

Software Function

| Virtual Cloud Gen Function |                                                                                                                                 |                                                                                |                                                                        | Abnormal Traffic, File, URL Collecting                              |                                 |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|------------------------------------------------------------------------|---------------------------------------------------------------------|---------------------------------|
| NGFW                       | User-based Policy Control                                                                                                       | IPSec VPN                                                                      | IKE(v1/v2), PKI(X.509)                                                 | Providing Terminal Security Information through Compliance Check    |                                 |
|                            | App/Device based Policy Control                                                                                                 |                                                                                | GRE/IPIP, L2TP, PPTP Tunneling                                         |                                                                     |                                 |
|                            | AD Setup Wizard for AD SSO Integration                                                                                          |                                                                                | 3DES, AES, SEED, ARIA, CAST, Blowfish, etc.                            |                                                                     |                                 |
|                            | QoS by Application and User ID                                                                                                  |                                                                                | MD5, SHA-1, SHA-256, SHA-512, HAS160, etc.                             | Terminal Security Information Collecting (Update, Security Setting) |                                 |
|                            | Self-user Authentication(Captive Portal) and SSO                                                                                | SSL VPN                                                                        | Full Tunnel mode                                                       |                                                                     |                                 |
| SaaS App Control           |                                                                                                                                 | Multi-Factor Authentication Support (3 <sup>rd</sup> Authentication)           |                                                                        |                                                                     |                                 |
| APT Response to Threat     | Providing APT Threat Analysis Function and Threat Intercepting, Function through Client in connection with Sandbox              | Contents Filtering Function                                                    |                                                                        | Management Function                                                 |                                 |
|                            | Support for Sharing Schemes for Detected Threat Information (Attacker/Supplier's IP and URLs, Malicious File Hash Values, etc.) | Anti-Virus & Anti-SPAM                                                         | Anti-Virus Engine (File-based or Stream-based)                         | Auto Scailing Support                                               |                                 |
| SSL Inspection             | HTTPS, SMTPS, POP3S, IMAPS, FTPS                                                                                                | Realtime Blackhole List(RBL)                                                   | Restriction on the Number of recipients, Bulk Mail Sending Restriction | Firmware Upgrade and Downgrade (Rollback)                           |                                 |
|                            | Application Control, IPS, DLP, WebFilter, Anti-X, etc.                                                                          | URL Filtering(Setting by Category)                                             | URL Expansion Check(URI Query Checking)                                | Policy Establishemt Multi R/W Function                              |                                 |
| UTM Function               |                                                                                                                                 | Global Categorized URL(Local/Cloud DB)                                         | Anonymizer Server List Blocking                                        | CLI Running & Packet Capture on GUI                                 |                                 |
| Legacy Firewall            | Domain Policy (URL Object)                                                                                                      | Warning Page Setting and Editing                                               | HTTP/HTTPS, FTP/FTPS, SMTP/SMTPS, POP3/POP3S, IMAP/IMAPS               | LDAP/RADIUS/TACACS+/OTP, etc. Manager Interface                     |                                 |
|                            | Check for Duplicate and Unused (not referenced) Policies                                                                        | DLP(Data Loss Prevention)                                                      | Information Leakage Control through Web Mail                           | Manager Authority Profile                                           |                                 |
|                            | Policy-based NAT & Interface-based NAT                                                                                          | Resident Registration No. & Card No. Registration/Examination and Blocking     | More than 39 General Purpose File Formats                              | Interworking with Open API & Other External Solutions               |                                 |
| IPS                        | Security Policy Group Setting                                                                                                   | Compressed File(ZIP, TAR, GZIP, ALZIP, BZIP, RAR, 7ZIP)                        | Filtering and Storing (Archive)                                        | SNMP(v1,2,3), Syslog Transmission                                   |                                 |
|                            | Activation Schedule by Security Policy                                                                                          | Client Security                                                                |                                                                        | DB-base Log Management (Compression Support)                        |                                 |
|                            | Signature Extracting and Applying Function by Auto Learning                                                                     | SSL VPN Client(PC, Linux, Android, iOS)                                        | Monitoring                                                             |                                                                     | Warning Alarm Threshold Setting |
| Anti-DDoS                  | PCRE (Normal expression type)                                                                                                   | Abnormal Sign Detecting, Isolating and Deleting                                | Report(Policy Details, Report Browser)                                 |                                                                     |                                 |
|                            | Multi-pattern Detecting Function (Parellel Detection)                                                                           | Traffic/Session Monitoring by App/User                                         |                                                                        |                                                                     |                                 |
|                            | Vulnerability Check Tools Interlocking, Sinature Optimization                                                                   | LACP, VLAN, Dynamic Asset Control                                              |                                                                        |                                                                     |                                 |
| Anti-DDoS                  | Application Layer Defense                                                                                                       | IPv6 Transition (Setting Tunneling, 6 to 4) & Translation (NAT64/NAT46, DNS64) |                                                                        |                                                                     |                                 |
|                            | Behavior based web attack defense, DrDoS(N:1) defense                                                                           | DHCP, DHCPv6 & RA Server                                                       |                                                                        |                                                                     |                                 |
|                            | Geo-based blocking and blacklisting (IPv4/IPv6)                                                                                 | DNS, DDNS, Split DNS                                                           |                                                                        |                                                                     |                                 |
| Anti-DDoS                  | Blocking Unknown and GRE Attacks                                                                                                | QoS(by IP, Application, Interface)                                             |                                                                        |                                                                     |                                 |
|                            |                                                                                                                                 | Routing Protocol (IPv4-OSPF/RIP/BGP, IPv6-OSPFv3/RIPng/BGP4+)                  |                                                                        |                                                                     |                                 |
|                            |                                                                                                                                 | GPRS Tunneling Packet Inspection Function Support (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

48 5~7F, Sogong-ro, Jung-gu, Seoul, Republic of Korea  
Tel 82.2.3783.6600 fax 82.2.3783.6499 www.secui.com Mon ~ Fri : 8 AM ~ 5 PM(Closed Sat, Sun, and Holidays)  
Copyright© SECUI All Rights Reserved. SECUI and BLUEMAX NGF are trademarks or registered trademarks of SECUI. Specifications and design are subject to change without notice for product improvement.

TEL 82-80-331-6600  
Technical Support/Infringement Response Center  
82-2-3783-6500  
Security Control Center 82-2-3782-4030

Security Intelligence Platform  
for All My Threat Management

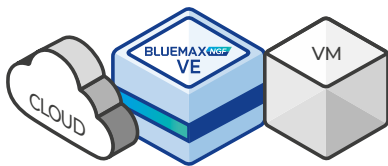
BLUEMAXNGF VE

Next Generation Firewall Virtual Edition  
Korea's First Next-Generation Firewall for Virtual Environment

SECUI

# Next Generation Firewall Virtual Edition

## BLUEMAX NGF VE

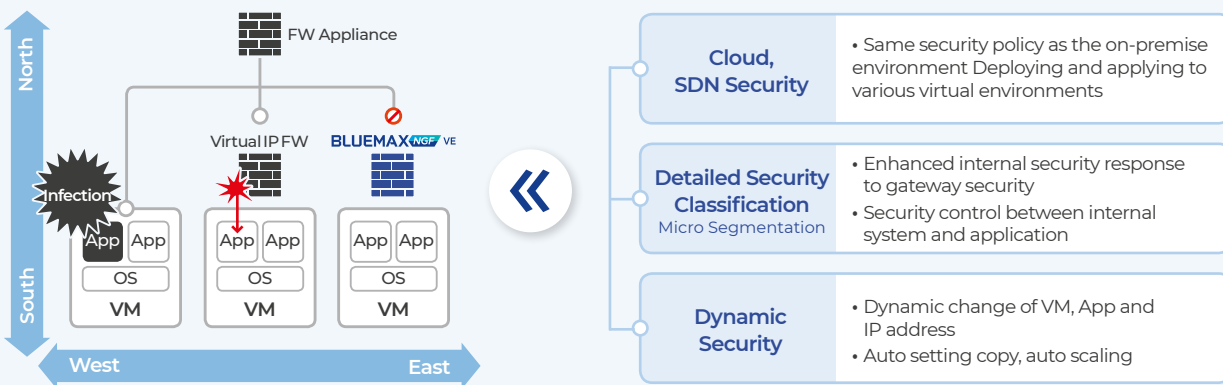


BLUEMAX NGF VE is the next-generation firewall for virtualized cloud network security. It is a virtualized version of the integrated security platform that detects and blocks all threats in various virtual environments and provides security availability with easy installation and Auto Scaling implementation.

### Support for Various Virtual Cloud Platforms



### Cloud Network Security



### Security Orchestration Support with RestAPI Interface



## BLUEMAX NGF VE Key Functions

### Auto Scaling



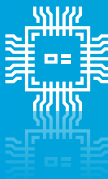
Increasing security availability by automatically expanding and operating BLUEMAX NGF VE in case of network traffic and system usage overload in virtual environment.

### User ID



By recognizing the user ID rather than IP, the user's mobility is guaranteed by applying the same security policy even the user accesses the network anytime and anywhere, and the the statistical data by user can be searched.

### App Control



It's possible to proactively cope with the attacks, which are difficult to be coped by the existing UTM, by pre-defining and analyzing the application in order to prevent the increase of vulnerabilities and the distribution of malware by domestic and international applications.

### SaaS App Control



Enhanced global cloud application control for security reinforcement against cloud-based SaaS application proliferation.

### Device Control



Proactively blocking the malware infection by controlling access to internal network and important business system through checking security setting of user terminal, required SW installation, security update status and backup/ encryption setting.

### File Type Control



Function to control files by type (documents, compressed files, images, multimedia, etc.) and orientation when applications are used, in order to prevent unauthorized file transfer and internal information leakage, and to proactively prevent external threats.

### Domain Object



This function is to use domain name as firewall object instead of IP, and collect IP, in real time and periodically, up to 2,048 IPs per domain considering cloud environment (portal, web hard).

### SSL Inspection



It automatically detects SSL sessions and decrypts SSL packets to apply to a variety of next-generation network security features, and improves traffic visibility for virtual environments.