

Security Intelligence Platform for All My Threat Management

# BLUEMAX **NGF**

Virtual Cloud Generation Firewall  
국내 최초 가상화, 클라우드 차세대 방화벽

**SECUI**

Virtual Cloud Generation Firewall

# BLUEMAX NGF

BLUEMAX NGF는 국내 최초의 가상화 클라우드 네트워크 보안을 위한 차세대 방화벽이며, 유무선 IT인프라환경의 모든 위협 요소를 탐지, 차단하는 통합보안플랫폼을 제공합니다. 가상화 기능을 통해 단일 제품으로도 다수의 방화벽 운영이 가능하며 안정된 고성능, 고가용성 HW 아키텍처와 애플리케이션 인지, 디바이스 인지 등 차세대 방화벽 기능과 SD-WAN 환경 지원, DNS/ VPN의 최신 위협 대응을 위한 보안 기능을 모두 제공합니다.



## SECURITY INTELLIGENCE PLATFORM

for All My Threat Management

### BLUEMAX NGF VE

- Public, Private 클라우드 환경의 통합보안
- On-Premise의 복잡한 보안 구성을 Virtual System으로 효율화

Virtual Cloud Security

### NETWORK SECURITY

- App 제어로 트래픽 가시성 보장
- User 인증으로 비인가 접근 방지

BLUEMAX NGF

Malware Protection

### BLUEMAX CLIENT

- Device의 Compliance 점검, 이상행위, 감염여부를 실시간 탐지하여 선제적 위협탐지 차단

### STIC CSOC

- STIC : Smart Update, 글로벌 위협정보 서비스
- CSOC : AI 기반 위협분석, 원격관제 서비스

Threat Intelligence

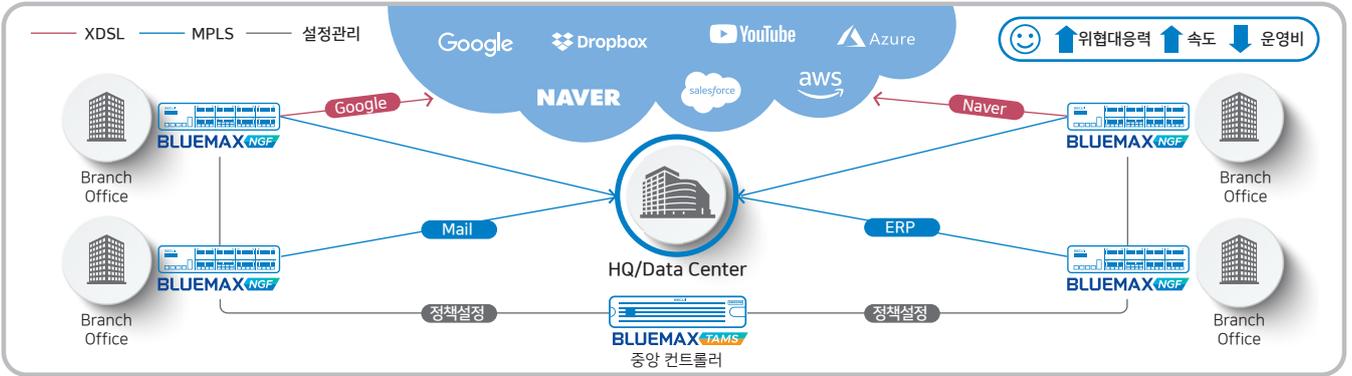
Security Automation

### BLUEMAX TAMS

- 수집된 위협정보, 보안로그, 취약점진단 결과를 종합 분석하여 보안정책 설정 자동화

# 신규 보안 위협 대응

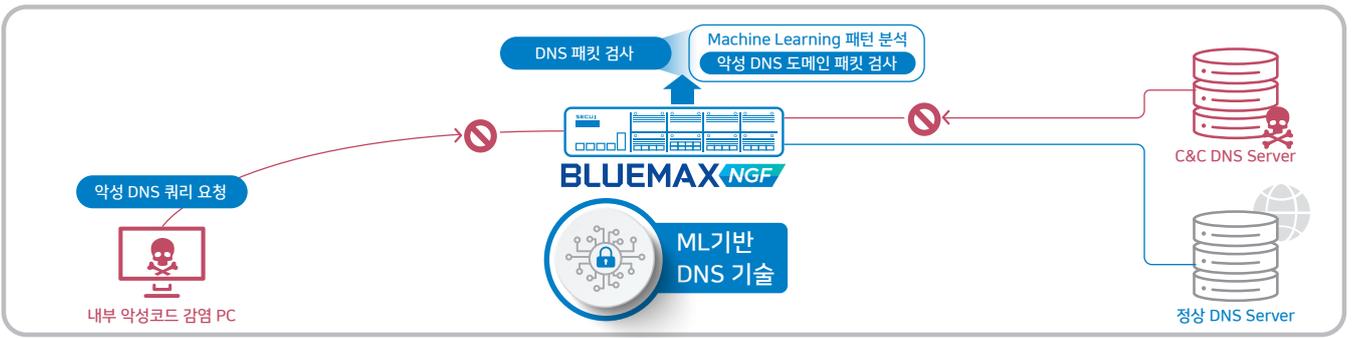
## 보안 SD-WAN | 차세대 방화벽 기반의 Secure SD-WAN으로 최적화된 네트워킹과 보안 위협 동시 대응



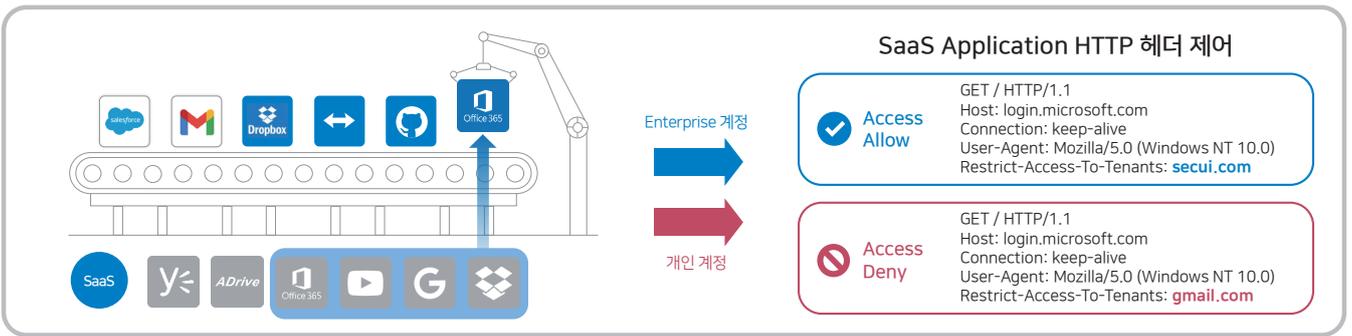
## 제로 트러스트 네트워크 | 디바이스의 보안상태, 사용자ID, App 정보기반으로 Zero Trust Network 정책 적용



## DNS Security | 머신러닝 기술을 방화벽에 탑재하여 알려지지 않은 보안 위협을 대응

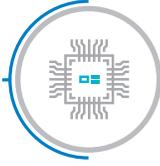


## SaaS Security | 웹 카테고리 기반 애플리케이션 제어 및 SaaS HTTP 헤더 제어



# 주요 기능

## App 제어



국내외 애플리케이션에 의한 취약점 증가, 악성코드 배포 등을 방지하기 위해 애플리케이션을 사전 정의하고 분석하여 기존 UTM에서 대응이 어려운 공격에 능동적으로 대처할 수 있는 기능

## 사용자 ID



IP가 아닌 사용자 ID를 인식하여 언제 어디서 네트워크에 접속하여도 동일한 보안 정책을 적용받아 사용자의 이동성을 보장하고 사용자별 통계 자료 조회 가능

## VPN 보안 강화



양자 컴퓨터를 활용한 공격에도 대응이 가능한 국제 공인 차세대 암호기술 PQC 알고리즘 탑재

## 도메인 객체



IP 대신 도메인명을 방화벽 객체로 사용하는 기능으로 클라우드 환경(포털, 웹하드)을 고려하여 도메인당 2,048개 까지 실시간 및 주기적으로 IP 수집

## 웹필터



82개이상의 카테고리로 분류된 글로벌DB사용, Unknown URL 정보는 CLOUD서버로 분석 요청하여 업데이트 수행하여 악성 URL정보에 대한 빠른 차단 수행

## 파일 유형 제어



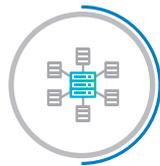
애플리케이션 사용 시 파일의 유형별 (문서, 압축 파일, 이미지, 멀티미디어 등), 방향별로 제어하여 비인가 파일 전송과 내부 정보 유출 방지 및 외부로부터 위협 예방

## SSL Inspection



SSL 세션을 자동 탐지, SSL 패킷을 복호화하여 다양한 차세대 네트워크 보안 기능에 적용하는 기능으로 H/W 가속기를 적용하여 기존 제품 대비 성능 강화

## Open API



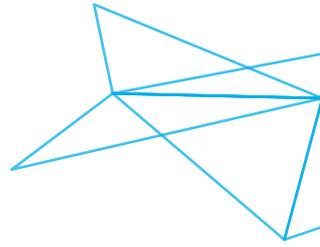
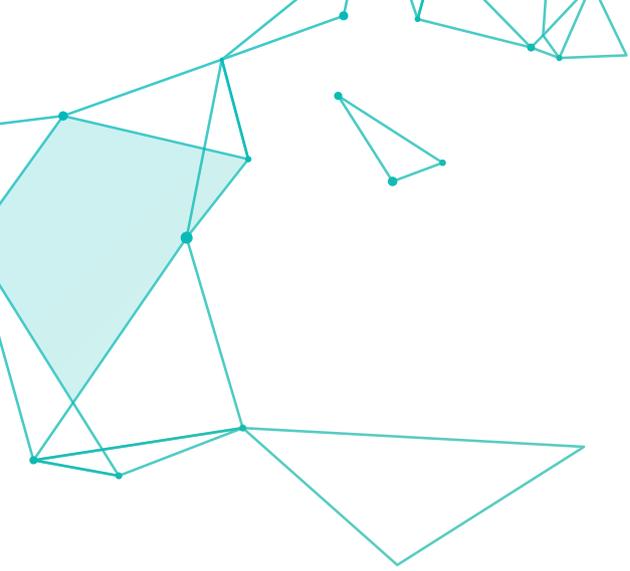
국내 뿐 아니라 글로벌 벤더의 통합 보안 관리 시스템, 취약점 진단 시스템, 보안 정책 분석 시스템과 유연하게 연동하여 Security Orchestration & Automation 구현

## Software Specification

NGFW	사용자 기반 정책 제어	Anti-Virus & Anti-SPAM	Anti-Virus Engine (File-based or Stream-based)	
	자체 사용자 인증(Captive Portal) 및 SSO 지원		Realtime Blackhole List(RBL)	
	SaaS 애플리케이션 제어		수신자 수 제한, 대량 메일 발송 제한	
	애플리케이션/디바이스 기반 정책 제어		URL Filtering(카테고리별 설정)	
	AD SSO 연동을 위한 AD 설정 마법사		경고페이지 설정 및 편집	
Virtual System	OT 프로토콜 인지 및 접근 제어	Web Filter	URL 확장 검사(URL 쿼리 검사)	
	애플리케이션별, 사용자 ID 별 QoS		IP 주소 도메인 차단	
	Virtual System 별 자원 할당		Global Categorized URL(로컬/클라우드 DB)	
APT 대응	토폴로지 맵으로 직관적 가상 네트워크 구성	DLP	HTTP 헤더 제어	
	관리자별 독립적인 운영 환경		Anonymizer 서버 목록 차단	
SSL Inspection	Sandbox 장비 연동한 APT 위협 분석 기능 제공		Device 제어	HTTP/HTTPS, FTP/FTPS, SMTP/SMTPS, POP3/POP3S, IMAP/IMAPS
	탐지된 위협 정보에 대한 공유 체계 지원			범용파일 포맷 39가지 이상
Legacy Firewall	HTTPS, SMTPS, POP3S, IMAPS, FTPS			네트워크
	APP Control, IPS, DLP, Web Filter 기능 및 외부 장비와 복호화 트래픽 연동	압축파일(ZIP, TAR, GZIP, ALZIP, BZIP, RAR, 7ZIP)		
	Hardware Acceleration	주민등록번호, 카드번호 등록/검사 및 차단		
IPS	Active-Active HA with L2/L3/L4	모니터링	필터 및 저장(아카이브)	
	보안 정책 그룹 설정		SSL VPN Client (Windows, Linux, Android, iOS)	
	도메인 정책(URL 객체)		Compliance 점검을 통한 단말 보안 상태 정보 제공	
	보안 정책별 활성화 스케줄		이상 징후 탐지, 격리, 삭제	
	중복 정책 및 미사용(미참조) 정책 검사		단말 보안 정보 수집(업데이트, 보안 설정)	
Anti DDoS	VXLAN 패킷 제어 정책	관리 기능	이상 트래픽, 파일, URL 수집	
	Policy-based NAT & Interface-based NAT		LACP, VLAN, 동적 자산 제어	
	머신러닝 기반 DNS 위협 탐지		QoS(IP, Application, 인터페이스별)	
IPSec VPN	정책 설정 화면과 로그 조회/분석 기능 연계		SD-WAN	IPv6 트랜지션(설정 터널링, 6to4) & 트랜스లే이션(NAT64, DNS64), NAT46
	정책 타임라인 관리 및 롤백			Routing Protocol(IPv4-OSPF/RIP/BGP, IPv6-OSPFv3/RIPng/BGP4+)
SSL VPN	프로파일 기반 시그니처 템플릿	관리 가능		DHCP, DHCPv6 및 RA 서버
	멀티패턴 탐지 기능(병렬 탐지)			DNS, DDNS, Split DNS
Anti-DDoS	PCRE(정규표현식)			관리 가능
	취약점 점검 도구 연동, 시그니처 최적화		Report(정책 상세, 리포트브라우저)	
	사용자 정의 시그니처 검증 기능		DB 기반 로그 관리(압축 지원)	
IPSec VPN	응용계층 방어	관리 가능	애플리케이션, 사용자별 트래픽/ 세션 모니터링	
	스마트 패턴 학습 방어		경고 알람 임계치 설정	
	행위 기반 웹 공격 방어, DRDoS(N:1) 방어		Firmware Upgrade and Downgrade (Rollback)	
SSL VPN	IKE(v1/v2), PKI(x509)		관리 가능	LDAP/RADIUS/TACACS+/OTP 등 관리자 접속
	Group VPN 기능			Setup Wizard, 설정 Multi R/W(Read/Write)
	GRE/IPIP, L2TP, PPTP Tunneling	관리자 권한 프로파일		
Anti-DDoS	양자 내성 암호화 PQC(Post Quantum Cryptography) 알고리즘 탑재	관리 가능		GUI 상에서의 CLI 실행 및 Packet Capture
	3DES, AES, SEED, ARIA, LEA, CAST, Blowfish, MD5, SHA-1, SHA-256, SHA-512, HAS160 등			Open API, 기타 외부 솔루션 연동
	자체 회선 장애 감지 기능		보안 컴플라이언스 자체 점검 지원	
Anti-DDoS	Full Tunnel mode		관리 가능	애플리케이션 기반 트래픽 경로 설정
	FIDO 생체인증			ZTP(Zero Touch Provisioning)
	Multi-Factor 인증 지원(3차 인증)	회선 품질 기반 트래픽 경로 설정 (*2년 하반기 예정)		
Anti-DDoS	PASS 앱 기반 간편 인증	관리 가능		

## Hardware Specification

BLUEMAX NGF	50	100	200	310	510	1100	1510	2100	5100	20000
<b>CPU</b>	2 Core	2 Core	4 Core	4 Core	8 Core	4 Core	10 Core	20 Core	32 Core	48 Core
<b>Memory</b>	4GB	4GB	4GB	8GB	8GB	8GB	16GB	32/64GB	64/128GB	96/288GB
<b>Storage</b>	<b>System</b>	16GB	16GB	32GB	64GB	128GB	128GB	256GB	128/256GB	128/512GB
	<b>Log</b>	-	-	-	1TB	1TB	1TB	1TB	1.92TB/RAID	1.92TB/RAID
<b>Interface</b>	<b>100GF</b>	-	-	-	-	-	-	-	(max2)	(max4)
	<b>40GF</b>	-	-	-	-	-	-	(max4)	(max8)	(max8)
	<b>10GF</b>	-	-	-	-	-	(max4)	2(max10)	10(max26)	10(max26)
	<b>1GF</b>	-	-	-	-	4	4(max8)	4(max8)	8(max40)	8(max40)
	<b>1GC</b>	4	4+4	4+8	8	8	8	8	8(max40)	8(max40)
<b>Power Supply</b>	Adapter	Adapter	Adapter	Single	Single	Single	Redundant	Redundant	Redundant	Redundant
<b>Throughput</b>	1Gbps	2Gbps	4Gbps	8Gbps	12Gbps	16Gbps	40Gbps	80Gbps	160Gbps	320Gbps



국내 최초 가상화, 클라우드 차세대 방화벽

# BLUEMAX<sup>NGF</sup>

**SECUI** (주) 시큐아이

서울특별시 중로구 중로 51 3~6F(중로2가, 종로타워)  
TEL 02-3783-6600 FAX 02-3783-6499  
www.secui.com

대표전화 **080-331-6600**

기술지원/침해대응센터 02-3783-6500  
보안관제센터 02-3782-4030  
평일 : 오전 8시 ~ 오후 5시 (토, 일, 공휴일 제외)

CERTIFICATION

