



- 완벽한 통합 위협 관리로 악성 공격으로부터 네트워크 보호
- 진정한 제로데이 방지 기능이 새로운 위협을 사전에 차단
- 새로운 기능! SSL VPN 탑재
- 8개의 10/100/1000 기가비트 이더넷 포트가 고속 연결 지원
- 고급 네트워킹 기능이 자원 관리, 트래픽 구축 및 가동 시간 최적화
- 모든 장비 및 서비스의 용이한 구성 및 관리
- 보다 치밀한 보호를 위한 통합된 보안 가입



환경 친화적 기능

대규모 네트워크를 위한 10/100/1000 기가비트 보안

Firebox® X Peak™ 는 WatchGuard® 의 통합 위협 관리 (UTM) 장비 중 가장 성능이 뛰어난 제품으로서 즉시 사용이 가능한 제로데이 보호 기능과 초당 멀티 기가비트의 방화벽 성능을 발휘합니다. 고급 네트워크 기능과 강력한 보안 성능이 결합된 Firebox X Peak 는 대규모 네트워크 환경의 요건들을 충족시킬 수 있는 탁월한 종합 보안 솔루션입니다.

완벽한 통합 보안 관리

Firebox X Peak 는 동급 제품 중 가장 포괄적인 보안 기능을 제공합니다. 내장형 애플리케이션 프록시, 상태 기반 패킷 방화벽, 완전한 기능을 갖춘 VPN 과 선택 사양인 보안 서비스가 결합하여 스파이웨어 차단, 침입 방지, 바이러스 차단, 스팸 차단 및 메일 바이러스 발생 방지, URL 필터링 기능 등을 하나의 강력한 장비에 완벽하게 통합함으로써 멀티포인트 솔루션 관리로 인한 시간과 비용이 현저하게 줄어듭니다.

진정한 제로데이 방어 기능

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

고성능

2.0 멀티 기가비트 방화벽과 최대 600 Mbps VPN 성능을 제공하는 Firebox X Peak 는 저회 제품군에 있는 UTM 솔루션 중 가장 뛰어난 성능을 제공합니다. 또한 전모델에 8개의 10/100/1000 기가비트 이더넷 포트가 장착되어 있어서 기가비트 WAN 연결뿐만 아니라 고속 LAN 백본 인프라를 지원합니다. 포트 활용도를 극대화하기 위해 내부, 외부 또는 옵션 등의 다양한 방식으로 8 개의 포트를 자유롭게 설정할 수 있습니다.

고급 네트워킹 성능

고급 네트워킹 기능은 지능적으로 자원을 관리하고 트래픽을 최적화함과 동시에 안정적인 연결을 보장하여 네트워크 가동시간을 늘려줍니다.

- VLAN 지원은 하드웨어 추가 구입 부담을 줄여주고 뛰어난 상호 운용성 보장.
- 멀티 WAN 로드 밸런싱, 고가용성, WAN/VPN 페일오버를 통해 성능, 중복성 및 안정성 향상.
- 동적 라우팅 및 트래픽 웨이핑을 통해 네트워크 유연성 및 효율성 극대화.
- 정책 기반 라우팅으로 서비스별 Outgoing 인터페이스를 지정하여 대역폭 관리 항상 및 비용 절감.
- 서버 로드 밸런싱을 통해 외부에 공개된 전자 상거래 웹서버들을 보다 손쉽게 보호.

직관적인 중앙 집중 관리

WatchGuard® System Manager (WSM) 를 사용하여 제품 배치 규모와 상관 없이 Firebox X 의 중앙 집중관리를

직관적으로 수행할 수 있습니다. 관리자가 쉽게 구성을 변경하고 적용하며, 데이터를 실시간으로 모니터링하고 관련 보고서를 생성할 수 있기 때문에 관리 시간과 비용이 절약됩니다.

원격 보안 접속

Firebox X Peak 를 사용하여 직원이 외부 어디에서 접속하던지 원격지 직원들을 쉽게 보호할 수 있습니다. 원격지 사용자가 본사 네트워크에 안전하게 액세스할 수 있도록 동급 제품 중에서 가장 다양한 원격 액세스 기능을 제공합니다.

- IPSec VPN, SSL VPN, PPTP 클라이언트.

인증을 편리하게 해주는 싱글 사인인 기능도 함께 제공합니다.

강력한 방어기능을 제공하는 통합보안 서비스

Firebox X 에 강력한 보안 가입서비스를 추가하여 위험한 공격 영역의 방어를 강화합니다. WSM 을 사용하여 모든 가입서비스들은 중앙집중 방식으로 관리할 수 있으며 최신 보호기능으로 항상 지속적으로 업데이트됩니다.

- **WebBlocker**
URL 필터링 기능은 악성 또는 부적합한 웹 콘텐츠에 HTTP와 HTTPS 를 통해 접근하지 못하도록 함으로써 직원 생산성을 증가시키고 보안 위험을 최소화합니다.
- 바이러스 발생 감지 기능을 제공하는 **spamBlocker**
스팸과 스팸에 포함된 바이러스 페이로드를 100% 차단합니다.
- 스파이웨어 차단기능을 제공하는 **게이트웨이 AV/IPS**
강력한 시그니처 기반의 보호 기능을 통해 알려진 스파이웨어, 바이러스, 트로이 목마, 웹 기반 공격 차단.

모델 업그레이드 및 확장성 지원

네트워크 보안 요구사항이 변경됨에 따라 소프트웨어 키를 다운로드하여 손쉽게 성능을 업그레이드 하거나 보안 가입을 추가할 수 있습니다.

환경 보호를 위한 노력

WatchGuard 는 재활용이 가능한 장비와 포장재를 사용하여 에너지 효율성이 높은 제품 생산에 최선을 다하고 있습니다. WatchGuard 는 위험 물질 사용에 대한 유럽 연합의 규제를 엄격하게 준수하고 있으며 환경 보호에 대한 책임이 전략적 비즈니스 요건을 구성하는 중요한 요소임을 인식하고 있습니다.

웹 기반의 공격 차단

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

필요사항

- **Firebox X Peak** 를 설치하여 진정한 제로데이 프로텍션 기능과 기가비트 성능 구현.
- **WebBlocker** 보안서비스에 가입하여 허가 받지 않은 웹 서핑을 관리하고, **게이트웨이 AV/IPS** 보안서비스에 가입하여 수상한 웹 트래픽과 다운로드된 파일을 실시간으로 차단.

방어 기능 강화 방법

- 애플리케이션 소프트웨어의 취약성으로 새로운 유형의 공격이 발생하면 **제로데이 프로텍션** 기능이 강력한 내장형 애플리케이션 프록시 기술을 통해 아직 알려지지 않은 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 공격 방지.
- **WebBlocker** 를 사용하면 직원들의 웹 서핑을 통제하여 생산성을 향상시키고 법적 책임을 줄여주는 동시에 악성 웹 콘텐츠로부터 네트워크 보호.
- **HTTPS URL 필터링** 기능은 사용자가 백도어를 통하여 웹 서핑 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 Peak 에 통합된 보안 가입을 이용한 주요 공격 영역에 대한 방어 기능 강화



원격 지점 및 모바일 사용자 보안

원격 지점에 근무하거나 재택 근무하는 직원들이 점차 늘어나면서 기업 자원과 데이터에 대한 신뢰할 수 있는 안전한 원격 접속 수단이 더욱 필요하게 되었습니다. 중앙 집중 관리 및 보고, 일관된 보안 정책 수립, 기존의 네트워크 자원과 애플리케이션의 상호 운용성, 신뢰할 수 있는 원격 접속과 같은 중요한 사안들은 신중하게 평가해야 합니다. 또한 내부 네트워크에 접근하기 전에 원격 장비들이 보안 정책을 준수하고 있는지 확인하는 것도 중요합니다.

필요 사항

- **Firebox X Peak** 를 설치하여 통합 위협 관리 및 멀티 기가비트 성능 구현.
- **Firebox X Edge** 장비를 추가하여 원격 사무실과 지점의 유/무선 네트워크 주변을 안전하게 보호하고 사용이 간편한 **WatchGuard System Manager (WSM)** 로 모든 보안 기능을 중앙에서 관리.

방어 기능을 강화하는 방법

- 중앙 정책 및 VPN 관리 기능으로 모든 지점 및 사용자에 걸쳐 일관된 보안 정책 적용이 가능.
- 암호화된 지점 및 이동 사용자 VPN 터널을 통해 네트워크 자원에 대한 안전한 원격 접속을 보장하여 원격 근무자 직원들의 생산성과 유연성 증대.
- 강력한 통합 위협 관리 기능이 스파이웨어, 바이러스, DoS 공격, 기타 동적 위협으로부터 원격 사무소 및 재택 근무자와 같은 확장된 네트워크 보호.
- 드래그앤드롭 방식으로 3 번의 클릭만으로 간편하게 원격 지점 VPN 을 생성하여 IT 관리비용을 절감.
- 멀티 기가비트 성능이 다양한 네트워크 환경 및 향후 네트워크 증대 요구에 맞춰 신뢰성, 가용성 및 유연성 보장.

사양	Firebox® X5500e WG55500 X5500e UTM 번들 WG55503	Firebox® X6500e WG56500 X6500e UTM 번들 WG56503	Firebox® X8500e WG58500 X8500e UTM 번들 WG58503	Firebox® X8500e-F WG58510 X8500e-F UTM 번들 WG58513
방화벽 성능*	2.0+ Gbps	2.3 Gbps	2.3 Gbps	2.3 Gbps
VPN 성능*	400 Mbps	600 Mbps	600 Mbps	600 Mbps
AV 성능*	140 Mbps	170 Mbps	200 Mbps	200 Mbps
게이트웨이 AV/IPS 및 스파이웨어 차단	옵션	옵션	옵션	옵션
URL 필터링 (HTTP 및 HTTPS)	옵션	옵션	옵션	옵션
스팸 차단 (바이러스 메일 발생 탐지)	옵션	옵션	옵션	옵션
인터페이스 10/100/1000	8	8	8	8 (4 copper/4 fiber)
시리얼 포트	1	1	1	1
VLAN 지원	75	75	75	75
Security Zones (incl.)	8	8	8	4 RJ45, 4 SFP GBIC
동시 세션	500,000	750,000	1,000,000	1,000,000
지원 노드 (LAN IPs)	무제한	무제한	무제한	무제한
지사 VPN 터널 (기본/최대)	750/750	750/750	750/750	750/750
이동 사용자 VPN 터널 - IPSec (기본/최대)	600/600	600/600	600/600	600/600
이동 사용자 VPN 터널 - SSL (기본/최대)	1000/1000	4000/4000	6000/6000	6000/6000
로컬 사용자 인증 DB 한도	5,000	6,000	8,000	8,000
모델 업그레이드 가능 여부	예	예	아니오	아니오

*환경 및 구성에 따라 성능에 차이가 있음

기능

보안 기능

- 상대 기반 패킷 방화벽
- Deep Application Inspection 방화벽
- 애플리케이션 프록시 - HTTP, SMTP, FTP, DNS, TCP, POP3
- 스파이웨어 차단
- DoS 및 DDoS 방어
- 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
- PPTP 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

X8500e-F 광 인터페이스

- Multi-mode Fiber (MMF)
- 1000 Base SX
- 850 nm
- LC 커넥터

고가용성

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

WAN 페일오버

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

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
- 서버 로드 밸런싱
- VoIP 및 화상 회의 지원

보안 가입

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

- 스파이웨어 차단 기능을 갖춘 Gateway AntiVirus/IPS
 - 무제한 파일 사이즈 AV 스캐닝
- 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

로그/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

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 48.2 cm)
장비 중량	12.4 lbs (5.62 Kg)
총 중량	13.8 lbs (6.25 Kg)
WEEE 중량	10.6 lbs (4.81 Kg)
AC 전원	100 - 240 VAC 오토센싱
전력 소모	미국: 80 와트 기타 국가: 1146 Cal/min 또는 273 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 비압축
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



X8500e-F 모델에서 4 개 동선 및 4 개 광 포트 지원 가능

전문가 가이드 및 지원

WatchGuard의 LiveSecurity® 서비스는 업계에서 가장 포괄적인 지원 및 유지관리 서비스로서 전세계 보안 전문가 팀과 협력하여 귀사의 복잡한 IT 관리 업무를 간소화합니다. LiveSecurity가 제공하는 서비스는 다음과 같습니다.

- 하드웨어 보증 - 사전 하드웨어 교체 포함
- 소프트웨어 업데이트
- 신속한 기술 지원
- 최신 보안 경보, 새로운 위협에 대처하는 방법에 대한 명확한 지침, 시간을 절약할 수 있도록 벤더 패치에 대한 직접 링크 제공
- 비디오, 팟캐스트, 최종 사용자를 위한 간편한 보안 교육 모듈 등이 포함된 첨단 교육 자료

Firebox X Peak 장비 구입 시 LiveSecurity 초기 90 일 또는 1년 가입 서비스를 선택하실 수 있습니다. 프리미엄 지원 서비스는 비즈니스 관련하여 인터넷 의존도가 매우 높은 기업들을 위해 제공됩니다.

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

이제 고성능 보안 장비와 함께 포괄적인 통합 위협 관리에 필요한 모든 보안 기능들을 단일 패키지로 간편하게 구입하실 수 있습니다. 파격적인 가격의 번들에 포함된 내용은 다음과 같습니다.

- Firebox X Peak e-Series 보안 장비
- WebBlocker*
- spamBlocker 및 바이러스 메일 발생 탐지*
- 스파이웨어 차단 기능을 갖춘 게이트웨이 AV/IPS*
- LiveSecurity® 서비스*

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

*1년 가입 혜택

무료!

30 일간 무료체험

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

Firebox X Peak 에 대한 자세한 내용은

www.watchguard.com/appliances 에 방문해 주세요.

주소: 서울특별시 강남구 삼성동 157-27 경암빌딩 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 치후에 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: WGCK66358_011008



방화벽 레벨 1



VPN



웹 필터링



침입 방지



스팸 차단



IPSec



방화벽

