

IBM Security Web Gateway Appliance AMP 5100

웹 애플리케이션 보호 기능이 내장된 차세대 웹 액세스 관리 솔루션



주요 특징

- 온라인 포털 및 비즈니스 이니셔티브에 대한 중앙집중식 사용자 인증, 권한 부여, 보안 세션 관리를 구현합니다
- IBM® X-FORCE® 연구개발 팀의 지원을 통해 웹 위협으로부터 사용자 액세스 및 애플리케이션을 보호합니다
- 배치 및 관리가 용이한 어플라이언스로 비용을 절감하고 복잡도를 낮춥니다
- 확장성이 뛰어나며 구성 가능한 솔루션으로 다양한 애플리케이션 환경을 지원합니다
- 로컬 관리 그래픽 사용자 인터페이스(GUI) 및 자동 서비스 업데이트로 설정 및 유지보수가 간소화됩니다
- 라이브 대시보드를 통해 어플라이언스의 전반적인 상태, 가용성, 성능을 모니터링할 수 있습니다

오늘날의 IT 환경에는 파트너, 고객, 소셜 미디어, 클라우드 컴퓨팅 및 모바일 엔드포인트가 포함되어 있으며, 중요한 비즈니스 애플리케이션에 대한 안전한 액세스 제공이 점점 어려워지고 있습니다. 이와 동시에, 애플리케이션 계층에서의 온라인 공격은 그 어느 때보다 교묘해지고 있습니다. 끊임없이 일어나고 있는 웹 기반 보안 공격에 효과적으로 대처하면서 다양한 애플리케이션 및 사용자 커뮤니티의 액세스 요구사항을 지원하려면 외부 위협에 대한 보호 및 모니터링 기능이 내장된 유연한 웹 액세스 관리 솔루션이 필요합니다.

IBM Security Web Gateway Appliance AMP 5100은 하드웨어 어플라이언스 기반 보안 솔루션으로서, 액세스를 제어하고 웹 기반 위협으로부터 애플리케이션을 보호합니다. 리버스 HTTP 프록시(WebSEAL) 기능과 웹 애플리케이션 방화벽 및 HTTP 프론트 엔드 로드 밸런서가 결합된 이 어플라이언스는 애플리케이션에 대한 안전한 액세스를 제공하면서 최신 위협으로부터 애플리케이션을 보호합니다. 확장성과 구성 가능성이 뛰어난 이 어플라이언스를 이용하면 비용을 절감하면서 웹 애플리케이션 관리 복잡도를 줄일 수 있습니다.

Security Web Gateway Appliance에는 정교한 어플라이언스 프레임워크, 프론트 엔드 로드 밸런서, 운영 체제 및 시스템 관리 간소화에 필요한 모든 소프트웨어가 사전 설치된 펌웨어 패키지로 포함되어 있습니다. Security Web Gateway Appliance는 배치가 용이한 단일 하드웨어 어플라이언스를 제공하며 여기에는 IBM X-FORCE 연구개발 팀이 지원하는 지속적인 웹 애플리케이션 보호와 업계 최고의 웹 액세스 관리가 포함됩니다.



IBM Security Access Manager for Web 소프트웨어 기능이 내장되어 있는 이 어플라이언스를 통해 IT 조직은 모바일 디바이스, 소셜 미디어 사이트, 클라우드 환경에서의 액세스를 포함하여 웹 애플리케이션에 대한 사용자 액세스를 모니터링 및 인증할 수 있습니다.

지능형 보안 공격으로부터 애플리케이션을 보호

Security Web Gateway Appliance에는 자체 내장 정책 서버 및 LDAP(Lightweight Directory Access Protocol) 레지스트리와 더불어, 사용자와 애플리케이션 서버 사이에 위치한 리버스 HTTP 프록시(WebSEAL) 기능이 있습니다. WebSEAL 프록시는 중앙집중식 인증 및 사용자 세션 관리, 웹 싱글 사인온, 광범위한 인증 기능을 제공합니다. WebSEAL을 통과한 요청은 인증 서비스에 의해 평가되며 사용자가 요청한 자원에 대한 액세스 권한을 부여할지 여부가 결정됩니다.

IBM X-FORCE 팀이 지원하는 PAM(Protocol Analysis Module)에 바탕을 둔 웹 애플리케이션 보호 기능은 웹 애플리케이션, 웹 2.0 및 데이터베이스를 웹 애플리케이션 방화벽과 동일한 수준으로 보호합니다. 모든 HTTP 트래픽을 스캔하여 탐지된 위협을 차단할 수 있으며, 애플리케이션 서버에 접근하는 것을 방지할 수 있습니다. 이 기능은 XSS(cross-site scripting), SQL 인젝션 등과 같은 다수의 웹 애플리케이션 취약성 공격을 사전에 차단합니다. IBM PAM(Protocol Analysis Module)을 설계한 X-FORCE 연구개발 팀은 위협을 선제적으로 방어하는 콘텐츠 업데이트를 제공하고 있습니다.

또한, 이 어플라이언스를 다른 IBM Security 솔루션(예: IBM Security Identity Manager 및 IBM Security Federated Identity Manager)과 통합하면 사용자 셀프 서비스 및 라이프사이클 관리, 컨텍스트 기반 액세스 제어, 통합 싱글 사인온과 같은 추가 기능을 얻을 수 있습니다.

Security Web Gateway Appliance를 IBM QRadar Security Intelligence Platform과도 통합할 수 있습니다. 이에 따라, 액세스 보안 관리의 간소화, 운영 비용 절감, 보안 규제준수 입증 가능하며 향후 수 년간 최신 외부 웹 위협에 선제적으로 대응할 수 있습니다.

변화하는 보안 요구사항에 적응

Security Web Gateway Appliance는 확장성과 구성 가능성이 뛰어나므로 다양한 애플리케이션 환경을 지원할 수 있습니다. 이 어플라이언스를 통해 고객, 비즈니스 파트너, 직원, 공급업체 및 유통업체는 클라우드, 모바일, 엔터프라이즈 포털 자원에 안전하게 액세스할 수 있습니다.



IBM Security Web Gateway Appliance

IT 복잡도를 줄이고 비용을 절감

사용이 편리하도록 Security Web Gateway Appliance와 패키징된 IBM Security Access Manager for Web 소프트웨어를 이용하면 다양한 웹 및 애플리케이션 자원에 대한 보안 정책을 강제화할 수 있습니다. 이 소프트웨어를 이용하면 별개의 개별 솔루션 관리에 따른 복잡도를 배제하고, 관리를 간소화하고, IT 비용을 절감하여 IT 직원들이 다른 전략적인 이니셔티브에 더 많은 시간을 할애하도록 할 수 있습니다.

Security Access Manager는 다음과 같은 기능을 제공합니다.

- 비즈니스 애플리케이션(예: 고객 관계 관리 및 전사적 자원 관리(ERP)) 및 직원 포털에 바로 사용 가능한 정책 기반의 보안
- Security Federated Identity Manager에 대한 통합 지원 – 클라우드 환경에서의 연합 사용자 액세스, 모바일 환경에서의 리스크 기반 액세스, 보안 세션 관리
- 오랜 시간이 소요되며 오류가 잦은 애플리케이션 단위가 아니라, 단 한 번에 이행되는 강력한 인증 지원
- 단일 배치에서 수백 만에 달하는 사용자를 지원할 수 있는 확장성, 고가용성, 성능
- 사업부 및 계열사에 대한 다수준 권한 위임 기능과 유연한 웹 기반 관리 인터페이스
- 10억 명의 사용자까지 확장 가능한 레지스트리와 특정 고객 표준이 될 수 있는 여타 주요 레지스트리에 대한 지원

고급 보안을 간단하게 구축

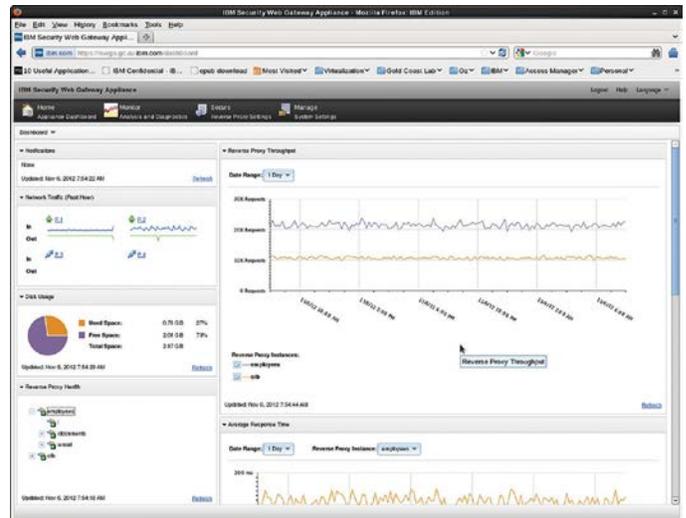
Security Web Gateway Appliance는 배치, 구성, 유지보수가 간단한 어플라이언스 폼팩터에서 견실한 상시 보안 기능을 제공합니다. 이를 통해 IT 조직은 가치 창출 시간을 단축하고 기술 투자수익률을 제고할 수 있습니다. 이 어플라이언스는 다음을 통해 구성을 능률화하고, 모니터링을 간소화하며 라이프사이클 관리 비용을 절감합니다.

- 운영 체제와 시스템 관리 간소화에 필요한 모든 소프트웨어가 사전 설치된 펌웨어
- 자동 서비스 업데이트 및 위협 정의에 대한 지원
- 현재 구성을 캡처하고 이미지 백업을 지원하는 스냅샷 기능
- 이전 구성으로 즉시 복원이 가능한 펌웨어 롤백 지원

- 지원 문제 해결에 필요한 추적과 주요 로그 파일을 캡처하는 옵션
- 기존의 개별 솔루션(예: HTTP 리버스 프록시 서버)을 통합하는 기능

웹 기반 대시보드로 환경을 관리

IT 효율을 제고할 수 있도록, Security Web Gateway Appliance는 하드웨어 및 HTTP 리버스 프록시를 구성하는 웹 기반 그래픽 관리 인터페이스를 제공합니다. IT 관리자는 이 웹 인터페이스에 포함된 대시보드를 이용하여 세부적인 성능, 워크로드, 응답 시간을 비롯한 전반적인 어플라이언스의 상태를 확인할 수 있습니다.



관리자가 전반적인 어플라이언스 상태를 확인할 수 있는 웹 기반 인터페이스

로드 밸런싱을 이용하여 가용성을 향상

네트워크 트래픽을 처리하는 디바이스는 고도의 신뢰성을 요합니다. IT 조직은 Security Web Gateway Appliance의 프론트 엔드 및 백엔드 로드 밸런싱 기능을 이용하여 신뢰성과 가용성을 향상시킬 수 있습니다. 프론트 엔드 로드 밸런싱 기능을 WebSEAL 기능 및 웹 애플리케이션 방화벽과 결합하면 액세스를 제어하고 웹 기반 공격으로부터 시스템을 보호할 수 있습니다. 네트워크 트래픽을 모니터링하고 여러 어플라이언스에 걸쳐 효율적으로 리라우팅함으로써 성능을 향상할 수 있습니다. 사용자 세션을 기반으로 백엔드 애플리케이션 서버와의 "일관성"을 유지할 수 있으며, 예비 어플라이언스를 구성하여 로드 밸런서의 장애복구 기능을 사용할 수 있습니다.

지속적인 규제준수를 입증

Security Web Gateway Appliance는 보안 규정, 산업 표준, 기업 정책에 대한 규제준수를 입증할 수 있는 또 다른 방식을 제공합니다. 사베인즈-옥슬리법, 개인정보보호법, 정보통신망법, 전자금융감독규정 등의 법규에는 구체적인 보안 정책 시행과, 지속적인 규제준수의 입증이 감사 통과에 필수적인 조건으로 규정되어 있습니다. IBM Security Web Gateway Appliance에 내장되어 있는 웹 애플리케이션 방화벽의 추가 보안 기능을 이용하면 감사 준비에 만전을 기할 수 있습니다.

IBM을 선택해야 하는 이유

IBM Security Web Gateway Appliance는 전세계의 기업이 신뢰하는 ID 및 액세스 관리 솔루션으로서, 최신 보안 위협으로부터 중요한 비즈니스 자원을 보호할 수 있는 입증된 기술입니다.

단순한 사용자 액세스 및 인증 외에도, IBM Security Web Gateway Appliance에는 확장된 IT 환경에 대한 차세대 웹 보안 관리 기능을 제공하는 IBM Security 솔루션들이 통합되어 있습니다. 일례로 Security Federated Identity Manager를 이용하면 여러 애플리케이션에 대한 통합 싱글 사인온, 디바이스 속성을 활성화하는 컨텍스트 기반 액세스 제어, 사용자 액세스 속성을 고려한 액세스 정책으로 보안 위험을 줄일 수 있습니다. IBM Security Policy Manager를 통해서도 보안 정책 관리를 중앙 집중화할 수 있으며 애플리케이션, 데이터베이스, 포털, 서비스에 대한 세밀한 데이터 액세스 제어를 할 수 있습니다.

새로운 위협이 나타나면, IBM은 제품, 서비스 및 비즈니스 파트너 솔루션의 완전한 포트폴리오로 고객의 핵심 보안 인프라 구축을 지원할 수 있습니다. IBM은 고객이 자사의 보안 취약성을 줄이고 전략적 이니셔티브의 성공에 주력할 수 있도록 지원하고 있습니다.

IBM Security Web Gateway Appliance 개요	
물리적 특성	<ul style="list-style-type: none"> • 1U 폼팩터 • H × W × D: 44.2 mm × 430.2 mm × 533.7 mm (1.74 in. × 17 in. × 21 in.) • 관리 인터페이스: 10/100/1000 • 애플리케이션 인터페이스: 10/100/1000 (IPv6 지원) • 지원 물리 매체 유형: RJ-45 • 예비 전원공급장치 • SSD(Solid-state storage)
시스템 사양	<ul style="list-style-type: none"> • Intel Core i7-2600 프로세서 • 32 GB 메모리 • 100 GB SSD • 6 네트워크 포트*
지원 웹 브라우저	<p>Microsoft Windows</p> <ul style="list-style-type: none"> • Google Chrome v19.0 이상 • Microsoft Internet Explorer v9 이상 • Mozilla Firefox v12.0 이상 <p>Linux/IBM AIX®/Solaris</p> <ul style="list-style-type: none"> • Mozilla Firefox v12.0 이상
성능 데이터 §	<ul style="list-style-type: none"> • 처리량: 최대 1.2 Gbps 또는 초당 25,000 요청 • 지연: ~ 0.8 ms • 대형 패킷 처리량: 최대 1.2 Gbps • 소형 패킷 처리량: 최대 초당 25,000 요청 • 인증 처리량: 최대 초당 1,500 로그인 • 동시 접속: 최대 30,000
전기 및 환경 파라미터	<ul style="list-style-type: none"> • 100 - 240 V, 전 범위

추가 정보

IBM Security Web Gateway Appliance에 관한 추가 정보는 가까운 IBM 영업대표 또는 IBM 비즈니스 파트너에게 문의하거나 다음 사이트를 방문하시기 바랍니다. ibm.com/security

IBM Security 솔루션 소개

IBM Security는 엔터프라이즈 보안 제품 및 서비스의 최첨단 통합 포트폴리오를 제공하고 있습니다. 세계적으로 인정받은 IBM X-FORCE 연구개발 팀이 지원하는 이 포트폴리오는 기업이 자사 직원, 인프라, 데이터, 애플리케이션을 포괄적으로 보호할 수

있는 보안 인텔리전스를 제공하며, ID 및 액세스 관리, 데이터베이스 보안, 애플리케이션 개발, 위험 관리, 엔드포인트 관리, 네트워크 보안 등을 위한 솔루션을 제공합니다. 이러한 솔루션을 통해 기업은 위험을 효과적으로 관리하고 모바일, 클라우드, 소셜 미디어 및 기타 엔터프라이즈 비즈니스 아키텍처에 대한 통합 보안을 구축할 수 있습니다. IBM은 세계 최대 규모의 보안 연구개발 및 서비스 제공 조직을 운영하고 있고, 130여 개국에서 매일 130억 건에 달하는 보안 이벤트를 모니터링하고 있으며, 3,000 건 이상의 보안 특허를 보유하고 있습니다.



또한, IBM Global Financing은 가장 비용 효과적이며 전략적인 방법으로 여러분의 비즈니스 요구사항에 부응하는 IT 솔루션을 확보할 수 있도록 돕고 있습니다. 신용 자격이 있는 고객들과 협력하여 귀사의 비즈니스 목표에 부합하는 IT Financing 솔루션을 맞춤형하고, 효과적으로 현금을 관리하며, 총소유비용을 향상시켜줍니다. IBM Global Financing은 중요한 IT 투자 및 귀사의 향후 비즈니스 추진을 위한 현명한 선택입니다. 보다 자세한 정보는 www.ibm.com/financing에서 확인하실 수 있습니다.

© Copyright IBM Corporation 2012

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
December 2012

IBM, IBM 로고, ibm.com, Tivoli, AIX 및 X-FORCE는 전세계 여러 국가에서 등록된 International Business Machines Corp.의 상표입니다. 기타 제품 및 서비스 이름은 IBM 또는 타사의 상표입니다. 현재 IBM 상표 목록은 웹 "저작권 및 상표 정보"(ibm.com/legal/copytrade.shtml)에 있습니다.

Intel 및 Intel 로고는 미국 또는 기타 국가에서 사용되는 Intel Corporation 또는 그 계열사의 상표 또는 등록상표입니다.

Linux는 미국 또는 기타 국가에서 사용되는 Linus Torvalds의 등록상표입니다.

Microsoft는 미국 또는 기타 국가에서 사용되는 Microsoft Corporation의 상표입니다.

이 문서는 최초 발행일을 기준으로 하며, 통지 없이 언제든지 변경될 수 있습니다.

이 문서의 정보는 상품성, 특정 목적에의 적합성에 대한 보증 및 타인의 권리 침해에 대한 보증이나 조건을 포함하여(단, 이에 한하지 않음) 명시적이든 묵시적이든 일체의 보증 없이 "현상태대로" 제공됩니다. IBM 제품에 대한 보증은 제품의 준거 계약 조항에 의거하여 제공됩니다.

법률과 규정을 준수하는지 확인해야 할 책임은 고객에게 있습니다. IBM은 법률 자문을 제공하지 않으며 IBM의 서비스나 제품을 통해 관련 법률이나 규정에 대한 고객의 준수 여부가 확인된다고 진술하거나 보증하지 않습니다.

우주 보안 관리제도에 대한 설명: IT 시스템 보안은 귀사 내/외부로부터의 부적절한 접근을 방지, 감지, 대응함으로써 시스템과 정보를 보호하는 일을 포함합니다. 부적절한 접근은 정보의 변경, 파괴 또는 유용을 초래하거나, 타 시스템에 대한 공격을 포함한 귀사 시스템에 대한 피해나 오용을 초래할 수 있습니다. 어떠한 IT 시스템이나 제품도 완벽하게 안전할 수 없으며, 단 하나의 제품이나 보안 조치만으로는 부적절한 접근을 완벽하게 방지하는 데 효과적이지 않을 수 있습니다. IBM 시스템과 제품은 종합적인 보안 접근방법의 일부로서 고안되며, 이러한 접근방법은 필연적으로 추가적인 실행절차를 수반하며 가장 효과적이기 위해서는 다른 시스템, 제품 또는 서비스가 필요할 수도 있습니다. IBM은 시스템과 제품이 임의의 당사자의 악의적 또는 불법적 행위로부터 영향을 받지 않는다는 것을 보장하지 않습니다.

* 이 포트 중의 2개는 어플라이언스 관리 전용입니다.

§ IBM Security Web Gateway Appliance에 인용되어 있는 성능 데이터는 일반적인 라이브 트래픽을 나타내는 HTTP 및 HTTPS 트래픽의 테스트 결과에 의거한 것입니다. 프로토콜 혼용 및 평균 패킷 크기와 같은 환경 요인들이 네트워크마다 다르므로, 측정된 성능 결과는 실제와 다를 수 있습니다. Security Web Gateway Appliance 처리량은 어플라이언스에 트래픽을 통과시켜 측정했으며 패킷 무손실(zero packet loss)과 낮은 응답 시간을 달성한 처리량을 측정하였습니다. 벤치마크 테스트에 사용된 Security Web Gateway Appliance는 작업자-스레드 = 300 및 최대 캐시 지속성 접속(maximum-cached-persistent-connection) = 300으로 구성되었으며, 동시 접속 테스트에서만 작업자-스레드를 30,000으로 설정했습니다. 대형 패킷 처리량은 두 가지 네트워크 인터페이스를 이용하여 두 애플리케이션 서버에 대한 TCP 접속을 통해 HTTP에 50 Kb 페이지를 요청하는 다중 클라이언트로 측정하였습니다. 소형 패킷 처리량은 TCP 접속을 통해 HTTP에 500 바이트 페이지를 요청하는 다중 클라이언트로 측정하였습니다. 인증 처리량은 100,000 사용자가 일시에 100 바이트 페이지를 요청하고 연결을 해제하는 HTTPS에 대한 다중 클라이언트 인증으로 측정하였습니다. 지연은 클라이언트 및 집합 애플리케이션 서버 역할을 모두 수행한 AIX 시스템 상에서 iptrace로 네트워크 트래픽을 캡처하여 측정하였습니다. 동시 접속은 10초 후에 응답한 서버에서 페이지를 요청한 다중 클라이언트로 측정하였습니다.

