CR-11-63

Chakra Max Core v2.0 인증보고서

인증번호 : KECS-CISS-0355-2011

2011년 12월

IT보안인증사무국

1. 제품 개요

Chakra Max Core v2.0는(이하 TOE)는 논리적으로 DB사용자와 보호대상DB 사이, 그리고 DB사용자의 PC에 각각 설치되어, 보호대상DB로 접속하여 데이터의 생성, 변경, 삭제 및 조회 활동을 하는 DB사용자에 대하여 접근통제와 감사기능을 수행하는 DB 접근통제 시스템이다.

TOE는 방화벽(Firewall) 시스템으로 보호되는 안전한 환경에 위치하고, 보호대상DB로의 접근 및 권한을 통제하여 보호대상DB에 대한 비 인가된 변경이나 파괴, 유출을 방지한다. 또한, TOE는 인가된 DB사용자의 보호대상DB로의 접근에 대한 감시 및 감사 기능과, 저장된 데이터의 변경 및 삭제 내역을 관리할 수 있는 기능을 제공하여 악의적인 내부 DB사용자의 정보 오용을 방지한다

TOE는 Chakra Max Server v2.0, Chakra Max Manager v2.0, Chakra Max Client v2.0으로 나뉘어 운영되며, 각 부분은 다음과 같은 역할을 수행한다.

- o Chakra Max Server v2.0: 패킷을 분석하여 보호대상DB로의 접근 권한, 접속 통제 기능을 수행하고, 감사데이터를 생성 및 조회 기능을 제공한다.
- o Chakra Max Manager v2.0: 보안관리자로 하여금 TOE의 보안관리 기능을 수행할 수 있는 GUI를 제공한다.
- o Chakra Max Client v2.0: DB사용자로 하여금 TOE의 보안정책에 따라 보호대상DB로 접근할 수 있는 라우팅 기능과, 결재 업무를 할 수 있는 GUI를 제공한다.

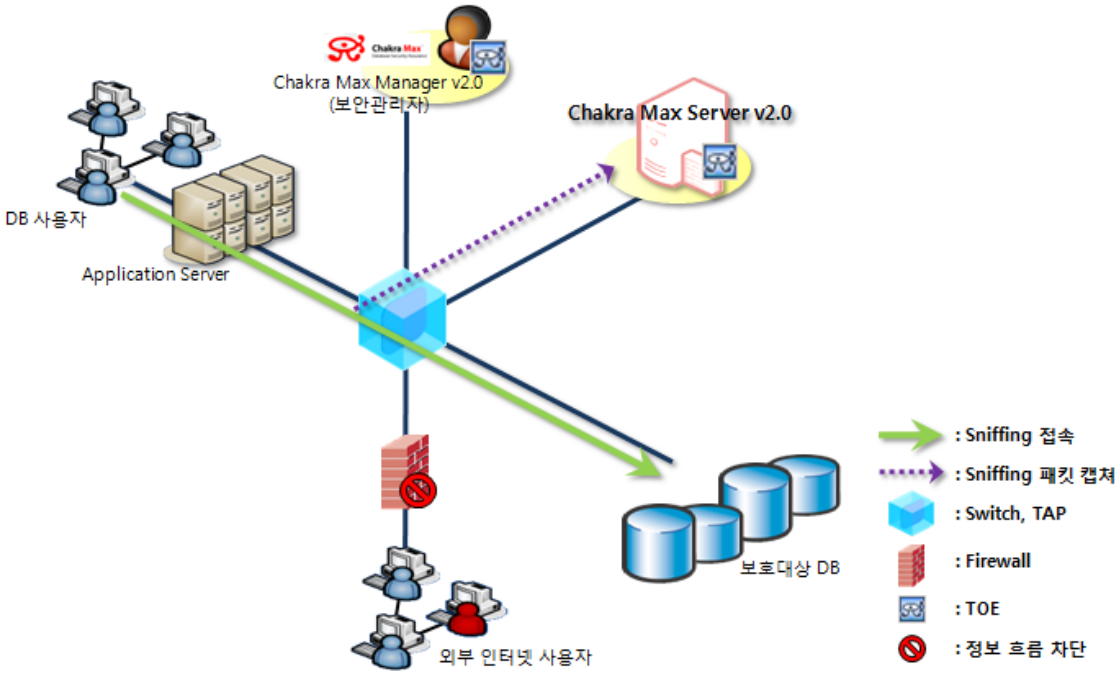
TOE가 보호하는 DBMS 종류는 다음과 같다.

- o Oracle 9i, 10g, 11g
- o MySQL v4, v5
- o MSSQL 2000, 2005, 2008
- o Teradata v12
- o DB2 UDB v8, v9
- o Sybase ASE v12, v15
- o Sybase IQ v12, v15
- o Informix v10, v11
- o Altibase v4, v5
- o Tibero v3, v4

TOE는 아래와 같이 Sniffing Mode, Gateway Mode로 구성할 수 있으며, 두 가지 Mode를 함께 구성하는 Hybrid Mode로 구성할 수 있다.

TOE는 Port Mirroring을 지원하는 Switch 또는 TAP을 통하여 네트워크 스트림에서 패킷을 캡쳐한다. 이와 같은 Sniffing 패킷 캡쳐 방식을 통하여 TOE는 Application Server를

통하여 수행되는 정형적인 SQL의 이력을 감시 및 통제한다. Sniffing Mode에서 TOE는 세션 단위에서 DB사용자의 접근을 통제할 수 있으며, 보안관리자는 실시간으로 불법 접근 DB사용자에 대한 세션을 차단시키는 것이 가능하다.

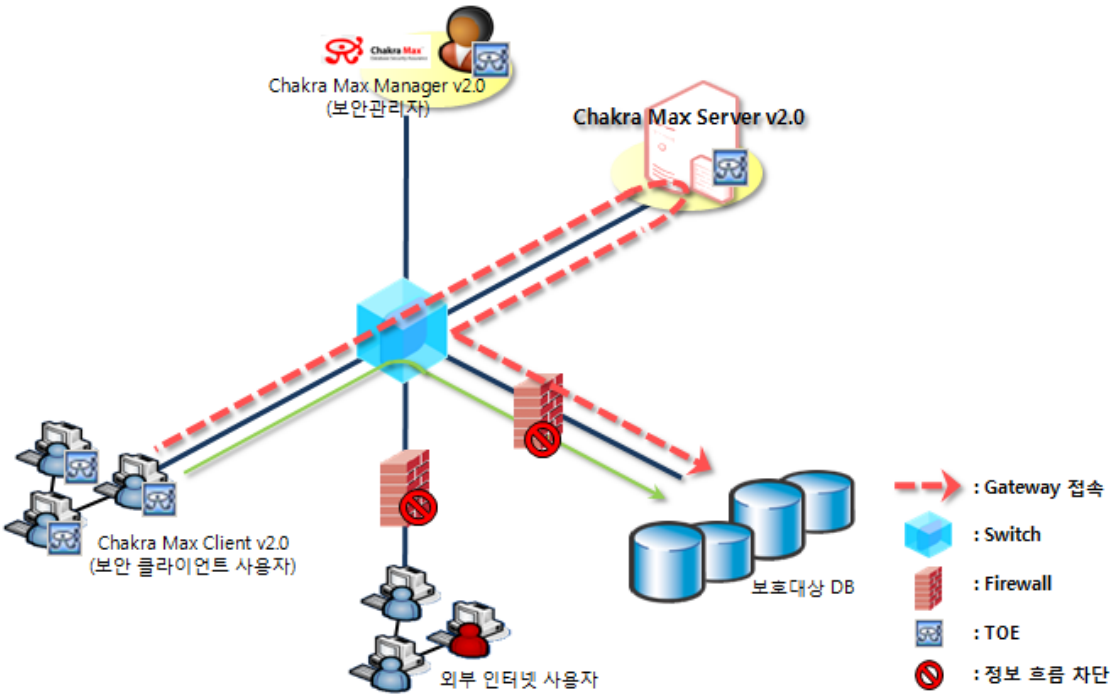


[그림 1] TOE 운영환경(스니핑 모드)

Gateway Mode에서 TOE는 보안 클라이언트 사용자들의 패킷을 TOE로 라우팅 하며, 보안 클라이언트 사용자들이 보호대상DB에 직접 접근하는 것을 금지시킨다. 따라서 보안 클라이언트 사용자들의 보호대상DB로의 접근은 모두 TOE를 경유하게 된다.

이와 같은 구성으로 TOE는 세션 및 SQL 단위에서 DB사용자의 접근을 통제할 수 있으며, 보안관리자는 실시간으로 불법적인 행동을 보이는 보안 클라이언트 사용자에 대한 세션 및 SQL 차단이 가능하다.

Gateway Mode에서 Chakra Max Client v2.0이 설치되지 않거나, 서비스를 실행하지 않은 PC에서의 DB 접속 세션은 방화벽 등의 IT 환경에 의해 차단된다.

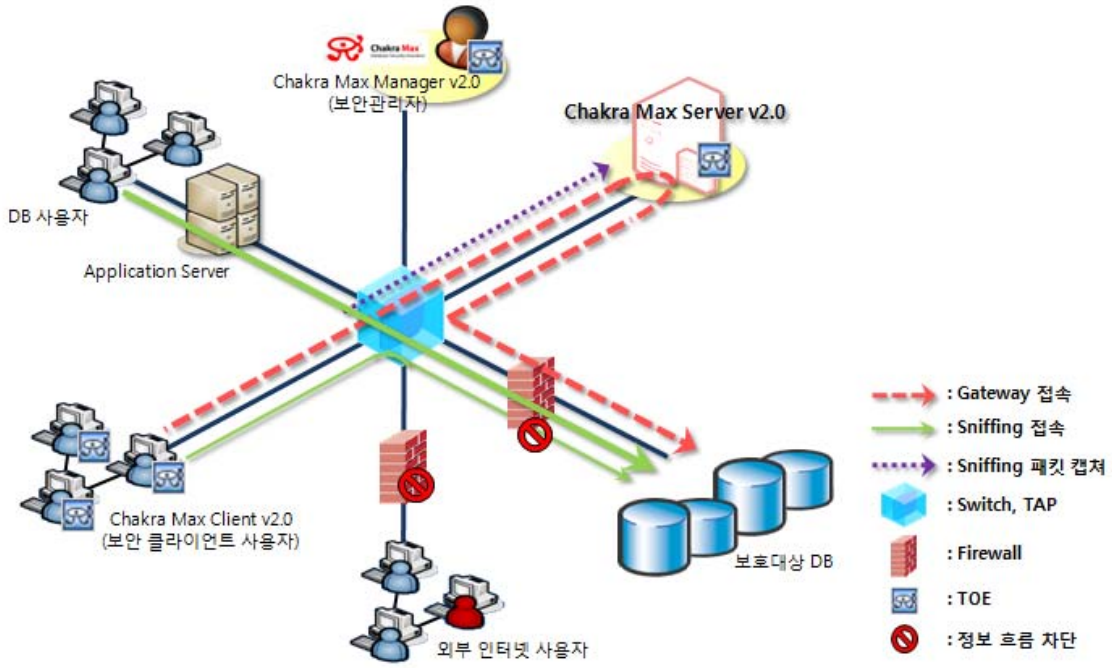


[그림 2] TOE 운영환경(Gateway 모드)

또한 TOE는 Hybrid Mode로 구성될 수 있는데, 이 구성은 Sniffing Mode와 Gateway Mode를 동시에 운영하는 것으로, 보안 클라이언트 사용자 그룹을 포함한 모든 DB사용자들의 보호대상DB 접근을 통합적으로 로깅, 통제, 감사, 관리한다.

Hybrid Mode에서 보호대상DB 앞단에 설치된 방화벽은 보안 클라이언트 사용자의 TOE 직접접속을 차단하고, 허용된 Application Server등에서만 Sniffing 접속이 가능하도록 네트워크 환경을 구성하여야 한다.

또한, Sniffing Mode와 Gateway Mode로 운영되는 사용자그룹은 네트워크에서 명확히 분리되어 운영되어야 하며, 각각의 운영 Mode에서 전송되는 패킷이 서로 섞이지 않도록 안전하게 구성하여야 한다.



[그림 3] TOE 운영환경(Hybrid 구성)

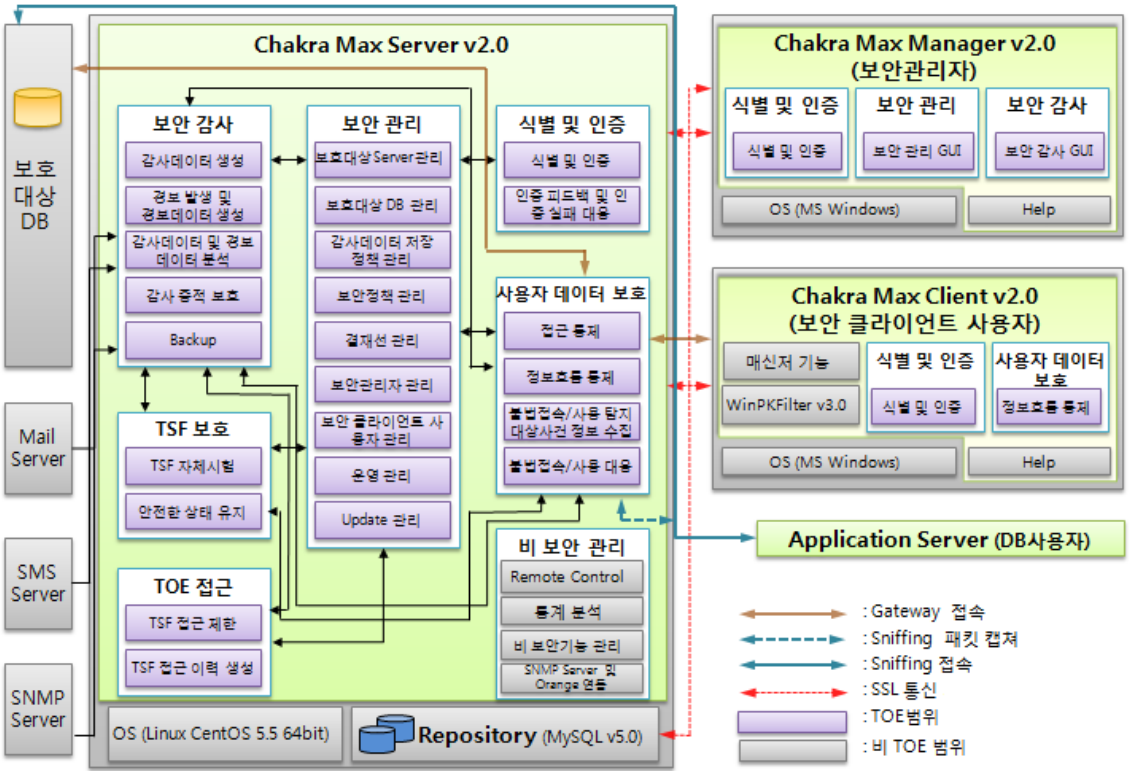
TOE 운영을 위한 하드웨어 및 소프트웨어의 주요사양은 아래와 같다.

TOE	환경	
	하드웨어	소프트웨어/펌웨어
Chakra Max Server v2.0	CPU: Dual Core 2.0Ghz Xeon CPU(64bit)* 2EA 이상 RAM: 4GB Main Memory 이상 NIC: 10/100/1000Mb NIC 3EA 이상 HDD: 80GB 이상	Linux CentOS v5.5 (Kernel 2.6.18) MySQL v5.0
Chakra Max Manager v2.0	CPU: Pentium P4 1.5GHz 이상 RAM: 1GB 이상 NIC: 10/100/1000Mb NIC 1EA이상 HDD: 600 MB 이상	MS Windows 2000/XP/2003/2005/Vista/7
Chakra Max Client v2.0	CPU: Pentium P4 1.5GHz 이상 RAM: 512MB 이상 NIC: 10/100/1000Mb NIC 1EA이상 HDD: 600 MB이상	MS Windows 2000/XP/2003/2005/Vista/7

[표 1] TOE 하드웨어 및 소프트웨어 주요 사양

2. 주요기능

TOE가 제공하는 보안기능은 다음과 같다.



[그림 4] 주요 보안 기능

3. 평가결과 요약

TOE에 대한 평가는 한국산업기술시험원에서 수행하였으며, 2011년 10월 18일에 평가 완료되었다. 평가는 제품이 공통평가기준 2부와 3부의 EAL4 평가보증등급을 만족하여, 공통평가기준 1부 191항에 따라 “적합” 한 것으로 평가하였다.

[인증제품 식별정보]

평가지침	정보보호시스템 평가·인증지침(2009.9.1) 정보보호제품 평가인증 수행규정(2011.7.20)
평가제품	Chakra Max Core v2.0
보호프로파일	없음
보안목표명세서	Chakra Max Core v2.0 보안목표명세서 V1.8
평가보고서	Chakra Max Core v2.0 평가결과보고서 V1.00
적합여부 평가결과	공통평가기준 2부 적합 공통평가기준 3부 적합
평가기준	정보보호시스템 공통평가기준 V3.1
평가방법론	정보보호시스템 공통평가방법론 V3.1
평가신청인	㈜웨어밸리
개발업체	㈜웨어밸리
평가자	한국산업기술시험원 조원준, 정좌진