

Software Specification

	Firewall	VPN	Web Security
Firewall	사용자 ID 기반 정책 제어	Encryption & Hash Algorithm with CMVP (3DES, AES, SEED, ARIA, SHA-1, SHA-256)	URL Reputation DB Categorized Global URL DB URL 확장 검사 (URI) Anonymizer를 통한 우회 차단 경고 페이지 설정 및 편집
	정책 자동 생성 마법사		
	Secure OS (SecuiOS)		
	Stateful Inspection		
	Router / Bridge 통합 운영		
	Classification Algorithm		
	도메인 / URL 객체 (FQDN)		
HA	사용자 식별 및 제어 (인증서 연동, AD SSO)	IPSec NAT Traversal DPD (Dead Peer Detection) MBB (Multi-Bandwidth Bonding) IKE v1, v2 Mobile VPN 지원	Web Filter URL Reputation DB Categorized Global URL DB URL 확장 검사 (URI) Anonymizer를 통한 우회 차단 경고 페이지 설정 및 편집
	국가별 IP 차단 (IPv4 / IPv6)		
	VLAN별 필터링		
	Active-Active HA with L2 / L3 switch		
NAT	세션 동기화	Gateway-Client	DLP Built-in 및 사용자 정의 키워드 지원 본문 및 첨부파일 내용 검색 정의된 탐지 결과 저장 기능 (HDD 내장 모델) HTTPS 등 암호화된 패킷에 대한 검색 지원
	Static, Dynamic NAT		
NAT	Interface Based NAT	SSL Full Tunnel Mode Mobile SSL VPN 지원	Network & Management Router, Bridge Mode 802.1Q VLAN 802.3ad Link Aggregation VoIP (H.323, SIP) 지원 Dynamic DNS (DDNS) RIP, OSPF, BGP
	Policy Based NAT		
IPS	Port Address Translation	Anti-X File-Based, Stream-Based 지원 검사 파일 크기 제한 없음 (Stream-Based 방식) HTTP, FTP, SMTP, POP3 Keyword 차단 기능	Management Multicasting Routing Protocol (PIM-SM v2, IGMP v1, v2) Policy Based Routing IPv6 Ready Dashboard, 사용자 / App 기반 Report / Log SNMP v1 / v2 / v3, Syslog 전송 Central Management Online Help 지원
	Pattern Matching Filtering (Signature DB)		
IPS	Policy Based Signature Filtering	Anti-Spam Real-Time Blocking List/Open Relay Database Server 수신자 수 및 대량 메일 발송 제한 메일 크기 제한	Network & Management Router, Bridge Mode 802.1Q VLAN 802.3ad Link Aggregation VoIP (H.323, SIP) 지원 Dynamic DNS (DDNS) RIP, OSPF, BGP
	User Defined Signature Filtering		
DDoS	Auto / Manual Signature Update	Application Control SSL Inspection 파일 유형 제어 App별 행위 / 트래픽 방향성 / QoS 제어 App 모니터링 Instant Messenger 제어 P2P, SNS 제어 Web Mail, Web Hard 제어	Network & Management Router, Bridge Mode 802.1Q VLAN 802.3ad Link Aggregation VoIP (H.323, SIP) 지원 Dynamic DNS (DDNS) RIP, OSPF, BGP
	Traffic Limit 기반 방어		
DDoS	Behavior 기반 방어	Application Control SSL Inspection 파일 유형 제어 App별 행위 / 트래픽 방향성 / QoS 제어 App 모니터링 Instant Messenger 제어 P2P, SNS 제어 Web Mail, Web Hard 제어	Network & Management Router, Bridge Mode 802.1Q VLAN 802.3ad Link Aggregation VoIP (H.323, SIP) 지원 Dynamic DNS (DDNS) RIP, OSPF, BGP
	Signature 기반 방어		
DDoS	Zero-day and Unknown Attack 방어	Application Control SSL Inspection 파일 유형 제어 App별 행위 / 트래픽 방향성 / QoS 제어 App 모니터링 Instant Messenger 제어 P2P, SNS 제어 Web Mail, Web Hard 제어	Network & Management Router, Bridge Mode 802.1Q VLAN 802.3ad Link Aggregation VoIP (H.323, SIP) 지원 Dynamic DNS (DDNS) RIP, OSPF, BGP
	Zero-day and Unknown Attack 방어		

Hardware Specification

SECUI MF2		50	110	300	800
CPU		2 Core	2 Core	2 Core	8 Core
Memory		2 GB	2 GB	4 GB	4 GB
HDD		-	-	500 GB	500 GB
Throughput	Firewall	300 Mbps(max 2G)	600 Mbps(max 3G)	1 Gbps(max 3G)	4 Gbps(max 7G)
	VPN	300 Mbps	300 Mbps	300 Mbps	1 Gbps
Network Interface	1G Copper	4	6	6	8
	1G Fiber	-	-	-	-
Power Supply		Adapter	Adapter	Single	Single
Dimension(WxDxH)		201 x 191 x 45	201 x 191 x 45	1U(430 x 238 x 44)	1U(431 x 381 x 44)
SECUI MF2		1300	1510 / 1520	2100 / 2200	3100
CPU		8 Core	4 Core	4 Core	10 Core
Memory		8 GB	8 GB	8 GB	16 GB
HDD		1 TB	1 TB	1 TB	2 TB
Throughput	Firewall	8 Gbps(max 11G)	10 Gbps(max 16G)	15 Gbps(max 40G)	30 Gbps(max 60G)
	VPN	1.5 Gbps	1.5 Gbps	2 Gbps	4 Gbps
Network Interface	1G Copper	8	8	8(max 24)	8(max 24)
	1G Fiber	4	4	8(max 24)	4(max 24)
	10G Fiber	-	-	-	4(max 12)
Power Supply		Single	Redundant	Redundant	Redundant
Dimension(WxDxH)		1U(431 x 381 x 44)	1U(430x450x44) / 1U(430x510x44)	2U(431 x 600 x 88) / 2U(431x577x88)	2U(431 x 600 x 88)

SECUI (주)시큐아이

서울특별시 중구 소공로 48 5-7F
tel 02 3783 6600 fax 02 3783 6499 www.secui.com

Copyright © SECUI All Rights Reserved. 본 카탈로그에 기재된 회사명, 상품명은 당사의 등록 상표입니다.
사인과 외관은 개량을 위해 예고 없이 변경되는 경우가 있습니다.

대표전화 080 331 6600

침해대응센터 02 3783 6500

평일 : 오전 8시 ~ 오후 5시 (토, 일, 공휴일 제외)

CERTIFICATIONS



SECUI MF2

v4

SECUI MF2 IS THE NEXT GENERATION FIREWALL

차세대 방화벽

SECUI

SECUI MF2

Next Generation Firewall

SECUI MF2는

국내 최초의 차세대 방화벽으로 최신 보안 위협에 효과적인 대응 방안을 제시합니다.

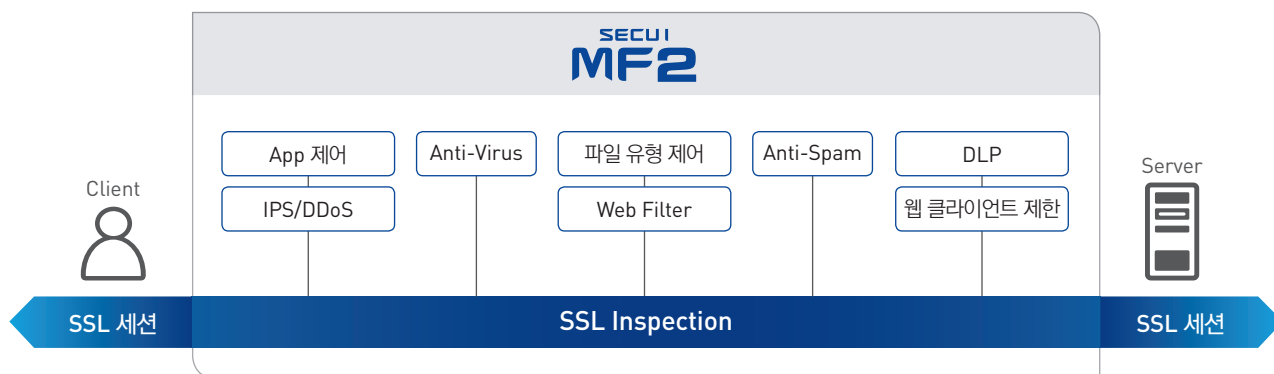


최근의 네트워크 환경은 범람하는 애플리케이션으로 인한 취약점 증가, 악성코드 등을 이용하는 고도화된 공격으로 경영 환경에 영향을 미치는 보안 위협의 출현이 빈번해졌습니다. 이러한 네트워크 환경에서 기존 방화벽 및 UTM으로 대응하기에는 어려움이 있어, 고도화된 공격에 능동적으로 대처하는 차세대 방화벽(Next Generation Firewall)이 등장 하게 되었습니다.

- 사용자, 애플리케이션 식별 및 제어
- 개인정보 및 기업정보 유출방지
- 클라우드 기반으로 분석된 URL 평판 DB로 악성코드 배포사이트 접근 차단
- SNORT, PCRE 패턴 지원의 IPS/DDoS 엔진을 탑재하여 정교한 유해 트래픽 차단
- IPSec VPN, SSL VPN 및 Mobile VPN 지원으로 스마트워크 환경 지원

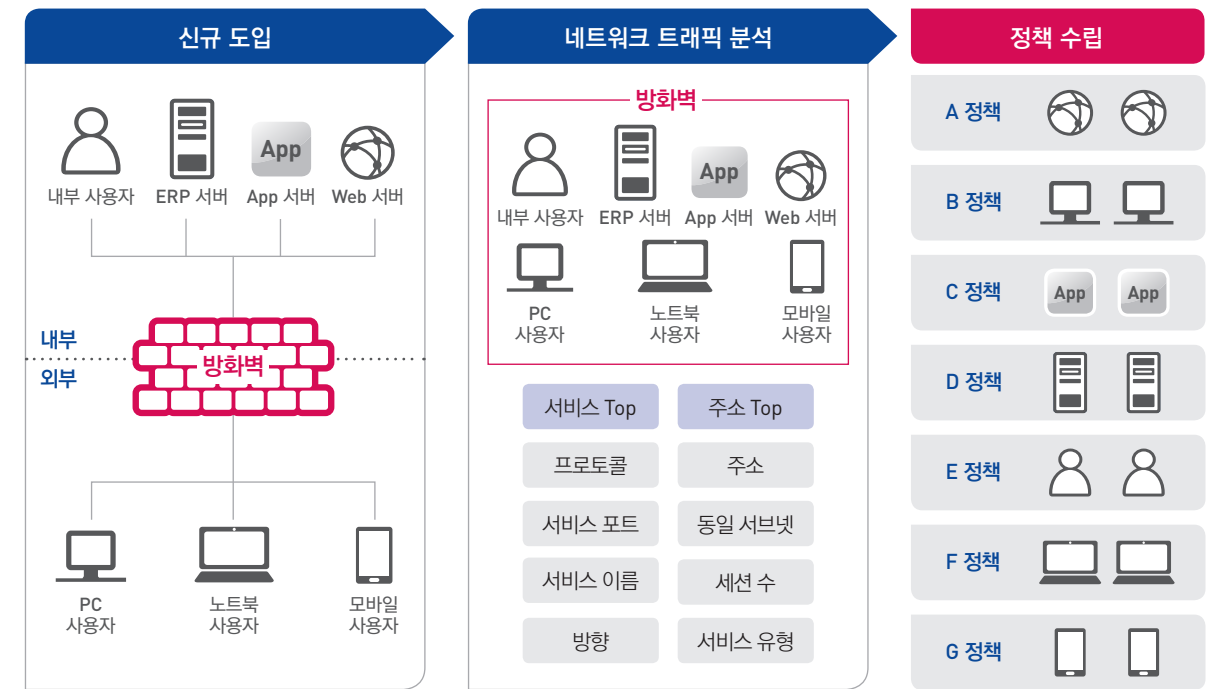
SSL Inspection

SSL 세션을 자동 탐지하고, SSL 패킷을 복호화하여 여러 애플리케이션 보안 기능에 적용함으로써 보안의 사각지대 해소



정책 자동 생성 마법사

방화벽을 통과하는 모든 트래픽 정보를 자동으로 객체화/정책화하여 정책 수립 소요시간 최소화



통합 로그

세션에 대한 보안 기능별 처리 결과를 한눈에 확인할 수 있으며, 보안 이벤트 추적 정보 제공으로 운영 편의성 향상에 기여

