



- 포괄적인 보호기능이 사용자의 네트워크를 악성 위협에서 안전하게 보호
- 진정한 제로데이 공격방지 기능이 새로운 위협을 사전에 차단
- 새로운 기능! SSL VPN 탑재
- 탁월한 네트워크 보안 관리로 시간 절약
- 지속적으로 업데이트되는 보안 가임을 통하여 최신 방지 기능 제공
- 업그레이드 가능한 통합 기능으로 비용 대비 성능 향상
- 긴급상황에서도 언제든지 글로벌 보안 전문 팀의 지원 가능

포괄적인 통합 보안 관리 솔루션

Firebox® X Core™ 통합 위협 관리 (UTM) 솔루션은 동급 보안 솔루션 중 가장 완벽한 보안 기능을 제공하며 스파이웨어, 스팸, 바이러스, 트로이 목마, 웹 기반 공격 및 기타 악성 프로그램으로부터 귀사의 소중한 네트워크를 안전하게 보호합니다. 이와 같이 강력한 통합 보안 솔루션은 여러 곳에 산재되어 있는 보안 시스템 관리에 필요한 시간과 비용을 줄여주며 복합적인 위협으로부터 탁월한 보호 기능을 제공합니다. 동시에 직관적인 관리툴을 이용한 고급 네트워킹 기능은 신속하고 안전한 비즈니스 데이터 연결성을 보장합니다.

신뢰할 수 있는 다계층 보안

Firebox X Core 는 지능형 다계층 아키텍처를 기반으로 합니다. 보안 계층들은 상호 연동하여 전체 보호기능을 강화시키는 동시에 계층간에 유입되는 트래픽 정보를 공유하여 성능 부하를 줄이고 조정할 수 있습니다. 결과적으로 성능저하 없이 안전한 네트워크 환경에 필요한 통합 보안 기능을 확보할 수 있습니다.

진정한 제로데이 방어 기능

Firebox X Core 는 사전 방어 기능이 내장되어 있어서 소프트웨어 보안 취약성으로 인한 새로운 형태의 네트워크 공격으로부터 귀사의 네트워크와 내부 사용자들을 안전하게 보호합니다. 정교한 프록시 기술에 기반을 둔 철저한 애플리케이션 검사 기능은 새로운 위협이 나타나는 즉시 이를 식별하고 차단하며 스파이웨어, 트로이목마, 웹, DoS, DDoS, DNS 포이즈닝, 버퍼 오버플로우 및 기타 공격에 대한 자동 방어기능을 제공합니다.

직관적인 중앙 관리 방식

WatchGuard® System Manager (WSM) 를 사용하여 장비 배치의 규모와 상관없이 Firebox X 의 중앙 집중 관리를 직관적으로 수행할 수 있습니다. 관리자는 손쉽게 컨피그를 생성하고 적용하며, 데이터를 실시간으로 모니터링하고 관련 보고서를 생성할 수 있기 때문에 관리시간과 비용이 절약됩니다.

강력한 방어기능을 제공하는 통합보안 서비스

Firebox X 에 강력한 보안 가입서비스를 추가하여 위험한 공격 영역의 방어를 강화합니다. 모든 가입서비스는 WSM 을 이용하여 중앙에서 관리할 수 있으며 최신 보호기능을 지속적으로 업데이트 합니다.

■ 스파이웨어 차단기능을 제공하는 게이트웨이 AV/IPS

강력한 시그니처 기반 보호 기능을 통해 게이트웨이에서 알려진 스파이웨어, 트로이 목마, 바이러스 및 웹 기반 공격 차단

■ 바이러스 발생 감지 기능을 제공하는 spamBlocker

원치 않는 이메일을 100% 차단하고 바이러스 메일 발생시 실시간 방어 기능을 제공하는 업계 최고의 스팸 차단 및 이메일 보호 솔루션 제공

■ WebBlocker

악성 또는 부적절한 웹 콘텐츠에 HTTP 와 HTTPS 를 통해 접근하지 못하도록 통제함으로써 직원들의 생산성을 증가시키고 보안 위험을 최소화합니다

원격 보안 연결

Firebox X Core 를 사용하여 직원이 어디에 있는지 원격지 직원을 쉽게 보호할 수 있습니다. 원격지 사용자가 본사 네트워크에 안전하게 액세스할 수 있도록 동급 제품 중에서 가장 다양한 원격 액세스 기능을 제공합니다.

- IPSec
- SSL VPN
- PPTP

편리한 인증을 위해 싱글 사인온 기능도 함께 제공합니다.

원격 보안 연결

WatchGuard LiveSecurity® 서비스에 가입하시면 전세계 보안 전문가 팀이 여러분의 복잡한 IT 관리 업무를 도와드립니다. LiveSecurity 가입 서비스에는 하드웨어 보증 (사전 교체 포함), 소프트웨어 업데이트, 신속한 기술 지원 서비스, 취약성에 대한 최신 경고 및 교육자료 지원 등이 포함됩니다.

투자 가치 보호

여러 개의 보안 솔루션을 설치, 관리, 업그레이드하는 비용을 고려한다면 왜 Firebox X UTM 솔루션이 투자 가치를 높일 수 있는지 분명해집니다. 단일 장비에 완벽하게 통합된 다중형 보호 기능은 초기 구입부터 유지보수 계약에 이르기까지 보안 솔루션 운용과 관련된 모든 측면의 비용 절감을 의미합니다.

보안요구 사항이 증대되면 새로운 기능을 손쉽게 추가하여 여러분의 내부 보안을 강화할 수 있습니다. 또한 더 높은 성능을 필요로 할때 간단한 라이선스 키를 사용하여 해당 제품 라인에서 상위 모델로 업그레이드할 수 있습니다. 점점 복잡해져가는 네트워크 요건에 맞춰 Fireware® 를 Fireware® Pro 고급 소프트웨어로 업그레이드하면 VLAN, 고가용성, QoS 등 확장된 네트워킹 기능들을 구현할 수 있습니다. 새 하드웨어를 구입하지 않아도 이 모든 기능들이 지원되며, 시중의 기타 어떤 보안 솔루션보다 탁월한 방식으로 네트워크 보안에 대한 귀사의 투자 가치를 보호합니다.

환경 보호를 위한 노력

WatchGuard 는 재활용이 가능한 장비와 포장재를 사용하며 에너지 효율성이 높은 제품을 생산합니다. WatchGuard 는 위험 물질사용에 대한 국제 규제를 엄격하게 준수하고 있으며 환경 보호에 대한 책임이 전략적 비즈니스 요건을 구성하는 중요한 요소임을 인식하고 있습니다.



환경 친화적 기능



웹 기반의 공격 차단

웹은 업무상 가장 유용한 도구이기도 하지만 사용자의 네트워크에 심각한 위협이 되기도 합니다. 웹 사이트 관리가 허술할 경우 사용자가 무사고, 또는 고의적으로 취약성을 노출시킨 결과 붓과 스파이웨어가 침투하여 세심한 주의가 요구되는 기업 데이터를 위험에 빠뜨리고 지원 센터에 관련 문의가 쇄도하게 됩니다. 위험에 취약한 네트워크는 DNS 캐시 포이즈닝, 버퍼 오버플로우, DoS (Denial of Service) 공격을 받기 쉽습니다.

필요 사항

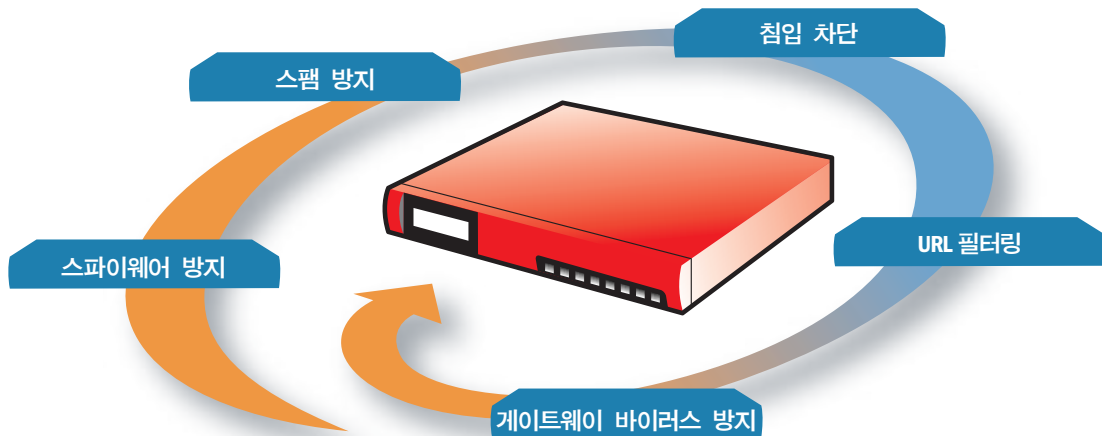
- **Firebox X Core** 를 설치하여 진정한 제로데이 공격방지 기능 구현
- **WebBlocker** 보안 서비스에 가입하여 허가 받지 않은 웹 서핑을 통제하고, **게이트웨이 AV/IPS** 보안 서비스를 활성화하여 수상한 웹 트래픽과 다운로드되는 파일을 실시간으로 차단

방어 기능을 강화하는 방법

- 애플리케이션 소프트웨어의 취약성으로 새로운 유형의 공격이 발생하면 진정한 제로데이 프로텍션 기능이 강력한 내장형 애플리케이션 프록시 기술을 통해 아직 알려지지 않은 새로운 위협으로부터 내부 네트워크 보호

- 다층적인 스파이웨어 차단 기능이 알려진 스파이웨어 사이트로의 접근 차단, 웹 서핑을 통해 네트워크로 침투하는 스파이웨어와 호스트로 접근을 시도하는 스파이웨어 차단
- 스파이웨어 차단 기능이 포함된 **Gateway AV/IPS** 의 정교한 보안 기능으로 바이러스, 트로이 목마, 봇 및 기타 악성 프로그램을 검사하여 알려진 위협 차단
- 웹 서버를 은폐하여 사용자의 시스템 정보를 악용한 해커의 네트워크 공격을 사전에 차단
- **WebBlocker** 를 사용하여 직원들의 웹 서핑을 통제하여 생산성을 향상시키고 법적 책임을 줄여주는 동시에 악성 웹 콘텐츠로부터 네트워크 보호
- **HTTPS URL** 필터링 기능은 사용자가 백도어를 통하여 웹서핑 금지 영역에 액세스하는 행위를 방지
- 지능형 계층 보안 아키텍처가 DNS 프록시와 함께 작동하여 네트워크 침입, **DoS** 공격 및 **DNS** 캐시 포이즈닝 차단
- 통합된 로깅, 보고, 알람 기능이 네트워크 활동에 대한 상세한 정보를 제공하여 관리자가 위협을 사전에 예방하거나 올바른 조치를 취할 수 있음

Firebox X Core 에 통합된 보안 서비스를 이용한 주요 공격 영역에 대한 방어 기능을 강화



이메일 기반 공격 차단

고객은 업무적으로 상당 부분을 이메일에 의존하기 때문에 네트워크 보안에 대한 위협없이, 안전하고 원활하게 이메일을 주고 받을 수 있어야 합니다. 하지만 이메일은 여전히 내부 네트워크에 악성 코드를 유포시킬 수 있는 가장 보편적인 수단입니다. 그리고 스팸 메일이 폭주할 경우 귀사의 이메일 시스템이 IT 관리자에게 가장 큰 부담으로 작용할 수 있습니다.

필요 사항

- **Firebox X Core** 를 설치하여 제로데이 방어기능 구현
- 이메일 트래픽을 검색하는 **게이트웨이 AV/IPS** 기능을 통하여 이메일 트래픽을 검색하며 알려진 스파이웨어, 웜, 바이러스, 트로이 목마 및 기타 악성 프로그램을 차단
- 업계 최고의 솔루션인 **spamBlocker** 를 통하여 정상 메일과 스팸 메일을 실시간으로 구분. **spamBlocker** 는 이메일을 통해 유입되는 바이러스를 100% 정확하게 인식하고 차단할 수 있는 강력한 바이러스 차단 기능을 제공

방어 기능을 강화하는 방법

- 강력한 애플리케이션 프록시 기술을 기반으로 하는 내장형 제로데이 방어 기능이 이메일로 유포되는 대표적인 악성 프로그램 유형을 사전에 차단
- **spamBlocker** 의 실시간 스팸 탐지 기능을 통해 이미지 기반 스팸을 포함하여 메시지 내용, 언어 또는 형식에 상관 없이 원치 않는 이메일을 최대 즉시 차단
- 스팸/AV 검역 서버를 이용해 스팸 또는 의심스러운 메일이 내부 네트워크로 유입되는 것을 차단하고 관리자 또는 사용자가 직접 이러한 스팸이나 메일을 리뷰할 수 있는 도구 제공
- **SMTP** 서버를 은폐하여 시스템 정보를 악용한 해커의 네트워크 공격 차단
- 통합형 게이트웨이 AV 가 첨부파일을 철저히 검사함으로써 스파이웨어, 바이러스, 웜, 기타 악성 프로그램이 네트워크를 침투하여 데스크톱 보안 애플리케이션을 무력화하기 전에 이를 사전에 차단
- 아웃바운드 이메일 AV 검색 기능이 외부로 나가는 이메일을 검사하여 스파이웨어, 바이러스, 웜, 트로이 목마 등이 제휴사, 고객 및 외부 네트워크의 기타 수신자에게 전송되지 못하도록 차단

사양	Firebox® X550e WG50550 X550e UTM 번들 WG50553	Firebox® X750e WG50750 X750e UTM 번들 WG50753	Firebox® X1250e WG51250 X1250e UTM 번들 WG51253
방화벽 성능†	300+ Mbps	750 Mbps	1.5 Gbps
VPN 성능†	35 Mbps	50 Mbps	100 Mbps
AV 성능†	50 Mbps	70 Mbps	100 Mbps
게이트웨이 AV/IPS 스파이웨어 차단	옵션	옵션	옵션
URL 필터링 (HTTP 및 HTTPS)	옵션	옵션	옵션
스팸 차단 및 바이러스 메일 발생 감지	옵션	옵션	옵션
인터페이스 10/100	4	8	0
인터페이스 10/100/1000	0	0	8
시리얼 포트	1	1	1
VLAN 지원*	25	25	25
Security Zone (기본)	4	8	8
동시 세션	25,000	75,000	200,000
지원 노드 (LAN IPs)	무제한	무제한	무제한
지사 VPN 터널 (기본/최대)	35/45	100/100	600/600
이동 사용자 VPN 터널 – IPsec (기본/최대)	5/75	50/100	400/400
이동 사용자 VPN 터널 – SSL (기본/최대)	1/75	1/300	1/500
로컬 사용자 인증 DB 한도	250	1,000	5,000
모델 업그레이드 가능 여부	예	예	아니오
Fireware® Pro 고급 장비 소프트웨어	옵션	옵션	옵션

†환경 및 구성에 따라 성능에 차이가 있음

*Fireware Pro 고급 펌웨어 업그레이드 시 지원

기능

보안 기능

- 상태 기반 패킷 방화벽
- Deep Application Inspection 방화벽
- 애플리케이션 프록시 - HTTP, SMTP, FTP, DNS, TCP, POP3
- 스파이웨어 차단
- DoS 및 DDoS, Progressive DDoS 방어
- 프로토콜 이상 탐지
- 행동 기반 분석
- 패턴 매칭
- 단편화된 패킷 재조합 차단
- 변조된 패킷 차단
- 정적 및 동적 차단 주소 리스트 제공
- 시간 기반 정책 설정
- 인스턴트 메시징 및 P2P 허용/거부

가상 사설망 (VPN)

- VPN
 - 암호화 (DES, 3DES, AES 128-, 192-, 256- 비트)
 - IPsec
 - SHA-1, MD5
 - IKE 사전 공유 키, Firebox 서드파티 인증
 - SSL - 초경량 클라이언트, Web Exchange
- PPTP 서버 및 Passthrough
- Dead Peer Detection (RFC 3706)
- 하드웨어 기반 암호화
- 드래그앤드롭 VPN 터널 생성

사용자 인증

- 편리한 Active Directory 인증 (싱글 사인온)
- XAUTH
 - RADIUS®, LDAP, Windows® Active Directory
- VASCO
- RSA SecurID®
- 웹 기반
- 로컬 인증

IP 주소 할당

- Static
- PPPoE 클라이언트
- DHCP 서버, 클라이언트, 릴레이
- Dynamic DNS 클라이언트

고가용성**

- HA Active/Passive
- 컨피그 동기화
- 세션 동기화
- VPN 터널 동기화

WAN 페일오버

- VPN 페일오버
- WAN 모드
 - Spill-over**
 - Round Robin
 - Failover
 - ECMP
 - Weighted Round Robin**

트래픽 제어**

- Quality of Service
 - 8 개 우선순위 큐방식
 - DiffServ
 - 더욱 정교해진 큐처리 방식

라우팅

- 정적 라우팅
- 동적 라우팅**
 - BGP4, OSPF, RIP v1, v2
- 정책 기반 라우팅**

네트워킹**

- 포트 독립성
- VLAN
 - Bridging, Tagging, Routed Mode
- Multi-WAN 및 서버 로드 밸런싱
- VoIP 및 화상 회의 지원

보안 서비스 가입

- spamBlocker
 - 스팸, 벌크 및 의심스러운 메일 검역서버에 격리
 - 바이러스 메일 발생 탐지

- 스파이웨어 차단 기능을 갖춘 Gateway AntiVirus/IPS
- WebBlocker

작동 모드

- Transparent/Drop-in 모드 (Layer 2)
- Routed 모드 (Layer 3)

네트워크 주소 변환

- 정적 NAT (포트 포워딩)
- 동적 NAT
- 1 대 1 NAT
- IPsec NAT Traversal
- 정책 기반 NAT
- 서버 로드밸런싱을 위한 Virtual IP 지원**

로깅/리포팅

- 다중 장비 로그 통합
- WebTrends® 호환 보고서 (WELF)
- HTML 및 PDF 보고서
- SQL 로그 데이터베이스
- 암호화된 로그 채널
- Syslog
- SNMP v2, v3

알람/통보

- SNMP
- 이메일
- 관리 시스템 알람

관리 소프트웨어††

- WatchGuard System Manager (WSM)

인증

- Common Criteria EAL4
- ICSA IPsec 및 ICSA Firewall
- West Coast Labs Checkmark

고객지원 & 유지보수

- 1년 하드웨어 보증
- 초기 90일 또는 1년 LiveSecurity® 서비스 가입

**Fireware Pro 고급 펌웨어 업그레이드 시 지원

†† Firebox X 550e는 싱글 노드 WSM 라이선스가 제공됩니다. 드래그 & 드롭 터널을 만들거나 X550e에서 여러 Firebox X Edge 기기를 관리하려면 옵션인 WSM 업그레이드 라이선스가 필요합니다.

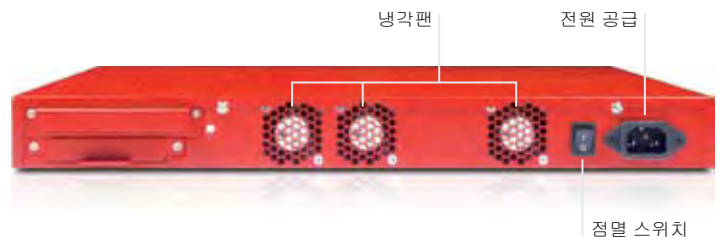
제원 및 전력

장비 제원	1.75" x 16.75" x 14.25" (4.5 x 42.6 x 36.2 cm)
포장 제원	7.25" x 21.75" x 19" (18.4 x 54.6 x 48.3 cm)
장비 중량	9.68 lbs (4.39 Kg)
총 중량	13.7 lbs (6.21 Kg)
WEEE 중량	10.6 lbs (4.81 Kg)
AC 전원	100 - 240 VAC 오토센싱
전력 소모	미국 : 60 와트 기타 국가: 860 Cal/min 또는 205 BTU/hr

랙 장착 가능성 예

환경

작동 온도	32 - 113° F (0 - 45° C)
비작동 온도	-40 - 158° F (-40 - 70° C)
작동 습도	10 - 85%
비작동 습도	10 - 95%, 131°F (55°C) 에서 비응축
비작동 무작위 진동	7 - 28 Hz 0.001 - 0.01 G2 per Hz
음향 잡음	20 - 25°C 에서 54 dBA
작동 기계 충격	20 G (11 Msec 간격 1/2 사인파)
WEEE/RoHS 준수	예


Fireware® Pro 로 업그레이드할 준비가 되었습니까?

점점 증가하는 네트워크 요구사항을 충족시키려면 Firebox X Core 를 Fireware 에서 WatchGuard 의 고급 소프트웨어인 Fireware Pro 로 업그레이드 하십시오. Fireware Pro 10 에서는 다음과 같이 더욱 강력해진 네트워크 기능들을 제공합니다.

- **트래픽 관리** - 업무 핵심 애플리케이션에 필요한 대역폭 보장
- **동적 라우팅 (BGP, OSPF)** - 라우팅 테이블을 동적으로 갱신함으로써 네트워크 유연성, 중복성, 효율성 극대화
- **고가용성 (Active/Passive)** - 대기모드 장비를 통한 하드웨어 가용성, WAN 페일오버 및 VPN 페일오버 제공
- **VLAN 지원** - 물리적 네트워크 구성 대신 논리적 네트워크 구성으로 하드웨어 구입 비용 절감, 트래픽 타입에 대한 통제 강화, 상호 운용성 극대화, 서브넷 생성 간소화
- **멀티 WAN 로드 밸런싱** - 여러 ISP 로 아웃바운드 트래픽을 분산시키고 트래픽 부하를 조절하여 네트워크 효율성 극대화
- **정책 기반 라우팅** - 서비스별로 아웃바운드 인터페이스를 지정하여 대역폭 관리 기능 향상 및 비용 절감
- **서버 로드 밸런싱** - 공개된 전자 상거래 웹서버들을 손쉽게 보호
- **SSL VPN** - SSL VPN 터널을 모델별 최대 지원 갯수로 증가시킴

자세한 내용을 원하시면 www.watchguard.com/appliances 에 방문해 주세요.

Core™ UTM 번들 - 파격적인 가격에 단일 솔루션, 단일 라이선스 구입

편리하게 단일 패키지로 구성된 Firebox X Core e-Series UTM 번들로 포괄적인 통합 위험 관리에 필요한 모든 솔루션을 구현하십시오. 각 패키지에 포함된 내용은 다음과 같습니다.

- Firebox X Core e-Series 보안 장비
- WebBlocker*
- spamBlocker*
- 스파이웨어 차단 기능을 제공하는 게이트웨이 AV/IPS*
- LiveSecurity® 서비스*

초기 구입부터 지속적인 보안 관리에 이르기까지 Firebox X Core e-Series 번들은 효율적인 네트워크 보안 관리를 보장함과 동시에 동급 최강의 UTM 솔루션을 제공합니다. 일괄 구매로 비용을 절약하십시오!

*1년 가입 서비스

무료!

30 일간 무료체험

Firebox X Core 를 구입하시면 **게이트웨이 AV/IPS, spamBlocker, WebBlocker** 를 30 일간 무료로 사용해 보실 수 있습니다. 자세한 사항은 가까운 리셀러에게 문의하세요.

주소: 서울시 강남구 삼성동 157-27 경양빌딩 18 층 A03 호 · 웹 : www.watchguard.com/kr · 한국 지사 : (02) 557-7833 · 팩스 : (02) 557-7838
이메일 : info@watchguard-apac.com

여기에서 명시적 또는 암시적 보증은 제공하고 있지 않습니다. 모든 장비 사양은 차후에 변경될 수 있으며 향후 출시될 제품 및 기능에 대한 사양은 공급 가능 기준으로 다시 제공됩니다. ©2008 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, WatchGuard 로고, Firebox, Fireware, LiveSecurity, Peak, Core 은 미국과 기타 국가에서 WatchGuard Technologies, Inc. 의 상표 또는 등록 상표입니다. 모든 다른 상표 또는 회사명은 해당 소유자의 재산입니다. 문서 번호: WGCK66360_013008

