



## Features & Specifications

### SSL VPN

#### Capabilities

- Recommended for small offices and SMBs with employees from 50 to 200
- Concurrent sessions: 25,000
- Concurrent SSL VPN tunnels: up to 30, basic 10 tunnels

#### Access Connections

- Network Extender (TCP / UDP)
- Standalone Network Extender client
- Network Place
- Application Proxy
- Personalized web portal
- SSL hardware accelerator
- Single Sign-On (SSO)

#### Applications & Management

- Network File Share (CIFS)
- Citrix client
- Terminal services (RDP5, RDP6)
- File Transfer Protocol (FTP)
- Telnet
- Supports MS Outlook Web Access (OWA)
- Virtual Network Computing (VNC)
- Secure Shell (SSH, SSHv2) support
- SRDP (Single Remote Desktop Protocol)
- WOL (Wake On LAN)
- Granular user policy management
- Supports mobile devices (Microsoft Windows Mobile 5.0 / 6.0 or compatible)
- Supports MS IIS NTLM (NT LAN Management) authentication
- SSL event log and monitor
- Web based data (HTTP, HTTPS)

#### 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 checking<sup>\*3</sup>

#### Compatible Web Browsers<sup>\*1</sup>

- 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<sup>\*1</sup>

- Microsoft Windows, Linux, and Apple Macintosh

### Firewall & Content Filtering

- Stateful Packet Inspection (SPI)
- Denial of Service (DOS) prevention
- Packet filter
- MAC filter
- Instruction 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
- Supports BiGuard CMS for centralized management

#### 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](http://www.biguard.com) in order to be able to use the update feature and firmware updates
3. To be available
4. All the specifications are subject to change without prior notice.

### IPSec VPN

- 10 IPSec VPN tunnels
- 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

### Wireless

- Compliant with IEEE 802.11n, 802.11g and 802.11b standards
- 2.4 GHz – 2.484 GHz frequency range
- Up to 300Mbps wireless link rate
- Wireless NAC (Network Access Control)
  - Up to 4 SSIDs setup
  - Guest account auto-generating
  - Guest account duration control
- WPS (Wi-Fi Protected Setup)
- 64 / 128 bits WEP supported for encryption
- Wireless Security with WPA-PSK / WPA2-PSK support
- Supports Wi-Fi WMM prioritization
- WDS repeater function support

### Network Protocols and Features

- Static IP, PPPoE and DHCP client connection to ISP
- NAT, static routing and RIP/2
- Dynamic Domain Name System (DDNS)
- Router mode
- Virtual server
- Hardware DMZ
- DHCP server
- SNTP
- SNMP
- Multi-NAT
- Transparent bridging

### Logging and Monitoring

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

### Hardware Specifications

#### Physical Interface

- 1 x 10 / 100 / 1000Mbps Gigabit WAN ports
- 4 x 10 / 100 / 1000Mbps Gigabit LAN ports (1 port can be configured as DMZ)
- 3 detachable 2.4GHz 2dBi SMA antenna

#### Physical Specifications

- Dimensions: 19" x 6.93" x 1.65"
- 1 x USB 2.0 host (Future extension)
- Power switch
- Reset button

#### Power Requirements

- Input: 15V DC, 1.6A

### Operating Environment

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

### Support and Service<sup>\*2</sup>

- Hardware Warranty for 1 years
- Features and Firmware Upgrade for 1 year

## 802.11n Gigabit SSL / IPSec VPN Gateway with Portal-based Wireless NAC

Concerned about your corporate Intranet being intruded while offering WLAN Internet/Intranet access?  
- With BiGuard S100N you can, with no risk or compromise to the security of your corporate network.

### BiGuard S100N

ideal for

- Small Offices
- SMBs
- Departments of SMEs



### Key Features

- Draft 802.11n wireless and delivers up to 300Mbps link rate
- Wireless NAC (Network Access Control)
- SSL VPN gateway plus solid router and firewall functions
- IPSec VPN capabilities
- Gigabit for both LAN and WAN connectivity
- Rich in SSL VPN applications
- Granular access policy management
- Personalized web portal
- Data encryption, user authentication and access control
- End Point Security (EPS) checking<sup>\*3</sup>
- Host security checking
- USB 2.0 port for plugging a 3G / HSDPA modem<sup>\*3</sup>
- Supports Wi-Fi Protected Setup (WPS) and WPA-PSK / WPA2-PSK
- Supports Wi-Fi WMM prioritization
- Quality of Service control
- Windows / Linux / Macintosh supported
- Microsoft Windows Mobile 5.0 / 6.0 compatible mobile devices supported

### Options for Business Growth

- BiGuard SSL VPN Tunnel Upgrades
- BiGuard Central Management System<sup>\*3</sup>
- BiGuard One-Time Password

With the increasing availability of wireless technology, small offices and SMBs are finding that WLAN deployment can allow them to increase the overall efficiency of their business but they still remain on the sideline. The most important reason is that they are concerned about the exposure of their sensitive corporate information over the WLAN network. Billion's BiGuard S100N is the perfect solutions for SMBs that need a flexible, secure wired and wireless connection, and always-on connectivity to the corporate resources. Integrated with portal-based wireless NAC (Network Access Control), the BiGuard S100N enables workers or visitors to roam freely, securely and seamlessly between subnets in an office building, or between different network types – LAN, WLAN and WAN – without the risk of unauthorized access to the corporate network. By establishing encrypted SSL VPN tunnels, mobile workers can securely access the intranet from any location, such as a branch office, home, or even a public kiosk. Gigabit WAN and LAN ports provide the bandwidth and speed needed for heavy bandwidth consuming applications like video streaming and critical business applications. "Energy efficient" features such as Smart Power Saving and Wake On LAN (WOL) allow the corporate networks to be more environmentally friendly and to increase cost savings without the compromise of their network performance.



## Benefits

### Comprehensive Security for WLAN, LAN and WAN Connection

Billion's BiGuard S100N delivers comprehensive security features to meet with the need of SMBs who concern about the security issue for the corporate network.

#### Wireless NAC (Network Access Control)

The Wireless NAC (Network Access Control) technology allows IT manager to set up 4 separated SSIDs (Service Set Identified) which enable a variety of WLAN users to have different security levels and privileges to access different parts of the network so that employees or visitors to the organization can enjoy the mobility without compromising security. Also, its rich guest access services allow administrator to configure, update, monitor and easily adjust the security policy of guest user accounts by using a customized web portal.

#### SSL VPN and IPSec VPN

The BiGuard S100N supports an array of enterprise-class security features including IPSec and SSL encryption to ensure the security of data transmission and user access authorization. This combination provides excellent deployment flexibility to small business operations for meeting the requirements of any remote access users – visitors to the organization, business partners, branch offices, mobile workers...etc.

#### End Point Security\*3 and Host Security Checking

The End Point Security (EPS) function enables IT administrators to configure and assure that the client-side PCs are protected with authorized security settings such as anti-virus software, patches, browsers, and files in order to prevent potential threats from the endpoint PC. Simultaneously, the host security checking feature enables IT managers to configure the identities of a remote PC by host name, IP address and MAC address in order to assure the authorized users and protect the corporate network from potential security threats.

#### WPA-PSK / WPA2-PSK and WEP

Wireless Protected Access(WPA-PSK / WPA2-PSK) and Wireless Encryption Protocol (WEP) ensure high-level data protection and WLAN access control.

#### Robust Firewall Security

Firewall, Stateful Packet Inspection (SPI), Denial of Service (DoS) prevention and URL filtering are all integrated to guard your network against malicious attacks. In addition the firewall features an e-mail alert service, activated whenever an attack occurs.

#### Two-factor authentication with BiGuard One-Time Password (Optional)

BiGuard One-Time Password, a car-key sized dongle, can be used with BiGuard S100N to enhance the security and the credibility of audit trails with strong, two-factor authentication. It can dynamically generate a 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.

### Great Mobility and Productivity

By deploying the wireless NAC feature of Billion's BiGuard S100N, you can provide your workers with more flexibility and secure wireless connection to the corporate network, and raise productivity as well as increase the overall efficiency of the business. In addition, the guest account setting allow visitors to your organization to access the wireless network, providing tools they need to help grow their business and yours. It also creates a professional and positive image of your company with customers, partners and visitors. Moreover, the BiGuard S100N offers industry-advanced SSL VPN applications such as Network Extender and supports a wide range of browsers, platforms and operating systems, providing remote users, mobile workers and external business partners with remote access to the corporate network to share files, check e-mail, and download documents as if they never left the office. A business traveler can log in via a mobile device like PDA, the SOHO or a graphic freelancer on Macintosh can even connect his Apple PC to customers' networks to remotely collaborate on a project. Secure remote access with BiGuard S100N is possible via any device from anywhere at anytime.

### Optimal Wireless Speeds and Coverage and Powerful Gigabit Connectivity

With an integrated draft 802.11n Wireless Access Point, the BiGuard S100N delivers up to 6 times the speed and 3 times the wireless coverage of an 802.11b / g network device. In addition, WMM (Wi-Fi Multimedia) feature prioritizes the wireless traffic and minimizes the delay in wireless networks for time-sensitive applications such as Voice over IP and video conferencing. The BiGuard S100N features Gigabit capability for LAN, WAN and DMZ ports, enabling faster transmission speeds 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.

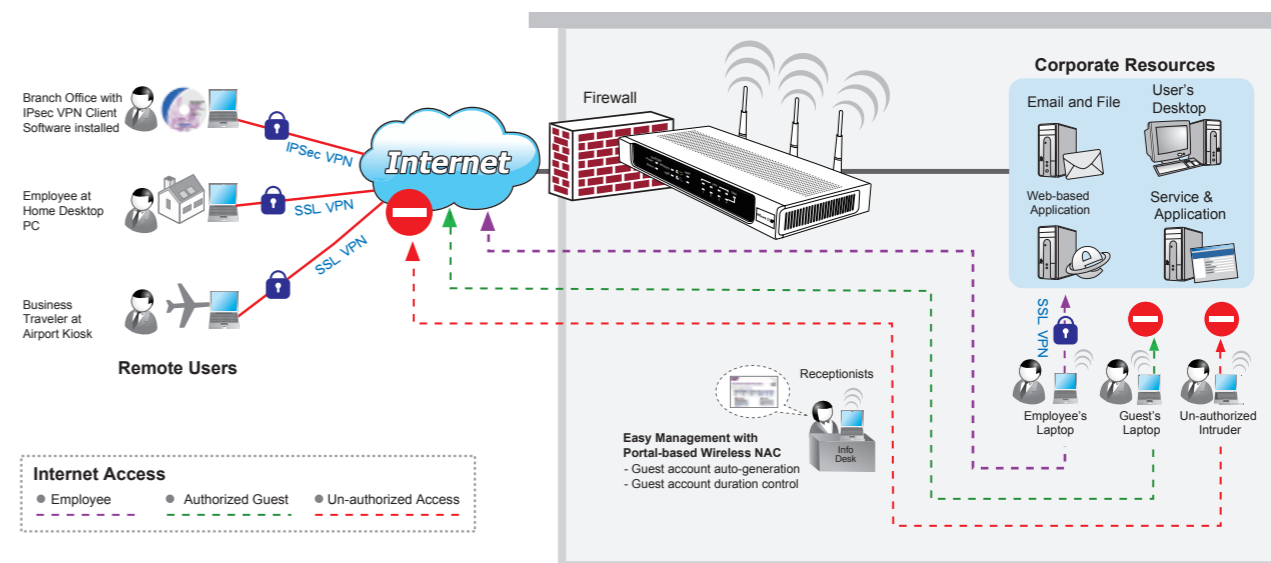
### 3G Mobility and Always-On Connection (Future extension)

With the BiGuard S100N you can connect a 3G / HSDPA USB modem to its built-in USB port. This enables you to use a 3G / HSDPA, UMTS, EDGE, GPRS, or GSM Internet connection, which allows downstream rates of up to 14.4Mbps possible. With the increasing popularity of the 3G standard, communication via the BiGuard S100N is becoming more convenient and widely available. You can even share your Internet connection with others even if you're in a meeting, or speeding across the country on a train. The auto fail-over feature ensures maximum connectivity and minimum interruption by quickly and automatically connecting to a 3G network in the event that your fixed line fails. The BiGuard S100N will then automatically reconnect to the fixed line connection when it's restored, reducing connection costs. These features are perfect for office situations where constant connection is paramount.

### Simple Ways to Go Green

Global warming is becoming a major threat in today's world. The BiGuard S100N is designed as an environment friendly networking solution for small offices and SMBs, allowing build up of their corporate network environment and turning their business green with energy efficient devices. With integrated Smart Power Saving technology, the BiGuard S100N has the ability to automatically detect the link status of each connected device and reduces power usage of ports that are idle. Additionally, this technology is able to analyze the length of any Ethernet cable for making the adjustment of power usage accordingly. The significant benefits for the organization are reduction in power consumption, adding of less heat to the environment, and also reduction of the operating cost. Moreover, the Wake on LAN (WOL) feature allows IT administrators to remotely shut down or wake up any devices in the network environment via SSL VPN tunnels from anywhere at any time when necessary. Furthermore, it complies with EU's RoHS directive and WEEE regulation to protect our environment from harmful substances.

## Access Applications and Business Activities



#### SSL VPN

- Wider range of comprehensive SSL VPN applications, feels like you've never left the office...
  - Network Extender
  - Application Proxy
  - Network Places
- Wide range of supported browsers, OS, and platforms
  - IE, Netscape, Firefox, Mozilla, Opera, Safari, Sun
  - Microsoft Windows, Linux, Macintosh
  - Mobile devices supported (Microsoft Windows Mobile 5.0 / 6.0 compatible)

#### Wireless NAC (Network Access Control)

- Multiple SSIDs, up to 4 SSID, to separate the traffic of guests and employees
- Three different types of WLAN access privileges
  - Bypass: temporary Internet access without authenticated SSL web portal
  - Authentication: authenticate Internet access via SSL web portal
  - Authentication plus SSL VPN: authenticate Internet access plus secure Intranet access via SSL VPN tunnels
- Easy management on guest accounts
  - Auto generation of guest accounts : even office receptionists can create new accounts for visitors simply via SSL portal page.
  - Guest account duration control: easy to set up how long the guest accounts will be used, like 30 minutes, 1 hour for guests and visitors, or even 3 months for short-term contractors.

#### Secure Remote Access

For business travelers, mobile workers, and branch offices

- Remote access to the corporate Intranet
- Employee connectivity, sales discount checking, and e-learning
- ERP system and order system connection
- E-mail box checking

For external customers and business partners

- Need to connect with business's ERP system
- Limited access to partner FTP servers for downloads and uploads

#### Wireless Connectivity

- General corporations to give visitors authorized Internet access over WLAN anywhere in office buildings, separate from Intranet access by their employees
- Manufacturers to give visiting buyers authorized Internet access, while the employees in the warehouse, in the factories, or in the office access the Intranet securely and simultaneously
- Healthcare service centers to enhance service quality by enabling mobile doctors and workers to securely access medical records while patients can access Internet
- Airport operators to give travelers and their workers different security levels of access over WLAN
- Conference / exhibition centers to provide exhibitors and visitors with separate wireless connectivity from their employees to enhance their service value
- Education / training organizations to provide quality learning environment by giving students and lecturers separate wireless connectivity from the access of their staff
- Department store workers are able to access the Intranet to manage inventory, and shoppers can gain access to the Internet whilst shopping
- Hotels and restaurants to offer customers Internet access, separate from their staff Intranet access over WLAN