

# Virtual Cloud Generation Firewall

# BLUEMAX

## NGF 100



BLUEMAX NGF 100은 SMB(SOHO) 환경에서 안정된 고성능, 고가용성 HW 아키텍처와 사용자 ID 연동 제어, Application 제어, Device 제어 기능을 제공하는 차세대 네트워크 보안 방화벽입니다.



## BLUEMAX NGF 특징점

장비 교체 없이 Legacy, NGFW mode 전환

기본 방화벽 성능이 우수한 Legacy FW mode와 정교한 보안 설정이 가능한 NGFW mode 동시 제공

Legacy FW mode (5-tuple)



NGFW mode (8-tuple)



## BLUEMAX NGF 주요 기능



### Application 제어

애플리케이션을 분석하여 기존 UTM에서 대응이 어려운 공격에 능동적으로 대처할 수 있는 기능



### SaaS App 제어

클라우드 기반 SaaS 애플리케이션 확산에 대한 보안 강화를 위해 글로벌 클라우드 애플리케이션 제어 기능 강화



### 파일 유형 제어

애플리케이션 사용 시 파일 유형별 제어로 비인가 파일 전송과 내부 정보 유출 방지 및 외부 위협 예방



### Device 제어

사용자 단말 보안 설정, 필수 SW 설치, 보안 업데이트 여부를 검사하여 중요 시스템 접근 제어 및 Malware 차단



### 사용자 ID 연동 제어

사용자 ID를 인식하여 언제 어디서 네트워크에 접속하여도 동일한 보안 정책 적용



### Open API

국내외 벤더의 통합 보안 관리 시스템, 취약점 진단 시스템, 보안 정책 분석 시스템과 유연하게 연동



### 도메인 객체

클라우드 환경(포털, 웹하드)을 고려하여 도메인 IP를 실시간 및 주기적으로 2,048개까지 수집



### SSL Inspection

SSL 세션을 자동 탐지, SSL 패킷을 복호화하여 다양한 차세대 네트워크 보안 기능에 적용하는 기능

# Software Specification

<b>Virtual Cloud Gen Function</b>					
NGFW	사용자 기반 정책 제어	Anti-DDoS	응용계층 방어	Client Security	SSL VPN Client(PC, Linux, Android, iOS)
	애플리케이션/디바이스 기반 정책 제어		행위기반 웹 공격 방어, DrDoS(N:1) 방어		이상 징후 탐지, 격리, 삭제
	AD SSO 연동을 위한 AD 설정 마법사		지역기반 차단 및 블랙리스트(IPv4/IPv6)		이상 트래픽, 파일, URL 수집
	애플리케이션별, 사용자 ID별 QoS	알려지지 않은 공격 및 GRE 공격 차단	Compliance 점검을 통한 단말 보안 상태 정보 제공		
	자체 사용자 인증(Captive Portal) 및 SSO	IKE(v1/v2), PKI(X.509)	단말 보안 정보 수집(업데이트, 보안 설정)		
SaaS 애플리케이션 제어	IPsec VPN	GRE/IPIP, L2TP, PPTP Tunneling			
APT (위협대응)	Sandbox 장비와 연동하여 APT 위협 분석 기능 제공 및 Client를 통한 위협 차단 기능 제공		3DES, AES, SEED, ARIA, CAST, Blowfish 등		<b>Management Function</b>
	탐지된 위협 정보(공격자/배포지 IP 및 URL, 악성 파일 Hash 값 등)에 대한 공유 체계 지원		MD5, SHA-1, SHA-256, SHA-512, HAST160 등		
SSL Inspection	HTTPS, SMTPS, POP3S, IMAPS, FTPS	<b>Contents Filtering Function</b>			Management
	Hardware Acceleration	Anti-Virus Engine(File-based or Stream-based)			
	Application Control, IPS, DLP, WebFilter, Anti-X 등	Anti-Virus & Anti-SPAM	Realtime Blackhole List(RBL)		관리자 권한 프로파일
<b>UTM Function</b>			수신자 수 제한, 대량메일 발송 제한		Open API, 기타 외부 솔루션 연동
Legacy Firewall	Active-Active HA with L2/L3/L4	Web Filter	URL Filtering(Category별 설정)		SNMP(v1,2,3), Syslog 전송
	도메인 정책(URL 객체)		URL 확장 검사(URI 쿼리 검사)		DB 기반 로그 관리(압축 지원)
	중복 정책 및 미사용(미참조) 정책 검사	Global Categorized URL (로컬/클라우드 DB)		경고 알람 임계치 설정	
	Policy-based NAT & Interface-based NAT	Anonymizer 서버목록 차단		Report(정책 상세, 리포트 브라우저)	
보안 정책 그룹 설정	경고페이지 설정 및 편집	DLP(Data Loss Prevention)	HTTP/HTTPS, FTP/FTPS, SMTP/SMTPS, POP3/POP3S, IMAP/IMAPS		애플리케이션, 사용자별 트래픽/세션 모니터링
보안 정책별 활성화 스케줄	웹메일을 통한 정보유출 제어		웹메일을 통한 정보유출 제어		LACP, VLAN, 동적자산 제어
자동 학습에 의한 시그니처 추출 및 적용 기능	주민등록번호, 카드번호 등록/검사 및 차단		SMTP/POP3S, IMAP/IMAPS		IPv6 트랜지션(설정 터널링, 6to4) & 트랜슬레이션 (NAT64/NAT46, DNS64)
IPS	PCRE(정규표현식)	범용파일 포맷 39가지 이상			DHCP, DHCPv6 및 RA서버
	멀티패턴 탐지 기능(병렬탐지)	압축파일(ZIP, TAR, GZIP, ALZIP, BZIP, RAR, 7ZIP)			DNS, DDNS, Split DNS
	취약점 점검 도구 연동, 시그니처 최적화	필터 및 저장(아카이브)			QoS(IP, Application, 인터페이스별)
SSL VPN	Full Tunnel mode				Routing Protocol(IPv4-OSPF/RIP/BGP, IPv6-OSPFv3/RIPng/BGP4+)
	Multi-Factor 인증 지원(3차 인증)				GPRS Tunneling 패킷 검사 기능 지원 (GTP Inspection)

# Hardware Specification

<b>Model Name</b>		<b>BLUEMAX NGF100</b>
<b>CPU</b>		2 Core
<b>Memory</b>		4 GB
<b>Storage</b>	<b>System</b>	16 GB
<b>Interface</b>	<b>1G Copper</b>	4+4(switch)
<b>Throughput</b>		2 Gbps
<b>CC (Concurrent)</b>		1,000,000
<b>Power Supply</b>		Adapter
<b>Dimension (WxDxH)</b>		230x237x44

## SECUI (주)시큐아이

서울특별시 중구 소공로 48 남산센트럴타워  
 tel 02 3783 6600 fax 02 3783 6499 www.secui.com

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

대표전화 **080-331-6600**

기술지원/침해대응센터 **02-3783-6500**

보안관제센터 **02-3782-4030**

평일 : 오전 8시 ~ 오후 5시 (토, 일, 공휴일 제외)

## CERTIFICATIONS

