

Virtual Cloud Generation Firewall

BLUEMAX NGF 2100



BLUEMAX NGF is Korea's first next-generation firewall for virtual cloud network security and provides an integrated security platform that detects and blocks all threats in the wired and wireless IT infrastructure environment. It can operate multiple firewalls with a single product through the virtualization function and provides all next-generation firewall functions, ranging from stable high-performance and high-availability HW architecture, application recognition, device recognition, support for SD-WAN environment, and security functions to respond to the latest threats of DNS/VPN.

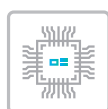
SECURITY INTELLIGENCE PLATFORM

for All My Threat Management



02

BLUEMAX NGF Main Function



App Control

Function to actively respond to attacks that are difficult to handle using existing UTM by pre-defining and analyzing applications to prevent increased vulnerabilities and distribution of malware by domestic and foreign applications



User ID

By recognizing user ID rather than IP, the same security policy is applied no matter when and where the network is accessed, ensuring user mobility and enabling the user to view statistical data.



Enhanced VPN Security

Equipped with the PQC algorithm, which is an internationally recognized next-generation encryption technology that can respond to attacks using quantum computers



Domain Object

Uses domain names instead of IPs as firewall objects, collects up to 2,048 IPs per domain in real time and/or periodically considering the cloud environment (portals, web hard drives).



Web Filter

Uses a global database classified into more than 82 categories and requests a cloud server to analyze unknown URL information for updates to quickly block malicious URL information.



File Type Control

When using the application, controls files by type (document, compressed file, image, multimedia, etc.) and direction to prevent unauthorized file transfers, internal information leaks, and external threats.



SSL Inspection

Automatically detects SSL sessions, decrypts SSL packets, and applies them to various next-generation network security functions. Improves performance compared to existing products by applying a hardware accelerator



Open API

Operates seamlessly with integrated security management systems, vulnerability diagnosis systems, and security policy analysis systems of domestic and international vendors to implement Security Orchestration & Automation.

NGFW	User-based policy control
	SECUI user authentication (captive portal) and SSO support
	SaaS application control
	Application/device-based policy control
	AD setup wizard for linking with AD SSO
Virtual System	OT protocol recognition and access control
	QoS per application and user ID
	Resource allocation per virtual system
Response to APT	Configuration of intuitive virtual network with topology maps
	Independent operating environment for each administrator
SSL Inspection	Provision of APT threat analysis function linked with sandbox equipment
	Supports sharing system for detected threat information
Legacy Firewall	HTTPS, SMTPS, POP3S, IMAPS, FTPS
	APP Control, IPS, DLP, Web Filter functions, and external equipment linked with decrypted traffic
	Hardware Acceleration
	Active-Active HA with L2/L3/L4
	Security policy group settings
IPS	Domain Policy (URL Object)
	Activation schedule by security policy
	Inspection of redundant and unused (unreferenced) policies
	VXLAN Packet Control Policy
	Policy-based NAT & Interface-based NAT
Anti DDoS	Detection of machine learning-based DNS threats
	Linking with policy setting screen and log inquiry/analysis functions
	Policy timeline management and rollback
	Signature Templates based on Profiles
	Multi-pattern detection function (parallel detection)
IPSec VPN	PCRE (regular expression)
	Linking with vulnerability inspection tool, optimizing signature
	Customized signature verification function
	Application layer defense
	Smart pattern learning defense
SSL VPN	Behavior-based web attack defense, DRDoS (N:1) defense
	IKE(v1/v2), PKI(x509)
	Group VPN 기능
	GRE/IPIP, L2TP, PPTP Tunneling
	Equipped with Post Quantum Cryptography (PQC) Algorithm
	3DES, AES, SEED, ARIA, LEA, CAST, Blowfish, MD5, SHA-1, SHA-256, SHA-512, HAS160 etc.
	SECUI line fault detection function
	Full Tunnel mode
	FIDO biometric authentication
	Multi-Factor Authentication Support (3rd Authentication)
	PASS app-based convenient authentication

Anti-Virus & Anti-SPAM	Anti-Virus Engine (File-based or Stream-based)
	Realtime Blackhole List(RBL)
Web Filter	Limiting the number of recipients and bulk mail sending
	URL Filtering (Settings by Category)
	Setting and editing warning pages
	URL expansion inspection (URL query inspection)
	IP address domain blocking
DLP	Global Categorized URL (Local/Cloud DB)
	HTTP header control
	Block Anonymizer Server List
	HTTP/HTTPS, FTP/FTPS, SMTP/ SMTPS, POP3/POP3S, IMAP/IMAPS
	More than 39 universal file formats
Device control	Control of information leakage through webmail
	Compressed files (ZIP, TAR, GZIP, ALZIP, BZIP, RAR, 7ZIP)
	Registration/inspection and blocking of resident registration number, card number
	Filter and save (archive)
	SSL VPN Client (Windows, Linux, Android, iOS)
Network	Provision of terminal security status information through compliance check
	Anomaly detection, isolation, and deletion
	Collection of terminal security information (update, security settings)
	Collection of abnormal traffic, files, and URLs
	LACP, VLAN, dynamic asset control
Monitoring	QoS (by IP, application, interface)
	IPv6 transition (configurable tunneling, 6to4) & Translation (NAT64, DNS64), NAT46
	Routing Protocol(IPv4-OSPF/RIP/ BGP, IPv6-OSPFv3/RIPng/BGP4+)
	DHCP, DHCPv6, and RA servers
	DNS, DDNS, Split DNS
Management Functions	SNMP (v1, 2, 3), Syslog transmission
	Report (Policy Details, Report Browser)
	DB-based log management (compression supported)
	Traffic/session monitoring by application and user
	Warning alarm threshold setting
SD-WAN	Firmware Upgrade and Downgrade (Rollback)
	Administrator access such as LDAP/RADIUS/TACACS+/OTP
	Setup Wizard, Setting Multi R/W(Read/Write)
	Administrator rights profile
	CLI execution and Packet Capture on GUI
	Linking with Open API, other external solution
	Supporting security compliance self-inspection
	Application-based traffic route setting
	ZTP(Zero Touch Provisioning)
	Line quality-based traffic route setting based on (Scheduled for the second half of 2024)

CPU		20 Core
Memory		32/64GB
Storage	System	128/256GB
	Log	1.92TB/RAID
Interface	100GF	-
	40GF	(max4)
	10GF	2(max10)
	1GF	8(max40)
	1GC	8(max40)
Power Supply		Redundant
Throughput		80Gbps

BLUEMAX NGF 2100
