변화하는 보안 환경에 선도하는 AI 기반 고성능 프리미엄 방화벽

BLUEMAX NGF PRO

Maximize Your Performance,
Powered by AI

SECUI

BLUEMAX **NGF PRO**

변화하는 보안 환경에 선도하는 AI 기반 고성능 프리미엄 방화벽

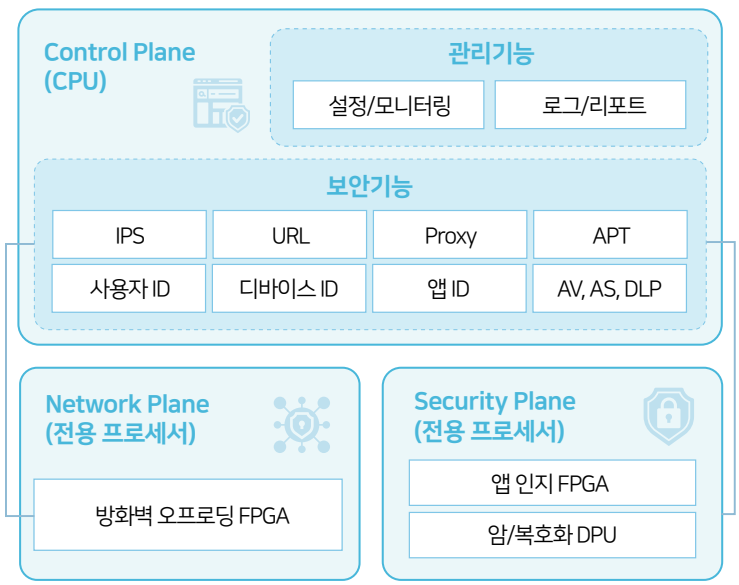


NGF PRO는 고성능 처리와 AI 기반 지능형 보안을 결합한 차세대 방화벽입니다. 급증하는 클라우드, IoT, 5G 기반 트래픽 환경에서 기존 방화벽의 처리 성능 한계를 극복하기 위해 고성능 보안 아키텍처가 요구되고 있습니다.애플리케이션 제어, 암호화 트래픽 분석 등 다양한 보안 기능을 수행함에 따라 기존 CPU 기반 처리 구조는 성능 한계에 도달하고 있습니다. **NGF PRO**는 HW 오프로딩 기반의 고성능 패킷 처리 아키텍처를 적용하여 이러한 한계를 근본적으로 해결합니다. 세션 처리, 트래픽 정밀 분석, 암호 트래픽 복호화 등 고부하 연산을 전용 하드웨어로 분산 처리하여 대용량 트래픽 환경에서도 빠르고 안정적인 보안 성능을 제공합니다.

또한 AI 기반 트래픽 분석 및 위협 탐지 기술을 통해 정상/비정상 행위를 정밀하게 식별하고 알려지지 않은 위협까지 선제적으로 탐지합니다. DNS, HTTP 등 다양한 프로토콜의 행위 패턴을 실시간으로 분석하여 이상 징후를 탐지하고 보안 대응을 자동화합니다. 이를 통해 변화하는 네트워크 환경에서도 안정적인 보안 운영과 확장성을 제공합니다.

SMART OFFLOAD ARCHITECTURE

CPU에서 처리하는 Control Plane과 전용 프로세서를 분리하여 패킷 고속 처리



Control Plane

- 설정/모니터링, 위협 분석, 보안 기능 수행

Network Plane

- 고속 패킷 처리 용 방화벽 FPGA로 트래픽 오프로딩 수행
  - Throughput ↑, Latency ↓

Security Plane

- 패턴 매칭전용 FPGA로 APP 트래픽 오프로딩 수행
  - APP 인지 처리 성능 ↑
- DPU 기반의 암호화 / 복호화 처리로 SSL 탐지/분석
  - SSL 암복호화 처리 성능 ↑

HYPERSCALE PERFORMANCE

최적의 하드웨어 아키텍처와 오프로딩 기술로 압도적인 성능 구현

Hyper-Fast Firewall

고속 패킷 처리 아키텍처로 압도적인 처리량과 초저지연 구현

64 Byte 소형 패킷 성능 극대화

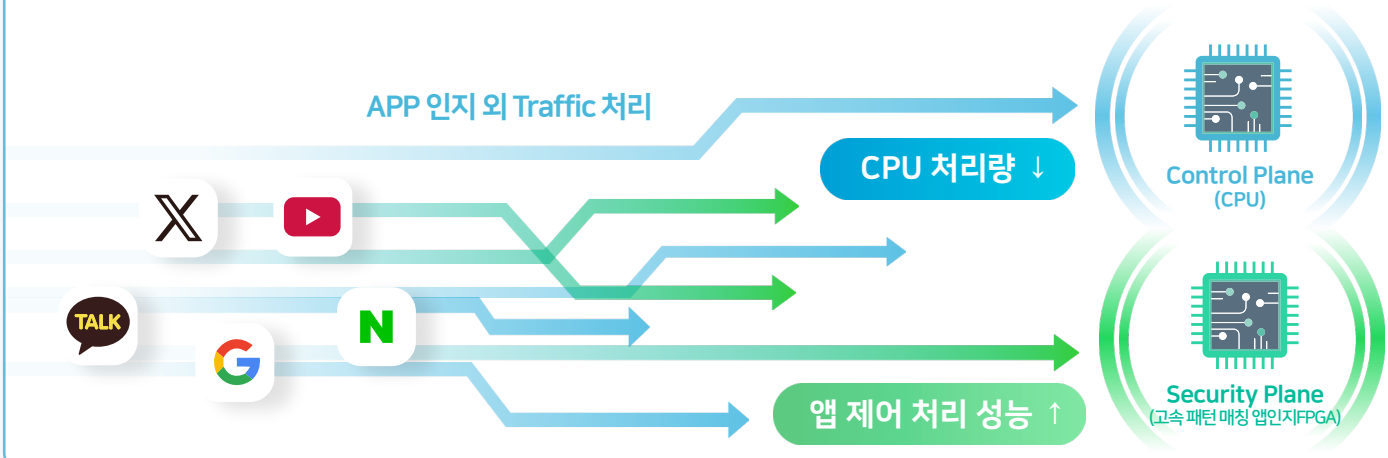
- 소형 패킷(64 Byte) 환경에서 Wired-Speed 보장
- 대용량 트래픽 환경에서도 보안 기능 성능 유지
- 압도적인 초당 패킷 처리량으로 트래픽 폭주에 대응

Latency(지연 시간) 획기적 단축

- 패킷 경로를 단순화하여 지연 시간 단축
- 금융 거래, VoIP, 영상 등 실시간 서비스 품질 보장
- 지터(Jitter) 최소화 네트워크 품질 안정성 유지

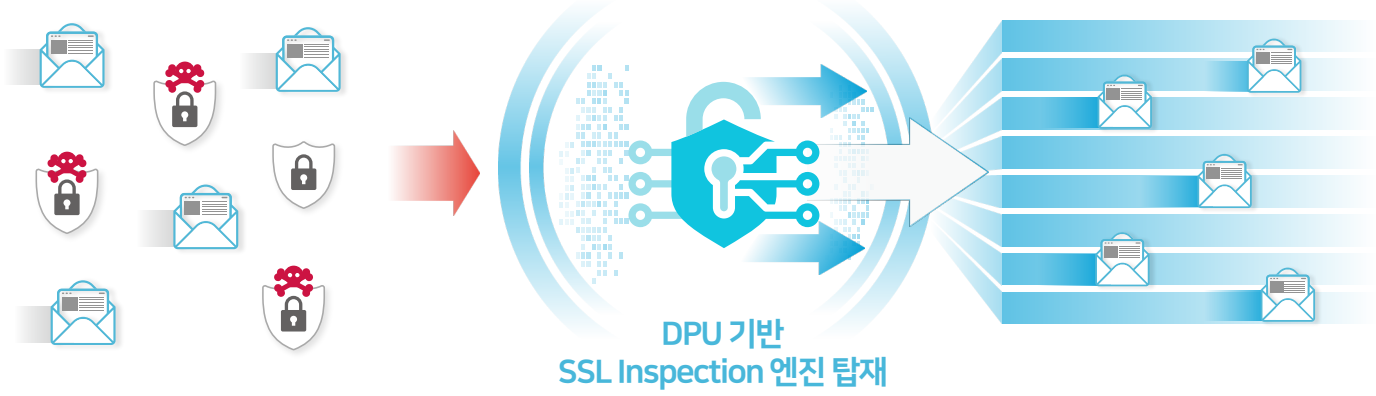
Intelligent App Control

고속 패턴 매칭 앱인지 FPGA를 통해 앱인지 처리 성능 향상



Turbo SSL Inspection

SSL 전용 프로세서를 활용하여 암호화 트래픽 고속 처리와 완벽한 가시성 보장



KEY FEATURES

AI-Powered Malware Prevention

- AI가 파일 구조를 파악하여 알려지지 않은 제로데이, 변종 완벽 차단
- PDF 취약점을 이용하는 Exploit 공격 차단
- 73만개 글로벌 아이콘 학습하여, 정상 파일로 위장한 악성 파일 검출
- 파일리스 기반 VB Script 공격 차단



HTTP/2 Traffic Inspection

- HTTP/2 기반의 최신 웹 환경에서도 안정적이고 강력한 보안 기능 제공
- 애플리케이션 인지, IPS, WebFilter 등 다양한 보안 기능을 통해 정교한 위협 탐지 및 통합 보안 적용 가능



AI-Powered APT Prevention

- 클라우드 기반 가상환경에서 AI로 악성 의심파일을 실행 및 행위 분석하여 악성 여부를 판별
- 분석결과를 장비에 반영하여 제로데이 위협에 선제 대응



DoH, DoT

- DNS-over-TLS, DNS-over-HTTPS와 같은 암호화된 DNS 트래픽에 대한 가시성 확보 및 통제 기능 제공
- 포트 변경, 서비스 객체 등 다양한 정책 설정 기능을 통해 유연한 보안 정책 적용 가능

* DoT(DNS-over-HTTPS)는 '26 지원 예정



AI-Powered Web Filtering

- 웹페이지 URL 문자열과 페이지 콘텐츠를 AI로 종합 분석하여 피싱 URL 탐지
- 로고, 레이아웃 등 시각적 특징을 기반으로 브랜드 사칭 여부를 판별하고 피싱 브랜드 탐지



CDR(Content Disarm and Reconstruction)

- 외부 위협 분석 솔루션과 연동하여 문서 내 악성코드를 제거하고 안전한 콘텐츠만 전달
- 방화벽 연계를 통해 파일 기반 위협에 대한 실시간 탐지·차단하여 네트워크 전반의 보안 수준 강화



AI-Powered DNS Security

- DNS 쿼리 문자열의 특징을 학습하여 비정상/악성 컨텐츠를 탐지하고, C&C 통신을 차단
- 기존 평판 기반 탐지와 AI 기반 분석을 결합하여 오탐을 최소화하고 높은 탐지 정확도 제공



Micro-segmentation

- 단일 장비에서 독립적인 Virtual System을 구성하여 테넌트별 트래픽 분리 및 안정적인 운영 환경 제공
- VRF(가상 라우팅)를 지원하여 Virtual System당 최대 256개의 가상 라우팅을 구성하고, 테넌트별 세분화된 보안 정책 적용과 유연한 확장성 제공



SOFTWARE SPECIFICATION

NGFW	사용자 기반 정책 제어
	자체 사용자 인증(Captive Portal) 및 SSO 지원
	SaaS 애플리케이션 제어
	애플리케이션/디바이스 기반 정책 제어
	AD SSO 연동을 위한 AD 설정 마법사
	OT 프로토콜 인지 및 접근 제어
	애플리케이션별, 사용자 ID 별 QoS
	HTTP/2 프로토콜 분석
Virtual System	Virtual System 별 자원 할당
	토폴로지 맵으로 직관적 가상 네트워크 구성
	관리자별 독립적인 운영 환경
AI Powered Threat Protection	Malware Prevention (악성 실행파일/PDF, VB스크립트, PE위변조탐지)
	APT Prevention (AI기반 Sandbox)
	Web Filtering (피싱URL, 피싱브랜드)
	DNS Security (비정상 DNS 쿼리 탐지)
SSL Inspection	HTTPS, SMTPS, POP3S, IMAPS, FTPS
	APP Control, IPS, DLP, Web Filter 기능 및 외부 장비와 복호화 트래픽 연동
	Hardware Acceleration
Legacy Firewall	Active-Active HA with L2/L3/L4
	보안 정책 그룹 설정
	도메인 정책(URL 객체)
	보안 정책별 활성화 스케줄 중복 정책 및 미사용(미참조) 정책 검사
	VXLAN 패킷 제어 정책
	Policy-based NAT & Interface-based NAT
	머신러닝 기반 DNS 위협 탐지
	정책 설정 화면과 로그 조회/분석 기능 연계
	정책 타임라인 관리 및 롤백
	Virtual Routing and Forwarding
	DNS over TLS
	Content Disarm and Reconstruction
IPS	프로파일 기반 시그니처 템플릿
	멀티패턴 탐지 기능(병렬 탐지)
	PCRE(정규표현식)
	취약점 점검 도구 연동, 시그니처 최적화
	사용자 정의 시그니처 검증 기능
Anti DDoS	응용계층 방어
	스마트 패턴 학습 방어
	행위 기반 웹 공격 방어, DRDoS(N:1) 방어
IPSec VPN	IKE(v1/v2), PKI(x509)
	Group VPN 기능
	GRE/IPIP, L2TP, PPTP Tunneling
	양자 내성 암호화 PQC(Post Quantum Cryptography) 알고리즘 탑재
	3DES, AES, SEED, ARIA, LEA, CAST, Blowfish, MD5, SHA-1, SHA-256, SHA-512, HAS160 등
	자체 회선 장애 감지 기능

SSL VPN	Full Tunnel mode
	FIDO 생체인증
	Multi-Factor 인증 지원(3차 인증)
	PASS 앱 기반 간편 인증
Anti-Virus & Anti-SPAM	Anti-Virus Engine (File-based or Stream-based)
	Realtime Blackhole List(RBL)
	수신자 수 제안, 대량 메일 발송 제안
Web Filter	URL Filtering(카테고리별 설정)
	경고페이지 설정 및 편집
	URL 확장 검사(URL 쿼리 검사)
	IP 주소 도메인 차단
	Global Categorized URL(로컬/클라우드 DB)
	HTTP 헤더 제어
	Anonymizer 서버 목록 차단
DLP	HTTP/HTTPS, FTP/FTPS, SMTP/ SMTPS, POP3/POP3S, IMAP/IMAPS
	범용파일 포맷 39가지 이상
	웹메일을 통한 정보 유출 제어
	압축파일(ZIP, TAR, GZIP, ALZIP, BZIP, RAR, 7ZIP)
	주민등록번호, 카드번호 등록/검사 및 차단
	필터 및 저장(아카이브)
Device 제어	SSL VPN Client (Windows, Linux, Android, iOS)
	Compliance 점검을 통한 단말 보안 상태 정보 제공
	이상 징후 탐지, 격리, 삭제
	단말 보안 정보 수집(업데이트, 보안 설정)
	이상 트래픽, 파일, URL 수집
네트워크	LACP, VLAN, 동적 자산 제어
	QoS(IP, Application, 인터페이스별)
	IPV6 트랜지션(설정 터널링, 6t04) & 트랜슬레이션(NAT64, DNS64), NAT46
	Routing Protocol(IPv4-OSPF/RIP/ BGP, IPv6-OSPFv3/RIPng/BGP4+)
	DHCP, DHCPV6 및 RA 서버
	DNS, DDNS, Split DNS
모니터링	SNMP(V1, 2, 3), Syslog 전송
	Report(정책 상세, 리포트브라우저)
	DB 기반 로그 관리(압축 지원)
	애플리케이션, 사용자별 트래픽/ 세션 모니터링
	경고 알람 임계치 설정
관리기능	Firmware Upgrade and Downgrade (Rollback)
	LDAP/RADIUS/TACACS+/OTP 등 관리자 접속
	Setup Wizard, # 8 Multi R/W(Read/Write)
	관리자 권한 프로파일
	GUI 상에서의 CLI 실행 및 Packet Capture
	Open API, 기타 외부 솔루션 연동
	보안 컴플라이언스 자체 점검 지원
SD-WAN	애플리케이션 기반 트래픽 경로 설정
	ZTP(Zero Touch Provisioning)
	회선 품질 기반 트래픽 경로 설정

HARDWARE SPECIFICATION

BLUEMAX		NGF 3000B PRO	NGF 3000 PRO	NGF 5000B PRO	NGF 5000 PRO
전용 프로세서/CPU		FPGA / 24 Core	FPGA / 24 Core	FPGA / 32 Core	FPGA, DPU / 48 Core
Memory		32 GB	64 GB	256 GB	256 GB
Storage	System	SSD 128 GB	SSD 128 GB	SSD 256 GB	SSD 256 GB
	Log	SSD 1TB	SSD 1TB	SSD 1.92TB(RAID)	SSD 1.92TB(RAID)
Interface	40GF/100GF	-	-	6	6
	1GF/10GF	16	16	18	18
	1GC(Bypass)	8	8	8	8
Power Supply		Redundant	Redundant	Redundant	Redundant
Throughput		160 / 160 Gbps (UDP 1518B / 64B)	30 Gbps (App 64KB)	390 / 320 Gbps (UDP 1518B / 64B)	100 Gbps (App 64KB)
Latency		4.0㎲	-	4.0㎲	-

* 본 사양은 출시 시점 및 SW업데이트 버전에 따라 변경될 수 있습니다.

변화하는 보안 환경에 선도하는 AI 기반 고성능 프리미엄 방화벽

BLUEMAX NGF PRO

SECUi (주) 시큐아이

서울특별시 종로구 종로 51 3~6F(종로2가, 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

Copyright® SECUi All Rights Reserved 본 카탈로그에 게재된 호명, 상품명은 당사의 등록 상표입니다. 사양은 개량을 위해 예고 없이 변경 되는 경우가 있습니다.