CR-19-13

SecureGuard VPN V2.0
인증보고서

인증번호 : NISS-0920-2019

2019년 3월

IT보안인증사무국

1. 제품 개요

SecureGuard VPN V2.0(이하 'TOE')는 외부의 신뢰되지 않은 네트워크 환경에서 외부 사용자들이 내부 네트워크로 접속할 때, 전용망과 같은 효과를 볼 수 있는 SSL VPN 방식의 가상사설망을 제공하는 가상사설망 제품이다. TOE는 네트워크 환경에서 가상사설망 기능(SSL VPN)을 제공하는 제품으로, 하드웨어 일체형 장비와 하드웨어 일체형 장비에 탑재되는 소프트웨어, 그리고 사용자 단말에 설치되는 소프트웨어를 포함하며 다음과 같이 식별된다.

TOE 및 TOE 구성요소 식별은 다음과 같다.

TOE 명	SecureGuard VPN V2.0
TOE 버전	SecureGuard VPN V2.0 (V2.0.0.6)
TOE 구성요소 및 상세버전	SecureGuard VPN Server V2.0 (V2.0.0.6)
	SecureGuard VPN Windows Client V2.0 (V2.0.0.6)
	SecureGuard VPN Linux Client V2.0 (V2.0.0.5)
	SecureGuard VPN Linux ARM Client V2.0 (V2.0.0.5)
	SecureGuard VPN Linux MIPS Client V2.0 (V2.0.0.5)
	SecureGuard VPN Mobile Client V2.0 (V2.0.0.6)
	SecureGuard VPN Mac Client V2.0 (V2.0.0.6)

[표 1] TOE 및 TOE 구성요소 식별

TOE의 물리적 범위에 포함되는 요소는 다음과 같다.

구분	식별 정보	세부 버전	배포파일	배포 형태
TOE명	SecureGuard VPN V2.0	V2.0.0.6	-	
TOE 구성 요소	SecureGuard VPN Server V2.0	V2.0.0.6	SGVPN20_Firmware _V2.0.0.6.iso	H/W 일체형 장비
	SecureGuard VPN Windows Client V2.0	V2.0.0.6	SVWClient_V2.0.0.6.exe	SW 형태로 CD 배포
	SecureGuard VPN Linux Client V2.0	V2.0.0.5	SVLClient_V2.0.0.5.tar.gz	
	SecureGuard VPN Linux ARM Client V2.0	V2.0.0.5	SVLAClient_V2.0.0.5.tar.gz	
	SecureGuard VPN Linux MIPS Client V2.0	V2.0.0.5	SVLMClient_V2.0.0.5.tar.gz	

구분	식별 정보	세부 버전	배포파일	배포 형태
	SecureGuard VPN Mobile Client V2.0	V2.0.0.6	SVMClient_V2.0.0.6.apk	
	SecureGuard VPN Mac Client V2.0	V2.0.0.6	SVMacClient_V2.0.0.6.dmg	
설명서	SecureGuard VPN V2.0 관리자 설명서 V1.1		SGVPN_V2.0_ADM_V1.1.pdf	전자파일 형태로 CD 배포
	SecureGuard VPN V2.0 사용자 설명서 V1.1		SGVPN_V2.0_USR_V1.1.pdf	
하드웨어 모델명	SGV-100, SGV-300, SGV-1000, SGV-3000, SGV-5000, SGV-10000			H/W 일체형 장비
제품 모델명	SecureGuard VPN server V2.0 100 SecureGuard VPN server V2.0 300 SecureGuard VPN server V2.0 1000 SecureGuard VPN server V2.0 3000 SecureGuard VPN server V2.0 5000 SecureGuard VPN server V2.0 10000			H/W 일체형 장비

[표 2] TOE 물리적 범위

TOE에 포함되는 3rd Party 라이브러리는 다음과 같다.

구성요소	소프트웨어
SVServer	TOMCAT 8.0.53
	JDK 1.8.0_60
	OpenSSL 1.0.2q
	PostgreSQL 10.4
	Sendmail 8.14.4
	NTPdate 4.2.6
	Net-snmp 5.7.3
	IPTABLES 1.4.7
	Openssh 7.9p1
	MagicCrypto V2.1.0
클라이언트	OpenSSL 1.0.2q
	MagicCrypto V2.1.0

[표 3] TOE에 포함되는 3rd Party

TOE에서 사용하는 검증필 암호모듈의 정보는 다음과 같다.

구분	세부구분	
검증필 암호모듈	암호모듈명	MagicCrypto V2.1.0
	검증번호	CM-118-2021.8
	개발사	(주)드림시큐리티
	검증일	2016-08-01

[표 4] 검증필 암호모듈

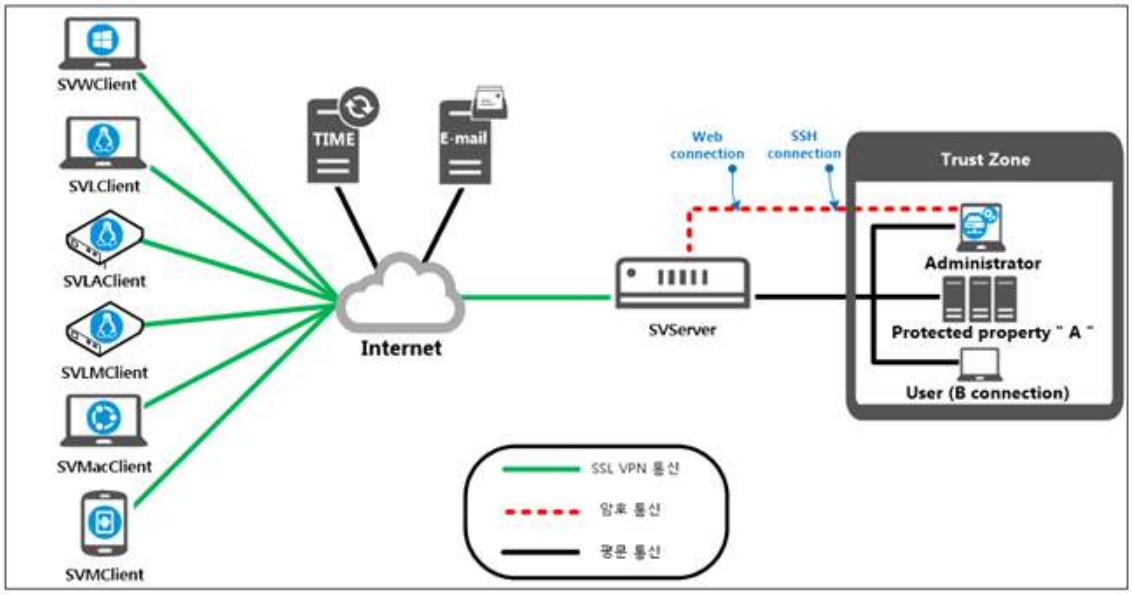
TOE의 하드웨어 일체형 장비 사양은 다음과 같다.

하드웨어 모델명	구분		사양
SGV-100	CPU		Intel® Celeron J1900 (2.0 GHz, 4 Cores)
	RAM		8 GB
	Storage	Flash memory	16 GB
		HDD	1 TB
	NIC		10/100/1000B-RJ45 6port
	Console 포트		RJ45 1port
	USB 포트		2port
	Power		Single
SGV-300	CPU		Intel® CoreTM i3-6100 (3.7 GHz, 2 Cores)
	RAM		8 GB
	Storage	Flash Memory	16 GB
		Storage	1 TB
	NIC		10/100/1000B-RJ45 6port
	Console 포트		RJ45 1port
	USB 포트		2port
	Power		Single
SGV-1000	CPU		Intel® Xeon® E3-1275 v5 (3.6 GHz, 4 Cores)
	RAM		16 GB
	Storage	Flash Memory	16 GB
		Storage	1 TB
	NIC		10/100/1000B-RJ45 6port 1G Base-F FPS 4port
	Console 포트		RJ45 1port
	USB 포트		2port
	Power		Dual

하드웨어 모델명	구분		사양
SGV-3000	CPU		Intel® Xeon® E3-1275 v5 (3.6 GHz, 4 Cores)
	RAM		16 GB
	Storage	Flash Memory	16 GB
		Storage	2 TB (1TB x 2 raid 구성)
	NIC		10/100/1000B-RJ45 8port 1G Base-F FPS 4port
	Console 포트		RJ45 1port
	USB 포트		USB * 2port
	Power		Dual
SGV-5000	CPU		Intel® Xeon® E5-2620 v4 x 2 (2.10 GHz, 8 Cores, 16 Threads, 20MB Cache)
	RAM		32 GB
	Storage	Flash Memory	16 GB
		Storage	2 TB (1TB x 2 raid 구성)
	NIC		10/100/1000 B-RJ45 10port 1G Base-F FPS 8port 10G Base-F FPS 4port
	Console 포트		RJ45 1port
	USB 포트		USB * 2port
	Power		Dual
SGV-10000	CPU		Intel® Xeon® E5-2650 v4 x 2 (2.20 GHz, 12 Cores, 24 Threads, 30MB Cache)
	RAM		64 GB
	Storage	Flash Memory	16 GB
		Storage	2 TB (1TB x 2 raid 구성)
	NIC		10/100/1000B-RJ45 10port 1 G Base-F FPS 8port 10 G Base-F FPS 4port
	Console 포트		RJ45 1port
	USB 포트		USB * 2port
	Power		Dual

[표 5] TOE 하드웨어 일체형 장비 사양

TOE가 보안기능을 수행하기 위한 운영환경은 다음과 같다.



[그림 1] TOE 운영환경

TOE는 SecureGuard VPN Server V2.0 (이하 'SVServer'로 통칭)와 SecureGuard VPN Windows Client V2.0 (이하 'SVWClient'), SecureGuard VPN Linux Client v2.0 (이하 'SVLClient'), SecureGuard VPN Linux ARM Client V2.0 (이하 'SVLAClient'), SecureGuard VPN Linux MIPS Client V2.0 (이하 'SVLMClient'), SecureGuard VPN Mobile Client V2.0 (이하 'SVMClient'), SecureGuard VPN Mac Client V2.0 (이하 'SVMacClient')의 클라이언트 6종으로 구성되어 운영된다.
TOE는 SVServer와 외부에서 접근하는 클라이언트 간 가상채널을 통해 안전하게 데이터를 전송하는 SSL VPN 기능을 지원한다. 관리자는 시리얼 통신을 사용하는 로컬 접속 또는 SSHv2 통신을 사용하는 터미널 접속, TLS V1.2 통신을 사용하는 웹 브라우저 접속을 통해 보안관리를 수행한다. 이때 TOE는 ID/PW를 통한 식별 및 인증 기능을 통과한 관리자에 대해서는 보안관리 기능을 제공한다.
TOE는 신뢰할 수 있는 Time Stamp를 제공하기 위해 NTP서버와 연동하며, 보안 위반 사건 발생 시 인가된 관리자에게 경고메일을 발송하기 위해 메일서버와 연동한다.
SecureGuard VPN Windows Client V2.0의 설치 및 운영에 필요한 하드웨어 사양은 다음과 같다.

구분	사양
CPU	Intel 2.6 GHz 이상
RAM	4 GB 이상
Storage	TOE 설치 및 운영에 필요한 공간 60 MB 이상
NIC	10/100/1000 Base-TX RJ45 포트 1개 이상

구분	사양
운영체제	Windows 7 Ultimate (32bit/64bit) Windows 8.1 Pro (64bit) Windows 10 Pro (32bit/64bit)
SW	Internet Explorer 11, Google Chrome 69

[표 6] SecureGuard VPN Windows Client 최소 설치/운영 사양

SecureGuard VPN Linux Client V2.0의 설치 및 운영에 필요한 하드웨어 사양은 다음과 같다.

구분	사양
CPU	Intel 2.6 GHz 이상
RAM	4 GB 이상
Storage	TOE 설치 및 운영에 필요한 공간 20 MB 이상
NIC	10/100/1000 Base-TX RJ45 포트 1개 이상
운영체제	CentOS 7.0 (Kernel 3.10.0, 64bit)

[표 7] SecureGuard VPN Linux Client V2.0 최소 설치/운영 사양

SecureGuard VPN Linux ARM Client V2.0의 설치 및 운영에 필요한 하드웨어 사양은 다음과 같다.

구분	사양
CPU	ARM Coretex-a5 Dual core 1Ghz 이상 (Armv7l / el12)
RAM	128 MB 이상
Storage	TOE 설치 및 운영에 필요한 공간 32 MB eMMC Flash 이상
NIC	10/100 Base-TX RJ45 포트 1개 이상
운영체제	OpenEmbedded Linux (LNX.LE.2.0.2-61050-9x15) (Kernel 3.0.21 32bit)

[표 8] SecureGuard VPN Linux ARM Client V2.0 최소 설치/운영 사양

SecureGuard VPN Linux MIPS Client V2.0의 설치 및 운영에 필요한 하드웨어 사양은 다음과 같다.

구분	사양
CPU	MIPS 32 24KTM core 400Mhz 이상 (Mipsel / el21)
RAM	128 MB 이상
Storage	TOE 설치 및 운영에 필요한 공간 32MB eMMC Flash 이상
NIC	10/100 Base-TX RJ45 포트 1개 이상
운영체제	eCos, Linux 2.6.36 SDK, OpenWrt (Kernel 2.6.36. 32bit)

[표 9] SecureGuard VPN Linux MIPS Client V2.0 최소 설치/운영 사양

SecureGuard VPN Mac Client V2.0의 설치 및 운영에 필요한 하드웨어 사양은 다음과 같다.

구분	사양
CPU	Intel 계열 2.4GHz Intel Core 2 Duo 프로세서 이상
RAM	2 GB 이상
Storage	TOE 설치 및 운영에 필요한 공간 20MB 이상
NIC	10/100/1000 Base-T * 1 port
운영체제	macOS Sierra 10.12.6 (Kernel 16.7.0, 64bit)

[표 10] SecureGuard VPN Mac Client V2.0 최소 설치/운영 사양

SecureGuard VPN Mobile Client V2.0의 설치 및 운영에 필요한 하드웨어 사양은 다음과 같다.

제품명	항목	내용
Samsung Galaxy S6 (SM-G920K)	Processor	Exynos 7 Octa(7420)
	RAM	3 GB
	Storage	TOE 설치 및 운영에 필요한 공간 20MB 이상
	Network	LTE (KT)
	운영체제	Android 7.0 (Nougat)
	커널버전	3.10.61
Samsung Galaxy S9+ (SM-G965N)	Processor	Exynos 9 Octa (9810)
	RAM	6 GB
	Storage	TOE 설치 및 운영에 필요한 공간 20MB 이상
	Network	LTE(KT)
	운영체제	Android 8.0 (Oreo)
	커널버전	4.9.5

[표 11] SecureGuard VPN Mobile Client V2.0 설치 사양

TOE의 보안관리를 위한 관리자 시스템 최소 사양은 다음과 같다.

구분	최소사양	
관리자 PC	CPU	Intel 2.6 GHz 이상
	RAM	4 GB 이상

구분	최소사양	
	Storage	TOE 운영에 필요한 공간 30GB 이상
	NIC	10/100/1000 Base-TX RJ45 포트 1개 이상
	운영체제	Windows 7 Ultimate 64bit Windows 8 Pro 64bit Windows 8.1 Pro 64bit Windows 10 Pro 64bit
	소프트웨어	Chrome 69 Internet Explorer 11 Firefox 62 SSHv2 통신 규약을 지원하는 소프트웨어

[표 12] TOE 관리자 시스템 최소 요구사양

TOE 운영에 필요한 외부 IT실체는 다음과 같다.

구분	용도
NTP 서버	신뢰할 수 있는 타임스탬프를 제공
Mail 서버	경보메일 발송을 위한 메일서버

[표 13] TOE와 운영에 필요한 외부 IT실체

인증 효력에 관한 고지: 상기 제품의 인증서는 IT보안인증사무국 또는 인증서를 인정하는 기관이 상기 제품에 대해 포괄적인 책임이 있음을 의미하지는 않는다.

2. 주요기능

TOE가 제공하는 보안기능은 다음과 같다.

■ 정보흐름통제

TOE는 VPN 클라이언트 실행 시 및 주기적으로 무결성 검사를 수행하여 무결성이 검증된 클라이언트만 접근을 허용하며, 무결성 검증 외 추가적으로 사용자 단말의 하드웨어 정보 및 MAC 주소를 이용한 클라이언트 PC 인증 그리고 사용자 IP를 이용한 클라이언트 IP인증을 지원한다. VPN 클라이언트 프로그램은 오프라인 배포를 통해 안전한 배포 절차를 따른다. 스마트폰(Android) 클라이언트의 경우, 루팅 여부에 대한 검사를 수행하며 루팅된 단말에 대해 접속 차단을 수행한다.

TOE에서 SSL VPN 통신은 관리자가 등록한 사용자만이 가능하며, SSL VPN 통신 상대간 상호인증은 인증서 기반을 통해 이루어진다. SVServer는 전송 패킷의 출발지, 포트번호와 같은 네트워크 특성에 따른 정보흐름통제 규칙을 제공하며, 추가적으로 접속 허용 시간에 따라 접근 통제를 수행하는 접속 허용 시간 정책을 제공한다.

■ 가상 채널

SVServer는 SVClient 와의 안전한 통신을 위해 SSL 프로토콜을 통한 가상 사설망을 생성한다. SVServer는 통신상대가 비정상적으로 종료되는 경우, 이를 탐지하여 설정된 시간(5분) 이후 해당 세션을 종료하는 기능을 제공한다.

■ 감사기록

SVServer는 감사기능 시작/종료, 관리자 로그인/아웃, 성공/실패, 제품설정, 보안기능 수행내역로그를 생성하며 감사데이터는 일시, 유형, 주체, 작업내역 및 결과를 상세히 포함한다. SVServer는 인가된 관리자가 제품 구성요소로부터 생성된 모든 감사 데이터를 검토하는 기능을 제공하며, 정보해석이 적합하도록 모든 감사데이터에 대해 기간과 조건에 따른 검색을 통한 선택적인 검토 기능을 제공한다. SVServer는 감사 증적내 감사로그에 대해 비인가된 삭제 또는 변경을 차단하기 위해 감사데이터를 삭제 또는 변경하는 UI 및 기능을 제공하지 않는다.

SVServer는 감사기록 저장소의 사용 용량이 인가된 관리자가 지정한 용량(50~95%)를 초과하는 경우 최상위 슈퍼 관리자 및 알람리스트에 등록된 메일 주소로 알람메일을 발송하고 웹관리 화면에 경고 메시지를 표시한다. 저장소 용량 포화 시(96% 이상) 가장 오래된 감사 레코드를 백업 후 저장소 상에서 삭제하여 용량을 95% 이하로 유지한다.

SVServer는 기본적으로 OS시간을 이용하며, NTP 동기화 기능을 지원하여 주요

사건에 대한 정확한 시간 정보를 제공한다.

■ 식별 및 인증

TOE는 관리자 및 사용자의 신원을 검증하기 위해 ID/PW 인증 기능을 제공하고 있으며, SVServer를 통해 다음의 3가지 보안관리 인터페이스를 제공한다.

첫째, 웹을 통해 보안관리를 수행하는 보안관리 웹 인터페이스로 해당 경로로 접근하는 대상은 IP 인증 /계정 식별 및 인증을 통과한 인가된 관리자이다. 계정의 종류(최상위 슈퍼관리자, 슈퍼관리자(읽기/쓰기), 서브관리자(읽기))에 따라 보안관리 웹에서 수행할 수 있는 활동(추가/수정/삭제/조회)이 제한된다. 접근을 시도한 대상이 지정된 인증 실패 횟수(2~5회)를 초과한 경우 계정의 종류에 따라 최상위 슈퍼관리자는 10분간 인증 지연, 슈퍼관리자 / 서브관리자는 계정이 잠겨 최상위 슈퍼 관리자가 계정을 잠김 해제할 때까지 접근 차단된다.

둘째, SSH 터미널을 통해 보안관리를 수행하는 SSH 인터페이스로 해당 경로로 접근하는 대상은 최상위 슈퍼 관리자 계정 식별 및 인증을 통과한 인가된 관리자이다. SSH 터미널에서 수행 가능한 보안관리 활동은 네트워크에 대한 상태 확인 및 조회만 가능하다. 접근을 시도한 대상이 지정된 인증 실패 횟수(2~5회)를 초과한 경우 10분간 인증 지연된다.

셋째, Serial 콘솔을 연결하여 터미널 접근하는 Serial 콘솔 인터페이스로 해당 경로로 접근하는 대상은 SSH 터미널과 마찬가지로 최상위 슈퍼 관리자 계정으로 식별 및 인증을 통과한 인가된 관리자이다. Serial 콘솔에서 수행 가능한 보안관리 활동은 SSH 터미널과 동일하다. 접근을 시도한 대상이 지정된 인증 실패 횟수(2~5회)를 초과한 경우 10분간 인증 지연된다.

SVClient는 사용자 계정에 대한 식별 및 인증을 통하여 SVServer와의 SSL VPN 통신 기능을 제공한다. 만약 식별 및 인증 단계에서 지정된 인증 실패 횟수(2~5회)를 초과한 대상은 최상위 슈퍼 관리자가 계정에 대한 잠김을 해제할 때까지 접근 차단된다.

관리자 및 사용자 계정의 패스워드 등록 시 보안성 기준에 따라 3가지 이상 조합 규칙(영문+숫자+특수문자)과 9자리 이상 40자 이하의 규칙을 만족해야 생성이 가능하다. 관리자 및 사용자의 인증이 진행되는 동안 패스워드는 ●으로 마스킹 되어 노출 위험을 차단한다. 관리자 및 사용자의 인증 실패 시, 피드백은 모두 동일하게 "인증에 실패하였습니다." 메시지를 표시하여 실패 이유에 대한 구체적인 이유를 제시하지 않는다.

제품 설치 후 관리자가 제품에 최초 접속 하려는 경우, 설치 시 등록한 ID 및 패스워드 변경을 강제화 하는 기능을 제공한다.

■ 보안관리

SVServer는 SSL 프로토콜을 사용한 웹 브라우저를 통해 특정 권한을 인가된 관리자만

접속을 허용하며 암호화된 웹 인터페이스를 통해 보안 관리를 한다. SVServer는 SSL VPN 접근제어 정책, SSL VPN을 위한 사용자, SSL 정책, 목적지 네트워크 등의 관리 기능을 제공한다. SVServer는 감사기록 백업 여부, 감사기록 저장소 설정 기능 등의 감사기록 관련 관리 기능을 제공하며, 인가된 관리자가 관리자별 인증 데이터를 설정할 수 있도록 한다. 인가된 관리자는 SVServer를 통해 저장된 감사 기록을 백업할 수 있다.

TOE는 웹브라우저와 SSHv2를 통해 인가된 관리자의 보안관리 기능을 제공한다. TOE의 관리자는 모든 권한을 가진 최상위 슈퍼 관리자와 관리자 계정 관리를 제외한 TOE에서 제공되는 보안관리(SSL VPN 정책, 감사 데이터 관리, 네트워크 인터페이스 관리, 환경 설정 등) 권한을 가지는 슈퍼 관리자, 모니터링 권한만 가지는 서브관리자로 구분되어 있다. 웹브라우저를 통해 식별 및 인증 절차를 성공적으로 마친 관리자는 할당된 권한에 해당하는 보안관리를 수행할 수 있다. 최상위 슈퍼 관리자가 SSHv2 통신을 지원하는 터미널 프로그램을 통해 TOE에 접속하여 보안관리를 수행하는 경우, 보안 관련 설정은 수행할 수 없고 모니터링 기능만 수행한다.

SVServer는 최초 접속 허용 IP 주소의 수를 1개로 제한하여 배포되며, 허용IP에서만 서버에 접속할 수 있다. 관리자는 각 계정마다 등록된 IP 주소에서만 TOE로 접근 가능하다.

■ 전송 데이터 보호

TOE는 물리적으로 분리된 SVServer와 SVClient간 SSL VPN 통신 시 전송 데이터에 대해 검증필 암호 모듈을 이용하여 기밀성 및 무결성을 보장한다. TOE는 관리자간의 웹 보안관리를 위한 전송 구간의 데이터를 HTTPS 프로토콜(TLS V1.2) 및 SSHv2 통신을 지원하는 터미널 프로그램을 통해 안전한 채널로 보호한다.

■ 자체 시험

TOE는 제품의 정확한 운영을 보장하기 위해 시동 시, TOE 운영 중 주기적으로 그리고 관리자의 요청에 의해 실행 프로그램을 대상으로 자체 시험을 수행하며 비정상 수행 발견 시 재 실행을 수행한다. 또한 시동 시, TOE 운영 중 주기적으로 그리고 관리자 요청에 의해 TOE 데이터와 실행 프로그램을 대상으로 무결성 검사를 수행하며 이를 통해 TOE 데이터와 기능에 대한 보호를 수행한다.

■ 안전한 세션 관리

TOE는 관리자 및 사용자에 대해 설정된 시간동안 동작이 없는 경우 세션 종료 기능을 제공한다. 또한 관리자 관리접속 및 사용자 접속 세션에 대해 동일 계정 및 동일 권한에 대한 동시 접속을 금지하여, 동시 세션의 최대 수를 1로 제한하는 기능을

수행한다.

■ VPN 클라이언트 보호

SVClient는 제품이 설치된 사용자 단말에 사용자 ID/패스워드와 감사데이터는 저장하지 않고, 운용 중 발생하는 감사데이터는 모두 SVServer에 전송한다. 운영과 관련된 개인키, 설정파일은 파일로 암호화하여 저장하며, 터널링 형성 후 개인키 등 삭제 대상 정보는 바로 삭제된다. 레지스트리에는 제품 설정값, 감사 데이터 등과 같은 주요 정보가 저장되지 않는다. 제품 실행 시 제품의 운영에 필요한 모든 파일에 대해 무결성을 점검하며, 무결성 훼손 감지 시 클라이언트 접속이 차단된다. 변조된 클라이언트는 오프라인으로 배포된 클라이언트 설치 파일을 재 설치함으로써 수동 복구하는 기능을 제공한다.

■ VPN 클라이언트와 서버간 안전한 연동

SVClient는 서버로부터 전송되는 파일에 대한 부인방지 및 무결성 보장을 위해 인가된 관리자가 사용자 추가 시 생성된 사용자 인증서를 통해 파일 생성 주체에 대한 전자서명을 검증하며 해당 인증서의 유효기간은 1년이다.

■ 암호지원

SSL VPN 통신을 통해 Gateway-To-Client간에 전송되는 사용자 데이터에 대해 암·복호화를 수행하고 있다. VPN 기능을 지원하기 위해 검증필 암호모듈(MagicCrypto V2.1.0)을 통해 암호화를 수행하며, 난수 이용시 검증필 암호모듈의 난수발생기를 사용한다. 암호키 및 암호화에 사용되는 핵심 보안 매개변수에 대한 접근 및 변경은 웹을 통해 인가된 관리자만 수행할 수 있으며, 암호키 및 핵심보안 매개변수는 사용자 단말에 검증필 암호모듈(MagicCrypto V2.1.0)을 통해 암호화 하여 안전하게 저장하여 사용한 후 삭제한다. VPN 통신에 사용되는 암호키는 연결 시마다 새로 생성하여 사용한 후 연결이 끊기면 해당 키를 파기 하고 키 유효기간 종료 시마다 키를 재협상 및 재생성하여, 이 후 연결시에는 새로운 암호키를 생성하여 이전에 생성했던 암호키를 재사용할 수 없다. 또한 암호화하여 저장된 공유키를 메모리에 로드 시에는 키가 평문으로 존재하지 않도록 한다. 키 수명에 따른 키 파기시 모든 암호키 및 보안 중요 매개변수를 '0'으로 바꿔 파기 시킨다.

3. 평가결과 요약

TOE에 대한 평가는 한국정보보안기술원에서 수행하였다. 평가는 제품이 공통평가기준 2부와 3부의 EAL4 평가보증등급을 만족하여, 공통평가기준 1부 305항에 따라 “적합”한 것으로 평가하였다.

[인증제품 식별정보]

평가지침	정보보호시스템 평가인증지침 (2017. 8. 24.) 정보보호제품 평가인증 수행규정 (2017. 9. 12.)
평가제품	SecureGuard VPN V2.0
보호프로파일	없음
보안요구사항	가상사설망 제품 보안요구사항 V1.0
보안목표명세서	SecureGuard VPN V2.0 보안목표명세서 V1.5
평가보고서	SecureGuard VPN V2.0 평가결과보고서 V1.20
적합여부 평가결과	공통평가기준 2부 적합 공통평가기준 3부 적합
평가기준	정보보호시스템 공통평가기준 V3.1 R2
평가방법론	정보보호시스템 공통평가방법론 V3.1 R2
검증필 암호모듈	MagicCrypto V2.1.0, (주)드림시큐리티
평가신청인	에스지앤㈜
개발업체	에스지앤㈜
평가기관	한국정보보안기술원