



The BiGuard SSL VPN Appliances

Three-in-one design makes SSL VPN even more Affordable

White Paper

Table of Contents

Three
Solutions
in One



Introduction of Virtual Private Network (VPN)	3
IPSec VPN	4
SSL VPN	5
The Advantages of BiGuard SSL VPN Appliances	6
Technology and Applications	8
Flexibility and Compatibility	10
- Fit into your existing network environments	
Summary	14

Three
Solutions
in One**BiGuard**

Three-in-one design makes SSL VPN even more Affordable

Providing secure remote access to company resources has become a critical requirement for companies needing to provide a productive and secure way for mobile users to access company resources from remote sites. Whether the mobile user is working in a remote office, Internet café, or a hotel room, an easy and secure remote access solution has become imperative to ensure continued productivity.

Virtual Private Network (VPN) – the methodology of remote access

VPN deployed in the business community has revolutionized the communication between headquarters, branch offices, and/or remote users. By leveraging the public Internet, Internet-based VPNs use encrypted tunnels between headquarters, branch offices, and/or remote users, and are becoming more popular and accepted by corporations for its security and cost-effectiveness compared to traditional leased lines or private networks such as ATM, MPLS, or Frame Relay. IPSec and SSL VPN are two of the popular solutions. SSL VPN is one of the remote access solutions designed with clientless, secure, remote access to company network resources, while the IPSec VPN solution requires the user to install and configure software on the client computer. Unlike IPSec VPN, SSL VPN totally relieves the end user of costly configuration effort but still provides the same security level as IPSec VPN solutions. In addition, SSL VPN works at the application-layer and, therefore, allows a granular access control policy to be implemented for each end user. This allows the system administrator to setup different users' access to different applications according to their job functions and trust levels.

This paper addresses the benefits of IPSec VPN and SSL VPN technologies for remote access and examines the security features integrated into the BiGuard SSL VPN Security Appliances. BiGuard SSL VPN Security Appliances are designed to provide the must-have security features for the secure remote access market. We also address the flexible design in both the hardware and software that allows BiGuard SSL VPN appliances to fit into all the network environments in an office. The total-solution, all-in-one design with integrated SSL VPN, firewall, and Internet access in one box is also highlighted in this paper. All the applications supported and the technologies behind them are addressed, too.

Three
Solutions
in One

BiGuard



IPSec VPN

Internet Protocol Security (IPSec) is a set of protocols and algorithms that provide data authentication, integrity, and confidentiality as data is transferred across IP networks. IPSec provides data security at the IP packet level, that is, network layer, and protects against possible security risks by protecting data against intruders. IPSec is widely used to establish VPN connections.

There are three major functions of IPSec:

- Confidentiality: Conceals data through encryption.
- Integrity: Ensures that contents did not change in transit.
- Authentication: Verifies that packets received are actually from the claimed sender.

IPSec VPNs use IPSec technology to setup a virtual private tunnel between two different sites to ensure data confidentiality, integrity, and authentication. With a very solid technology background, IPSec VPN can offer organizations a secure and cost effective way to connect different sites, delivering transparent connectivity and resilience to meet the most changing and demanding network environments.

IPSec VPN transports the packets at the IP layer and therefore is able to setup a secure and transparent connection between the two sites. As IPSec VPN will transport all the IP layer packets to the remote site, the connection through IPSec VPN will grant full network access rights between the two sites for the network users. This will introduce a security risk if the remote site is not a trusted network. For most organizations, IPSec VPN is an ideal solution to support site-to-site secure connections.

IPSec is an ideal solution to connect site-to-site for two trusted networks and supports full network access for each end user. However, for remote access VPN applications, the following drawbacks will be encountered.

Three
Solutions
in One



The drawbacks of IPSec VPN solutions

1. The remote user has to install IPSec VPN client software on the remote computer and perform VPN configuration setup. The required installation, maintenance, and troubleshooting will introduce additional administration headaches and costs to the organization.
2. Most mobile users in the remote office or hotel room attempting to connect to the office IPSec gateway will encounter NAT traversal issue. There are a lot of compatibility problems with the remote client IPSec software, the NAT router, and the IPSec gateway.
3. IPSec VPN will route the traffic from the remote computer to the office network without any restriction, resulting in a security risk if the remote computer is connected from a public area like an airport or Internet café.

SSL VPN

SSL, short for **Secure Socket Layer**, is a protocol originally developed by Netscape to ensure the secure transmission of Internet transactions for electronic commerce applications. SSL uses keys (e.g. RSA) to encrypt/decrypt data and authenticate user access. It is used to prevent malicious invasion, data theft, eavesdropping, and phishing. SSL is widely adopted by standard web browsers such as Internet Explorer and Netscape.

Through the characteristic of confidentiality, SSL can be used to create a tunnel along an entire network stack to create a VPN (Virtual Private Network). Users can create a SSL VPN tunnel from any location with Internet access using a standard web browser to access corporate applications, files sharing and Intranet database. Without the need to pre-install and pre-configure client software, it becomes convenient and user-friendly for SOHO and SMB users, mobile workers, and customers to acquire information they need from anywhere, at any time.

The advantages over IPSec VPN solution

1. The SSL protocol is built into all Internet browsers. The user does not have to install client software and do configuration setup and therefore reduces the administrative headaches and support requirements.
2. Internet browser is installed on all computers. Remote mobile users are supposed to be able to access the company network resources from any place on any device with an Internet browser.

Three
Solutions
in One



3. SSL VPN works with application layer protocols and therefore allows the system administrators to define a granular access control policy for each application and each user. This will guarantee more security to the remote mobile users whether they are in a trusted area, like a branch office, or in an untrusted area, like an airport kiosk or Internet café.

4. The SSL VPN protocol and the transportation of application layers through the connection reduce the potential for NAT compatibility complications normally found with IPsec VPN client solutions.

A strong security solution for remote access

The BiGuard SSL VPN appliances are based on cutting-edge SSL technologies. They combine all the benefits of IPsec VPN in terms of security and connectivity with SSL VPN capability to allow granular access control, enhanced remote access security, and have no NAT compatibility issues.

Strong Encryption Algorithms

BiGuard SSL VPN appliances are encrypted with SSL/TLS. The data stream is encrypted, including the IP header information. BiGuard SSL VPN appliances support the most advanced security algorithms.

Host Security Checking

As the remote site computer is able to access company network resources, it is very important to establish a host security checking policy for the remote computers before allowing them to access the company network. You can setup to checks on the IP address, MAC address, and computer name. You can setup checks the registry settings, firewall settings, Windows version, OS patch, and application settings before granting access rights to the remote user. (This feature will be supported Q1 2007.)

Cache Cleaner

BiGuard SSL VPN appliances support a cache cleaner function that deletes all temporary Internet files, cookies and browser history when the user logs out or closes the web browser, thus ensuring that confidential data has been removed from the computer.

The cache cleaner function is able to make sure it will fulfill its function when the user logs out successfully. The problem with this function is that if the browser crashes during the connection, some data might still remain on a public computer. Internet cafés and airport

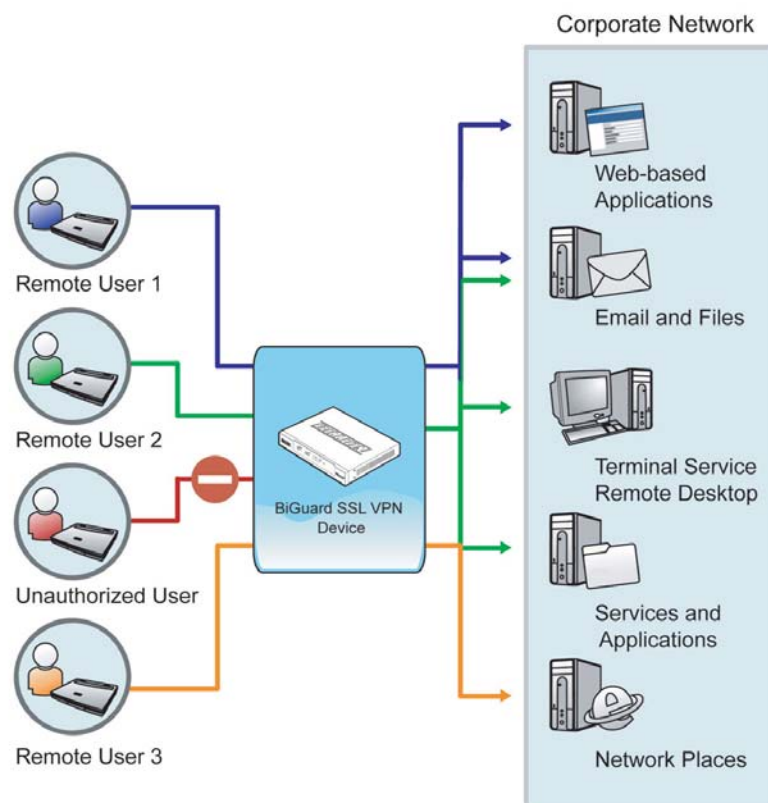
Three Solutions in One



kiosks are by their nature not secure places to view confidential data and to access company network resources from. Billion suggests setting up very restricted access policies for the accounts that will be mostly likely to access through Internet cafés or airport kiosks.

Granular Access Control

The BiGuard SSL VPN appliances work on the application layer and are able to grant different access privileges for different users to access different applications. By using granular access control, the system administrator is able to further guarantee access security by giving only restricted network access privileges to the mobile users who might access company network from insecure public places like Internet cafés and airport kiosks.



Worm Blocking

As SSL VPN works at the application layer, only the defined applications or networks are allowed to route through the SSL connection, worms cannot traverse from the client machine to the office network, providing inherently better security.

Three
Solutions
in One

BiGuard



A total remote access solution to meet different user requirements

BiGuard SSL VPN appliances are designed not only to meet all different user requirements for secure remote access but also to deploy successfully in different network environments. In addition, BiGuard SSL VPN appliances are the first in the world to integrate SSL VPN, Firewall, and Internet access into one box to provide a cost effective and total solution for SOHO/SMB/SME users.

Network Extender provides a transparent IP tunnel for trusted users to access all network resources. BiGuard SSL VPN appliances support Network Extender technology to virtually extend the connection to the central office network and allow the user to access office resources seamlessly from anywhere, as if they had never left the office. Users can remotely access office files and applications through their computer or PDA, as if they were using a computer in the corporate network. A sales person on a business trip, who needs to know the product inventory can use the Network Extender technology in BiGuard SSL VPN appliances to connect to the corporate network and access the stock database to check instead of phoning back to the office to request the information.

Transport Extender provides a transparent service tunnel for users to access client server applications. BiGuard SSL VPN appliances support Transport Extender technology to enable specific remote users or specific remote groups of users to use the SSL VPN connection 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. For instance, when a user remotely accesses MS Outlook e-mail, 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 are using MS Outlook in the office when in fact they are really somewhere else.

My Network Places provides network places function for users to access company network resources. Just like the Windows Network Neighborhood, My Network Places allows users to browse network files in the office network. From a home computer, the user can connect directly to My Network Places and access information inside the office -- there is no need to go back to the office if the user has forgotten an important document.

Three
Solutions
in One



Application Proxy

FTP Client provides client function to remote access company files. BiGuard SSL VPN appliances support File Transfer Protocol (FTP) client function to access an FTP server on the internal network, or any other network segment that can be reached by the SSL VPN appliance, including the Internet. The remote user communicates with the BiGuard SSL VPN appliance via an SSL VPN connection and is granted the appropriate permissions of the user to upload, download or create folders just like FTP client software.

HTTP/HTTPS provides an HTTP/HTTPS proxy function to access company resources through the web interface. BiGuard SSL VPN appliances support HTTP/HTTPS proxy function to access HTTP/HTTPS servers on the internal network, or any other network segment that can be reached by the BiGuard SSL VPN appliance, including the Internet. The remote user communicates with the BiGuard SSL VPN appliances via the HTTP/HTTPS protocol using a URL which is defined by the administrator. The BiGuard SSL VPN appliance will then redirect the HTTP/HTTPS session data to the configured HTTP/HTTPS server.

Terminal Service and VNC provides Terminal Service and VNC functions to access remote computers. BiGuard SSL VPN appliances support both Terminal Service (RDP5) and VNC functions to allow users to access the remote computers. Terminal Server is built into all Windows 2003 servers and Windows XP Professional desktop systems. It allows users to log in remotely from BiGuard SSL VPN appliances. By logging in, users create client sessions to the server. Terminal Server works by knowing how to respond to a BiGuard SSL VPN appliance client process. This "terminal client" will present the user with a window that simulates a local monitor. The Terminal Server manages all computing resources for the user and provides each user with their own environment. The server receives and processes all keystrokes and mouse clicks sent by each client and directs display output (audio and video) to the client as appropriate. Users have access to all of their authorized network resources and can run any application made available to them on the server. All the applications supported by Windows 2003 Server can be run via the Terminal Server.

VNC, or Virtual Network Computing, is software that makes it possible to view and interact

Three
Solutions
in One

BiGuard



with a computer from any other computer or device connected to the Internet. A VNC client is built into BiGuard SSL VPN appliances, so a person can connect to and interact with the company servers from a computer at home seamlessly.

Telnet, SSH BiGuard SSL VPN appliances provide Telnet, SSH services for administrators to remotely manage network resources. Telnet is a protocol that allows the user to connect to remote computers over a TCP/IP network. BiGuard SSL VPN appliances contain a built-in Java-based Telnet client to make a connection to a Telnet server.

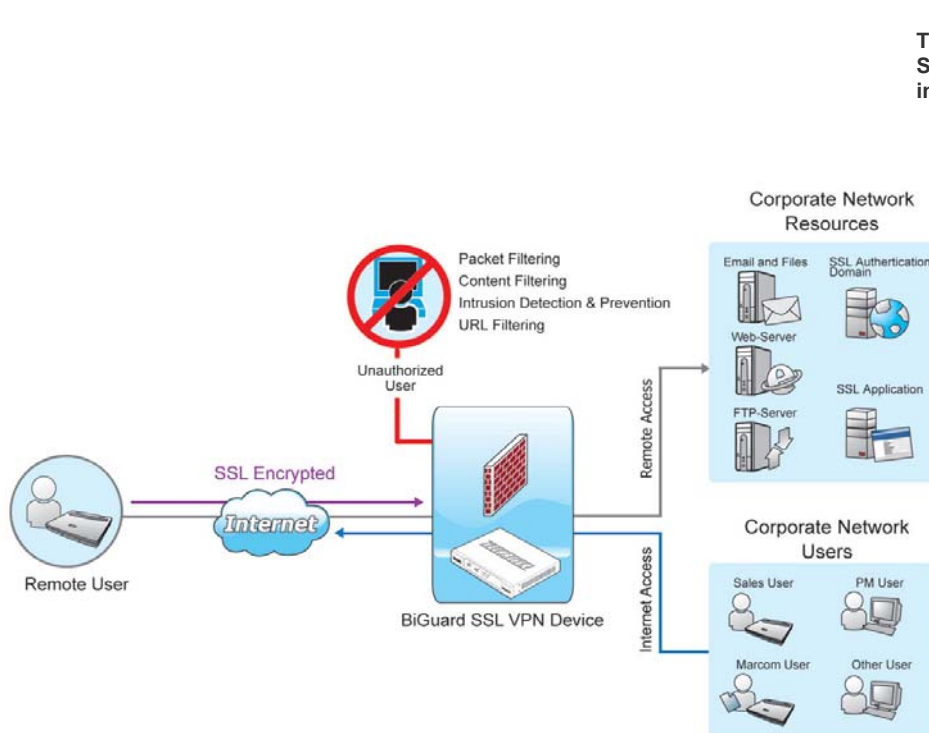
To protect user account from interception on the Internet, we suggest using SSH instead of Telnet. Since SSH encrypts all traffic with a public-private key scheme, only the SSH server can decrypt it and anyone who intercepts the data in transit will have only garbage data. BiGuard SSL VPN appliances contain a built-in Java-based SSH client to make the connection.

Fit into your existing network environments

BiGuard SSL VPN appliances are designed to meet all the requirements for SOHO/SMB/SME users. They integrate all the cutting-edge security technologies to become a truly trusted device. They provide all the functions and features that businesses require. In addition to all these, they are cost-effective and can be deployed to into any existing network environment.

All-in-one, Remote Access, Firewall, Internet Access

BiGuard SSL VPN appliances are the first devices in the world to integrate SSL VPN remote access functions, advanced firewall features, and Internet access functions into one box. In addition to the SSL VPN remote access functions, BiGuard SSL VPN appliances can be installed as the gateway to the Internet for the whole organization and at the same time the BiGuard SSL VPN can function as a firewall to prevent hacker and intruder attacks. This will be the most cost-effective network deployment.

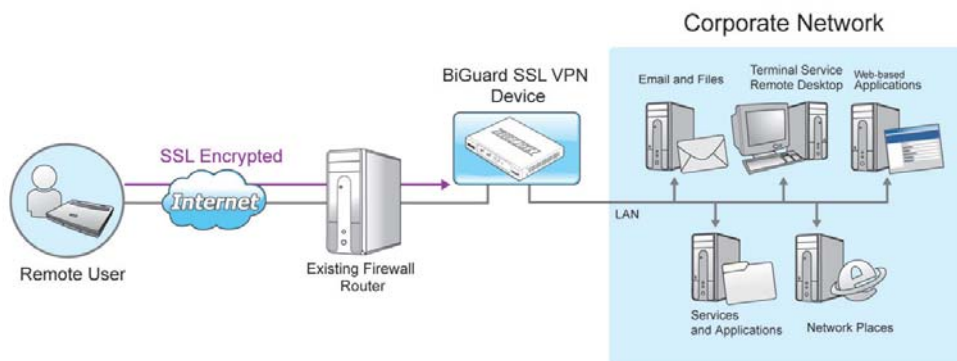


Three Solutions in One



Acting as a pure SSL VPN concentrator behind an existing firewall router

For some organizations with an existing firewall and router setup, the BiGuard SSL VPN appliance can function as a pure SSL VPN concentrator and slot into the existing network environment. In general, BiGuard SSL VPN appliances can be setup behind an existing firewall router and function as a SSL VPN concentrator for all the network servers that need to be securely accessed via the Internet. The system administrator has to setup to redirect port 443 (SSL port number) from the existing firewall to the BiGuard SSL VPN appliances. All the network servers that need to be securely accessed from remote sites must be routable from the appliance.



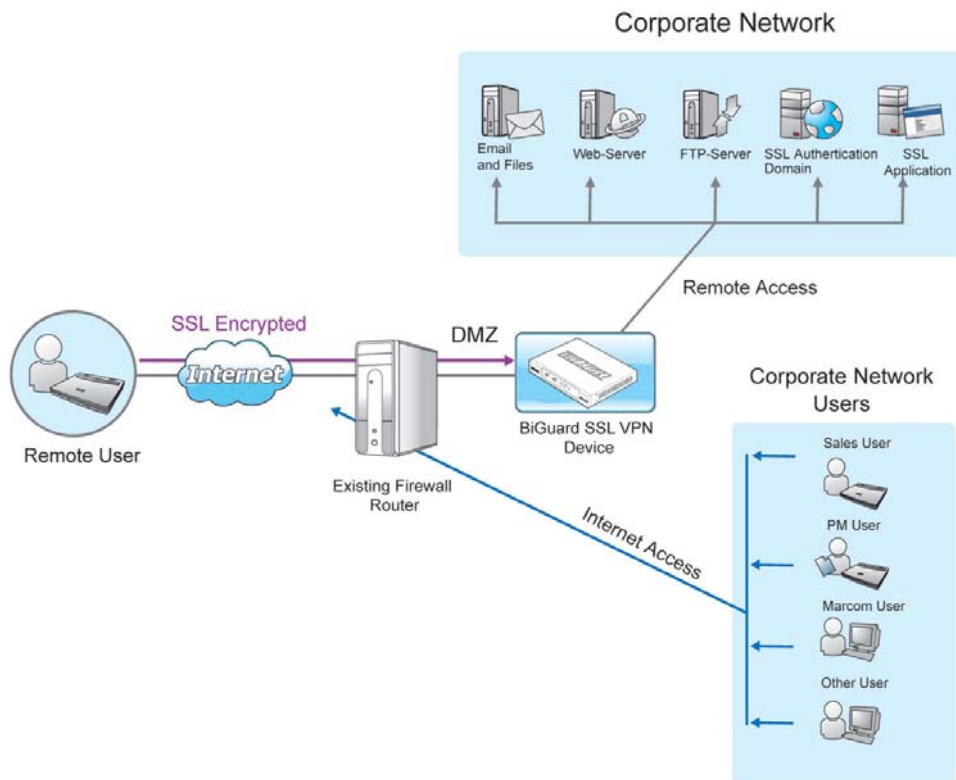
Fitting into a DMZ behind an existing firewall router

For some organizations with existing firewall router setup, the system administrator might

Three Solutions in One

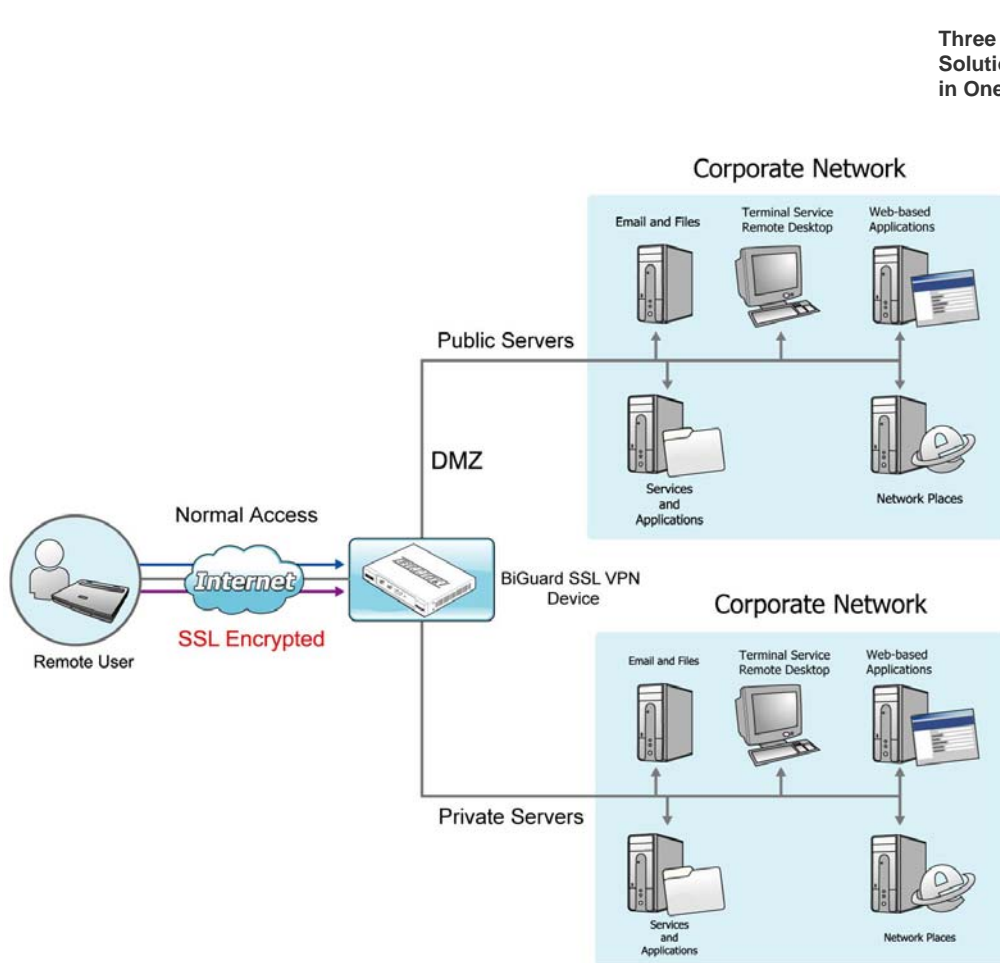


already have set up a DMZ in the existing firewall router for the office network to allow some network servers to be accessible from the Internet. In this kind of network configuration, the BiGuard SSL VPN appliance will sit in the DMZ and be accessible from Internet and function as a SSL VPN concentrator to redirect the SSL traffic to the servers in the private network.



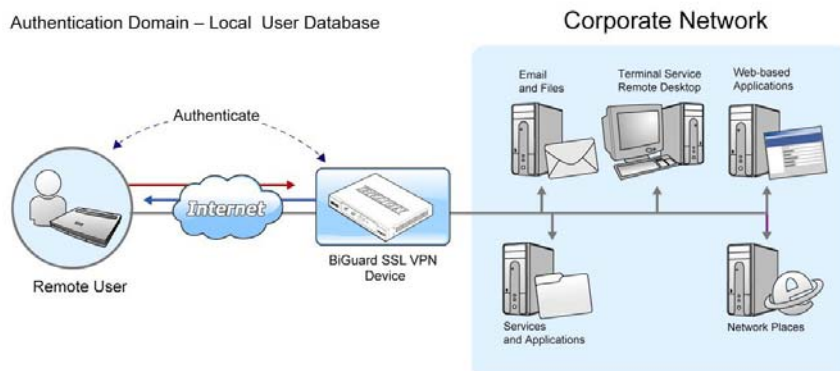
All-in-one, public server in DMZ, private server in LAN

BiGuard SSL VPN appliances support a hardware DMZ port to support some public servers that are accessible from the Internet. This will be very convenient for organizations to support general public web access through the DMZ to public servers and at the same time support secure remote access to private servers for trusted remote users.



Compatible with the existing Authentication Domain

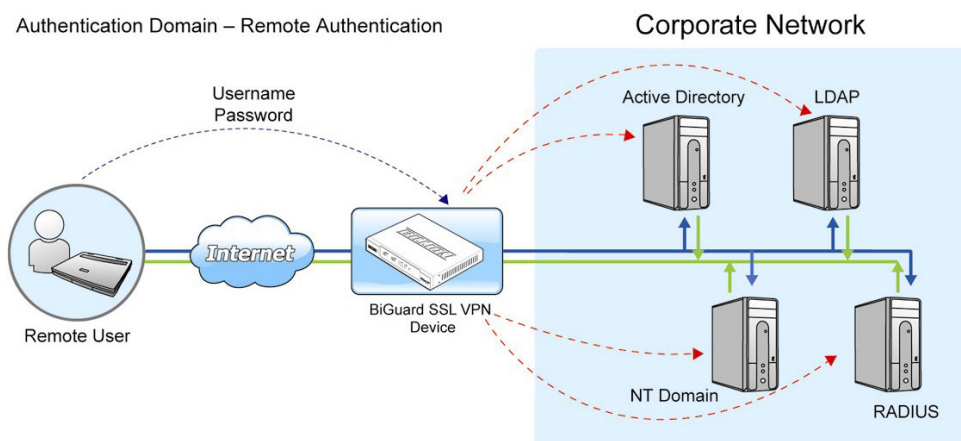
The flexible design of BiGuard SSL VPN appliances means they are able to communicate with almost all the authentication domain mechanisms in an organization’s network. For small offices, if there are no authentication domain mechanisms deployed to authenticate network users, users can use the local user database supported in BiGuard SSL VPN appliances to authenticate remote users.



Three Solutions in One



For enterprises with authentication domain authentication mechanisms deployed, BiGuard SSL VPN appliances can support Active Directory, LDAP, NT Domain, and RADIUS authentication methods.



Integrating the complete routing technology into one box

BiGuard SSL VPN appliances integrate the complete routing technology, including static routing, dynamic routing, RIP1/RIP2, static WAN connection, DHCP client WAN connection, and PPPoE WAN connection. In addition, the devices also support the most advanced bandwidth management control system, Dynamic Domain Name System, Virtual Server, DHCP server, Hardware DMZ, Multi-NAT, and SNTP. Complete logging and monitoring are also supported, including system logs, email alerts and logs of attacks, and system status monitoring.

All-in-one, SSL VPN, Firewall, Internet Access

BiGuard SSL VPN appliances support the most advanced firewall features, including Stateful Packet Inspection (SPI), Denial of Service (DoS) prevention, Packet Filter, Intrusion Detection, URL filters, and Java Applet/ActiveX/Cookie blocking. The appliances also support the most commonly used WAN access protocols to used connect to ISPs.

Summary

SSL VPN technology is able to support clientless remote access, hassle free system management, and allows mobile users to access the application from any place with via a browser interface.

Three
Solutions
in One

BiGuard



SSL VPN supports the same security level as IPSec VPN while the protocol nature enables it to function as secure remote access solution. On the other hand, IPSec VPN will be well suited for site-to-site connections where broad and persistent network connections are required.

The BiGuard SSL VPN appliances are based on cutting edge SSL technologies, combining all the benefits of IPSec VPN in terms of security and connectivity with the SSL VPN capability of allowing granular access control, and enhanced remote access security with no NAT compatibility issues.

In addition, the all-in-one design, with SSL VPN, Firewall, and Internet Access integrated into one box, makes the BiGuard SSL VPN appliances a cost-effective and flexible investment for SOHO/SMB/SME users to meet their secure remote access needs.

White Paper - BiGuard SSL VPN Appliances

Copyright © Billion Electric Co., Ltd. All rights reserved.

BiGuard User Registration: www.biguard.com

Technical support: biguardsupport@billion.com

E-mail: sales@billion.com; marketing@billion.com

www.billion.com