**Features & Specifications**

**SSL VPN**
- Capabilities:
  - Secure Shell (SSH, SSHv2) support
  - Telnet
  - Terminal services (RDP5, RDP6)
  - Network File Share (CIFS)
  - Application Proxy
  - Standalone Network Extender client
- SSL hardware/soft accelerators
- Concurrent sessions: 25,000
- Maximum users: 50,000
- SSL, TLS
- Digital certificate
- Private key management
- User authentication
- User access control
- Wireless NAC (Network Access Control)
- Supports mobile devices
- Mobile authentication
- IPv6

**IPSec VPN**
- Capabilities:
  - 10 IPSec VPN tunnels
  - Manual key / Internet Key Exchange (IKE) authentication and key management
  - Authentication (MD5 / SHA-1)
  - IKEv2 / IKEv3 encryption
- IPSec Authentication Header (AH)
- IP Encapsulating Security Payload (ESP)
- Authentication (MD5 / SHA-1)
- Supports MD5 / SHA-1
- Mobile authentication
- Wireless NAC (Network Access Control)
- Supports mobile devices
- Mobile authentication
- IPv6

**BiGuard S100N**
- Ideal for:
  - Small Offices
  - SMBs
  - Departments of SMEs
- Features:
  - Draught 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
  - Host security checking
  - USB 2.0 port for plugging a 3G / HSDPA modem
  - Supports Wi-Fi Protected Setup (WPS) and WPA-PSK / WPA2-PSK
  - Supports Wi-Fi WMM prioritization
  - Quality of Service control
  - Wireless / 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
  - 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 corporate resources and always-on connectivity. The BiGuard S100N - ideal for Small Offices / SMBs / Departments of SMEs - provides all small offices and SMBs with the best solution to meet their networking requirement 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)
- SSL VPN and IPSec VPN
- Endpoint Security and Host Security Checking
- Two-factor authentication with BiGuard One-Time Password (Optional)
- Robust Firewall Security

The Wireless NAC (Network Access Control) technology allows IT managers to set up a variety of security rules for different user groups, enabling users to use different services based on their different levels of access. The wireless NAC technology ensures that un-authorized wireless access is prohibited by deploying a variety of security features. When a user logs in, the system will directly check the user’s credentials and if they are valid, the user can access the network. The wireless NAC technology also provides a high level of security for clients, such as wireless desktops, laptops, mobile devices, and Wi-Fi hotspots. The system provides a high level of protection against unauthorized access and unauthorized users, as well as preventing virus attacks. The BiGuard S100N technology is able 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 and adjust the power usage of those ports accordingly. The network is protected from eavesdropping and unauthorized access.

SSL VPN and IPSec VPN

SSL VPN technology is widely used in many countries and is very convenient. It can provide users with secure remote access to the corporate network, and the data transmitted is protected by SSL encryption. This technology provides a secure connection for users working from home or remote locations, enabling them to access the corporate network as if they were in the office, without the need for a dedicated physical connection. SSL VPN is suitable for a wide range of applications, including remote access to corporate resources, secure file sharing, and remote management of networks. The BiGuard S100N technology supports both SSL and IPSec VPN, providing a high level of security for the network.

Endpoint Security and Host Security Checking

The BiGuard S100N technology provides a variety of endpoint security features, including anti-virus, anti-spyware, anti-malware, and anti-thief. These features are designed to protect the corporate network from potential threats, and they can be easily configured by IT managers. The system also provides a high level of protection against unauthorized users and protects the corporate network from potential security threats.

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

The BiGuard One-Time Password technology is a key feature of the BiGuard S100N technology. It provides a high level of security for users who need to access the corporate network. The system generates a 6-digit PIN dynamically, which can be used to verify the user’s identity. This technology is widely used for secure remote access and can be easily integrated into existing security systems.

Robust Firewall Security

The BiGuard S100N technology provides a comprehensive firewall solution that protects the corporate network from potential threats. The firewall can be configured to block unauthorized access, prevent data theft, and prevent malicious attacks. The system is designed to provide a high level of protection against potential threats, and it can be easily configured by IT managers.

Great Mobility and Productivity

By deploying the BiGuard S100N technology, you can provide your employees with more flexibility and secure wireless access to the corporate network. This technology facilitates the growth of your business and increases the overall productivity of your employees. The BiGuard S100N technology supports a variety of mobile devices, which means that your employees can access the corporate network from anywhere, even from remote locations. Additionally, the system provides a high level of security for mobile devices, which helps to prevent data theft and malicious attacks.

Optimal Wireless Speeds and Coverage and Powerful Gigabit Connectivity

With an integrated 802.11n wireless access point, the BiGuard S100N delivers up to 5 times the speed and 3 times the wireless coverage of an 802.11b/g network device. In addition, WMM (Wi-Fi Multimedia) prioritizes the wireless traffic and minimizes the delays in wireless time-sensitive applications such as Voice over IP and video conferencing. The BiGuard S100N technology is capable of delivering high-speed wireless access to LAN, WAN and DMZ ports, enabling faster transmission speeds for remote access, internal connections or cloud networking. This design gives small and medium sized enterprises an edge in today’s business environments where mobile workers, business partners and travelers can access the corporate network from anywhere, at any time.

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

With the BiGuard S100N technology, you can connect a 3G/HDSPA USB modem to your BiGuard S100N device. This enables you to use a 3G/HDSPA, UMTS, EDGE, GPRS, or GSM Internet connection, which allows downstream rates of up to 14.4Mbps possible. The increasing popularity of the 3G standard, combined with the BiGuard S100N functionality, makes it 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-bellflower feature ensures maximum connection 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 technology is designed as an environmental-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 technology 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 usage across the whole life of the network devices, increasing the overall cost reduction of the operating cost, and also reduction of the operating cost of the network devices. The Wi-Fi based on the LAN (WLC) 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 RoHS directive and WEEE regulation to protect our environment from harmful substances.

Access Applications and Business Activities

Secure Remote Access

For business travelers, mobile workers, and branch offices

- Remote access to the corporate Intranet
- Employee connectivity, relax discount checking, and e-learning
- ERP system and order system connection
- Email 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

Corporates Resources

Email and File

Service & Application

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
- Biometric: temporary internet access without authenticated SSL web portal
- Authentication: authenticated internet access via SSL
- Authentication plus SSL: authenticated internet access plus secure internet access via SSL

Easy management on guest accounts

- Auto generation of guest accounts: even office receptionists can create new accounts for visitors simply by SSL portal pages
- Guest account duration control: easy to set up how long the guest accounts will be used, like 30 minutes, 1 hour for guests or visitors, or even 3 months for short-term contracts.

Wireless Connectivity

- General access to guests visitors: authorized Internet access over VLAN anywhere in the office building, separate from Internet 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 Internet security and simultaneously
- Health care 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 VLAN
- Conference / exhibition centers to provide exhibitors, and visitors with separate wireless connectivity from their employees to enhance their service value
- Education / learning organizations to provide quality learning environment by giving students and accesses separate wireless connectivity from the access of their staff
- Traveling corporate employees to have access to the Internet 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 Internet access over VLAN