데이터 시트

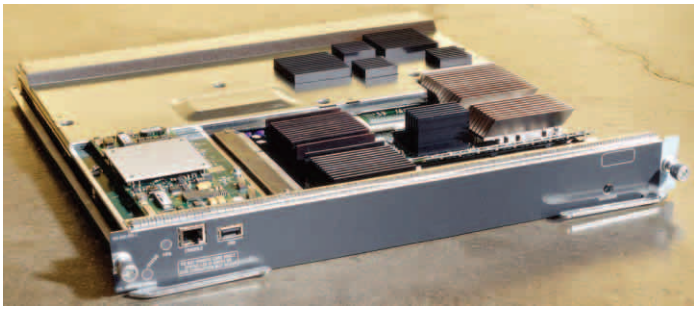
Cisco Catalyst® 6500 Series 및 Cisco 7600 Series용 SSL Services Module

SSL Service Module은 Cisco Catalyst® 6500 Series 및 Cisco 7600 Series 인터넷 라우터용 통합 서비스 모듈로, SSL(Secure Sockets Layer)를 통해 트래픽 보안과 관련하여 프로세서를 집중적으로 사용하는 각종 작업 부담을 덜어 주고, 웹 사이트에서 지원하는 안전한 연결의 수를 늘리며, 고성능 웹 서버 팜의 운영 복잡성을 줄여 줍니다.

SSL Service Module의 주요 기능에는 다음이 포함됩니다.

- *Server SSL 오프 로드(offload)* – SSL과 관련된 모든 기능을 수행하여, 서버들이 고속 투명 텍스트(clear text) 트래픽을 처리할 수 있게 해 줌
- *확장 가능한 성능* –Catalyst 6500 스위치에 SSL 모듈을 추가 설치함으로써 추가적인 성능 요건을 손쉽게 충족할 있음
- *지속성(Stickiness)* – CSM(Content Switching Module)의 통합 모드(Integrated Mode)에서 클라이언트가 새로운 세션 ID를 요청할 경우에도 지속성(persistence)을 유지함
- *인증서 최적화(Certificate optimization)* – 고객 및 인증서 승인 약정(certificate authority agreement)에 따라서 각 서버마다 사본을 하나씩 사용하는 대신, 하나의 인증서 사본만을 공통적으로 사용하여 비용을 절감함

그림 1



최대 4개의 SSL 서비스 모듈을 각 섀시에 설치할 수 있으므로 업계 최고의 SSL 세션 설정 속도와 벌크 암호 처리 용량을 제공하고 최고로 많은 동시 연결을 지원함.

- 모듈 당 1초에 2,500 개의 연결 설정 – 모든 SSL 모듈들이 설치된 경우, 섀시 당 10,000개 연결 가능
- 섀시 모듈 당 300 Mbps 벌크 암호 처리 용량 – 모든 SSL 모듈들이 설치된 경우, 섀시 당 1.2 Gbps
- 60,000개의 동시 고객 연결 – 모든 SSL 모듈이 설치된 경우, 섀시 당 240,000개의 연결

SSL Service Module이 모든 SSL 프로세싱을 담당하므로, 최종 사용자가 접속하는 웹 및 전자상거래(e-Commerce) 서버들은 더 많은 컨텐츠 요청과 온라인 거래를 처리할 수 있게 되어, 암호화 데이터를 사용하는 전자상거래 및 기타 안전한 사이트들의 성능이 몇 배나 향상 됩니다.

전자상거래가 계속 증가하고 점차 더 많은 애플리케이션들이 사용되고 있으므로, 기업 대 소비자(B2C) 및 기업 대 기업(B2B) 간의 거래에서 보안이 더욱 필요하게 되었습니다. 70%의 소비자들은 B2C 거래에서 자신들의 신용카드 번호를 누군가가 절취할 것이라는 두려움 때문에 온라인 거래를 회피하고 있다고 분석가들은 추산하고 있습니다.

따라서, SSL(Secure Sockets Layer)은 안전한 전자상거래를 위한 사실상의 표준이 되었습니다.

기업들은 업무를 합리화하고, 대고객 서비스를 개선하고 거래를 효과적으로 체결하기 위하여 인터넷을 이용하고 있습니다. 또한, 기업들은 기존의 애플리케이션들을 웹으로 이전하여 이 애플리케이션들을 인트라넷이나 엑스트라넷에서 사용될 수 있도록 개방하고 있으므로, 기밀 정보에 대한 안전하고 인증된 고속 접속 기능이 필요하게 되었습니다. 기업들은 인증, 암호화 및 해독 프로세싱을 위하여 SSL 가속기를 점차 더 많이 사용하고 있습니다.

SSL Service Module의 주요 이점

종래의 클라이언트/서버 SSL 모델의 경우, SSL 프로세싱 기능은 SSL NIC 카드를 통하여 서버에 내장되었습니다. 이 구형 모델은 다음과 같은 단점을 가지고 있습니다.

- 클라이언트가 새로운 SSL ID를 요청하면 세션이 단절되어 지속적인 연결이 이루어지지 않으므로 수익 감소를 초래함
- 서버 팜의 각 서버에 대하여 따로 인증서 사본을 구입하여야 하므로 불필요한 비용이 증가함
- SSL 트랜잭션 용량을 확충하기 위하여 웹 서버를 추가해야 하므로, 비용이 증가하고 서버 팜 전체의 가동 중단 시간이 증가함
- SSL 세션을 설정하기 위하여 웹 서버들의 처리 능력이 낭비되므로 시스템 비용이 상승함

시스코는 다음과 같은 이점을 제공하는 통합 SSL Service Module을 도입하여 이러한 단점을 해결하였습니다.

비용 효율적인 솔루션

SSL Service Module은 시장에 나와 있는 모든 SSL 가속기 중에서 최고의 가격 대비 성능을 제공합니다. 유지 비용이 Cisco Catalyst 섀시의 유지 계약에 포함되므로, 년간 서비스 계약 비용을 절감해 줍니다. 프로세싱이 많은 SSL 터미네이션의 부담을 웹 서버로부터 덜어 주므로, SSL Service Module을 이용하면 추가 서버를 구입할 필요가 없습니다. 하나의 섀시에 복수의 모듈을 설치할 수 있으므로, 랙의 공간을 절감하여, 랙 공간이 제약된 경우에는 특히 요긴합니다.

서버 SSL 오프로드(offload)

SSL Service Module은 웹 서버의 SSL 터미네이션 기능을 담당하므로, 웹 서버의 성능이 향상됩니다. 아울러 CSM(Cisco Content Switching Module)과 같은 컨텐츠 처리 스위치가 표준 로드 밸런싱 알고리즘을 사용하여 SSL 모듈들 간에 SSL 트래픽을 균형 있게 배분하고, SSL 모듈로 SSL 세션의 ID 지속성을 유지해 주므로, 전체적인 성능이 더욱 증대됩니다.

확장 가능한 성능

Integrated Content Switching Modules 또는 외부 로드 밸런싱 장치들이 HTTPS의 안전한 컨텐츠 요청을 복수의 Cisco SSL 서비스 모듈에 고르게 배분할 수 있으므로 SSL 터미네이션 성능을 극대화하고 SSL 확장성을 제공합니다. SSL 모듈들은 웹 서버 대신 SSL 프로세싱을 처리해 주므로 웹 서버들은 사용자들의 웹 사용 속도를 저하시키지 않고서 최대 트래픽 요구를 처리할 수 있게 됩니다. SSL 프로세싱은 스위치에 집중화되어 있으므로, 프로세싱의 중단 없이 모듈을 간편하게 추가하여 용량을 쉽게 확장할 수 있습니다.

지속적 연결

통합모드(Integrated Mode)에서, SSL Service Module과 CSM은 클라이언트 브라우저들이 SSL ID를 재협상(renegotiate)하거나 발신 IP 주소가 변경된 경우에도 지속적인 클라이언트와 SSL 장치간의 세션을 유지해 줍니다. 이러한 경우는 무선 트래픽 흐름에서 자주 발생하거나 트래픽이 게이트웨이를 통하여 이동할 때 발생합니다. SSL Service Module과 CSM은 또한 클라이언트들을 특정 웹에 묶어 두기 위한 쿠키 스티키(cookie sticky)를 사용하여 연결 지속성을 유지하므로 전반적인 사용자 속도를 최적화해 줍니다. 아울러, SSL 모듈들이 장애대비형 구성(redundant configuration)으로 설치되면, 하드웨어 장애가 발생하더라도 사용자 세션 상태는 계속 유지됩니다.

간편한 관리 및 구성

또한, SSL Service Module은 인프라 내에 SSL 프로세싱을 통합하고 Cisco Catalyst 6500 Switch의 모든 포트를 SSL 포트로 기능하도록 해 줍니다. SSL Service Module은 웹 서버로 보내는 사용자 데이터를 암호화해 주며, 보안 관리를 간편하게 해 주고, Netscape 및 VeriSign을 포함하는 다양한 인증서를 이용하여 개인 정보, 사용자 기밀성 및 신원 확인 기능을 제공합니다.

고가용성

SSL 모듈과 CSM이 Cisco Catalyst 6500 구성 내에 설치되면, SSL 트래픽은 장애 발생 시에도 유지됩니다. SSL Module의 장애 복구 기능과 Content Switching Module은 고도의 장애 방지 솔루션을 제공합니다.

인증서 원가 절감

SSL 인증서는 복수 웹 서버 프론트 엔드(front end) 설치된 Cisco SSL 모듈에 모두 상주하므로, 인증서 관리가 한 곳에 집중되어 개별 서버 별로 인증서를 따로 구입하거나 관리할 필요가 없게 되어 라이센싱 비용을 절감해 줍니다.

표 1 SSL Service Module의 특징

주요 특징	이점
시스템 용량 및 성능	• 모듈 당 1초에 2,500 연결 설정 – 섀시 당 10K • 60K 동시 클라이언트 연결 – 섀시 당 240K • 300 Mbps 벌크 속도 암호화 – 섀시 당 1.2 Gbps • 256 키 쌍(pair) • 256 키 인증서 • 최대 2K 키 사이즈 • 256 프록시 서버
해시 알고리즘	• MD5(Message Digest 5) • SHA1
암호 슈트	• SSL_RSA_WITH_RC4_128_MD5 • SSL_RSA_WITH_RC4_128_SHA • SSL_RSA_WITH_DES_CSC_SHA • SSL_RSA_WITH_3DES_EDE_CBC_SHA

표 1 SSL Service Module의 특징

주요 특징	이점
핸드쉐이크 (Handshake) 프로토콜	• SSL 3.0 • SSL 3.1/TLS 1.0 • SSL 2.0 (Client Hello) • 세션 재사용 • 세션 재협상
알고리즘	• RC4 • DES • 3DES • RSA • DH • DSA
공용 키 인프라	• RSA 키 쌍(pair) 생성 • 서버 인증서 등록 • 서버 키 및 인증서 임포트 • 서버 키 및 인증서 엑스포트 • 키 및 인증서 갱신 • 서버 인증서의 자동 등록
네트워크 주소 변환	• Client NAT • Server NAT/PAT(Port Address Translation)
확장성	• 동일 장치에 여러 SSL 모듈 장착 가능
고가용성	• CSM을 통해 여러 SSL 모듈 간에 트래픽이 균형 있게 유지됨
서버 로드 밸런싱과 통합	• CSM 장착 Cisco Catalyst 6500 Switch에 긴밀 통합
모니터링	• SSL 세션에 대한 다양한 통계 및 모니터링 기능
핫스와핑 가능	• 온라인 삽입 및 제거
보안 키 저장	• 사설 NVRAM 스토리지에 키가 저장됨
단독형 모드	• 외부 서버 로드 밸런싱 장치와 함께 단독형 구성으로 사용 가능
SSL Session ID 지속성	• SSL 모듈은 세션의 지속성을 유지함

구성 모드 및 트래픽 흐름

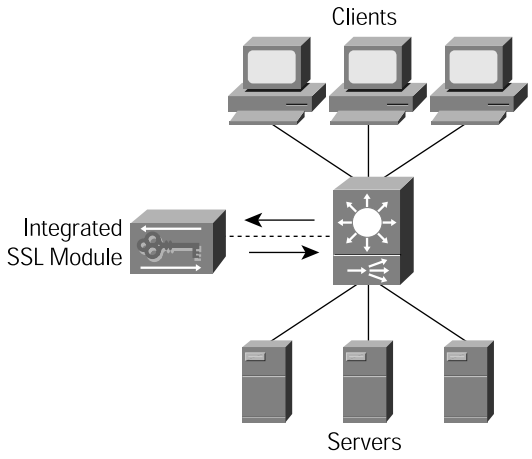
Cisco SSL Service Module은 2가지 기본 구성 방식으로 설치될 수 있습니다.

- 통합 모드 – CSM과 통합 설치
- 단독형 모드 – 외부 서버 로드 밸런싱 장치 사용

통합 모드 구성

표 2에서 보는 바와 같이 SSL Module을 CSM과 통합 설치하면 클라이언트와 서버 간에 암호화된 트래픽 흐름 및 로드 밸런싱된 연결 기능을 제공합니다.

그림 2
SSL Module 통합 모드 구성



클라이언트는 표준 SSL 포트 443을 통하여 암호화된 트래픽을 보냅니다. CSM은 포트 443의 트래픽을 인식하고 SSL 모듈이 설치된 내부 "서버 팜" 으로 해당 암호화 트래픽을 균등하게 배분하여 전달합니다. 선택된 SSL Service Module은 트래픽의 암호를 해독하고, SSL Session ID를 부착하여, CSM 상의 VIP(Versatile Interface Processor)로 투명 텍스트 연결 과정을 시작하여, "해독된 SSL 트래픽"을 수신하도록 구성된 포트(예를 들어 포트 81)로 해당 트래픽을 보냅니다.

CSM은 해독된 트래픽을 받아서 웹 서버를 선택한 후 로드 밸런싱을 결정하고 트래픽을 전달합니다. CSM이 웹 서버로부터 응답 트래픽을 수신하면, 이를 해당 연결을 개시한 SSL Service Module로 보냅니다.

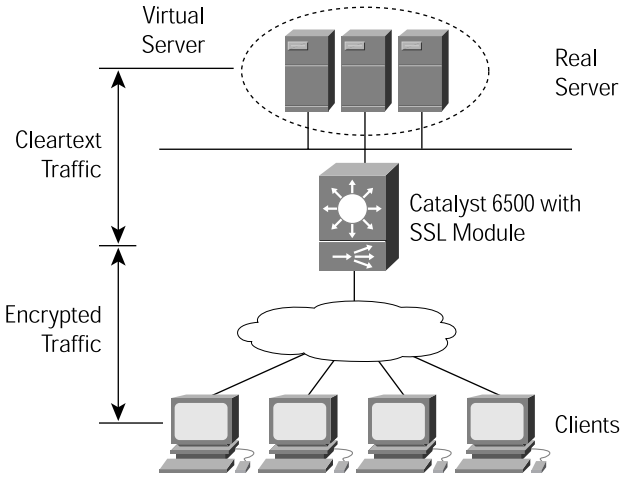
*SSL Module*은 암호화되지 않은 트래픽을 받아서 암호화한 후, 포트 443에서 다시 CSM으로 보냅니다. CSM은 암호화된 트래픽을 받아서 다시 클라이언트로 보냅니다.

주: 선택된 SSL Module과 클라이언트는 해당 흐름을 구성하는 모든 TCP 연결에 SSL Session ID를 사용합니다. CSM은 또한 해당 SSL Session ID의 일부 데이터를 사용하여 선택된 SSL Service Module을 해당 클라이언트에 지속적으로 연결되도록 합니다. 클라이언트가 SSL Service Module로부터 새로운 SSL 세션 ID를 요청할 때, CSM은 해당 클라이언트와 선택된 SSL Service Module 간의 연결을 지속적으로 유지되도록 할 수 있습니다.

CSS 또는 기타 서버 로드 밸런싱 장치에서의 독립형 모드

그림3에서 보여 주는 독립형 모드의 경우, SSL Service Module은 서버 로드 밸런싱 기능(하드웨어 또는 소프트웨어)이 없는 Cisco Catalyst 6500 새시에 설치됩니다.

그림 3
SSL Module 독립형 모드 구성



Catalyst 6500는 트래픽 흐름을 클라이언트나 서버로부터 SSL 모듈로 보내기 위하여 SSL 모듈 IP 주소와 포트 번호를 연계하는 정보가 들어있는 ACL(Access Control Lists)을 사용합니다. 클라이언트에서 서버로 전송되는 트래픽의 경우에는, ACL은 SSL 포트인 포트 433으로 보내야 할 데이터 흐름을 식별합니다. Catalyst 6500은 ACL 내용과 연계되지 않은 보통 데이터 트래픽은 SSL 모듈로 먼저 보내지 않고 서버로 곧 바로 전송되도록 허용합니다.

독립형 모드의 트래픽 흐름은 다음과 같은 예외 사항을 제외하고 통합 모드의 흐름과 매우 유사합니다.

- SSL 세션의 ID 지속 연결 기능은 지원되지 않음
- 클라이언트와 서버는 별도의 서브네트에 속해 있어야 함
- 서버는 실제 서버 주소 또는 실제 서버들의 집합에 부여된 가상 주소일 수 있음
- 서버의 로드 밸런싱 장치의 용량에 따라서 쿠키 지속(cookie sticky) 기능은 지원되거나 안될 수도 있음

주문 정보

제품 번호	설명
WS-SVC-SSL-1-K9	SSL Service Module
WS-SVC-SSL-1-K9=	예비용 SSL Service Module
SC-SVC-SSL-1.1-K9	SSL Service Module Software Release 1.1
SC-SVC-SSL-1.1-K9=	예비용 SSL Service Module Software Release 1.1

라이센스

라이센스가 필요없음.

시스템 요건

- Supervisor 2/MSFC2(Multilayer Switch Feature Card 2)
- Native Cisco IOS(r) 소프트웨어 릴리즈 12.1(13)E 이상
- Hybrid CatOS 최소 소프트웨어 릴리즈 7.5(1)
- Cisco Catalyst 6500 Series Switch 또는 Cisco 7600 Series Internet Router에서 슬롯 1개 점유
- 동일 섀시에서 최대 4개의 SSL 모듈 장착 가능

환경 조건

운용 온도: 32 ~ 104°F (0 ~ 40°C)
보관 온도: -40 ~ 167°F (-40 ~ 75°C)
상대 습도: 10% ~ 90%, 비응축
운용 고도: -60 ~ 4000m

규정 준수

안전

UL 1950
CSA C22.2 No. 950-95
EN60950
EN60825-1
TS001
CE 표시
IEC 60950
AS/NZS3260

EMI

FCC Part 15 Class A
ICES-003 Class A
VCCI Class B
EN55022 Class B
CISPR22 Class B
CE 표시
AS/NZS3548 Class B

NEBS

SR-3580-NEBS: Criteria Levels (Level 3 Compliant)
GR-63-CORE-NEBS: Physical Protection
GR-1089-CORE-NEBS: EMC and Safety

ETSI

ETS-300386-2 Switching Equipment

통신

ITU-T G.610
ITU-T G0.703
ITU-T G0.707
ITU-T G.783 Sections 9-10
ITU-T G0.784
ITU-T G0.803
ITU-T G0.813
ITU-T G0.825
ITU-T G0.826
ITU-T G0.841
ITU-T G.957 Table 3
ITU-T G0.958
ITU-T I.361
ITU-T I.363
ITU I.432
ITU-T Q0.2110
ITU-T Q0.2130
ITU-T Q0.2140
ITU-T Q0.2931
ITU-T O.151
ITU-T O.171
ETSI ETS 300 417-1-1
TAS SC BISDN (1998)
ACA TS 026 (1997)
BABT /TC/139 (Draft 1e)

www.cisco.com/kr

2003-07-30

■ Gold 파트너	• (주)데이콤아이엔	02-6250-4700	• (주)데이타크레프트코리아	02-6256-7000	• (주)인네트	02-3451-5300
	• 한국아이비엠(주)	02-3781-7800	• (주)콤텍시스템	02-3289-0114	• 쌍용정보통신(주)	02-2262-8114
	• 에스넷시스템(주)	02-3469-2400	• 현대정보기술	02-2129-4111	• (주)링네트	02-6675-1216
	• 한국후지쯔(주)	02-3787-6000	• 한국휴렛팩커드(주)	02-2199-0114	• 케이디씨정보통신(주)	02-3459-0500
■ Silver 파트너	• (주)시스폴	02-6009-6009	• 한국NCR	02-3279-4423	• 한국유니시스(주)	02-768-1114,1432
	• (주)인성정보	02-3400-7000	• 포스데이타주식회사	031-779-2114		
■ Local SI 파트너	• (주)LG씨엔에스	02-6276-2821	• 이스텔시스템즈(주)	031-467-7079	• SK씨앤씨(주)	02-2196-7114/8114
	• 대우정보시스템(주)	02-3708-8642				
■ Global 파트너	• 이퀀트코리아	02-3782-2600				
■ Local 디스트리뷰터	• (주)소프트뱅크코리아	02-2187-0114	• (주)인큐브테크	02-3497-9303	• (주)아이넷뱅크	02-3400-7486
	• SK Global	02-3788-3673				
■ IPT 파트너	• 청호정보통신	02-3498-3114	• LG기공	02-2630-5156		
■ WLAN 전문 파트너	• (주)에어키	02-584-3717	• (주)텔레트론INC	02-2105-2300		
■ VPN/Security 전문 파트너	• 코코넛	02-6007-0133	• TISS	051-743-5940	• 이노비스	02-6288-1500
■ NMS 전문 파트너	• (주)넷브레인	02-573-7799				
■ CN 전문 파트너	• 메버릭시스템	02-6283-7425				
■ Workgroup Storage 전문 파트너	• 메크로임펙트	02-3446-3508				