

Virtual Cloud Generation Firewall

BLUEMAX

NGF 20000



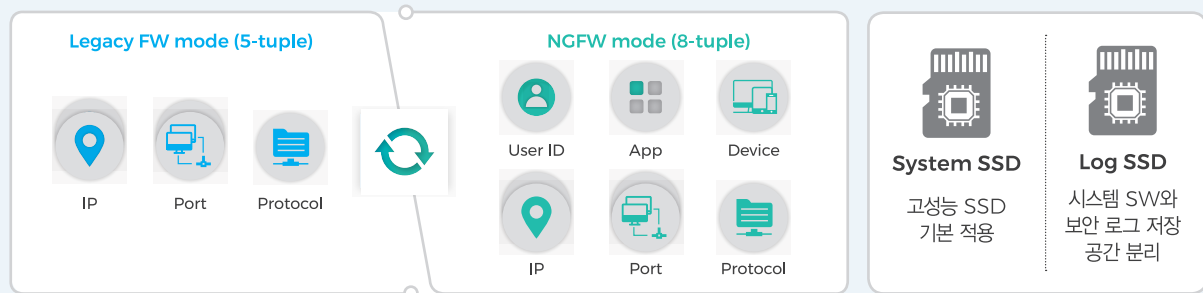
BLUEMAX NGF20000은 Enterprise(Data Center) 환경에서 안정된 고성능, 고가용성 HW 아키텍처와 사용자ID 연동 제어, Application 제어, Device 제어 기능을 제공하는 가상화 클라우드 차세대 방화벽입니다.



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

고가용성 HW 아키텍처로
무중단 서비스 제공



BLUEMAX NGF 주요 기능

- Virtual System**
On-Premise의 복잡한 보안 구성을 단일 HW장비의 Virtual System으로 효율화
- SaaS App 제어**
클라우드 기반 SaaS 애플리케이션 확산에 대한 보안 강화를 위해 글로벌 클라우드 애플리케이션 제어 기능 강화
- Application 제어**
애플리케이션을 분석하여 기존 UTM에서 대응이 어려운 공격에 능동적으로 대처할 수 있는 기능
- 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

Virtual Cloud Gen Function				Client Security	
NCFW	사용자 기반 정책 제어	Anti-DDoS	응용계층 방어	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 방법사		스마트 패턴 학습 방어	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)		
Virtual System	SaaS 애플리케이션 제어	IPSec VPN	GRE/IPIP, L2TP, PPTP Tunneling	Management Function	
	Virtual System별 자원 할당		3DES, AES, SEED, ARIA, CAST, Blowfish, MD5, SHA-1, SHA-256, SHA-512, HAS160 등	Firmware Upgrade and Downgrade(Rollback)	
	토폴로지 맵으로 직관적 가상 네트워크 구성	Group VPN 기능	SSL VPN	정책 설정 Multi R/W 기능	
관리자별 독립적인 운영 환경	Full Tunnel mode	GUI상에서의 CLI 실행 및 Packet Capture			
APT (위협대응)	Sandbox 장비와 연동하여 APT 위협 분석 기능 제공 및 Client를 통한 위협 차단 기능 제공	Contents Filtering Function		LDAP/RADIUS/TACACS+/OTP 등 관리자 접속	
	탐지된 위협 정보(공격자/배포지 IP 및 URL, 악성 파일 Hash 값 등)에 대한 공유 체계 지원	Anti-Virus Engine(File-based or Stream-based)	Multi-Factor 인증 지원(3차 인증)		관리자 권한 프로파일
SSL Inspection	HTTPS, SMTPS, POP3S, IMAPS, FTPS	Anti-Virus & Anti-SPAM	Realtime Blackhole List(RBL)	Open API, 기타 외부 솔루션 연동	
	Hardware Acceleration	수신자 수 제한, 대량메일 발송 제한	URL Filtering(Category별 설정)	SNMP(V1,2,3), Syslog 전송	
UTM Function	App Control, IPS, DLP, WebFilter 기능 및 외부 보안 장비와 복호화 트래픽 연동	Web Filter	URL 확장 검사(URI 쿼리 검사)	DB 기반 로그 관리(압축 지원)	
	Active-Active HA with L2/L3/L4		Global Categorized URL (로컬/클라우드 DB)	경고 알람 임계치 설정	
	도메인 정책(URL 객체)	Anonymizer 서버목록 차단	Report(정책 상세, 리포트 브라우저)		애플리케이션, 사용자별 트래픽/세션 모니터링
Legacy Firewall	중복 정책 및 미사용(미참조) 정책 검사	DLP(Data Loss Prevention)	HTTP/HTTPS, FTP/FTPS, SMTP/SMTPS, POP3/POP3S, IMAP/IMAPS	LACP, VLAN, 동적자산 제어	
	Policy-based NAT & Interface-based NAT		웹메일을 통한 정보유출 제어	IPv6 트랜지션(설정 터널링, 6to4) & 트랜스레이션 (NAT64/NAT46, DNS64)	
	보안 정책 그룹 설정		주민등록번호, 카드번호 등록/검사 및 차단	DHCP, DHCPv6 및 RA서버	
IPS	보안 정책별 활성화 스케줄	범용파일 포맷 39가지 이상	필터 및 저장(아카이브)	DNS, DDNS, Split DNS	
	프로파일기반 시그니처 템플릿	암출파일(ZIP, TAR, GZIP, ALZIP, BZIP, RAR, 7ZIP)	QoS(IP, Application, 인터페이스별)		
	PCRE(정규표현식)	멀티패턴 탐지 기능(병렬탐지)	Routing Protocol(IPv4-OSPF/RIP/BGP, IPv6-OSPFv3/RIPng/BGP4+)		
취약점 점검 도구 연동, 시그니처 최적화				GPRS Tunneling 패킷 검사 기능 지원 (GTP Inspection)	

Hardware Specification

Model Name		BLUEMAX NGF 20000
CPU		48 Core
Memory		96/288 GB
Storage	System	128/512 GB
	Log	1.92 TB/RAID
Interface	100G Fiber	(max 4)
	40G Fiber	(max 8)
	10G Fiber	10(max 26)
	1G Fiber	8(max 40)
	1G Copper	8(max 40)
	Mgmt	2
Throughput		320 Gbps
CC (Concurrent)		60,000,000
Power Supply		Redundant
Dimension (WxDxH)		2U(438x685x88)

SECUI (주)시큐아이

서울특별시 종로구 종로 51 3~6F(종로2가, 종로타워)
 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

