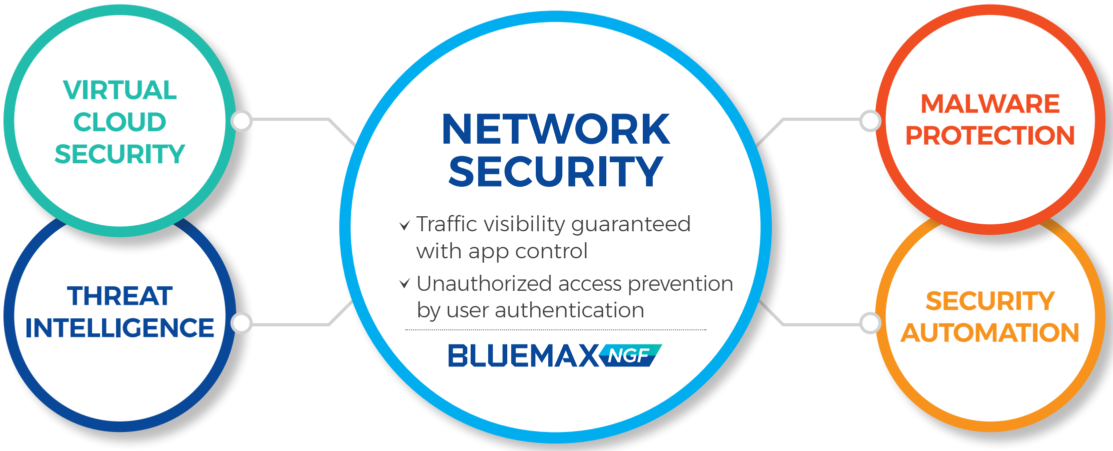
Virtual Cloud Generation Firewall

BLUEMAX

NGF 200

BLUEMAX NGF 200, a next-generation network security firewall that provides the stable high-performance, high-availability HW architecture and user ID interface control, application control and device control in the SMB(SOHO) environment.



VIRTUAL CLOUD SECURITY

THREAT INTELLIGENCE

NETWORK SECURITY

- ✓ Traffic visibility guaranteed with app control
- ✓ Unauthorized access prevention by user authentication

BLUEMAX NGF

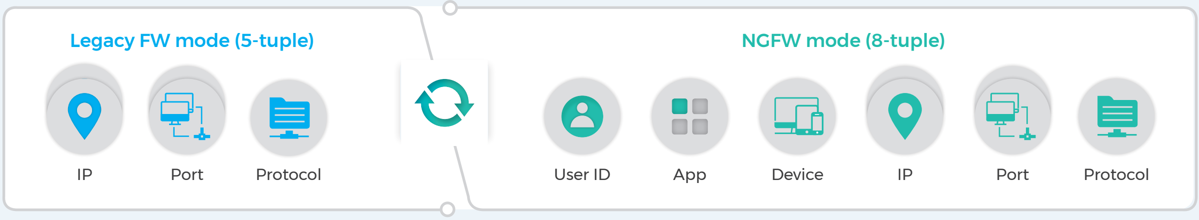
MALWARE PROTECTION

SECURITY AUTOMATION

Features of BLUEMAX NGF

Legacy and NGFW mode switch without an equipment replacement

Simultaneously providing both Legacy FW mode of excellence basic firewall performance and NGFW mode of precise security set up.



Legacy FW mode (5-tuple)

IP · Port · Protocol

NGFW mode (8-tuple)

User ID · App · Device · IP · Port · Protocol

Key functions of BLUEMAX NGF

Application control

The function to analyze applications and respond provocatively to attacks that are difficult to handle with existing UTM

SaaS App control

Reinforcing the global application control function in order to reinforce the security to deal with the proliferation of cloud-based SaaS applications

File type control

Preventing unauthorized file transmissions, internal information leakages and external threats by controlling individual files by file type using applications

Device control

Controlling the access to important files and blocks malware by user terminal security set up, mandatory SW installation and security update checkup.

User ID interface control

Applying the same security policy by recognizing user ID no matter when and where the user connects to the network

Open API

Flexibly interfacing with the integrated security management system, vulnerability diagnostics system and security policy analysis system of both local and overseas vendors

Domain object

Periodically Collecting up to 2,048 domain IPs in real time according to the cloud environment (portal and webhard)

SSL Inspection

The function to detect SSL sessions automatically and decrypt SSL packets to apply them to various next-generation network security functions.

Software Specification

Virtual Cloud Gen Function

NGFW	User-based policy control
	Application/device-based policy control
	AD setup wizard for AD SSO interface
	QoS for each application and each user ID
	Own user authentication (Captive Portal) and SSO
	SaaS application control
APT (responding to threats)	APT threat analysis function by interfacing with Sandbox equipment and a threat blocking function through Clients
	Information sharing of detected threats information (attacker/ IP and URL of the place of distribution, malicious file hash value etc.)
SSL Inspection	HTTPS, SMTPS, POP3S, IMAPS, FTPS
	Hardware Acceleration
	Application Control, IPS, DLP, WebFilter, Anti-X, etc.

UTM Function

Legacy Firewall	Active-Active HA with L2/L3/L4
	Domain poliay (URL object)
	Duplication policy & unued (non-referenced) policy inspection
	Policy-based NAT & Interface-based NAT
	Setting up the security policy group
	Activation scheculing by securiy policy
IPS	Signature exporting & applying fucuntion by auto-learning
	PCRE (Regular expression)
	Detection of multi-pattern (parallel detection)
	Working with vulnerability checking tool, signature optimization

SSL VPN	Full Tunnel mode
	Supporting Multi-Factor authentication (3rd authentication)
Anti-DDoS	Application layer defense
	Behavior-based web attack defense and DrDoS (N:1)
	Region-based blocking and blacklist (IPv4/IPv6)
	Blocking unknown attacks and GRE attacks
IPSec VPN	IKE(v1/v2), PKI(X.509)
	GRE/IPIP, L2TP, PPTP Tunneling
	3DES, AES, SEED, ARIA, CAST, Blowfish, etc.
	MD5, SHA-1, SHA-256, SHA-512, HAS160, etc.

Contents Filtering Function

Anti-Virus & Anti-SPAM	Anti-Virus Engine(File-based or Stream-based)
	Realtime Blackhole List(RBL)
	Restriction on the number of recipients and bulk mail transmission
Web Filter	URL Filtering (settings by category)
	URL extension check (URI query inspection)
	Global Categorized URL (local/cloud DB)
	Blocking the Anonymizer server list
	Warning page setting and editing
DLP(Data Loss Prevention)	HTTP/HTTPS, FTP/FTPS, SMTP/SMTPS, POP3/POP3S, IMAP/IMAPS
	Control of the information leakage through webmail
	Registration/inspection and blockade of ID and credit card numbers
	39 or more general-purpose file formats
	Compressed file (ZIP, TAR, GZIP, ALZIP, BZIP, RAR, 7ZIP)
	Filter and save (archive)

Client Security

- SSL VPN Client(PC, Linux, Android, iOS)
- Abnormal detection, isolation and deletion
- Collection of abnormal traffic, files and URLs
- Provision of terminal security status information through compliance inspection
- Collection of terminal security information (update, security settings)

Management Function

Management	Firmware Upgrade and Downgrade(Rollback)
	Policy settings Multi R/W function
	CLI execution and Packet Capture on GUI
	Administrator access to LDAP/ RADIUS/TACACS+/OTP, etc.
	Administrator privilege profile
	Open API and other external solution interface
Monitoring	SNMP (v1,2,3), Syslog transmission
	DB-based log management (supporting compression)
	Warning alarm threshold settings
	Report (policy details, report browser)
	Monitoring of Application, Traffic/Session by user
Networking	LACP, VLAN, dynamic asset control
	IPv6 transition (settings tunneling, 6to4) & translation (NAT64/NAT46, DNS64)
	DHCP, DHCPv6 and RA server
	DNS, DDNS, Split DNS
	QoS (by IP, Application and interface)
	Routing Protocol (IPv4-OSPF/RIP/BGP, IPv6-OSPFv3/RIPng/BGP4+)
	GPRS Tunneling packet inspection support (GTP Inspection)

Hardware Specification

Model Name		BLUEMAX NGF 200
CPU		4 Core
Memory		4 GB
Storage	System	32 GB
Interface	1G Copper	4+8(switch)
Throughput		4 Gbps
CC (Concurrent)		1,500,000
Power Supply		Adapter
Dimension (WxDxH)		230x237x44

SECUI (주)시큐아이

5~7F 48 Sogong-ro, Jung-gu, Seoul
tel 02 3783 6600 fax 02 3783 6499 www.secui.com

a representative telephone **080 331 6600**
Infringement Response Center **02 3783 6500**
Infringement Response Center **02 3783 6500**
Weekday : 8 a.m. ~ 5 p.m. (Excluding Saturdays, days, and holidays)

CERTIFICATIONS