Security Intelligence Platform
for All My Threat Management

BLUEMAX NGF VE

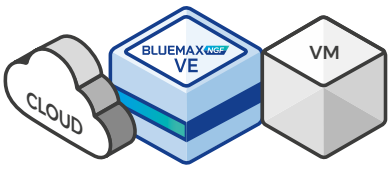
Next Generation Firewall **Virtual Edition**

국내 최초 가상 환경을 위한 차세대 방화벽

SECUI

Next Generation Firewall Virtual Edition

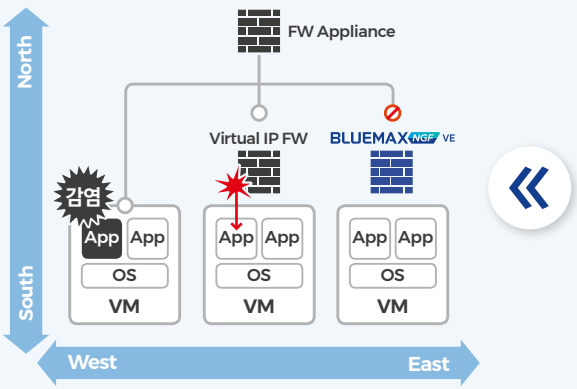
BLUEMAX NGF VE



BLUEMAX NGF VE는 가상화 클라우드 네트워크 보안을 위한 차세대 방화벽이며, 다양한 가상 환경의 모든 위협 요소를 탐지·차단하고 편리한 설치와 Auto Scaling 구현으로 보안 가용성을 제공하는 통합보안 플랫폼의 가상화 버전입니다.

다양한 가상화 클라우드 플랫폼 지원

가상 환경 내외부 위협 차단 최적화



클라우드, SDN 보안
- On-premise 환경과 동일 수준의 보안 정책 다양한 가상 환경에 배포 및 적용

보안 세분화 Micro Segmentation
- 관문 보안의 내부 침해 대응 강화
- 내부 시스템, App간의 보안 통제

동적 보안
- VM, App, IP 주소의 동적 변화
- 자동 설정 복사, 자동 스케일링

Rest API 연동으로 Security Orchestration 지원

Policy
- 방화벽 정책 통합관리
- 정책 컴플라이언스 준수 확인
- 정책 다운로드를 통한 이력관리

Profile/Object
- URL/DLP/파일유형 객체 목록 조회
- 공격 시그니처 업데이트
- 정책 예외 객체 및 사용자 설정

Log/Management
- 다양한 방식의 로그 제공으로 시스템간 로그 통합 및 분석 가능
- 컴플라이언스에 따른 보고서 편집

System Configuration
- 시스템 운영정보조회 및 SW 패치
- 시스템 백업 및 복구 관리

BLUEMAX NGF VE 주요 기능

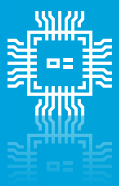
Auto Scaling

가상 환경의 네트워크 트래픽 및
시스템 사용량 과부하 발생 시,
BLUEMAX NGF VE를 자동 확장
운영하여 보안 가용성 강화

사용자 ID

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

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

SaaS App 제어

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

Device 제어

사용자 단말의 보안 설정, 필수 SW 설치 여부,
보안 업데이트 현황, 백업/암호화 설정 여부를
검사하여 내부망과 중요 업무 시스템에 대한
접근을 제어함으로써 Malware 감염을
원천 차단

파일 유형 제어

애플리케이션 사용 시 파일을 유형별
(문서, 압축 파일, 이미지, 멀티미디어 등),
방향별로 제어하여 비인가 파일 전송과
내부 정보 유출 방지 및 외부 위협으로부터
예방

도메인 객체

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

SSL Inspection

SSL 세션을 자동 탐지, SSL 패킷을
복호화하여 다양한 차세대 네트워크
보안 기능에 적용하는 기능으로
가상 환경에 대한 트래픽 가시성 향상

Software Function

Virtual Cloud Gen Function

NGFW	사용자 기반 정책 제어
	애플리케이션/디바이스 기반 정책 제어
	AD SSO 연동을 위한 AD 설정 마법사
	애플리케이션별, 사용자 ID별 QoS
	자체 사용자 인증(Captive Portal) 및 SSO
	SaaS 애플리케이션 제어
APT (위협대응)	Sandbox 장비와 연동하여 APT 위협 분석 기능 제공 및 Client를 통한 위협 차단 기능 제공
	탐지된 위협 정보(공격자/배포지 IP 및 URL, 악성 파일 Hash 값 등)에 대한 공유 체계 지원
SSL Inspection	HTTPS, SMTPS, POP3S, IMAPS, FTPS
	Application Control, IPS, DLP, WebFilter, Anti-X 등

UTM Function

Legacy Firewall	도메인 정책(URL 객체)
	중복 정책 및 미사용(미참조) 정책 검사
	Policy-based NAT & Interface-based NAT
	보안 정책 그룹 설정
	보안 정책별 활성화 스케줄
IPS	자동 학습에 의한 시그니처 추출 및 적용 기능
	PCRE(정규표현식)
	멀티패턴 탐지 기능(병렬탐지)
	취약점 점검 도구 연동, 시그니처 최적화
Anti-DDoS	응용계층 방어
	행위기반 웹 공격 방어, DrDoS(N:1) 방어
	지역기반 차단 및 블랙리스트(IPv4/IPv6)
	알려지지 않은 공격 및 GRE 공격 차단
IPSec VPN	IKE(v1/v2), PKI(X.509)
	GRE/IPIP, L2TP, PPTP Tunneling
	3DES, AES, SEED, ARIA, CAST, Blowfish 등
	MD5, SHA-1, SHA-256, SHA-512, HAS160 등
SSL VPN	Full Tunnel mode
	Multi-Factor 인증 지원(3차 인증)

Contents Filtering Function

Anti-Virus & Anti-SPAM	Anti-Virus Engine (File-based or Stream-based)
	Realtime Blackhole List(RBL)
	수신자 수 제한, 대량메일 발송 제한
Web Filter	URL Filtering(Category별 설정)
	URL 확장 검사(URI 쿼리 검사)
	Global Categorized URL(로컬/클라우드 DB)
	Anonymizer 서버목록 차단
	경고페이지 설정 및 편집
DLP(Data Loss Prevention)	HTTP/HTTPS, FTP/FTPS, SMTP/SMTPS, POP3/POP3S, IMAP/IMAPS
	웹메일을 통한 정보 유출 제어
	주민등록번호, 카드번호 등록/검사 및 차단
	범용파일 포맷 39가지 이상
	압축파일(ZIP, TAR, GZIP, ALZIP, BZIP, RAR, 7ZIP)
	필터 및 저장(아카이브)

Client Security

SSL VPN Client(PC, Linux, Android, iOS)
이상 징후 탐지, 격리, 삭제
이상 트래픽, 파일, URL 수집
Compliance 점검을 통한 단말 보안 상태 정보 제공
단말 보안 정보 수집(업데이트, 보안 설정)

Management Function

Management	Auto Scailing 지원
	Firmware Upgrade and Downgrade (Rollback)
	정책 설정 Multi R/W 기능
	GUI상에서의 CLI 실행 및 Packet Capture
	LDAP/RADIUS/TACACS+/OTP 등 관리자 접속
	관리자 권한 프로파일
	Open API, 기타 외부 솔루션 연동
Monitoring	SNMP(v1,2,3), Syslog 전송
	DB 기반 로그 관리(압축 지원)
	경고 알람 임계치 설정
	Report(정책 상세, 리포트 브라우저)
	애플리케이션, 사용자별 트래픽/세션 모니터링
Networking	LACP, VLAN, 동적자산 제어
	IPv6 트랜지션(설정 터널링, 6to4) & 트랜슬레이션(NAT64/NAT46, DNS64)
	DHCP, DHCPv6 및 RA서버
	DNS, DDNS, Split DNS
	QoS(IP, Application, 인터페이스별)
	Routing Protocol (IPv4-OSPF/RIP/BGP, IPv6-OSPFv3/RIPng/BGP4+)
	GPRS Tunneling 패킷 검사 기능 지원 (GTP Inspection)

Software Specification

BLUEMAX NGF VE	100	200	300	500	1000
Virtualization Platform	VMware, Citrix Xen, Hyper-V, KVM, AWS, Azure, Openstack				
vCPU Support	1	2	4	6	8
Memory Support	4 GB	4 GB	8 GB	8 GB	8 GB
Storage Support (Min/Max)	128 GB / 2 TB				
Throughput	2 Gbps	4 Gbps	6 Gbps	8 Gbps	10 Gbps
CC (Concurrent)	1,000,000	1,500,000	2,000,000	3,000,000	5,000,000

SECUI (주)시큐아이

서울특별시 중구 소공로 48 우리금융남산타워
tel 02 3783 6600 **fax** 02 3783 6499 www.secui.com 평일 : 오전 8시 ~ 오후 5시 (토, 일, 공휴일 제외)

대표전화 **080-331-6600**
기술지원/침해대응센터 **02-3783-6500**
보안관제센터 **02-3782-4030**