신부고시 제2005-25호)
평가방법론	정보보호시스템 공통평가방법론 V2.3 (2005. 8)
평가신청인	(주)시큐아이닷컴
개발업체	(주)시큐아이닷컴
평가자	한국정보보호진흥원 보안성평가단 평가2팀 조규민, 오용석, 박현미, 노영주
인증담당자	IT보안인증사무국

본 제품의 평가범위는 아래 식별된 펌웨어 버전의 보안 기능을 포함하고, 하드웨어 및 운영체제는 포함하지 않는다.

o SECUINXG V1.6 펌웨어 : V1.2.5.R

(다음의 설치 운용 하드웨어에 출고 시 설치하여 고객에 제공됨)

본 제품의 시스템 요구사항은 다음 [표 2]와 같다.

[표 2] SECUINXG V1.6 시스템 사양

o TOE 설치 운용 환경 하드웨어:

항목	사양	비고
CPU	Dual Xeon 3.2GHz	
Main Memory	2GB	
HDD	400 GB * 2	400GB 한개는 Mirroring
NIC	12 (1 Gbps * 12) Ports + 콘솔용 1 port	RJ-45 Type 4 Ports Fiber Type 8 Ports
USB	USB 2.0 * 1 Ports	초기 이미지 설치용
운영체제	SecuiOS V1.1	

관리 콘솔은 관리자 프로그램이 설치되어 TOE의 운영과 관리를 담당하는 PC를 말한다. 이러한 관리 콘솔의 설치 운용을 위해 당사에서는 아래와 같은 물리적 하드웨어 사양을 권고한다.

o TOE 관리 콘솔 설치 운용 환경 :

관리자 콘솔	최소 사양	비고
CPU	Pentium III 133MHz 이상	
Main Memory	256MB 이상	
HDD	40 GB 이상	
NIC	1개 이상	
시리얼	1개	DB9 type
운영체제	Windows XP Service Pack 2	
웹브라우저	Internet Explorer Version 5.5 이상	SSL 지원 128bit 이상으로 패치요함

3. 보안정책

평가제품은 아래와 같은 보안정책을 준수하여 운영된다.

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

안전한관리 인가된 관리자는 안전한 방법으로 TOE를 관리해야 한다.

4. 가정사항 및 범위

4.1 가정사항

평가제품은 아래와 같은 가정사항을 준수하여 설치 및 운용되어야 한다.

A.물리적보안	
TOE는 인가된 자만이 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 의무를 수행한다.	
A.운영체제보강	
TOE에 의해 필요하지 않은 운영체제상의 서비스나 수단 등을 제거하는 작업과 운영체제상의 취약점에 대한 보강작업을 수행하여 운영체제에 대한 신뢰성과 안정성을 보장한다.	
A.유일한연결점	
TOE는 네트워크상에 설치 운영되는 경우, 네트워크를 외부망과 내부망으로 분기해 주며, 외부망과 내부망간의 모든 통신은 TOE를 통해서만 이루어집니다.	
A.운영체제시간	**보안목표명세서 작성자에 의하여 추가**
TOE는 하부 운영체제와 외부 NTP 서버에서 안전하게 타임소스를 제공받는다.	
A.SSL인증서	**보안목표명세서 작성자에 의하여 추가**
TOE의 관리접속을 위한 SSL 인증서는 TOE 자체 사설인증서를 사용하며 자체적으로 안전하게 관리됩니다.	
A.안전한TOE외부서버	**보안목표명세서 작성자에 의하여 추가**
TOE의 안전한 기능 동작을 위해 TOE 외부에 존재하는 NTP 서버와 시큐아이 업데이트서버는 안전하다.	

4.2 위협 대응범위

평가제품은 TOE가 요구하는 IT 환경에 적합한 수준의 보안위협에 대한 대처방법을 제공하고 있으며, 평가제품을 비정상적으로 운용되도록 하는 직접적인 물리적 공격에 대한 대처방법을 제공하고 있지 않다. 그러나, 평가제품은 평가제품과 연결된 네트워크에서 낮은 수준의 전문지식, 자원, 동기를 가진 위협원에 의해 발생하는 논리적 공격에 대한 대처방법을 제공한다.

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

5. 제품정보

TOE는 다음 그림과 같이 외부의 신뢰되지 않는 네트워크의 접점에 TOE를 설치함으로써 외부의 불법적인 침입 및 공격을 방지할 수 있도록 침입방지기능을 제공한다.

아래의 그림에서 TOE는 물리적 경계 및 범위에 서술된 운영체제를 기반으로 동작하며, (주)시큐아이닷컴에서 제조하는 하드웨어에 설치하여 사용한다.

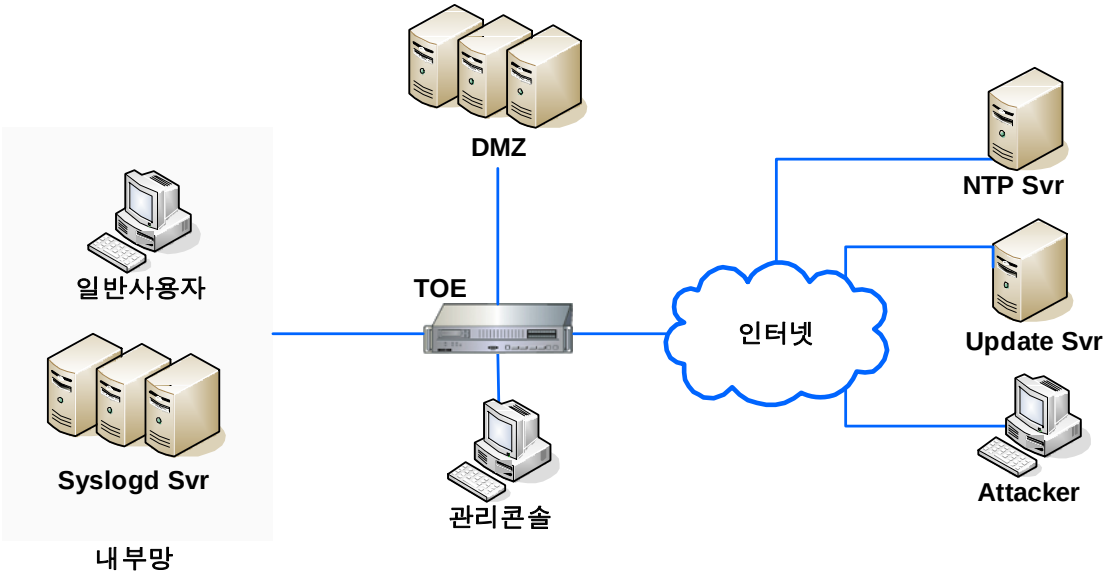

그림 1 TOE 사용 환경

제품은 크게 시스템의 기본적인 운영환경을 제공하는 SecuiOS, 시스템 자원을 제공하는 하드웨어, 그리고 침입방지시스템 보안기능을 제공하는 보안 소프트웨어로 구성된다. 이 중 TOE는 보안소프트웨어에 해당한다. 다음 그림은 TOE의 보안 소프트웨어 아키텍처를 나타내고 있으며 이 보안 소프트웨어는 또다시 Kernel Level 서브시스템과 Application Level 서브시스템으로 구분된다.

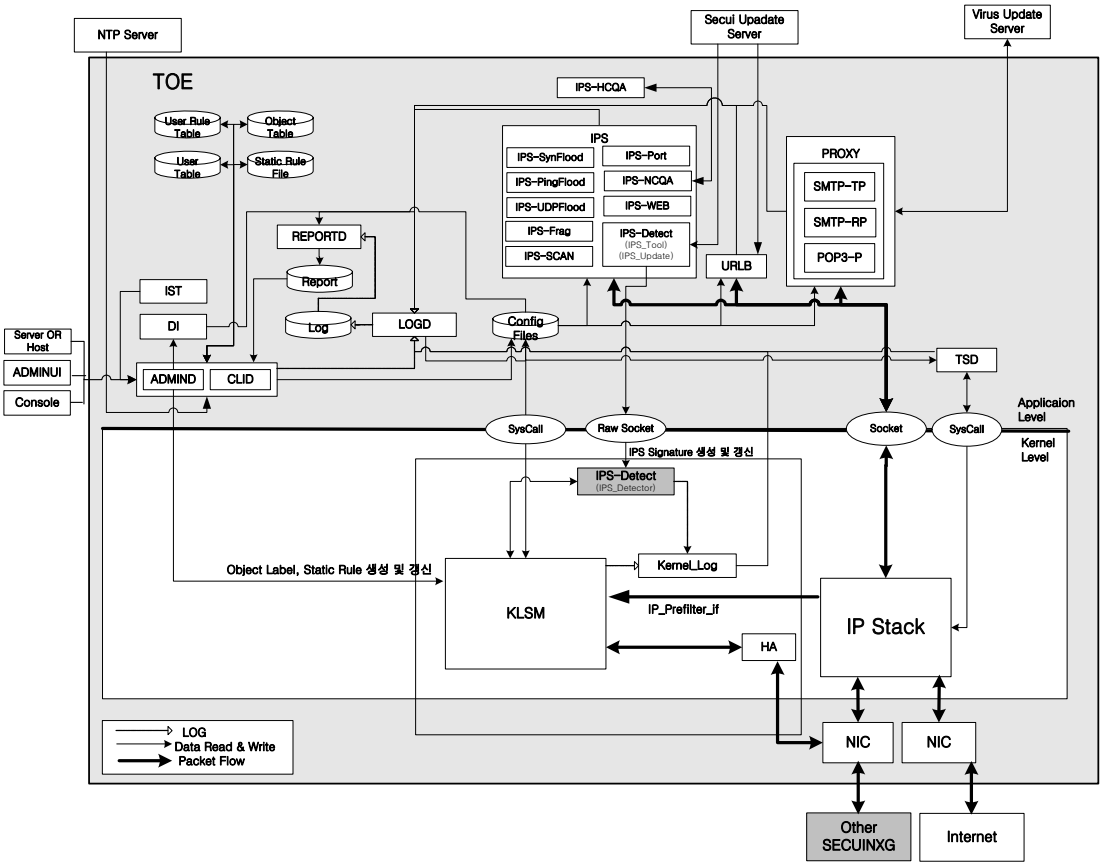

그림 2 TOE Architecture

6. 설명서

평가제품이 제공하는 설명서는 아래와 같다:

- SECUINXG V1.6 관리자설명서 V1.5, 2007년 5월 29일

7. 제품시험

7.1 개발자 시험

- **시험방법**

개발자는 제품의 보안기능을 고려하여 시험항목을 도출하였다. 각 시험항목은 시험서에 서술되어 있다. 시험서에 서술된 각 시험항목은 아래의 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, 기본설계 시험 등 시험의 타당성을 평가하였다. 평가자는 개발자의 시험 및 시험결과가 평가환경에 적합함을 검증하였다.

- **시험환경**

시험서에 서술된 시험환경은 시험을 위한 구성, 평가제품, TOE가 설치된 서버 등 세부 환경을 포함하고 있다. 또한, 각 시험항목을 시험하기 위해 필요한 시험도구 등 세부적인 시험환경을 서술하고 있다.

- **시험범위 분석/기본설계 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

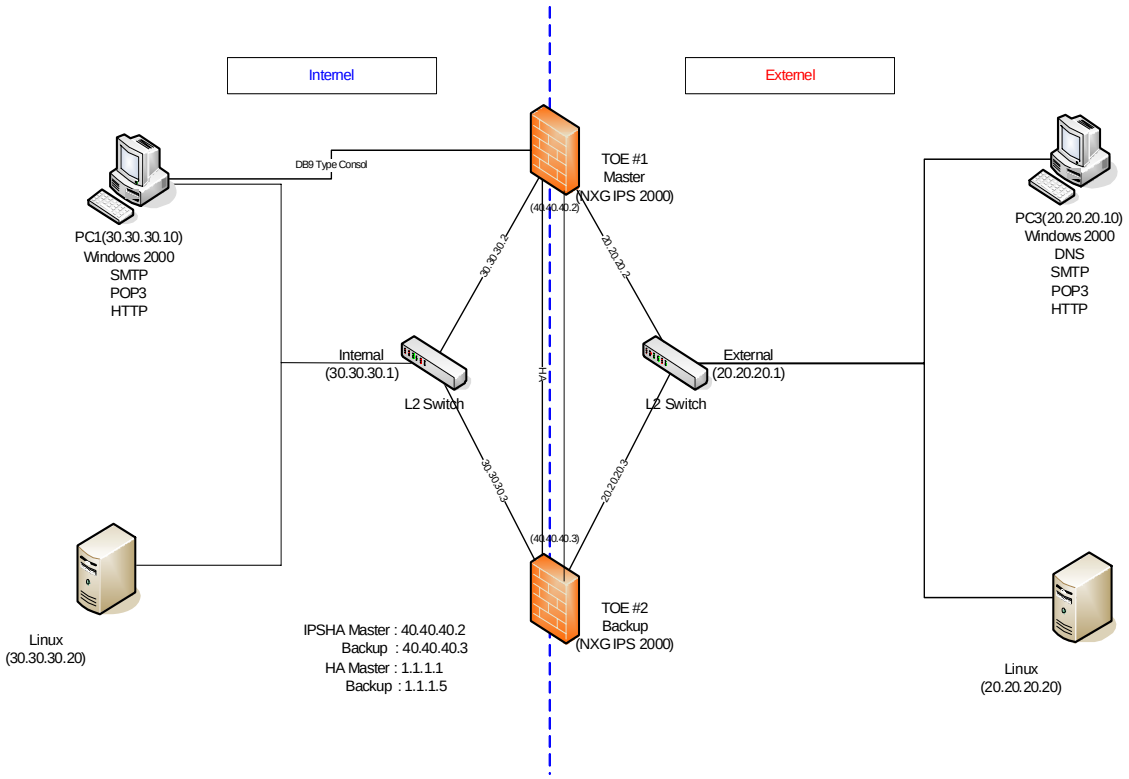

그림 2 TOE 설치 환경

평가자는 다음 표와 같은 보안기능에 대하여 시험을 수행하였다.

TSF	설명
보안감사 및 감사 데이터의 생성 및 보호 (Audit)	TOE를 통하는 모든 패킷들과 TOE에서 실행되는 모든 프로세스에 대한 감사 데이터를 생성하고 관리자가 생성된 감사 데이터를 조회, 분석 및 통합하여서 관리할 수 있도록 한다. 또한 감사 데이터를 보호하기 위해서 감사 데이터가 저장되는 파일 시스템을 관리한다.
보 안 관 리 (SEC_MAN)	관리자는 관리자 프로그램을 통해서 또는 관리 콘솔을 통해서만이 관리 기능에 대해 행동을 결정, 중지, 개시, 행동 변경할 수 있다. 관리자가 관리자 프로그램을 작동시키기 위해서 그리고 TOE와 관리자가 직접 상호작용하기 위해선 먼저 관리자 식별 및 인증 절차를 거쳐야만 된다. 그러므로 이러한 기능을 수행하는 능력은 인가된 관리자에게로만 제한됨을 보장할 수 있다.
불법적인 접근으로부터 내부 자산 및	TOE는 접근 주체인 TOE를 통해서 정보를 송수신하는 내/외부망 IT 실체에 대해 식별 및 인증을 한 후 IP 주소 정보

내부 정보보호 (Firewall)	와 보안등급(1~20)과 같은 보안 속성에 기반 하여 정보흐름통제 규칙을 적용하여 IT 실체가 접근 권한을 가지는지 판단합니다. 주체는 TOE를 통해서 전송되는 네트워크 패킷을 Destination URI(uniform resource identifier), 시간, 패킷의 헤더와 데이터 정보와 같은 보안속성을 허용, 거부, 거절(ICMP), 거절(Reset)의 오퍼레이션을 허용한다. 접근 객체에 접근 권한이 없을 경우 해당 사용자의 연결을 종료시킴으로써 접근 통제를 한다. TOE에서의 정보흐름통제 기능에는 임의적 접근통제, 강제적 접근통제가 있으며 그 외 기타 추가적인 규칙에 기반한 접근통제와 같은 기능도 있다.
불법적인 접근 및 공격의 방지 (IPS)	호스트와 네트워크의 자원을 고갈시키거나 알려진 취약성을 통하여 가용성에 문제를 유발시키는 해킹 공격이 존재합니다. 이를 방지하기 위해 불법적인 접근 및 공격을 탐지하여서 이런 공격으로부터 방지하기 위한 침입방지기능(IPS)이 필요합니다.
TOE 사용자의 식별 및 인증 (UI&AD)	TOE의 사용자는 시스템 자체를 관리하는 인가된 관리자가 존재합니다. 인가된 관리자는 TOE에 등록이 되어야 하며, 관리자는 TOE을 통해서 사용자에 대한 식별 및 인증 과정을 거쳐야 합니다.
TSF 안정성 (TSF_SAFER)	TSF 데이터 무결성 검사와 TSF 데이터의 무결성이 깨졌을 경우, 이에 대한 대응을 지원하며, TOE 자체가 시스템이 정확한지 시험하기 위한 기능과 TSF 간에 안전한 경로를 통한 통신을 보장하기 위해서 암호 알고리즘에 의해 암호화된 통신을 지원합니다. 이는 TSF간에 통신되는 데이터를 보호하기 위한 기능입니다.
네트워크 트래픽 제어 (Traffic_Control)	트래픽 조절 기능은 정책에 합치되는 트래픽을 지정한 대역폭만큼만 차지하도록 설정하는 기능이다. 특정 트래픽의 폭주가 다른 네트워크 사용에 지장을 초래하지 않도록 하고 특정 트래픽을 여타의 트래픽으로부터 보호하고자 하는데 활용할 수 있다.
프로세스 감시 (Mon_Process)	프로세스 감시 기능은 System에 동작되고 있는 보안 기능별 Application Process의 동작 여부를 감시하는 기능이다. 이 기능을 통해 관리자가 설정한 보안 기능이 임의의 에러에 의해 중단되지 않고 지속적인 서비스를 제공하게 한다.

9. 평가결과

평가는 정보보호시스템 공통평가기준 V2.3, 정보보호시스템 공통평가방법론 V2.3을 적용하였다. 평가는 평가제품이 정보보호시스템 공통평가기준 2부, 정보보호시스템 공통평가기준 3부의 EAL4 평가보증등급 요구사항을 만족한다고 평가하였다. 자세한 평가결과는 평가보고서에 서술되어 있다.

- **보안목표명세서 평가 (ASE)**

평가자는 ASE 공통평가방법론 작업단위를 적용하여 평가하였다.

보안목표명세서 소개는 완벽하고 보안목표명세서의 다른 부분과 일관성이 있으며 보안목표명세서를 정확하게 식별하고 있다. TOE 설명은 TOE 목적 및 그 기능성을 이해할 수 있도록 설명하며, 조리 있고 완벽하며 내부적으로 일관성이 있으며, 보안목표명세서의 다른 부분과 일관성 있게 서술되어 있다.

보안환경은 TOE와 TOE 보안환경에서 유도된 명확하고 일관된 보안상의 문제를 가정사항, 위협, 조직의 보안정책으로 정의하여 제공하고 있으며, 완전하고 일관성 있게 서술되어 있다. 보안목적은 식별된 위협을 만족시키며 식별된 조직의 보안정책을 달성하며, 서술된 가정사항을 만족시키고 있다.

IT 보안요구사항은 완전하고 일관성 있게 서술되어 있으며, 보안목적을 달성하기 위한 TOE의 개발에 알맞은 기반을 제공하고 있다. TOE 요약명세는 보안기능과 보증척도를 정확하고 일관성 있게 정의하고, 서술된 TOE 보안요구사항을 만족하고 있다. 보안목표명세서는 수용하는 보호프로파일을 정확히 실체화하고 있다.

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

- **형상관리 평가 (ACM)**

평가자는 ACM 공통평가방법론 작업단위를 적용하여 평가하였다. 형상관리 문서로부터 개발자가 구현 표현에 대한 수정을 위해 자동화 도구를 사용하여 통제하고 있음을 확인하였다. 형상관리 문서로부터 개발자가 TOE 및 TOE와 관련된 형상항목을 명확하게 식별하고 있으며, 이러한 항목들을 변경하는 능력은 적절히 통제됨을 확인하였다. 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 및 운영 평가 (ADO)**

평가자는 ADO 공통평가방법론 작업단위를 적용하여 평가하였다. 배포 문서는 TOE를 사용자 측에 배포하는 경우 TOE의 보안을 유지하고 TOE의 변경 및 대체를 탐지하기 위한 모든 절차를 서술하고 있다. TOE의 안전한 설치, 생성 시동을 위한 절차 및 단계는 문서화되어 있으며, 그 결과 TOE는 안전하게 환경구성됨을 확인하였다.

따라서, 배포 및 운영 문서는 개발자가 의도한 방식과 동일하게 TOE가 설치, 생성, 시동되며, TOE가 변경되지 않고 배포됨을 보장하기에 적절하다.

- **개발 평가 (ADV)**

평가자는 ADV 공통평가방법론 작업단위를 적용하여 평가하였다. 기능명세는 TOE 보안기능을 적절히 서술하고 있으며, TOE 보안기능이 보안목표명세서의 보안기능요구사항을 만족시키기에 충분함을 설명하고 있다. 또한, TOE 외부 인터페이스를 적절하게 서술하고 있다. 보안정책모델은 보안정책의 규칙과 특징을 기술하는 데 명확하고 일관성이 있으며, 기능명세에 기술된 보안기능과 대응하도록 기술하고 있다.

기본설계는 TSF를 주요 구성 요소인 서브시스템으로 서술하고 있으며, 서브시스템의 인터페이스를 적절하게 서술하며, 기능명세를 정확하게 실현하고 있다. 상세설계는 TOE 보안기능의 내부 동작을 모듈과 모듈간의 상호관계 및 종속관계에 관하여 서술하고 있다. 상세설계는 보안목표명세서의 보안기능요구사항을 만족하기에 충분하며, 기본설계를 정확하고 효과적으로 정교화하고 있다.

구현의 표현은 보안목표명세서의 보안기능요구사항을 만족하기에 충분하며, 상세설계를 정확하게 실현하고 있다. 표현의 일치성은 개발자가 보안목표명세서의 요구사항을 기능명세, 기본설계, 상세설계, 구현의 표현으로 정확하고 완벽하게 구현했음을 보여준다.

따라서, 개발에서 TOE 외부 인터페이스를 설명하는 기능명세, TOE 구조를 내부 서브시스템으로 설명하는 기본설계, TOE 구조를 내부 모듈로 설명하는 상세설계, 소스코드 수준의 설명인 구현의 표현, 이러한 TOE 표현방법의 일관성을 보장하기 위해 서로 대응시키는 표현의 일치성 문서는 TOE 보안기능을 제공하는 방법을 이해하기에 적절하다.

- **설명서 평가 (AGD)**

평가자는 AGD 공통평가방법론 작업단위를 적용하여 평가하였다. 관리자설명서에는 관리자가 보안관리 인터페이스에 접속하는 방법과 보안관리 인터페이스에서 제공되는 각 메뉴에 대한 설명과 주의사항을 실례를 들어 서술하고 있다. 관리자설명서에서 서술된 내용이 정확하게 수행됨을 확인하였다.

- **생명주기 지원 평가 (ALC)**

평가자는 ALC 공통평가방법론 작업단위를 적용하여 평가하였다. 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 도구를 포함하여 TOE를 개발하고 유지보수하는 동안 개발자가 사용하는 절차를 적절하게 서술하고 있다.

- **시험 평가 (ATE)**

평가자는 ATE 공통평가방법론 작업단위를 적용하여 평가하였다. 시험서에는 보안목표명세서에 명시된 보안기능에 대해서 시험목적, 단계별 시험 절차 및 시험결과를 서술하고 결과를 예시하고 있다. 제공된 개발 과정별 기능시험의 시험 과정을 반복 수행하여 시험서에 서술된 시험 내용이 정확함을 확인하였으며 개발 과정에서 구현된 보안기능의 동작이 일치함을 확인하였다. 또한 평가자 독립적인 시험을 수행하여 개발자 시험의 정확성을 확인하였다.

- **취약성 평가 (AVA)**

평가자는 AVA 공통평가방법론 작업단위를 적용하여 평가하였다. 오용 분석에서 설명서가 오해되지 않고 불합리하지 않으며 상충되지 않음을 확인하였으며, 모든 운영모드에 대한 안전한 절차가 다루어졌으며, 설명서를 사용하면 TOE의 불안전한 상태를 방지 및 탐지할 수 있음을 확인하였다. 기능강도 선언은 보안목표명세서의 모든 확률 및 순열 메커니즘에 대하여 선언되었으며, 개발자의 기능강도 선언에 대한 분석은 정확함을 확인하였다.

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 낮은 수준의 공격 수준을 가진 공격자에 의해 악용 가능한 취약성을 가지지 않음을 확인하였다.

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

10. 권고사항

- SECUINXG V1.6 제품은 H/W 일체형 제품으로 보안목표명세서 및 평가보고서에 기술한 H/W 환경하에서 평가받은 것이므로, 해당 H/W에 설치되어 사용되어야 한다.

- 본 TOE는 NAT 기능이 없으므로, 내부 IP 주소가 외부에 노출될 수 있음을 유의하여 사용하여야 한다.

- 감사기록 저장공간 소진으로 임계치에 도달하는 경우 관리자 통보 기능을 제공하지만, 관리자는 통보 기능에만 의존하지 말고 지속적으로 저장공간 사용량을 점검하고, 감사기록 백업 기능을 사용해야 한다.

- 서비스 거부 공격(Denial Of Service)에 의한 시스템 자원의 낭비를 최소화하기 위하여 관리자는 사용자 수와 시스템 하드웨어 성능에 적합하도록 동시 연결 세션 수를 설정하여야한다.

- 최신의 유해코드에 대처하기 위해서는 Signature의 업데이트가 주기적으로 수행되어야 하며, 본 TOE는 제품 평가 시, Signature를 100개로 한정되어 평가되었음을 유념해야한다.

- 바이러스 엔진 및 유해정보 DB에 대한 업데이트를 수시로 수행하여야 한다.

- 평가제품의 보안기능이 내부망의 모든 자원을 보호할 수는 없으므로 내부망 각각의 시스템에 대해서도 강력한 보안정책 권고 및 운영체제 및 응용프로그램에 대해 항상 최신의 보안 패치가 이루어지도록 해야 한다.

11. 약어 및 용어 정의

아래의 약어 및 용어가 본 보고서에서 사용되었다.

(1) 약어

CC 공통평가기준(Common Criteria)
EAL 평가보증등급(Evaluation Assurance Level)
PP 보호프로파일(Protection Profile)
SOF 기능강도(Strength of Function)
ST 보안목표명세서(Security Target)
TOE 평가대상(Target of Evaluation)
TSC TSF 통제범위(TSF Scope of Control)

(2) 용어

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 사용자로 설치자, 슈퍼관리자, 관리자, 모니터 계정이 존재

외부 IT 실체
TOE 외부에서 TOE와 상호 작용하는 안전하거나 안전하지 않은 모든 IT 제품이나 시스템

SecuiOS
시큐아이닷컴㈜에서 자체 개발한 어플라이언스형 네트워크 보안 게이트웨이를 위한 운영 체제로, TOE의 보안기능을 지원하기 위한 최소한의 사양만으로 구성되어 있다. 크게 프로세스 관리 기능(Process Management), 메모리 관리 기능(Memory Management), 파일시스템 관리 기능(File System Management), 네트워크 통신 기능(Network Communication)의 네가지의 기능을 구현하였다.

12. 참고문헌

인증기관은 아래의 문서를 사용하여 본 인증보고서를 작성하였다:

[1] 정보보호시스템 공통평가기준 (2005. 5. 21)
[2] 정보보호시스템 공통평가방법론 V2.3
[3] 정보보호시스템 평가·인증 지침 (2007. 5. 30)
[4] 정보보호제품 평가인증 수행규정 (2007. 1. 1)
[5] SECUINXG V1.6 보안목표명세서 V1.11 (2007. 5. 29)
[6] SECUINXG V1.6 평가결과보고서, 발행버전 1.0 (2007. 6. 4)

※ 인증효력유지 내역

1. SECUINXG V1.6 변경승인(2007.9.21)

· 변경사항

구분	인증제품	변경승인제품			
모델명	SECUINXG 2000 V1.6	SECUINXG 1000	SECUINXG 400	SECUINXG 200	SECUINXG 100
CPU	Dual Xeon 3.2GHz	Intel Merom 2.67GHz	Intel Yonah Celeron 1.7	Intel M-Celeron 1.2	Intel Celeron 600
Main Memory	2GB	1GB	512MB	512MB	512MB
HDD	400GB×2	400GB	250GB	없음	없음
NIC	12(1Gbps×12) ports	10 ports	8 ports	4 ports	6 ports
USB	USB 2.0×1 port	USB 2.0×2 ports	USB 2.0×2 ports	USB 2.0×2 ports	USB 2.0×1 port
Console port	1 port	변경없음	변경없음	변경없음	변경없음
운영체제	SecuiOS V1.1	변경없음	변경없음	변경없음	변경없음

· 검토결과

인증제품인 2000 모델에 CPU, Memory, NIC 등의 성능향상 후 인증효력유지를 신청한 100, 200, 400, 1000 모델에 대해 보안영향분석서, 보안기능 및 취약성 분석 시험을 통한 시험결과 TOE의 보안기능 및 보증 범위에 영향을 미치지 않는 것으로 확인되어 이를 승인함

2. SECUINXG V1.6 변경승인(2007.12.12)

· 변경사항

구분	인증제품	변경승인제품
모델명	SECUINXG 2000	SECUINXG 800
CPU	Dual Xeon 3.2GHz	Intel Core 2 Duo 1.66GHz
Main Memory	2GB	1GB
HDD	400GB×2	400GB
CF Card	-	512MB
NIC	12(1Gbps×12) ports	10(1Gbps×10) ports
USB	USB 2.0×1port	-
Console port	1 port	1 port
운영체제	SecuiOS V1.1	SecuiOS V1.1

· 검토결과

인증제품인 2000 모델에 CPU, Memory, NIC 등 일부 부품 변경 후 인증효력유지를 신청한 800 모델에 대해 보안영향분석서, 보안기능 및 취약성 분석시험을 통한 시험결과 TOE의 보안기능 및 보증 범위에 영향을 미치지 않는 것으로 확인되어 이를 승인함