Features & Specifications

SSL VPN

Capabilities

- Recommended for medium-sized enterprises with 500 to 1,000 employees
- Concurrent sessions: 120,000
- Concurrent SSL VPN tunnels: up to 200, basic 50 tunnels
- Maximum throughput: 60Mbps

Access Connections

- Network Extender (TCP/UDP)
- Standalone Network Extender client
- Transport Extender (TCP/UDP)
- SSL hardware accelerator
- Application Proxy
- Personalized Web Portal
- Single Sign-On (SSO)

Applications & Management

- My Network Places (Web CIFS)
- SSL event log and monitor
- Citrix client
- Terminal services (RDP5, RDP6)
- File Transfer Protocol (FTP)
- Telnet
- Supports MS Outlook Web Access (OWA)
- Virtual Network Computing (VNC)
- Secure Shell (SSH) support
- Web based data (HTTP, HTTPS)
- AD / LDAP account import
- Granular User Policy Management
- Supports mobile devices (Microsoft Windows Mobile 5.0/6.0 or compatible)
- Supports MS IIS NTLM (NT LAN Management) authentication

Security

- SSL encryption
- Web cache cleaner
- Local Database
- Digital Certificate
- Self-Signed Certificate
- User Access Control
- Authentication Domains: RADIUS, LDAP, Active Directory, NT Domain
- Host Security Checking
- End Point Security (EPS)

Compatible Web Browsers*1

- Microsoft Internet Explorer 6.0 and newer versions
- Netscape 7.0 and newer versions
- Opera 9.0 and newer versions
- Firefox 1.5 and newer versions
- Safari 2.0 and newer versions
- Mozilla 1.7 and newer versions
- Sun JRE 1.3 and newer versions

Supported Operating Systems*1

- Microsoft Windows, Linux, and Apple Macintosh

Firewall & Content Filtering

- Stateful Packet Inspection (SPI)
- Denial of Service (DoS) prevention
- Packet Filter
- Intrusion Detection
- URL Filter
- Java Applet/Active X/Cookie Blocking

Quality of Service Control

- Supports DiffServ approach
- Traffic prioritization and bandwidth management based on IP protocol, port number and IP address

Web-Based Management

- Easy-to-use web based user interface
- Group account settings on access applications
- Firmware upgrades through web-based interface
- Local and remote management through HTTP and HTTPS
- Multi-language web interface
- Remote dial-in configuration (RS-232) (CLI for RS-232 port)
- Supports BiGuard CMS for centralized management

Two-Factor Authentication

- Event-based Algorithm Tokens
- Dynamic One-Time Password
- OATH Algorithm
- 5 BiGuard OTP tokens included inbox
- 6-Digit Numeric LCD Display
- Authentication Interoperability: Secure Web Access and RADIUS

IPSec VPN*3

- 30 IPSec VPN tunnels
- Up to 200Mbps IPSec VPN throughput
- Manual key, Internet Key Exchange (IKE) authentication and Key Management
- Authentication (MD5 / SHA-1)
- DES/3DES encryption
- AES 128/192/256 encryption
- IP Authentication Header (AH)
- IP Encapsulating Security Payload (ESP)
- Dynamic VPN (FQDN) support
- Supports remote access and office-to-office IPSec connections

Availability and Resilience

- Load balancing
  - Traffic Management
  - Protocol binding
- Automatic fail-over and VPN fail-over
- High Availability (Device Redundancy)

Logging and Monitoring

- Centralized logs
- System log
- E-mail alerts and Intrusion logs
- System status monitoring

Network Protocols and Features

- Static IP, PPPoE and DHCP client connection to ISP
- NAT, static routing and RIP1/2
- Dynamic Domain Name System (DDNS)
- Router Mode
- Virtual Server
- Hardware DMZ
- DHCP Server
- SNTP
- SNMP
- Multi-NAT
- Transparent Bridging
- Port base VLAN*3

Hardware Specifications

Physical Interface

- 2 x 10/100/1000Mbps Gigabit WAN ports
- 8 x 10/100/1000Mbps Gigabit LAN ports (1 port can be configured as DMZ)
- 1 x RS232 Serial port
- 2 x USB 2.0 hosts
- RS232 console port
- Power switch
- Reset button

Physical Specifications

- 1U rack-mount
- Processor / Flash: Multi-Core MIPS64 / 64MB
- Memory: 1GB
- Dimensions: 19" x 8.27" x 1.73" (482 x 210 x 44mm with bracket) (390 x 210 x 44mm without bracket)

Power Requirements

- Input Voltage (Operation): 90 to 264VAC Full Range
- Input Frequency (Operation): 47 to 63Hz
- Input Current: Max. 0.95A @115Vac/60Hz at max. load
- Efficiency: ≧ 80% @115Vac/60Hz or 230Vac/50Hz at max. load
- Output power: 12V/3.5A (42W)
- Power Supply MTBF: 100,000 hours at 25°C (110Vac & 220Vac)

Operating Environment

- Operating temperature: 0 to 40°C
- Storage temperature: -20 to 70°C
- Humidity: 20 to 95% non-condensing

Support and Services*2

- Instant*Chat* Support 5x8 Service for 180 days
- Hardware Warranty for 2 years
- Feature and Firmware Updates for 1 year

*** Notes:**

1. Please refer to http://www.billion.com/product/biguard/sslvpnbrowser.htm for updates of all supported browsers and OS platforms.
2. Users are strongly recommended to register the products on www.biguard.com in order to be able to use the update feature and firmware updates as well as Instant*Chat* Support 5x8 Service.
3. To be released.
4. All the specifications are subject to change without prior notice.

V.032608

Billion Electric Co., Ltd.
8F, No. 192, Sec. 2, Chung Hsing Road,
Hsin Tien City, Taipei County, Taiwan

TEL: +886-2-29145665
FAX: +886-2-29186731, +886-2-29182895
E-mail: sales@billion.com

www.billion.com

BiGuard S6000

Dual-WAN SSL/IPSec VPN Giga SME Appliance

Key Features

- Dual WAN
- Auto Fail-over and Load Balancing
- Both LAN and WAN Gigabit connectivity
- SSL VPN gateway plus solid router functions
- Clientless connectivity
- Wide range of web browsers supported
- Rich in SSL VPN access connections
- Granular Access Policy Management
- Windows / Linux / Macintosh supported
- Mobile devices supported
- AD / LDAP Account Import
- Group Account Setting
- Personalized Web Portal
- Data encryption, user authentication and access control
- End Point Security Checking
- Host Security Checking
- IPSec VPN capabilities*3
- Robust Firewall security
- Quality of Service Control
- Hardware DMZ
- BiGuard One-Time Password tokens included

Other Options

- Instant*Chat* Support 5x8 Service
- Instant*Chat* Support 7x24 Service*3
- Feature and Firmware Updates
- BiGuard SSL VPN Tunnel Upgrades
- BiGuard Central Management System
- BiGuard One-Time Password

Great Mobility and Productivity

The BiGuard S6000 Dual-WAN SSL/IPSec VPN Giga SME Appliance integrates cutting-edge SSL VPN technology for SMEs to establish private encrypted tunnels, without the need for VPN software pre-installation on client PCs, through the public Internet to securely access corporate resources from any location, such as a branch office, hotel, home, cyber café, or even a public kiosk. It offers corporate-class advanced SSL VPN connections such as Network Extender, Transport Extender, and Application Proxy. Remote users using different kinds of browsers, platforms and operating systems can all access files in the central office. External business partners or business travelers, even using just MS Outlook Web Access (OWA), can be authorized to access the corporate network from a remote site as if they never left the office. A business traveler using a mobile device like a PDA can access the corporate network, the SOHO or a freelancer on a Macintosh can even connect his Mac to customers' networks to remotely collaborate on a project. Secure remote Intranet access with the BiGuard S6000 Dual-WAN SSL/IPSec VPN Giga SME Appliance is possible via any device from anywhere any time.

Powerful Gigabit Connectivity

Not only sharing files, checking e-mail, and downloading documents, but also remote access to applications like Enterprise Resources Planning (ERP) applications or remote surveillance; all of which are needed by today's SMEs and enterprise departments for diverse remote access needs. Billion continues to provide advanced enterprise-class BiGuard SSL VPN appliances. Imbedded with high-performance CPUs, the BiGuard S6000 Dual-WAN SSL/IPSec VPN Giga SME Appliance features Gigabit capability for LAN, WAN and DMZ ports, enabling faster transmission speeds, no matter for remote access, internal connections or outbound networking. This design gives small-and-medium sized enterprises an edge in today's business environments where mobile workers, business partners and traveling employees are increasingly on the road, and for whom connectivity problems and data security should be the last thing on their mind.

Flexibility, Scalability and Resilience

Both SSL VPN and IPSec VPN are remote access solutions and complementary technologies. The BiGuard S6000 Dual-WAN SSL/IPSec VPN Giga SME Appliance offers both IPSec VPN and SSL VPN capabilities combined in a single platform. This design provides excellent deployment flexibility to SMEs for meeting the requirements of both remote access and Lan-to-Lan branch office connections. Load Balancing and Auto Fail-over features are integrated to ensure optimal bandwidth sharing for multiple PCs in your office, or provide network redundancy in case one connection should fail. All of these are to keep your business online for mission-critical or important Internet-based applications.

Single Box with Low Cost of Ownership

Billion's BiGuard S6000 Dual-WAN SSL/IPSec VPN Giga SME Appliance integrates SSL VPN, IPSec, firewall and router functions in one single box. Thanks to integrated IPSec VPN access technology, the additional cost for deploying extra platforms for IPSec VPN is eliminated. Aimed at a low total cost of ownership, the BiGuard SSL VPN box is affordable for SMEs. IT administrators no longer need to buy an extra device to manage remote Intranet access, nor install and maintain additional equipment for data security. The integrated router and firewall functions provide administrators with a perfect solution to manage all connections and file sharing of remote access. It is easier to simply integrate these functions into one BiGuard SSL VPN device instead of buying several independent networking devices.

Ease of Management

Managing various groups of remote users for certain access applications and policies and maintaining the user accounts in a SME are a hassle for IT administrators. Group Account Setting featured in the BiGuard S6000 Dual-WAN SSL/IPSec VPN Giga SME Appliance addresses administrators' concerns. AD/LDAP Account Import makes it easy for IT administrators of enterprises to manage intranets by importing existing accounts from AD/LDAP servers into a BiGuard SSL VPN device. IT administrators configure the gateway to control the resources and applications available to different groups of users. Access policies, authorizations and authentication mechanisms can all be set up as well. After this setting, each user will have an easy-to-manage Personalized Web Portal, which displays the applications according to the user's access settings.

Comprehensive Security

The security of remote access is even more concerned by IT administrators. The BiGuard S6000 Dual-WAN SSL/IPSec VPN Giga SME Appliance supports rich advanced security features. The support of cache cleaner function makes sure that the user's data will be cleaned up without record after user's log out from a remote site. The End Point Security function enables IT administrators to check the identity of a remote PC and its security policy settings when a user logs in from that device. Granular Access Control makes setting up different users allowed to access different applications possible. One-Time Password enforces the user to input different password every time when log in. Access Policy settings enable administrators to set up different users with different access rules. Strong firewall security provides access protection from hackers and other attacks. Access security with the BiGuard SSL VPN Giga SME Appliance, no matter locally or from remote sites, is assured with these comprehensive security features.

Management Options for Growth

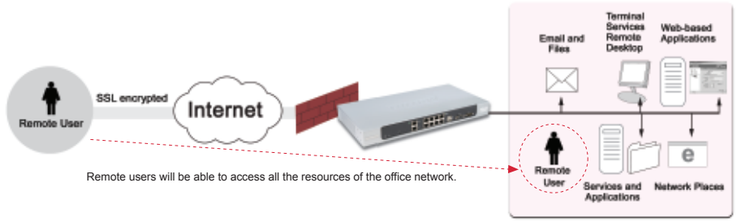
A total SSL VPN solution is made possible by offering optional support: SSL VPN Tunnel Upgrades, BiGuard's Central Management System, and BiGuard One-Time Password (OTP). In case of a growing need for remote access, just upgrade the BiGuard SSL VPN gateway by adding more SSL VPN tunnels. The Central management System enables administrators in the head office or service providers to centrally manage all the BiGuard SSL devices, which enable remote configuration from a central site to save on maintenance efforts. In addition, the BiGuard OTP, a car-key sized token, is used to create a two-factor authentication by using a dynamically generated 6-digit PIN. Combined with your existing static password this results in a greatly reduced risk of unauthorized access to corporate network resources by intruders. The InstantChat Support and Firmware Updates services are also available for a certain duration from purchase date and continues optionally after that.

Powering communications with Security

Technology & Applications

Network Extender

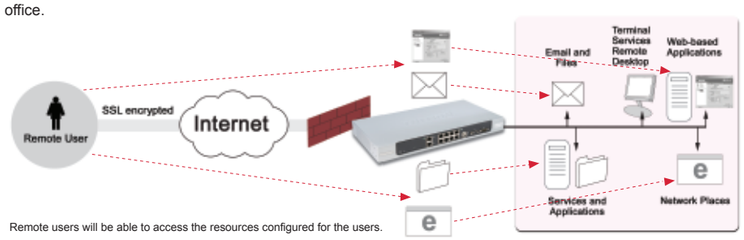
Virtually extending your connection to the central office network allows you to access your office resources seamlessly from anywhere — as if you'd never left the office. You can remotely access office files and applications through your computer, desktop or laptop, as if you were using a computer in your corporate network. A sales person on a business trip who needs to know the product inventory can use the Network Extender technology in the BiGuard S6000, to connect to the corporate network and access the stock database to check, instead of phoning back to head office and asking.



Remote users will be able to access all the resources of the office network.

Transport Extender

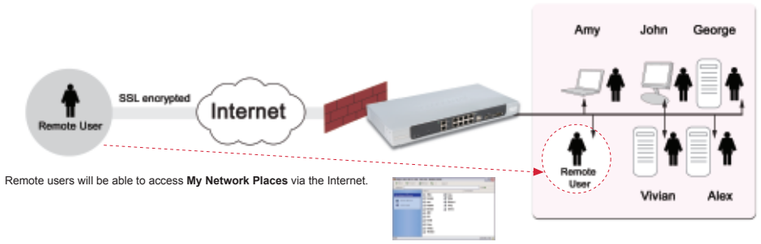
Enables specific remote users or specific remote groups of users to use the SSL VPN tunnel to connect to the corporate network to access the services as configured by IT administrators. Therefore the remote user does not have to change any specific settings in the web portal to make the service work. When a user remotely accesses MS Outlook e-mail, for instance, the Transport Extender technology will transport the e-mail service through the SSL VPN tunnel to the e-mail server in the corporate network, as configured by the IT administrator. Since the remote user doesn't have to modify any settings in the web portal, the remote user will feel as if they're using MS Outlook in the office.



Remote users will be able to access the resources configured for the users.

My Network Places

Just like the Windows Network Neighborhood, My Network Places allows users to browse network files on the office network. From a home computer or PDA, users can connect directly to My Network Places and access information inside the office — from now on there is no need to go back to the office if users forget an important document.



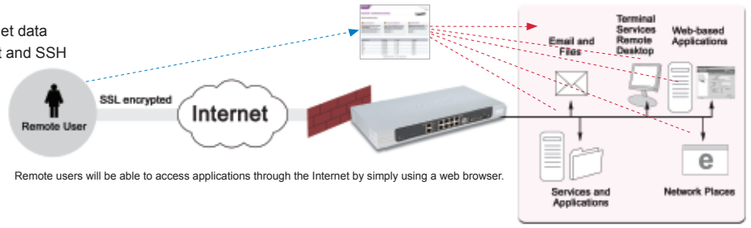
Remote users will be able to access **My Network Places** via the Internet.

Application Proxy

Supports most commonly used applications through a web-based interface. The great advantage of the application proxy is that there is no need to pre-install any client software for the applications users intend to download and share.

The supported applications include:

- Remote desktop service such as Terminal Services (RDP5, RDP6), VNC
- HTTP- and HTTPS-based intranet data
- Remote control protocols: Telnet and SSH
- File Transfer Protocol (FTP)
- Network File sharing (CIFS)
- Citrix Client
- Outlook Web Access (OWA)



Remote users will be able to access applications through the Internet by simply using a web browser.

Easy Management

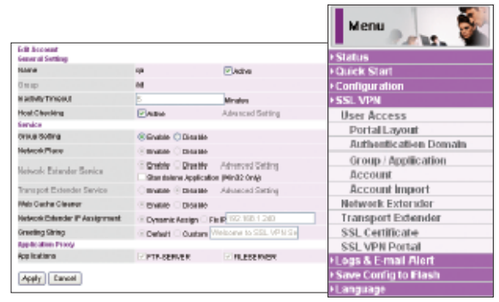
Web-based Management Interface

Through the web management interface, grouping users and customizing applications becomes quick and easy. The administrator's interface enables administrators to configure the BiGuard S6000 device and authorize access applications to different users according to different authorization levels. The end-user's web portal interface is a customized interface to support the user to run the authorized applications by just click and run.

The Quick Start Wizard provides administrators with a simple step-by-step guide to create, manage, and delete SSL VPN user accounts for remote users. The BiGuard S6000 Dual-WAN SSL/IPSec VPN Giga SME Appliance also provides administrators with user-friendly tools such as SSL VPN logs to monitor remote users' access.

Group Account Management

IT administrators can utilize the AD/LDAP Account Import feature to manage intranets by importing existing accounts from AD/LDAP servers into a BiGuard S6000 device. In addition, Group Account Setting makes it easy for IT administrators to set up and grant different kinds of user groups on certain access applications. If an IT administrator needs to set up many "sales" users in a single group who need to retrieve the price information and other files in the intranet while traveling, administrators can easily group them up and configure authorized applications for that group. From time to time, should new users be added, IT administrators simply authorize new users in the same user group the use of the same authorized applications and inherit the existing Group Account Settings. The Group Account Settings feature saves the effort of setting up various kinds of users and access authorizations through a one-time setup.



Personalized Application Portal

The applications for each individual remote user are personalized, all the applications each individual is allowed to access are shown in the web portal. A simply mouse click can start an application shown in the web portal. By using a standard web browser, remote users can access their personalized portal page.

InstantChat Support Service

The MSN-like, web-based Instant*Chat* Support Service provides users with online technical support during office hours by logging on to http://www.biguard.com/.

After logging onto the website, you can click on Instant*Chat* Support Service and send messages to request support help and "virtually" chat with a Billion support specialist regarding the usage, implementation and configuration of the BiGuard S6000 Dual-WAN SSL/IPSec VPN Giga SME Appliance.

During standard office hours, typically 5x8, and if necessary, the technical assistant can remotely diagnose the event log of the device to help identify software and hardware problem.

During "chat", you can send files to the specialist, and record all chat transcripts by email or print-out. Once your support issue is solved, you can rate the support service you just received, so that your feedback can be used to further improve the service quality of the Instant*Chat* Support team.

To receive Instant*Chat* Support Service, you will first need to complete the product registration on http://www.biguard.com/. This support service is offered as a courtesy for the first 180 days from product registration.