



LOCKED DOWN. FREED UP.

BLUE RIDGE VPN CLIENT

SECURE ENTERPRISE CONNECTIVITY, ANYTIME, ANYWHERE

The Blue Ridge/Secure Network Client is an application for Windows 2000, Window XP, and Vista that securely connects a remote user to a private or Home Network across public IP networks such as the Internet. The remote user may connect over any IP-capable medium including dial-up, wireless, cable modems, Ethernet, ISDN, xDSL, ATM, and cellular modems. Once connected, the Client can access network resources as if the workstation were physically located on the corporate network.

The Client communicates securely across a public IP network to a Blue Ridge BorderGuard located on the corporate network. Traffic between the Client and the BorderGuard can be encrypted, authenticated, compressed, and digitally signed to prevent eavesdropping, data tampering, and unauthorized access. All of the security features of the Blue Ridge secure network system are transparent to the Client. The Blue Ridge/Secure Network Client employs state of the art cryptographic techniques for security but is easy to use for end users.

The Blue Ridge/Secure Network Client has been designed to support a mix of future, current and legacy servers and applications typically encountered in businesses today. It works with virtually any networking protocol as evidenced by its wide deployment across a diverse set of commercial and government enterprises.

Depending on the X.509 certificate issued to the user, the same certificate used to authenticate to an Active Directory server can be used to authenticate the user to the Blue Ridge secure network. In this case, there is a single sign-on required and the user is presented with the actual Active Directory logon during the authentication process. Other key features include:

- Optimized for Windows XP/2000 and Vista
- Pre-login provides streamlined registration, authentication, and quick network access
- Supports mandatory mutual authentication via digital certificates delivering ease of use and best-of-breed security
- Encryption and encapsulation of delivered data assures privacy and data integrity
- Built-in two factor authentication using USB Tokens or Smartcards maximizes implementation flexibility
- Optional X.509 compatibility via Blue Ridge Networks *Open Authentication Architecture*™
- Optional Blue Ridge/Secure Mobile Office Solutions ensure world-wide remote access through support of dial-up, Wi-Fi, EV-DO, and hotel broadband

- Quick to Deploy and Implement
- Low Total Cost of Ownership
- Easily Connect Anytime, Anywhere
- Ensures Highest Levels of Data Privacy and Integrity
- Supports latest Commercial and Government Standards

Built-In Two-Factor Authentication

The public key is placed in a specially constructed secure storage device to prevent copying. Local access to the key is controlled by a password. The Blue Ridge/Secure Network Client software uses a hard drive, Smartcard, or USB-based secure storage authentication device for the user's public keys. The user's public key is encrypted under a key that is partly derived from the token, and partly derived from a user-supplied password. This feature is unique to Blue Ridge Networks and offers the very best in secure authentication without the costly investment of standing up a PKI infrastructure or external RADIUS/RAS servers.

Open Authentication Architecture for X.509

The Blue Ridge/Secure Network Client offers an open standards based authentication architecture (X.509) which is compatible with a broad array of identity and access management solutions that enable commercial and federal (DoD/Civilian) enterprises to comply with the latest regulations and mandates such as DoD PKI and HSPD-12.

Active Directory Integration

The Blue Ridge/Secure Network Client was engineered to optimize access to networks, applications and data. By creating a true NDIS layer Ethernet compatible interface to the Windows client, Active Directory authentication can proceed in a normal manner following tunnel establishment. Unlike other SSL or IPsec clients which require intermediary servers such as IAS or RADIUS, the Network Client communicates directly with the end-user's Active Directory authentication enabling policies to be enforced directly at the endpoint as if the individual was on the corporate LAN.

BorderGuard Client Tunnel-Lock

Tunnel-Lock is a BorderGuard centric security filter that enforces corporate access policy for remote access clients. With the Blue Ridge/Secure Network Client Tunnel-Lock filter applied, secure access to the corporate network resources is assured by blocking all unwanted traffic on the network from which the end-user is connecting. The application of this filter is performed during the client installation process, and cannot be disabled by the end-user. This filter effectively "locks-down" a company laptop to only one possible destination – the corporate network via the secure tunnel. This enables the company to utilize the corporate firewall as a single point of change for security policy management, and have it extend immediately to remote access users.

Dynamic DNS Lookup

A BorderGuard can be configured with a secondary DNS entry, such that if a remote access user cannot connect via the BorderGuard's pre-configured IP address, the DNS name provides the alternate path. This can be useful in disaster recovery situations where the BorderGuard is moved quickly and users must connect to a different IP address. It also enables an easy migration path from one ISP to another.

Supported Algorithms and Keys

- Encryption: AES128, AES192, AES256
- SHA-1 Data Integrity Check
- LZS Compression
- RSA and Diffie-Hellman 1024 bit keys

Minimum Client System Requirements

- Microsoft Windows 2000, XP (SP2 of above), Vista
- 64 MB memory
- 8 MB free disk space

The diagram below illustrates how Tunnel-Lock, developed by Blue Ridge Networks, locks down devices to only the enterprise network with which they are intended to communicate. Remote devices cannot open direct connections to the Internet nor can they communicate with unsecured guest networks. Tunnel-Lock also extends the protections and policies to all remote devices enforced by the enterprise firewall — regardless of where those devices are.

