



# The BiGuard SSL VPN Appliances

BiGuard SSL VPN Gateway  
VPN functionality and introduction

White Paper

## Table of Contents

|   |   |
|---|---|
| Foreword.....   | 3 |
| Introduction of Virtual Private Network (VPN).....                | 4 |
| IPSec VPN.....  | 4 |
| SSL VPN.....  | 4 |
| Three in one design.....  | 5 |
| Authentication Domain Technology.....                             | 6 |
| Compatibility of authentication domain name.....                  | 6 |
| Integrate complete Router technology into SSL VPN<br>product..... | 9 |
| Conclusion.....   | 9 |

## BiGuard SSL VPN Gateway VPN functionality and introduction

### Foreword

It's an important issue on enterprise's information security to protect the confidential information. With the increasing mobile workers, IT administrators must not only ensure that the business travelers and the external partners remote access stably and conveniently, but also remain the security while remote access. Therefore, it is a challenge for IT administrators to protect the damage from the hacker.

Recently, Virtual Private Network is rapidly becoming a popular method of the remote access. Mobile workers can access their office resource seamlessly from everywhere by using VPN. In addition, enterprises also keep in touch with their employees and co-work with their partners.

This article shows that Billion's BiGuard SSL VPN Security Appliance series offer both IPSec VPN capabilities and SSL VPN capabilities on a single platform. Therefore, Billion's BiGuard SSL VPN Security Appliance series are just for security remote access market. At the same time, it also explains the feature of the Active Directory (AD) and Lightweight Directory Access Protocol (LDAP). When the users log-in successfully, how to remote access their office resource by using Billion's BiGuard SSL VPN Security Appliance series. Finally, it emphasizes the advantage of Billion's BiGuard SSL VPN Security Appliance series. With Billion's BiGuard SSL VPN Security Appliance series, IT administrators can make a granular access control and reinforce the security of remote access. Billion's BiGuard SSL VPN Security Appliance series integrate SSL VPN encryption as well as firewall and router in one box, so they will be suitable in the security remote access in the SOHO/SMB/SME market.

## Introduction of Virtual Private Network; VPN

To provide a secure long distance access is a key requirement for those enterprises whose employees need to work from remote places to require the resource of an enterprise. If enterprises want to keep their productivity under the environment of their employees working from remote offices, internet cafes or hotels, then they need a solution to solve the difficulty of acquiring company's resource from remote places. VPN (Virtual Private Network) is a technology built upon the current Internet infrastructure. It creates secure encrypted VPN tunnels between two points, e.g. a remote user and an enterprise headquarter. Since VPN is more secure and cost effective than those traditional leased line or private networks, such as ATM (Asynchronous Transfer Mode), MPLS (Multiprotocol Label Switching), or Frame Relay, so VPN is widely accepted and recognized by enterprises. IPSec (IP Security) and SSL VPN (Secure Socket Layer Virtual Private Network) are the best solutions for enterprises for secure data transmission.

## IPSec VPN

By using the IPSec technology, users are required to be authenticated before a virtual private tunnel between two points are created to ensure a secure encrypted data transmission between the two points. In order to fulfill enterprises' requirements, IPSec VPN provides a secure and cost effective approach to allow enterprises to establish remote connections to and from all over the world.

IPSec is an ideal solution to be used in two reliable networks for site-to-site or client-to-site information exchange. However it has its disadvantages presented below:

- 1.The remote user will be required to install IPSec VPN client software in his/her computer, and run VPN configuration. This is an overhead that will cause the enterprise to increase the cost of routine operation in installation, maintenance and trouble shooting for IPSec VPN.
- 2.IPSec VPN will likely be faced with the problem of NAT traversal which causes the compatibility problems for remote client's IPSec software, NAT (Net Address Translation) router and IPSec gateway.

## SSL VPN

SSL is a protocol created by Netscape. It was created for secure business transaction in e-commerce. SSL uses a private key (eg. RSA) for user authentication. The private key is also used in signing and encrypting the data transmission. It provides secure communications on the internet and can prevents hackers, information theft, eavesdropping, and internet fraud during information exchange. SSL is currently supported by standard web browsers such as IE

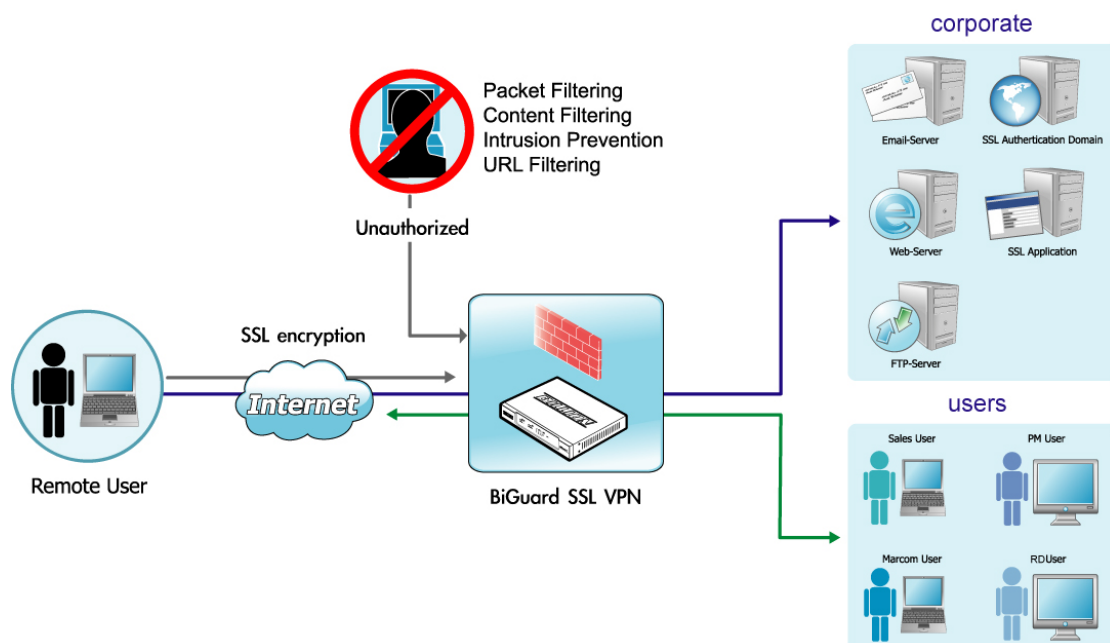
and FireFox. Users are able to access internet browsers to establish a SSL VPN tunnel to access enterprise's internal applications, file sharing and file servers. For SOHO, SMB (Small Medium Business) or users who need to access information any time, SSL VPN is the convenient tool.

SSL is an ideal resolution suitable for use under two reliable networks to establish client-to-site VPN. The advantages are presented below:

1. SSL protocol is support by standard internet browsers. Users do not need to install the client side software set up the configuration. It decreases the cost of management and supplementary requirement.
2. SSL VPN uses the protocol of the application layer to allow administrator to apply granular access control policy upon applications for users. It ensures remote users have more secure communication on Internet.
3. SSL VPN protocol connects through the application layer which decreases the compatibility problem that exists between IPSec VPN and NAT.

### Three in one design

BiGuard SSL VPN integrates routers, firewalls and SSL VPN into one secure product. It possesses the best solutions and many powerful functions to crave for. There is no complicated setup and operation management for BiGuard SSL VPN. Users do not need to buy other routers, hardware or firewall devices, as BiGuard SSL VPN combines the advantages of all 3 products into one. Figure 1 is a flow chart of SSL VPN placed in a corporate scenario.



**Figure 1 BiGuard SSL VPN flow chart**

## Authentication Domain Technology

Enterprises can use Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) authentication technology in a distribute network environment to provide user level browser, extension, flexibility and distribute security service. AD and LDAP allows IT personnel, administrator and users to be authenticated when trying to access company's intranet environment.

AD technology uses LDAP as its core protocol by using the Domain Name (DN) for the domain name of AD domain. Example; A domain name of AD is "cnc.billion-nt.hq". However, LDAP defines domain name by different rules which consists of Common Name (CN) and Domain Country (DC), eg. "cn=users, dc=test, dc=bgs10, dc=com, dc=tw". BiGuard SSL VPN is able to create a new Group in terms of AD or LDAP authentic domain to manage and authenticate remote users.

## Compatibility of authentication domain name

BiGuard SSL VPN is a flexible product in its authentication mechanism. For those enterprises that do not have authentication domain servers, they can make use of the Local Database to authenticate remote users, as shown in Figure 2. For those enterprises that do have the authentication domain servers, BiGuard SSL VPN supports Active Directory, LDAP, NT Domain and RADIUS to authenticate remote users, as shown in Figure 3.

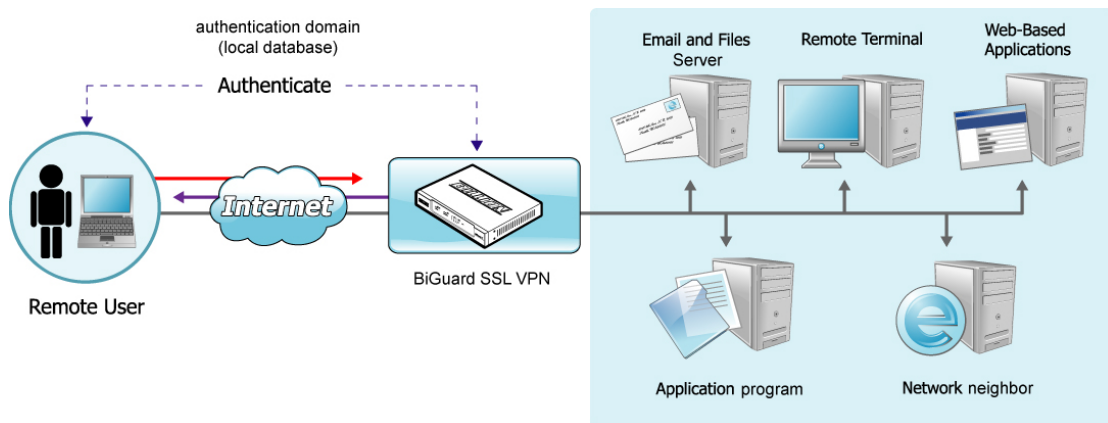
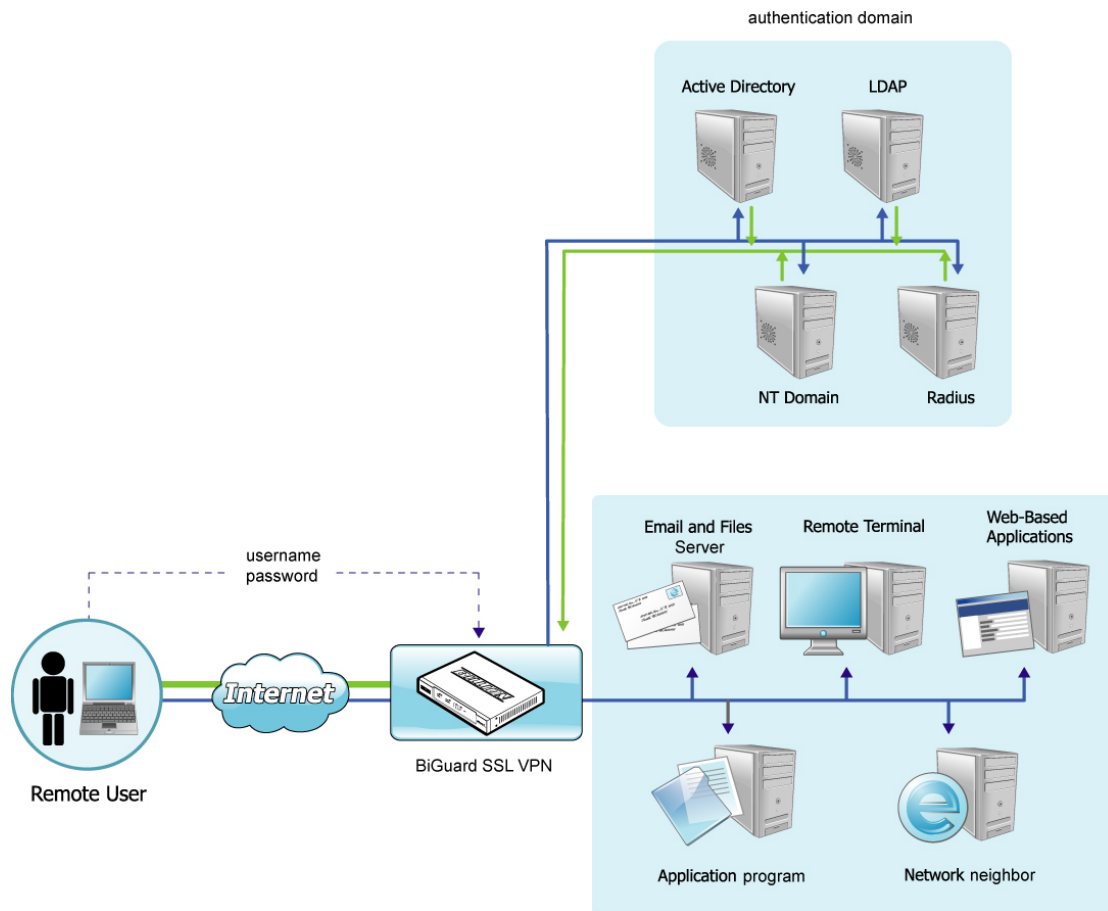


Figure 2 BiGuard SSL VPN using Local Database to authenticate remote users.



**Figure 3 BiGuard SSL VPN using the authentication domain mechanism to authenticate remote users.**

BiGuard SSL VPN's user management can utilize the existing AD or LDAP servers from the company's internal network to locate the user accounts. The administrator can easily group users into a designated Group by simply clicking a few buttons. In Figure 4, it illustrates the result of requesting the user list from authentication domain servers such as AD or LDAP before adding a new user. The administrator can check the checkbox to import the user names to the selected group in the BiGuard SSL router. To save time, the administrator can just check the checkbox Select All to import all the user names from the AD or LDAP authentication servers into the router. Figure 5 illustrates the result of clicking "Apply" button to add new users to Router. Therefore, those new added users are able to access enterprise internal information from remote places through BiGuard SSL VPN after authenticating by AD or LDAP authentication servers.

Select Account(s) to add <<First <Prev Page 6/8 Next> Last>>

| Select all <input type="checkbox"/> |                                     | Change group  |              |         |
|-------------------------------------|-------------------------------------|---------------|--------------|---------|
| #                                   | Selected                            | User Name     | Add to group | Status  |
| 51                                  | <input type="checkbox"/>            | otis          | Test         |         |
| 52                                  | <input type="checkbox"/>            | otischang     | Test         |         |
| 53                                  | <input type="checkbox"/>            | pattywu       | Test         |         |
| 54                                  | <input type="checkbox"/>            | petershih     | Taipei_2K    | Existed |
| 55                                  | <input type="checkbox"/>            | porcupinechen | Taipei_2K    | Existed |
| 56                                  | <input type="checkbox"/>            | pqanj         | Taipei_2K    | Existed |
| 57                                  | <input type="checkbox"/>            | pqatest       | Taipei_2K    | Existed |
| 58                                  | <input checked="" type="checkbox"/> | raymondwu     | Test         |         |
| 59                                  | <input type="checkbox"/>            | riachang      | Taipei_2K    | Existed |
| 60                                  | <input type="checkbox"/>            | robert        | Test         |         |

Apply Cancel

Figure 4 Illustrates the example of enquiry users in the authentication domain server.

Select Account(s) to add <<First <Prev Page 1/8 Next> Last>>

| Select all <input type="checkbox"/> |                                     | Change group    |              |          |
|-------------------------------------|-------------------------------------|-----------------|--------------|----------|
| #                                   | Selected                            | User Name       | Add to group | Status   |
| 1                                   | <input checked="" type="checkbox"/> | otis            | Test         | Succeed! |
| 2                                   | <input checked="" type="checkbox"/> | otischang       | Test         | Succeed! |
| 3                                   | <input checked="" type="checkbox"/> | pattywu         | Test         | Succeed! |
| 4                                   | <input checked="" type="checkbox"/> | raymondwu       | Test         | Succeed! |
| 5                                   | <input checked="" type="checkbox"/> | robert          | Test         | Succeed! |
| 6                                   | <input type="checkbox"/>            | Administrator   | Test         |          |
| 7                                   | <input type="checkbox"/>            | Guest           | Test         |          |
| 8                                   | <input type="checkbox"/>            | IUSR_2K-SERVER  | Test         |          |
| 9                                   | <input type="checkbox"/>            | IUSR_2K-SERVER2 | Test         |          |
| 10                                  | <input type="checkbox"/>            | WAM_2K-SERVER   | Test         |          |

Apply Clear

Microsoft Internet Explorer

Account(s) added successfully!

確定

Figure 5 Illustrates the example of confirming new users to Router.

## **Integrate complete Router technology into SSL VPN product**

BiGuard SSL VPN integrates complete Router technology, including static Router, dynamic Router, RIP1/RIP2, static WAN, DHCP client and PPPoE. Besides, BiGuard SSL VPN supports most of the bandwidth management system such as, Dynamic Domain Name System, Virtual servers, DHCP servers, hardware DMZ, multiple NAT and SNTP. It also supports complete log and surveillance, including the system record, email alters, the attack record, and monitoring system status. BiGuard SSL VPN supports the most advanced firewall function, including Stateful Packet Inspection (SPI), Denial of Service (DoS), Packet Filter, Intrusion Detection, URL filters and able to block Java Applet/ActiveX/Cookies. This safety device also supports the ISP's most widely used WAN protocol.

## **Conclusion**

The remote user will not be required to install SSL VPN client software in his/her computer. The technology provides remote users to access through any standard internet browsers from anywhere in the world. SSL VPN has the same level of security as IPsec VPN for providing a secure remote access solution. BiGuard SSL VPN plays a role as a pioneer in SSL technology. BiGuard SSL VPN integrates the advantage of IPsec VPN in security and connection with the ability of SSL VPN. It reaches granular access control and enhances the security from remote places and solves the compatibility problem caused by NAT. Besides, this complete design integrates SSL VPN, firewall and Internet all into one, thus making BiGuard SSL VPN a secure device. BiGuard SSL VPN is now one of the most popular investments for those SOHO/SMB/SME users. It possesses cost effective and flexible solutions which is able to fulfill the need of secure remote access.

### **White Paper - BiGuard SSL VPN Gateways**

Copyright © Billion Electric Co., Ltd.

---

**BiGuard Product Registration** : [www.biguard.com](http://www.biguard.com)

**Technology Support** : [support@billion.com](mailto:support@billion.com)

[www.billion.com](http://www.billion.com)