세계 10대 은행 중 한 곳, Entrust nShield HSM으로 고객과 제휴 기업에 신뢰성 있고 안정적인 웹 서비스 제공

비즈니스적 난관

온라인상 고객을 마주하는 어느 기업이나 서비스를 이용하는 사용자를 대상으로 인증을 시행합니다. 세계적인 은행도 마찬가지입니다. 인터넷과 온라인 거래의 광범위한 성장에 따라, 온라인과 클라우드 상에서 주고받는 중요 데이터에 대한 위협 또한 더욱 커졌습니다.

온라인 서비스는 로그인 메커니즘을 이용해 최종 사용자의 브라우저를 웹 서버에 연결하는데, 이때 인터넷상에서 데이터를 암호화하는 기술인 보안 소켓 계층(SSL)이 이 연결에 보안을 제공합니다. SSL 표준(브라우저상에서 자물쇠 기호로 표시되는 기술로, 공식 명칭은 전송 계층 보안 또는 TLS)은 온갖 유형의 인터넷 통신을 보호하는 실질적인 보안 방식입니다.

« 계속해서 증가하는 인터넷 트래픽과 하트블리드 등의 다양한 SSL 기반 악성 소프트웨어의 공격에 직면하여 이 세계적인 은행은 은행 시스템을 감염시킬 수 있는 숨은 바이러스나 다른 악성 소프트웨어가 없도록 SSL 트래픽을 안전하게 검사하는 역량을 확대하고 강화해야 했습니다. »

세계 주요 은행

신뢰성 있고 안정적인 웹 서비스를 사용자에게 제공하려면 기업들은 비밀 유지, 무결성, 웹 서비스에서 처리하는 데이터의 유효성 문제를 해결해야만 합니다. 계속해서 증가하는 인터넷 트래픽과 하트블리드 등의 다양한 SSL 기반 악성 소프트웨어의 공격에 직면하여 이 세계적인 은행은 은행 시스템을 감염시킬 수 있는 숨은 바이러스나 다른 악성 소프트웨어가 없도록 SSL 트래픽을 안전하게 검사하는 역량을 확대하고 강화해야 했습니다. 구체적으로, 이 프로젝트의 주안점은 은행의 제휴사나 자회사, 임직원이 생성하는 트래픽을 검사하는 것이었습니다.

기술적 난관

오늘날 네트워크를 오가는 암호화된 트래픽의 양이 증가하면서 숨은 악성 코드가 탐지망을 벗어나 SSL을 공격의 매개체로 삼기도 합니다. SSL 검사는 암호화된 데이터 내에 숨은 잠재 위험 요소를 차단하는 데 사용됩니다.

SSL 검사에는 웹사이트 트래픽을 가로채 복호화, 검사, 재암호화하여 최종 목적지로 전송하는 과정이 포함됩니다.

하드웨어 보안 모듈(HSM)은 복호화와 재암호화 과정에서 증가하는 SSL 키 사용에 대하여 한층 더한 보안을 제공합니다. 검사가 가능하도록 트래픽을 복호화, 검사 및 재암호화하고 (트래픽이 다시 복호화되는) 웹 서버로 전송된다는 점은 이 과정에서 필요한 키를 좀 더 빈번하게 찾아야 한다는 의미입니다. 일반적으로, 사용하는 모든 키는 서로 다릅니다. 따라서 더욱 강력한 보안이 필요합니다.

HSM은 신뢰점을 제공하여 중요한 네트워크 연결을 보호할 뿐만 아니라 연결의 신뢰성을 높여줍니다. 은행의 보안 설계자에 따르면, 하드웨어 보안 모듈(HSM) 없이도 인터넷 트래픽을 검사할 수는 있지만 위험도가 크게 상승합니다.

ENTRUST.COM/HSM에서 자세히 보기

세계 주요 은행

웹 트래픽을 복호화하는 기술을 보호해야 하는데, 이는 복호화 키를 안전하게 보호하는 것을 의미하고, 복호화 키의 보안이 바로 HSM이 제공하는 기능입니다.

솔루션

은행은 Entrust nShield Connect HSM를 구축해, 서로 약 10km 떨어진 두 곳의 데이터센터에서 동일한 2개의 '액티브/액티브' 구성을 구현했습니다. Entrust nShield Connect HSM은 오늘날 프록시 서버 45개의 보안 요건을 충족하고도 여유롭게 추가 수용이 가능합니다.

결과

Entrust nShield HSM은 레거시 시스템에 대비해 최소 5배의 수용량을 달성할 것으로 나타납니다. 이는 기업이 시스템 확장에 맞춰 인터넷 트래픽을 검사해 숨어있을 수 있는 악성 코드를 확인하거나 보안을 보장하도록 합니다.

이 세계 주요 은행은 10년 이상 Entrust와 협력해왔으며 사실상 Entrust를 지정 HSM 제공업체로 선택했는데, 이는 관련 기술과 보안 문제에 대한 Entrust의 풍부한 경험 때문입니다. Entrust는 전문 서비스팀 또한 투입하여 HSM을 설치하고 은행 임직원을 대상으로 실무 교육을 실시했습니다.

세계 주요 은행

비즈니스적 요구

- 사용자에게 신뢰성 있고 안정적인 웹 서비스 제공

기술적 요구

- 증가하는 사내 인터넷 트래픽 양을 모니터링하고, 모니터링 기술 보호
- 기업의 핵심 IT 인프라 보호

솔루션

- Entrust nShield Connect HSM의 '액티브/액티브' 운용 방식으로 SSL 키 관리 및 보안

결과

- FIPS 140-2 레벨3 인증, 공동 평가 기준 EAL4+ 인증 보안
- 레거시 시스템 대비 5배 수용량
- 향후 필요에 따라 간편하게 확장 가능

ENTRUST 소개

Entrust는 믿을 수 있는 신원, 결제 및 데이터 보호를 가능케 함으로써 안전한 세상을 유지합니다. 사람들은 국경을 넘고, 구매를 하고, 전자 정부 서비스에 접속하고 기업 네트워크에 로그인하는 것이 원활하고 안전한 경험이기를 오늘날, 그 어느 때보다도 더 요구합니다. Entrust는 이와 같은 모든 상호작용의 핵심에 있는 디지털 보안 및 자격 증명 발급 솔루션에 있어 견줄 데 없는 다양성을 자랑합니다. 2,500명이 넘는 동료 및 글로벌 파트너로 구성된 네트워크, 그리고 150개국 이상의 고객을 보유한 당사는 세계에서 가장 신뢰 받는 기관들의 신뢰를 받고 있습니다.

에서 자세히 보기
entrust.com/HSM

ENTRUST

연락처:
HSMinfo@entrust.com