



LOCKED DOWN. FREED UP.

---

**Blue Ridge Networks  
Managed Service**

# **VPN System Administrator's Guide**

BLUE RIDGE NETWORKS MANAGED SERVICE

# VPN System Administrator's Guide

---



14120 PARKE LONG COURT, SUITE 103  
CHANTILLY, VIRGINIA 20151  
[WWW.BLUERIDGENETWORKS.COM](http://WWW.BLUERIDGENETWORKS.COM)

All Products are provided with RESTRICTED RIGHTS.

Use, duplication or disclosure by the Government is subject to restrictions set forth herein and in subparagraphs (a) through (d) of the Commercial Computer-Restricted Rights clause at FAR 52.227-19, as applicable.

# Table of Contents

INTRODUCTION.....	II
VPNHELP DESK SUPPORT .....	III
NOTICE .....	III
DOCUMENT HISTORY.....	III
<b>WHAT IS BLUE RIDGE NETWORKS VPN?.....</b>	<b>1</b>
WHAT THE TUNNELING DOES .....	1
HOW IT WORKS.....	3
THE BORDERGUARD.....	4
TECHNOLOGY CERTIFICATIONS .....	5
<b>INSTALLATION PLANNING.....</b>	<b>6</b>
PHYSICAL REQUIREMENTS .....	7
OUTSIDE NETWORK REQUIREMENTS AND EXAMPLES .....	7
SELECTING THE INSIDE (HOME) NETWORK .....	8
REQUIREMENTS FOR THE HOME NETWORK.....	8
MULTIPLE BORDERGUARDS.....	9
SENDING IN THE FORMS.....	10
BORDERGUARD INSTALLATION .....	10
CUSTOM INSTALLATIONS .....	11
<b>BORDERGUARD MAINTENANCE AND SUPPORT.....</b>	<b>12</b>
<b>A QUICK USER TROUBLESHOOTING GUIDE.....</b>	<b>13</b>
<b>FREQUENTLY ASKED QUESTIONS .....</b>	<b>15</b>
INSTALLATION FREQUENTLY ASKED QUESTIONS.....	15
OPERATIONS FREQUENTLY ASKED QUESTIONS .....	16
SECURITY FREQUENTLY ASKED QUESTIONS.....	16
VPN CLIENT FREQUENTLY ASKED QUESTIONS .....	18
<b>PLACING A SERVICE CALL.....</b>	<b>20</b>
<b>APPENDIX A – CORPORATE FIREWALL CONFIGURATIONS .....</b>	<b>21</b>
IP PROTOCOL 50 AND UDP PORT 820 ACCESS .....	21
<b>APPENDIX B – DPFPING UTILITY .....</b>	<b>25</b>
IP PROTOCOL 50 AND UDP PORT 820 PING .....	25

## Introduction

The Blue Ridge Networks VPN Managed Service is designed to provide easy to use, secure access to an organization’s private computer network from anywhere using the Internet. For this to be useful, the networks need to be in place and running, or your users have nothing to connect to!

This manual is written for the benefit of the network administrator who is responsible for keeping an organization’s computer networks up and running, for ensuring that the organization has safe, firewalled connectivity to the Internet, and who possibly maintains some of the organization’s server computers as well.

It’s the job of Blue Ridge Networks, in conjunction with your organization’s administrative people, to grant and remove access to the proper users, provide technical support for those users, ensure that we expand our capacity at your site when it is needed, and ensure that our equipment is properly configured and remains in operation. We also ensure that resources on remote sites are available easily and securely. However, we’re dependent on *your* network (and your

ISP's) to provide the needed connectivity for your users. We'll explain how we'll work with you to minimize the effort on your part.

Because it's intended for technical people, this is a somewhat technical document. However, we've tried to make it understandable to all system and network administrators, and we'll explain network administration issues that everyone might not be familiar with.

## VPN Help Desk Support

The Blue Ridge Networks Customer Service Group information is as follows:

**Phone:**..... (703) 631-0583 / (800) 704-5234  
**FAX:** ..... (703) 631-9588  
**e-mail:** ..... support@blueridgenetworks.com  
**Hours:**..... Help desk support 24 x 7  
Engineering support 9am to 6pm Eastern Time, Monday through Friday  
**Address:** ..... 14120 Parke Long Court, Suite 103, Chantilly, Virginia 20151

Please provide the following:

- Product version number.
- Computer hardware used.
- Description of the problem, including on-screen messages received.

## Notice

Blue Ridge Networks makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Blue Ridge Networks shall not be liable for errors contained herein, or direct, indirect, special, incidental, or consequential damages in connection with the furnishing, performance, or use of this material.

No part of this work may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or by any information storage or retrieval system, except as expressly permitted by Blue Ridge Networks.

Blue Ridge Networks reserves the right to make corrections, updates, revisions, or changes to the information contained herein.

Microsoft Windows, Windows 98, Windows NT, Windows 2000, Windows XP, and MS-DOS are trademarks of Microsoft Corporation. Ethernet is a registered trademark of Xerox Corporation. All other trademarks used in this document are the property of their respective owners.

## Document History

Revision 5.3	03-25-05
Revision 5.2	12-08-04
Revision 5.1	09-10-04
Revision 5.0	02-26-04
Revision 4.1	08-28-02
Revision 4.0	04-22-02
Revision 3.0	01-17-01
Revision 2.0	06-24-00
Initial Release	04-15-99

# What is Blue Ridge Networks VPN?

Blue Ridge Networks (BRN) VPN is fundamentally two things:

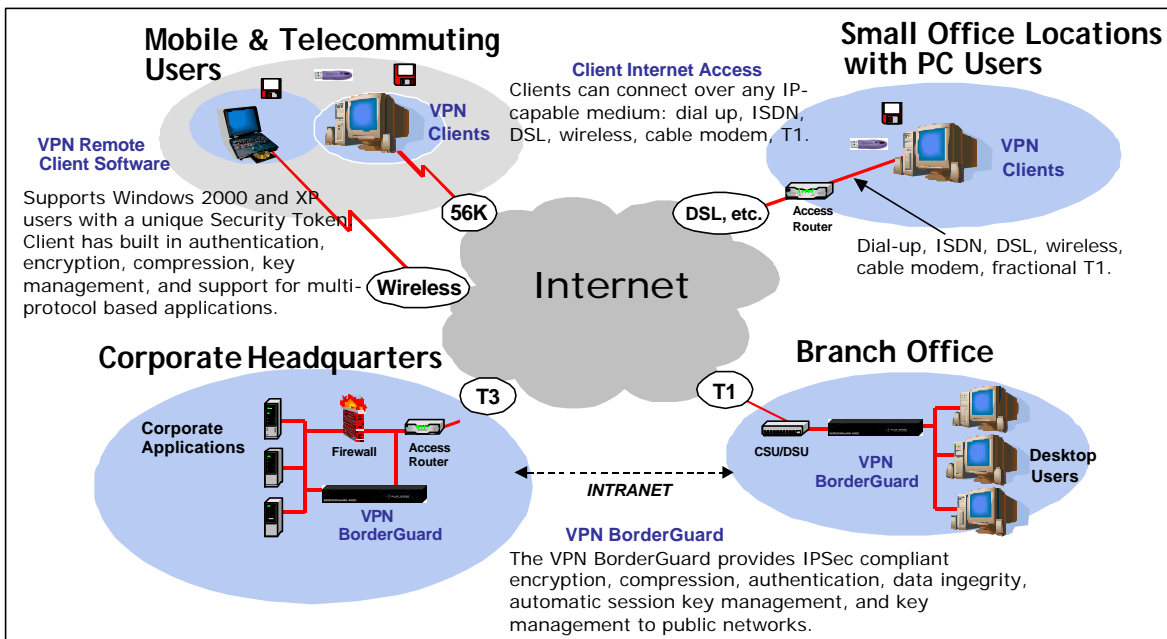
It's a *network tunneling* system that creates a Virtual Private Network (VPN) consisting of remote office individuals and users. Users in another connected site merely access your resources directly, with no additional VPN Client software required. They function as if they are connected to the Ethernet inside your corporate network. Using the BRN VPN Client, any remote, Internet-connected user appears to be present on your corporate network, in all senses of the term. If they're in a hotel room, at a wireless hot spot, sitting at a LAN-connected desktop at another site, or at home with a cable modem, all software applications function as if they're connected to an Ethernet inside your organization.

It's a *security* system, using very strong cryptography, built-in Public Key Infrastructure (PKI), and authentication techniques. That makes this transportation of your outside users to the inside of your organization safe and prudent.

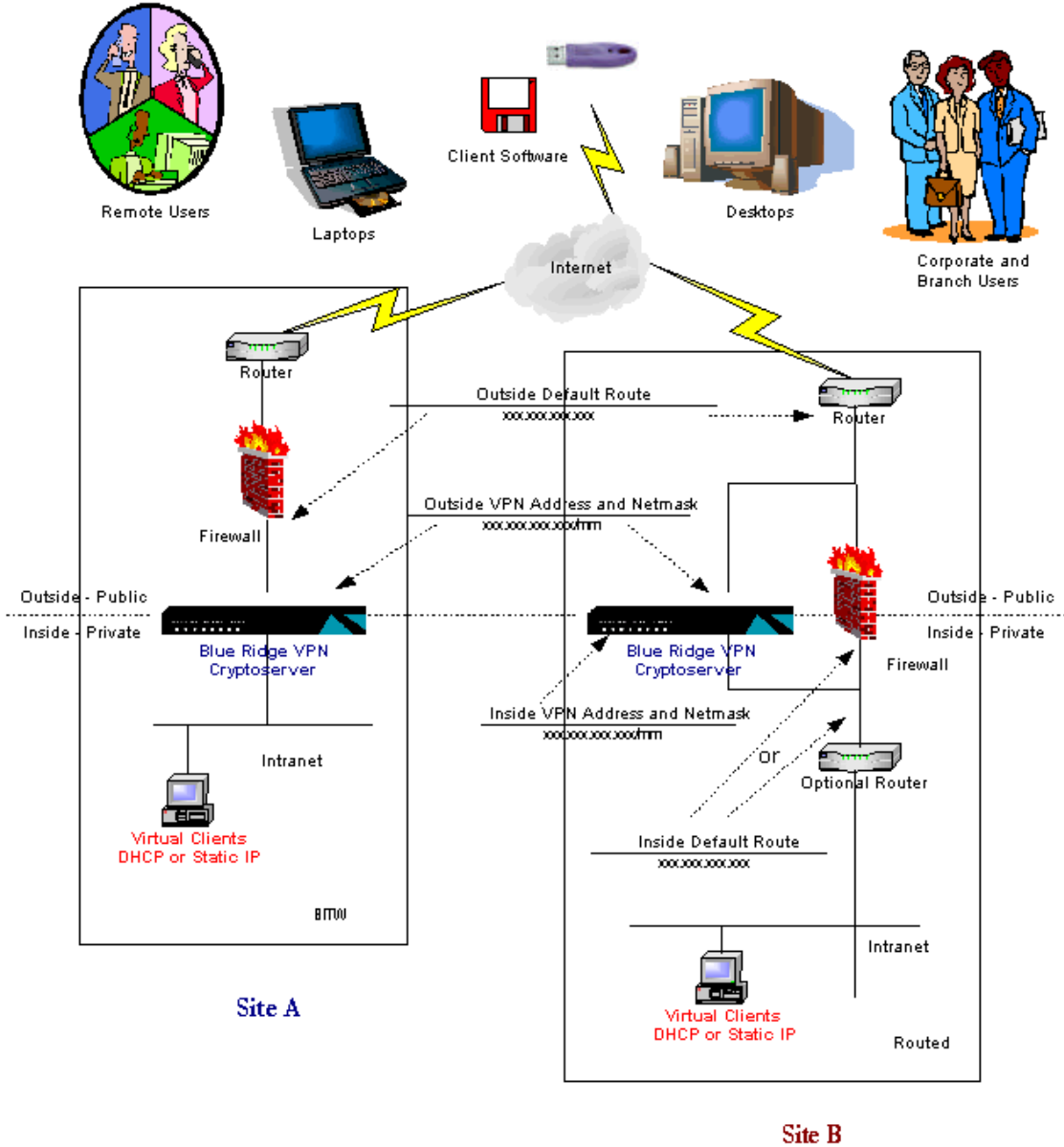
## What the Tunneling Does

Blue Ridge Networks uses a recognized approach to network connectivity called Layer 2 Tunneling. This general technique is used by sophisticated network switching gear such as VLAN products and Layer 2 switches to make one physical "Ethernet" logically appear to be composed of desktops, servers, and office LAN's that may physically be in separate locations.

Let's look at how BRN specifically accomplishes this. First, the following picture shows the physical things that are present for a BRN VPN user to access Corporate Headquarters or a Branch Office, called a *Home Network*.



*(Network configurations for VPN sites do not need to be the same at each location.)*



The net result of all the work by the physical equipment and networking software is that the remote user's machine is securely transported virtually onto the Home Network within your organization. This Home Network can be located in the Corporate Headquarters or any of the Branch Offices. Essentially all network packets generated by the user's computer are placed in a cryptographic network wrapper, directed through the Blue Ridge Networks VPN BorderGuard, and introduced on the Home Network. Packets on the Home Network that are of interest to the user are captured by the BorderGuard and sent back to the user's host machine.

If a user in one office wishes to access resources in another VPN-connected office, the connection is made simply by clicking the resource through Network Neighborhood, or by mapping a drive to the share. There is nothing else required to initiate the secure connection. The network security at each site determines the access allowed once a user is connected.

When a remote access user connects to the corporate network using the VPN Client, the user appears as if they are “at their desk” locally. They’ll have an IP address on the Home Network. Access to Windows and Novell file and print servers is available, based on network security. They can perform Windows resource sharing via NetBEUI. If they wish to access the Internet (or if someone on the Internet accesses *them*), they’ll do so through your firewall, despite the fact that they’re physically out in the Internet. They can access computers elsewhere on your Intranet, if they could do so while sitting directly connected to the Home Network. All internal firewalls, access controls, and misuse detection systems that you use internally will remain in effect.

This secure VPN takes place mainly between the pieces that we provide: the Blue Ridge Networks VPN BorderGuard network appliances that we provide for your sites, and optional VPN Client software for the user’s computer for remote access.

## How It Works

Let’s step through a connection cycle (assuming the equipment is in place) to get a better idea of what’s going on.

### Site-to-Site VPN

Blue Ridge Networks VPN BorderGuards first create secure tunnels between your VPN-connected intranets. After this point, all traffic between those intranets is encrypted, travels safely through the tunnel, and then is decrypted into its original form at the destination. This process is not visible to the user, but takes place in the background. No additional software is required on the user’s computer to initiate this secure connection. The network message exchange is highly secure, and uses public key cryptography (PKI) to establish the identity of one BorderGuard to the other.

### Remote Access VPN Client Software

Remote users not located in any of the VPN-connected sites need Blue Ridge Networks VPN Client software to make the secure connection. First, the remote user installs the VPN Client software on their laptop or desktop computer running Windows 2000 or XP. Installing the software merely enables the remote computer to send the proper protocols to a BorderGuard anywhere, but doesn’t permit them to connect. Think of it as installing Dial-up Networking without having an ISP account.

For those corporations requiring additional security, BRN offers a separate integrated filter called Tunnel-Lock™. The Blue Ridge Networks VPN Client with the Tunnel-Lock filter applied provides secure access to home network resources by blocking all unwanted traffic on the guest network (the network the user is connecting from, called the outer stack in the TCP/IP stack). Tunnel-Lock in permanent mode effectively “locks down” a company laptop to only one possible destination – your corporate network by way of our high-security VPN tunnel. This enables you to use your corporate firewall as a single point of change for security policy management.

This implementation of the Tunnel-Lock permits full NetBIOS access. When connected to the home network, the VPN Client can participate in a Windows workgroup, NT domain, and can access network shares. More information on this filter can be found in the Blue Ridge Networks VPN Client Users Guide.

Blue Ridge also offers an option for the VPN Client to be started at boot-up, pre-GINA. This auto-logon client starts the VPN tunnel back to your corporate network when the laptop or desktop is booted up and gains Internet connectivity. The authentication USB iKey must be present in the PC for this service to start, but the user does not need to key in a password. The next login screen presented to the user is your domain login.

### Remote Access VPN Client Subscriptions / Public Key Authentication

Next, a *subscription* is generated for the remote access user, built with the Public Key Infrastructure (PKI), from the Blue Ridge Networks Secure Operations Center. The subscription consists of two pieces: an *authentication token* – either a token diskette that cannot be easily reproduced or a USB iKey device, and a *pass phrase* that must be used to unlock that token. This is called *two-factor authentication* (something you have, something you know) where both must be present to connect. Two-factor authentication is the basis for most high security systems; Bank ATM cards are an example.

These PKI subscriptions are managed by BRN. There's an individual in your organization, the Administrative Contact, who's responsible for letting us know which individuals should be granted access, or have it revoked. It's our job to get those users up and running and keep them up and running. Once a user receives a token diskette or USB iKey with associated PKI subscription information, the subscription can be updated via electronic means such as ftp or email, if necessary.

## Remote Access Users Connecting to the Internet

Using the standard VPN Client, the remote access user's next step is to gain access for their computer to the Internet. They could dial into an ISP with Dial-up Networking; they could be hardwired into a LAN at some other organization's site; they could be in a public wireless hot spot; they could have some form of home or office access such as Cable Modem or DSL. **The only thing that's significant is that they must be able to send and receive TCP/IP packets while establishing their Blue Ridge Networks VPN Client connection.**

During the time the user is connected to the Internet, they can perform all the Internet-type things such as telnet, FTP, Web browsing, etc.

## Remote Access VPN Users Invoking a Subscription

The remote access user will click on the VPN Client symbol on their desktop, enter their VPN pass phrase, and then click on the Connect button (after the initial connection properties are set). This starts a process that validates that the token (a USB iKey device, floppy disk, or hard drive signature) is present on their machine, dials up to their ISP if required, and then begins a network negotiation with the BorderGuard at your site.

The network message exchange is highly secure, and uses public key cryptography (PKI) to establish the identity of the user to the BorderGuard (and also, to validate the BorderGuard's identity to the user's computer). The BorderGuard keeps records of subscribed users and their public keys, and will only allow users with currently valid subscriptions to connect.

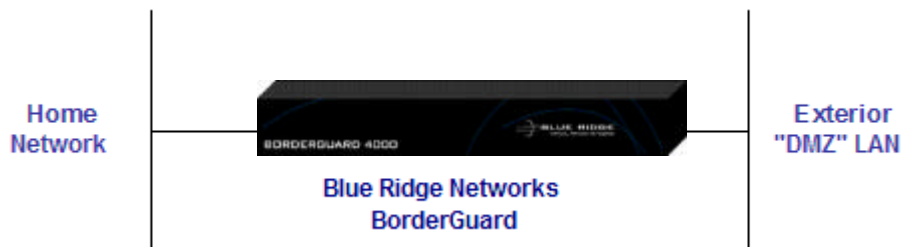
If the authentication iKey/token, password, public keys, and subscription status are all verified, the user gets connected. A logical Ethernet interface, built as part of the software installation process, becomes active on the user's host. All Windows networking applications are "bound" to this new logical interface, and all packets travel through the tunnel. The VPN Client software gathers their messages, cryptographically wrapped, and delivers them to the BorderGuard via the Internet connection, which could be a second, "real" Ethernet interface.

When the tunneled packets arrive at the BorderGuard, they are cryptographically validated and unwrapped, then presented in their original form on the Home Network.

The second function of the BorderGuard is to promiscuously listen on the Home Network, and relay packets to each connected user that matters to their software. This includes multicast traffic on the LAN (with a few filtered exceptions) and all unicast traffic directed to that user's MAC address.

## The BorderGuard

The last item to notice in this introduction is the Blue Ridge Networks BorderGuard. We'll need to work together to best locate it in your network.



The BorderGuard is fundamentally a highly secure, sophisticated network appliance that is designed to do one job and do it well. It's a small, stealthy device, typically deployed with two auto-sensing 10/100/1000 Ethernet interfaces, and one auto-sensing 10/100 Ethernet interface. One is attached to an "outside" LAN — typically the

LAN between your ISP's access router and your firewall that contains your mail servers, public Web servers, etc. Firewall designers often refer to this as the "DMZ" LAN, since it is the only one with full exposure to Internet traffic. It is also possible to deploy a one-port BorderGuard located inside the firewall. In this case, the firewall must be configured to allow IP Protocol Type 50 or UDP Protocol 820 packets to and from the BorderGuard.

The second interface is connected to your Home Network. It's also a 10/100/1000 connection, and is the network on which the users perceive themselves to be connected.

The third interface is a 10/100 connection, and generally not used in a standard deployment. If you are running a wireless network at your location, it can be used to secure the wireless network through the BorderGuard and then into your internal network, ensuring that your data is transferred safely through the wireless connection.

All you generally need to do is to connect the BorderGuard properly and ensure that it stays connected. It's the job of our Network Operations Center to keep working properly — by adding and deleting user subscriptions and supporting changes to your network configuration.

Larger scale configurations may consist of several BorderGuards connected between these Home Networks in parallel, or different BorderGuards that are connected to different Home Networks in your configuration. The Blue Ridge Networks VPN System is highly scalable.

## Technology Certifications

Blue Ridge Networks technology continually meets and exceeds the most rigorous testing anywhere. When it comes to securing your information, you can rest easy knowing that your information remains within your organization.

### FIPS

The Federal Information Processing Standard (FIPS) is awarded under the National Institute of Standards and Technology's cryptographic Module Validation Program. The Blue Ridge Networks BorderGuard secure communications platform earned both FIPS 140-1 Level 2 and FIPS 140-2 Level 2 validations.



### DoD SPOCK

Blue Ridge Networks earned three Security Proof of Concept Keystone (SPOCK) program validations since 1995. SPOCK is a joint government-industry consortium sponsored by the Department of Defense to demonstrate security features of commercial and government products that can support high assurance security architectures.



### Common Criteria

Common Criteria is an international standard agreed to by six major industrialized nations for verification of Security Protocols. Blue Ridge Networks earned the EAL Common Criteria Level 3 certification.



### HIPAA

Keeping personal medical information confidential is and will increasingly be important in the years to come. Blue Ridge Networks technology is compliant with the guidelines as set forth in the Health Insurance Portability and Accountability Act (HIPAA) of 1996.



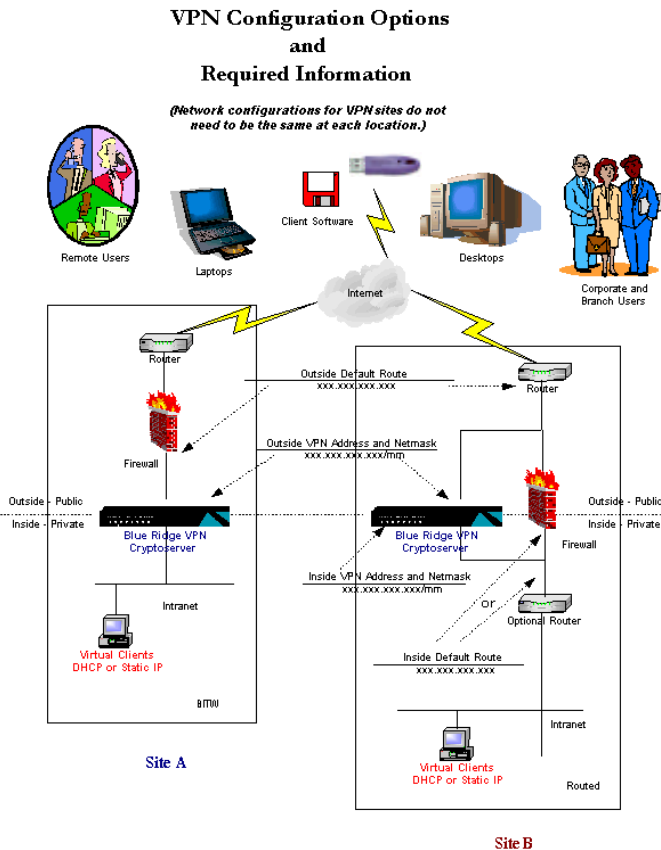
# Installation Planning

The Blue Ridge Networks VPN BorderGuards we provide for your configuration must fit into your network properly. To do this we need to gather information on your network structure.

The basic procedure is as follows:

- You'll plan the site configuration, including the number of sites to be connected and the estimated number of users at each site. That information is sent to Blue Ridge Networks.
- We'll configure the required number of BorderGuards, ready to drop into your networks, and deliver them to you.
- You'll physically cable them into the networks, and then notify us when you're finished.
- We'll begin the ongoing configuration and monitoring of the BorderGuards.

So, let's work through the details of what is needed to configure your Blue Ridge Networks VPN BorderGuards. Follow the examples in the figure below for a sample network setup for Site A and Site B.



## Physical Requirements

The BorderGuard is a small unit, about 12" x 16" x 2". It needs normal AC power, and has two RJ45 10/100/1000 and one 10/100 receptacles for connection to the inside and outside Ethernet ports, and other custom configurations.

It can be operated in any normal office or communications closet environment. It's power requirements (2 amps max) and heat dissipation are minimal. Rack mounting kits are included with each unit.

## Outside Network Requirements and Examples

The outside Ethernet has a few requirements that we'll need for successful operation. Follow the picture above for some samples of network placement.

- **Site A** places the Blue Ridge Networks VPN BorderGuard in line with and behind the firewall. In this configuration, the BorderGuard will pick up traffic from Site A destined to a resource on Site B. The BorderGuard will then start the secure tunnel to Site B, encrypt the packets, and then send them through this tunnel. The BorderGuard on Site B will decrypt the packets and forward them on to the proper destination within the intranet. No changes need to be made in the network infrastructure to support this, other than to configure the firewall to accept IP Protocol Type 50 or UDP Port 820 packets. Traffic not destined to a resource on Site B will be passed to the firewall for routing.
- **Site B** places the Blue Ridge Networks VPN BorderGuard in parallel to the firewall. In this configuration, the firewall and internal routers must have static routes added to them so they can direct traffic destined to the IP address ranges in Site A to their Site B BorderGuard for transport. All of the remote IP addresses in Site A need to be added to the policy of the Site B BorderGuard. In this way, such traffic is picked up by the Site B BorderGuard, encrypted, and sent via the secure tunnel to the Site A BorderGuard, where the packets will be decrypted. Traffic not routed to the Site B BorderGuard will be handled by the firewall and the policies it contains.
- Remote users can connect to the Blue Ridge Networks VPN BorderGuard in either configuration model via VPN Client software and a valid subscription to the Home Network.

## Full-time Internet Connection

Your site must be connected to the Internet through your ISP on a permanent, dedicated basis.

The type of connection to the ISP isn't important, so long as it is reliable and dedicated. Speeds of at least 56K bits per second are strongly recommended. And of course, the total bandwidth available to your remote access users can never be greater than the bandwidth to your ISP.

## External Fixed Public IP address for the BorderGuard

The BorderGuards each need a statically assigned IP address on your exterior LAN that is a "public" IP address directly accessible to anyone connected to the Internet. If your organization is using Network Address Translation (NAT), one public IP address must be statically mapped to the BorderGuard's assigned private inside IP address on your internal network if using IP Protocol 50. If your BorderGuard is encrypting via UDP Port 820, any combination of NAT and Port Address Translation (PAT) is supported. See Appendix A for more detailed information. Your subscribed users will be sending secure messages to this assigned public IP address.

Along with that address, we'll need the subnet mask for your exterior network and the gateway IP address of the router leading to the Internet.

The BorderGuards also support external DNS lookup of the public IP address for the device. If you advertise the DNS "name" for the BorderGuard on your external DNS server and the IP address changes, merely re-advertise the DNS name with the new IP address, and remote access users will be able to locate the device in the new location. This is especially useful for disaster recovery situations, or in changing ISP providers.

## 10/100/1000 connection

The BorderGuard uses auto-sensing 10/100/1000 connections and has standard RJ45 jacks for that purpose.

## Connectivity verification IP address

Part of our job at Blue Ridge Networks is to continuously monitor the state and availability of the BorderGuard, and to take action if it's out of service. Part of that action may be calling *you* to see if there's a local problem.

In most cases, a BorderGuard may be unavailable because you're having a basic network outage, scheduled maintenance, power outages, etc.

If we can't reach the BorderGuard, we'll ping the IP address you provided as the default gateway to see if we can reach it. If we can't ping it, we'll assume that your network is down. If we can ping it, we'll presume it's a BorderGuard problem and let you know if we need your input and assistance.

The best address for us to test ping for most customers is the inside IP address of your access router. You may also provide us with another IP address for our diagnostic purposes.

## Selecting the Inside (Home) Network

If your site is of even moderate size, you may have several independent LAN's on your campus or Intranet, connected by routers. Which of these several potential Home Networks should the BorderGuard be connected to?

The way to answer that question is to ask: if those same users showed up on site with their computers, Ethernet cables in hand, which LAN would you connect them to?

For many networks, it really doesn't matter all that much — your routers may permit full connectivity between all the LAN's at your site, and all services are available from all locations. In that case, it's probably best to pick a central network that is a short number of hops away from any potential destination.

Other organizations may have internal policy gateways or firewalls, for example a firewall between the rest of the company and the HR or financial departments. In that case, you'll have to connect the BorderGuard to the LAN that has the needed access for a desktop machine.

If you have different users who must be connected through to different LAN's to do their job, then you'll need separate BorderGuards for each class of user, and separate subscriptions that give them access to only the authorized BorderGuard.

## Requirements for the Home Network

Each Home Network has requirements of its own. Let's take a look at them.

### DHCP service

DHCP service is recommended if your connecting users use TCP/IP protocols for any purpose, such as email or Web browsing.

This **D**ynamic **H**ost **C**onfiguration **P**rotocol (DHCP) is a standard that permits non-server hosts attached to the network to get their key TCP/IP configuration on the fly — a unique IP address suitable for that network, a subnet mask, and an exterior gateway address. Other data can be provided via DHCP as well, such as Windows Internet Name Service (WINS) and Domain Name Service (DNS) information.

It's ideally suited for simple management of desktop hosts, and particularly for transient users such as VPN Clients. Since IP addresses are assigned dynamically, you don't need to administer and track a unique IP address for each of your potential users. You can just assign a pool of them on your DHCP server that will be issued as people connect, and that expire after a pre-determined length of time.

If you have a much larger group of remote VPN Client users than you have IP addresses to go around, you might change the "lease duration" for these addresses to several hours, rather than the common default of three days. See the FAQ on tuning DHCP later in this document.

If you're not running DHCP and aren't sure how to do it, please refer to the FAQ on this topic later in this manual.

We also support configurations where you cannot or do not wish to use DHCP. In that case, it will be the job of your Administrative Contact to provide us with a unique, fixed IP address pool on the Home Network to adequately cover the number of subscribed users.

Additionally, we can support a mix of DHCP and statically assigned IP addresses for VPN Clients on the Home Network. You just need to identify the choice in the box on the New User Enrollment form.

## BorderGuard Internal Static IP address

This is a fixed address, valid on the Home Network, which is assigned to the BorderGuard. Its normal use is to permit internal access by Blue Ridge Networks personnel to the BorderGuard via ping and SNMP, so that the unit can be verified as healthy by internal management software.

This internal address does not need to be reachable or valid on the Internet. Thus, there is no problem if your site uses proxy servers, network address translation (NAT), and the like to connect to the Internet.

## 10/100/1000 connection

Just as with the exterior network, an RJ45 jack is provided on the BorderGuard for connection to your auto-sensing 10/100/1000T hub.

## Estimated number of Blue Ridge Networks Remote Access VPN Users

We will use this information, along with the number of paid subscriptions, to determine the initial number of VPN BorderGuards to be installed on each Home Network. We're asking you to provide the number of subscribers, as opposed to the estimated number of concurrently connected users.

## Multiple BorderGuards

The Blue Ridge Networks VPN BorderGuard is engineered so that several of them may be connected in parallel for concurrent operation. There are three reasons to do this:

### Remote Access Redundancy

A second unit for remote access can be placed along with the first, and can automatically assume the primary BorderGuard's load should it fail. It is your organization's decision if you want this extra assurance of availability, and there is an additional charge for the extra BorderGuard.

If we detect a failure and can't resolve it with your help, we send you a pre-configured replacement unit via overnight delivery.

When considering the costs and benefits, you should bear in mind that if a single BorderGuard fails, your users would need new subscriptions to connect to its replacement unit. Blue Ridge Networks will automatically generate the new subscriptions. Installing them is a simple process, but it does require the user's attention and consent for the update. As the BorderGuard is a security device, we make sure that the user's computer will connect to only properly authorized BorderGuards — we authenticate the *site* to the *user's* computer, not just the more common act of authenticating the *user* to the *site*. This is the Blue Ridge Networks VPN bi-lateral authentication.

### Site-to-Site Redundancy

The BorderGuards support Virtual Router Redundancy Protocol (VRRP) to become "hot spares" with automatic failover capability. If different ISPs terminate in the same inside network, this failover capability will allow the network to continue with virtually no disruption in service if one of the ISP connection fails. Additionally, if a power failure or hardware failure causes loss of connectivity in one BorderGuard, VRRP will allow the immediate failover to the alternate BorderGuard.

To use VRRP at a site requires an additional BorderGuard, and all hosts on the internal network must be configured with a virtual IP as the default gateway for the segment.

## Added Capacity

We'll take your population of users and spread their work over multiple BorderGuards. We can support any number of active users with multiple BorderGuards. There is no direct charge for these added BorderGuards, but it is Blue Ridge Networks' decision to install an extra unit based on our monitoring of your user client activity and the level of service we've guaranteed to you.

These added BorderGuards will provide redundancy once installed. In order to get them, you need to enroll enough users to saturate your existing BorderGuards.

## Connection to alternate Home Networks

As mentioned previously, you may have several administratively different Home Networks to meet the needs of particular employees or users in your organization.

We consider each one of these dissimilar Home Networks to be a different "site." Each will have a different BorderGuard, and, if large enough, will have redundant BorderGuards for each Home Network. It's also possible to link up physically separate sites through BorderGuards, such as remote branch offices.

For each BorderGuard you require, each one will need:

- A distinct external IP address on the outside LAN.
- A distinct internal IP address on the Home Network. Redundant or added capacity BorderGuards are attached to the same Home Network; BorderGuards for alternate sites (Home Networks) are attached to the proper network.

## Sending In the Forms

All the information required to complete the forms has been covered. Follow the guidelines in the figure at the beginning of this chapter to determine the proper IP addresses required. Space is provided to specify two Blue Ridge Networks VPN BorderGuards for each internal network, if desired. A separate form should be used for each independent Access Point or site. Please completely fill in each form, as we require all the data that these forms request. Fax the completed forms to us at **1-703-631-9588**, or email to [support@blueridgenetworks.com](mailto:support@blueridgenetworks.com).

When we receive them, we'll configure the BorderGuards for your network environment, and ship them to the "shipping address" that you provide in the form. The next step is their physical installation at your site.

## BorderGuard Installation

Installation is a fairly simple process, since we have done all the preliminary work in setting up the configuration information on the unit. All you need to do is plug it in. Each unit that you receive will be configured with the access point (Home Network) name that you chose, and the IP addresses assigned to the units.

- Place the unit in its planned location and plug in the AC power. There is a rocker switch next to the power connector on the back of the unit that must be turned on.
- Connect the two Ethernet LAN's using 10/100/1000 cabling. Since the Ethernet interfaces look the same, you *can* inadvertently connect the two LAN's backwards on the unit (and it won't work that way), so take a careful look at the diagrams below to see which cable goes in which slot.

For the BorderGuard 5600 model shown below, the inside LAN connects through the EN01 port on the right of the group, and the outside LAN connects through the EN02 port in the middle. No connection is required in the EN03 port.



BorderGuard 4000 Model

Once it's installed, try to ping both the inside and outside IP addresses that you designated for the unit. It should respond. In addition, the unit responds to very basic SNMP requests, and can be reported as "alive" by your SNMP based network management system, if you have one.

After you get a response (or if it still doesn't seem to be working after you've rechecked the connections) call the Blue Ridge Networks Secure Operations Center at **1-703-631-0583** or **1-800-704-5234**. We'll contact the unit through secure management channels, and begin active monitoring of the unit's status. Your users may connect to the Home Network from that point on.

If you have received multiple BorderGuards, please install and verify connectivity to each of them before calling us.

## Custom Installations

Sometimes you may have a network configuration that isn't adaptable to the placement of the Blue Ridge Networks VPN BorderGuard as we've discussed it here.

The BorderGuards are versatile devices that can operate in many different environments. However, because networks and firewalls *are* so diverse these days, our network engineers will need to work with you to determine the best strategy for installing the BorderGuard, and possibly modifying the setup of your network.

Such installations are special services, and carry a time and materials consulting charge.

Please contact your sales representative to discuss Custom Installation if you have any of the following situations. We can usually get things running for you.

- Your Home Network is physically distant from the firewall network, so you can't cable any unit to both the Home Network and the DMZ network next to your ISP access router.
- The access router *is* your firewall. You use packet filtering in the router to prevent illicit traffic from entering your installation.
- You have a single-function Internet box that combines the ISP connection, firewall, and perhaps Mail and Web service in a single unit.

# BorderGuard Maintenance and Support

Maintenance and support are our job. However, there are a number of circumstances under which we'll have to get in contact with one another.

## Disconnecting the unit for network maintenance

Call or email our Secure Operations Center (1-800-704-5234, [support@blueridgenetworks.com](mailto:support@blueridgenetworks.com)) in advance if you know you need to disconnect the unit temporarily. That way, we'll realize why we can't reach the BorderGuard. Otherwise, we'll ping the designated IP address you gave to us to see if you're having a broad network outage. If we can reach that IP address but not the BorderGuard, we will call you as part of our standard service to let you know the unit's down and to help troubleshoot the problem if needed.

## Changing your network configuration

Networks change. Sometimes the IP addresses or subnet masks assigned to a network will change. Sometimes you will want to move a cluster of BorderGuards from one Home Network to another. There is a reconfiguration charge for these BorderGuards when this occurs.

To make the change, fill out a new Customer Site Survey form and fax it to Blue Ridge Networks Operations at **1-703-631-9588**. We will call you back at the contact number in your previous site survey to verify that you're the author of the form, and to discuss the configuration and timing of the change. Note that these changes may require that all users' subscriptions be updated. This update process can be done via email, if desired.

Depending on the nature of the change, we will either reconfigure the unit from our Secure Operations Center, or we will ship you replacement BorderGuards. The old BorderGuards must be returned after the changeover is complete.

## Expansion of Capacity

Blue Ridge Networks VPN monitors the utilization of your BorderGuards. Since we're providing a service (not a product), it's our job to provide more BorderGuards if the current ones are over-used.

We'll call you if we need to put more BorderGuards into the network, and ask you to add to the Customer Site Survey form with additional IP addresses for the new BorderGuard. Then, just as before, we'll ship the pre-configured unit to you for physical installation.

# A Quick User Troubleshooting Guide

Users should call us if they don't know how to proceed. But sometimes you may wish to say something more helpful than "Call these folks at..." if one of your people has a problem. Here's a quick guide:

**Is this the first time the user is connecting through Blue Ridge Networks VPN, or have they substantially reconfigured their system since the last time they connected?** If this is the case, definitely have them call us. We're up to speed on software installation and subscription initiation problems that you don't need to handle.

**Can they successfully connect to the Internet?** Ask them to do some Internet activity after they connect to their ISP — browse a Web site, ping a well-known host, etc. If they aren't getting connected to their Internet Service Provider at all, then this is a conventional problem that their ISP is equipped to solve. Do they have a domain listed in their dial-up networking logon (they should not)?

**Are they Blue Ridge Networks VPN connected?** Verify that the PC icon in the Windows system tray is green. If it is black, yellow, red, or doesn't appear, then they are not connected through Blue Ridge Networks VPN. If they haven't gotten that far, then possibly the user is having validation or authentication problems, or the BorderGuards are inaccessible from the user's location on the Internet.

- **Is their token validation successful?** Do they insert their Blue Ridge Networks VPN token device, enter their Pass Phrase, and does the status box proceed to say that they're attempting to connect to the BorderGuard? If not, they're having problems such as a bad token device or a forgotten Pass Phrase. Have them call us.
- **Is the BorderGuard reachable from the Internet?** You can try to ping the BorderGuard's outside address from your internal workstation, or ask the user to do it from their host.
- **Is the user behind a firewall?** Users may be connecting from behind other organizational firewalls that don't permit Blue Ridge Networks VPN traffic (or any VPN traffic) to flow out of that site, or allow the returning traffic to come back in. Although we can operate in many of these environments, some cooperation from the network administrator of the remote site may be required to make it work. Blue Ridge Networks VPN requires that IP protocol type 50 or UDP Port 820 packets be allowed in and out of the network.

A utility is included in the VPN Client installation to assist in troubleshooting end-user connections through personal firewalls. This utility allows the user to ping the public address of the BorderGuard using either IP50 or UDP820 protocol to verify connectivity between their PC and the BorderGuard. It is not ICMP ping, which may be blocked by the corporate firewall. Further instructions for using this **dpfping utility** are included in **Appendix B** of this document.

**The Blue Ridge Networks VPN connection seems fine, but the user can't reach the services needed.**

Possibly there is an internal problem in your networks.

- The user's computer has improperly configured IPX or NetBEUI bindings.
- A server is down or unreachable from the user's Home Network.

Determine if the user can reach *any* services that are known to be currently available on the Home Network. If their computer can find some services but not others using the *same* protocol (TCP/IP, SPX/IPX, and NetBEUI), then it sounds like an administration problem in your network. It's hard for our system to only let part of the traffic through.

If TCP/IP on the Home Network seems available to the user, but IPX or NetBEUI services are not, then the bindings in the user's networking Control Panel may be at fault. We have VPN Client Utilities to manage these bindings that are discussed in the VPN Client User Guide. This document may be downloaded from the Blue Ridge Networks VPN Web site at [www.blueridgenetworks.com](http://www.blueridgenetworks.com).

If none of these guidelines seem to resolve the issue, then give us a call at **1-703-631-0583** or **1-800-704-5234** — that's what we're here for.

# Frequently Asked Questions

## Installation Frequently Asked Questions

I don't use DHCP on my internal networks. How can I get it running?

To make DHCP available to your VPN Client users, you need two things:

- A block of IP addresses, valid on your internal network that can be dynamically assigned to new computers as they "arrive" on that network. These addresses cannot be statically assigned to other hosts at the same time. The block needs to be somewhat larger than the maximum number of concurrently connected Blue Ridge Networks VPN users you expect to have on that Home Network.
- "DHCP Server" software running on some server host on that network, or possibly on a nearby subnet.

DHCP Server capability is available for an increasingly wide variety of servers.

There is a simple solution if you have a reliable host running Windows NT Server somewhere on the Home Network. Windows Servers have the "DHCP Manager" service, which may be activated to serve that network. Install it as a TCP/IP Service on the Network Control Panel, and then invoke the DHCP Manager to assign it addresses to work with.

An increasing number of UNIX servers from IBM, SGI, HP, Sun Solaris, etc. have supported DHCP servers available with their operating systems.

For other server systems such as Linux, FreeBSD and SunOS, there are both commercially supported packages and reliable versions of DHCP freeware available, which can be installed on these machines. The "DHCP FAQ" Web site at <http://web.syr.edu/~jmwobus/comfaqs/dhcp.faq.html> has pointers to many of them, as well as a lot of useful information about using DHCP in various configurations.

Finally, many routers offer a "DHCP relay" service, which will allow a DHCP server on *another* network to receive DHCP address requests

Since DHCP does not distinguish between physically local clients and those coming in through Blue Ridge Networks VPN, it's easy to test your DHCP service in advance. Just configure a Windows host to "Obtain an IP address from the DHCP Server" in the TCP/IP Properties section of the Networking Control panel. Attach it to the Home Network, and see if it gets one of the addresses. You can verify this by seeing if it successfully uses TCP/IP services at that point.

How do I fine-tune DHCP for use with Blue Ridge Networks VPN?

With the factory settings provided by vendors such as Microsoft, the standard DHCP server is designed to assign addresses to desktop systems that are powered on and left running for long intervals.

Blue Ridge Networks VPN Clients are sometimes (but not always) more transient. If you have a larger pool of users than you have IP addresses for them, and they repeatedly log on and off, the normal DHCP server will "save" addresses for currently disconnected users and won't have any left for the new users.

This is managed through a DHCP variable called the “lease” time. When a DHCP client requester gets an address, it takes note of its lease time and must have its lease “renewed” with the server when that time expires. If it isn’t renewed (because the client isn’t there any more,) it goes back into the pool of available addresses. Setting this time down to about one hour will assure that a sufficient number are available.

Most DHCP servers have an alarm or event log that will let you know if they’re running out of IP addresses to assign. It’s a good idea to check this during periods of high activity.

The only place I can put the BorderGuard’s external port is behind the firewall. That’s because:

- The targeted Home Network is physically distant from my Internet access point.
- The access router *is* my firewall. My firewall is a packet filter installed in the router.
- There are political reasons why I can’t connect to that network.

We can work with many of these configurations as a Custom Installation. Please see the section on Custom Installations for more information.

## Operations Frequently Asked Questions

You’re monitoring the BorderGuards. Won’t that eat up bandwidth on the link to my ISP?

It’s really pretty slight. We send a message when people connect or disconnect, a flurry when we’re adding or removing subscriptions, plus a monitoring heartbeat that sends a message each way about every 15 seconds.

Can I monitor these BorderGuards through my network management system?

Yes. They will respond to pings, and they provide a really basic SNMP MIB that identifies the unit and says it’s alive. Since it’s a security device, we don’t disclose detailed information about its current state.

There’s a “console” port on the back of the BorderGuard. Can I log on?

No. It’s protected by a password that we don’t disclose. The security of the BorderGuard could be defeated if the console was accessible.

## Security Frequently Asked Questions

Isn’t this BorderGuard going around my firewall? Isn’t that a hazard to my site’s information?

We are connected to points both inside and outside the firewall, but no, it’s not a security risk. The entire purpose of the unit is to let your *authorized* users get to resources behind your firewall. We’ve gone to a great deal of effort to ensure that only cryptographically authenticated users and their traffic can introduce *anything* on your interior nets through the BorderGuard. We complement the services provided by your firewall. Remember, Blue Ridge Networks VPN customers include the United State Intelligence community.

You say that you use cryptography. Is it good stuff?

We think it’s the strongest that’s commercially available, and there are reasons we think so.

The simple answer is that the cryptographic system used in the PC software and the BorderGuard technology has over eleven years of history. Blue Ridge Networks first deployed our generation one BorderGuard in 1994. We are now deploying generation five, and developing generation six. During this

time, it has become the commercial package of choice for internal use within the Federal Intelligence Agencies.

A more detailed answer is that it's a system that requires two-factor authentication, has built-in PKI, uses RSA public keys, and employs the Diffie-Hellman automated key exchange to establish a session.

If you want more details, information and white papers are available under Support on the Blue Ridge Networks Web site, or just give us a call.

### Authenticated users can connect to resources on the Home Network. Can others connect to resources on the remote user's computer?

Yes, they can. As far as everyone's software is concerned, all currently connected Blue Ridge Networks VPN users are "on" the Home Network LAN. So if the remote user's PC has Print or File Sharing turned on, then others can use those resources if they have the correct passwords.

The user's machine could deliberately be a "server" and provide remote resources to others on the Home LAN, remote or not. The only exception is that IPX Servers can't be remote— this is because we filter out the *incredibly* prolific SAP advertisement messages that IPX servers send to one another.

If all of your users are employees or contractors of your organization, this is probably a good thing — they can share resources directly with one another. If you are using Blue Ridge Networks VPN to let in users from multiple other organizations, you need to let them be aware of the potential access to *each other's* computers while they are both connected.

If this access is not desirable, Blue Ridge Networks offers a separate integrated filter called Tunnel-Lock. The VPN Client with the Tunnel-Lock filter applied provides secure access to home network resources by blocking all unwanted traffic on the guest network (the network the user is connecting from, called the outer stack in the TCP/IP stack).

This implementation of the Tunnel-Lock on a Windows 2000 or Windows XP VPN Client permits full NetBIOS access. When connected to the home network, the VPN Client can participate in a Windows workgroup, NT domain, and can access network shares. More information on this filter can be found in the Blue Ridge Networks VPN Client Users Guide.

### One type of attack I've read about is that hackers can get into a user's PC while they're on the Internet, and then attack my site through the authenticated connection. Can you avoid this?

Yes, we can prevent this. If you set things up properly, all user traffic will flow to and from your Home Network, and the user's PC will ignore all significant traffic coming from outside.

For Windows 98 systems, all traffic of a basic protocol type (TCP/IP, for example) is "bound" to a specific interface. When the user is Blue Ridge Networks VPN connected, we bind traffic to the pseudo-interface leading to the Home Network. Incoming traffic over the "real" TCP/IP connection doesn't get very far, because no applications are set up to respond to it.

For Windows NT, XP, and Windows 2000 systems, it's more sophisticated networking software can concurrently accept traffic from multiple IP interfaces and direct them to applications. In other words, traffic to your Home Network is routed through the secure tunnel, but traffic going elsewhere can proceed over the "real" connection.

### Can people attack my network by hacking into the BorderGuard?

No, and we've had classified people give it a try. The BorderGuard runs an embedded control program that doesn't provide a set of backdoor services.

The only thing the BorderGuard will pay any attention to from the outside is:

- ICMP ping requests of up to 4K in size.

- SNMP gets for a really basic MIB.
- Our cryptographically, fully encapsulated wrapped packets using IP protocol type 50 or UDP Port 820.

Our remote management and monitoring of your BorderGuard uses the same cryptographic tunneling technology as your site. There is no known way for someone else to penetrate the unit from the Internet.

### Can Blue Ridge Networks Operations and employees get into my network?

Theoretically, we could do that. But think of us as you do your corporate Bank. Our reputation and business depends on groups like your company trusting us, and we have operational procedures in place to ensure that "extra" subscriptions don't get made, much like a bank makes sure that "extra" credit cards don't come into existence, and your money is safe.

Under normal operational conditions, your internal machines are not accessible from any Blue Ridge Networks computer system, in or out of its Secure Operations Center. If someone were to successfully physically attack Blue Ridge Networks Operations it still wouldn't give them access to your network.

## VPN Client Frequently Asked Questions

### Which operating systems does the VPN Client support?

The Blue Ridge Networks VPN Client may be installed on Windows ME, Windows 4.0 with Service Pack 4 or above, Windows 2000 with Service Pack 1 or above, and Windows XP. Microsoft TCP/IP is required for the VPN Client to work properly.

### Can I use my token on different operating systems?

The same token, either floppy-based or USB iKey, can be used on any Windows PC with the Blue Ridge Networks VPN Client software loaded.

### What are the types of access I may use to connect to my Home Network?

The VPN Client supports dial-up connections to an Internet Service Provider or an intranet Remote Access Server. The VPN Client may also be provided connectivity through a wireless, DSL, ISDN, cable/modem, or an Ethernet connection on a Guest network. The VPN Client will also work behind Network Address Translation (NAT), Proxy, and Port Address Translation (PAT) devices.

### What is the difference between a token and a subscription?

A token is a specially prepared disk or iKey that contains the VPN Client subscription and security authorization required for access to the Home Network. The disk is copy protected to prevent replication of the token, and the iKey is generated with code unique to Blue Ridge Networks. A subscription contains encrypted VPN Client and BorderGuard information, which allows the user to be authenticated to the Home Network. The user must be in possession of both the authentication token or iKey device and the subscription information, including the password, to connect to the Home Network.

### What happens when I transfer my token to the hard drive? Can I transfer it back?

The token transfer utility moves the token from the floppy disk to the hard drive, and is part of the Utilities accessed from the Remote Client window. In Windows NT, 2000, and XP, the token is placed in the user's profile directory. In Windows 98, the token is placed in the VPN Client directory. Simply run the token transfer utility again to move the token back to the original floppy disk. The original token disk is required if the user wishes to transfer the token back from the hard drive. The subscription cannot be moved from the USB iKey device.

### What happens if I lose my token?

If a user loses either the floppy-based token or the USB iKey, you need to contact Blue Ridge Networks to request a replacement.

#### What do I do if I forget my password?

If a user forgets the password, contact Blue Ridge Networks. We have a record of the original password at the time of issue, and can remind the user after verifying his/her identity. If the user changed the password from the original assignment, we can email the user a new subscription with a new password.

#### How do I update my subscription if I am sent a new one?

Users must update their subscription if they receive a new one from Blue Ridge Networks. The updated subscription may be sent on a floppy disk, via e-mail, or accessed through an FTP server, and does not require a new token or iKey. The subscription information filenames are "subsinfo.dat" and "contact.dat" and will require a password to access them. Click on the Utilities button on the VPN Client window, choose the Update Subscriptions button, and then follow the instructions on the screen. The original password will not change. For more detailed information, refer to the Blue Ridge Networks VPN Client User Guide, available from the Blue Ridge Networks' web site at [www.blueridgenetworks.com](http://www.blueridgenetworks.com).

#### Can multiple users share the same workstation?

As long as the user does not transfer the token to the hard drive, any number of users can access the VPN Client software on a workstation with their own unique token and password.

#### Where can I go for help on troubleshooting and status messages?

The Blue Ridge Networks VPN Client User Guide contains a comprehensive section on Client error and status messages. This Guide may be downloaded from the Blue Ridge Networks web site, under the Customer Support section at [www.blueridgenetworks.com](http://www.blueridgenetworks.com).

## Placing a Service Call

We're dedicated to providing our customers with a hassle free call experience. In order for us to quickly provide you with technical assistance, we ask that you have some basic information ready before placing a service call.

- Your Customer Name
- The name of the Home Network access point or site you designated in the Customer Site Survey.
- If a particular user is having a problem, we'll need the user's name as provided to us by your Administrative Contact. We may need to know how to contact that user if they are not at their normal location.
- A problem description.

We do not want placing a service call to be a difficult or time-consuming process. We'll assist you in getting the service you require.

Should the need arise, we have a managed escalation process to ensure that any problems are addressed at the proper technical level.

At Blue Ridge Networks VPN, our Customer Service Center staff stands ready to assist you. All you have to do is to get the above information ready, and call us at **1-703-631-0583** or **1-800-704-5234**, or email us at [support@blueridgenetworks.com](mailto:support@blueridgenetworks.com). We'll take it from there.



# Appendix A – Corporate Firewall Configurations

## IP Protocol 50 and UDP Port 820 Access

### Overview

The versions of Windows 2000 and Windows XP Blue Ridge Networks VPN Client software feature an additional encapsulation protocol. Consistent with a VPN industry direction, Blue Ridge Networks has adopted a UDP protocol for encapsulating encrypted VPN packets. This is a departure from past VPN Client versions that used IP-50 (IPSec ESP). There are several benefits from this change:

1. IP-50 uses a raw IP packet format with no upper layer ports in the header. This has created a fundamental incompatibility with the prevalent use of port mappers commonly found in broadband NAT firewalls. VPN Clients using the UDP encapsulation will work from behind network address translation perimeters.
2. Microsoft no longer supports the use of IP-50 on their Windows XP Operating System.
3. The use of an IPSec client from behind a firewall always required a change to the default firewall policy. Many firewall policies will permit the creation of a UDP session from the trusted side to the outside. This will be a major benefit to traveling VPN users in need of a secure connection to their home networks.

If firewall policies need adjustment to allow VPN connections with the UDP encapsulation technique, the same logic previously used with IP-50 is still applicable. All recent versions of the Blue Ridge Networks VPN Client will initiate connections to a BorderGuard fixed IP address and a UDP port address of 820. VPN Clients will use a randomly selected upper range UDP from port address. Firewalls that require explicit policy changes should pass packets to and from BorderGuard IP addresses using UDP port 820.

BorderGuards will continue to support IP-50 for older versions of the VPN Client and for management sleeves to the Blue Ridge Networks VPN Manager.

### UDP Port 820

The User Datagram Protocol (UDP) offers a minimal transport service - non-guaranteed datagram delivery - and gives applications direct access to the datagram service of the IP layer. UDP is used by applications that do not require the level of service of TCP, or that wish to use communications services (e.g., multicast or broadcast delivery) not available from TCP. UDP is almost a null protocol; the only services it provides over IP are checksumming of data and multiplexing by port number.

### Allowing UDP Port 820

Packets between the Blue Ridge Networks VPN Client and the BorderGuard on the Home Network may use UDP Port 820. This User Datagram Protocol (UDP) is defined to make available a datagram mode of packet-

switched computer communication in the environment of an interconnected set of computer networks. This protocol assumes that the Internet Protocol (IP) is used as the underlying protocol.

Any firewall or filtering device that exists between the VPN Client and BorderGuard must allow UDP Port 820 packets to pass.

Allow UDP 820 + <valid destination IP address>

A more comprehensive security policy would be to allow UDP packets to pass only when the destination IP address of an incoming packet is the home network BorderGuard (the source addresses for VPN Clients or mobile users will be indeterminate). This policy would maintain that only encrypted, authenticated packets be allowed through the firewall to the home network.

Firewalls or routers that do packet filtering on the corporate or home network will need to be examined or configured to permit these packets. Internet Service Providers will unlikely be filtering UDP Port 820 unless special arrangements have been previously made.

### Cisco Pix Sample Example for UDP Port 820

The following is an example of opening up UDP Port 820 on Cisco routers.

Existing access lists are updated to ensure compatibility:

!Existing configuration:

```
interface Serial0
ip access-group 110 in
ip access-group 111 out
```

!

!Access lists 110 and 111 are updated to add the following:

!

```
access-list 110 permit udp any {CS IP address} eq 17
access-list 110 permit udp any eq 820 any eq 820
```

!

```
access-list 111 permit udp any {CS IP address} eq 17
access-list 111 permit udp any eq 820 any eq 820
```

IP Protocol 50

### IPSec Technologies

IPSec combines several different security technologies into a complete system to provide confidentiality, integrity, and authenticity. In particular, IPSec uses:

- ✓ Diffie-Hellman key exchange for deriving key material between peers on a public network.
- ✓ Public key cryptography for signing the Diffie-Hellman exchanges to guarantee the identity of the two parties and avoid man-in-the-middle attacks.
- ✓ Bulk encryption algorithms, such as 3DES, for encrypting the data.
- ✓ Keyed hash algorithms, such as HMAC, combined with traditional hash algorithms such as MD5 or SHA for providing packet authentication.
- ✓ Digital certificates signed by a certificate authority to act as digital ID cards.

### Details of IPSec

IPSec combines the aforementioned security technologies into a complete system that provides confidentiality, integrity, and authenticity of IP datagrams. IPSec actually refers to several related protocols as defined in the RFC 2401-2411 and 2451 (the original IPSec RFCs 1825-1829 are now obsolete). These standards include:

- ✓ IP Security Protocol proper, which defines the information to add to an IP packet to enable confidentiality, integrity, and authenticity controls as well as defining how to encrypt the packet data.

- ✓ Internet Key Exchange, which negotiates the security association between two entities and exchanges key material. It is not necessary to use IKE, but manually configuring security associations is a difficult and manually intensive process. IKE should be used in most real-world applications to enable large-scale secure communications.

IKE uses UDP port 500 referred on the access-lists.

### Allowing IP protocol 50

Packets between the Blue Ridge Networks VPN Client and the BorderGuard on the Home Network may use IP protocol 50. (NOT Port 50.) This protocol type is reserved for encapsulated security payloads [RFC1827] and [RFC2406]. The IP Packet Protocol type field is the 10th octet in the header of an IP datagram. Any firewall or filtering device that exists between the VPN Client and BorderGuard must allow IP protocol 50 packets to pass.

Allow IP protocol 50 + <valid destination IP address>

A more comprehensive security policy would be to allow IP protocol 50 packets to pass only when the destination IP address of an incoming packet is the home network BorderGuard (the source addresses for VPN Clients or mobile users will be indeterminate). This policy would maintain that only encrypted, authenticated packets be allowed through the firewall to the home network.

Firewalls or routers that do packet filtering on the corporate or home network will need to be examined or configured to permit these packets. Internet Service Providers will unlikely be filtering IP Protocol 50 unless special arrangements have been previously made.

### Cisco Pix Sample Example for IP Protocol 50

The following information must be entered on the Cisco access-list to permit IPSec traffic through the router, according to Cisco. The following is an example of IPSec configuration where IKE will be used to establish the security associations.

Existing access lists are updated to ensure compatibility with IPSec:

! Existing configuration:

```
interface Serial0
ip access-group 110 in
ip access-group 111 out
```

!

! Access lists 110 and 111 are updated to add the following (to allow IPSec and IKE traffic):

!

```
access-list 110 permit 50 any any
access-list 110 permit 51 any any
access-list 110 permit udp any eq 500 any eq 500
```

!

```
access-list 111 permit 50 any any
access-list 111 permit 51 any any
access-list 111 permit udp any eq 500 any eq 500
```

### Netopia Firewall/Routers – R9100 v4.6 Example

The following describes how to allow IP Protocol Type 50 access through a Netopia unit and to map a static NAT to the Blue Ridge Networks VPN BorderGuard or to a Blue Ridge Networks VPN Client.

1. Reset the box to factory settings. (Under Utilities & Diagnostics, revert to factory defaults.)
2. Easy Setup
  - a. IP address (of public side)
  - b. Netmask
  - c. PPP over Ethernet? No

- d. Ethernet = private (inside) IP address
- 3. Reset the unit
- 4. System Configuration
  - a. Network Protocol Setup
    - i. IP Setup
      - 1. NAT
        - a. Add public range (Name, choose static)
        - b. Add map list
      - ii. Filter Set
        - 1. Display Change
          - a. Select Basic Firewall
            - i. Add Input
            - ii. Enable=yes
            - iii. Forward=yes
            - iv. Destination IP of BorderGuard and Netmask
            - v. Protocol=50
          - b. Add
        - 2. Move Input Filter
          - a. Select IP50 filter and move to top
        - 3. ESC out
    - ii. Wan
      - 1. EN
        - a. NAT Map List (choose name of map)
        - b. Filter set (basic Firewall with IP50 modification)
      - 2. ESC out
    - ii. Restart System

# Appendix B – DPFping Utility

## IP Protocol 50 and UDP Port 820 Ping

### Overview

DPFPing is a DOS-based utility created to verify IP Protocol 50 and UDP Port 820 access from any site to any BorderGuard. BorderGuards will respond with the message "DPF is alive" when pinged through this utility. A "network unreachable" message usually means that IP Protocol 50 or UDP Port 820 is blocked.

### Operation

DPFPing operates in two modes:

*dpfping <dest ip addr>* sends a packet with IP Protocol 50 to the destination IP which contains control information to have the packet echoed back to the originator, still as an IP Protocol 50 or UDP packet. Thus if a dpfping of this type fails, then some entity is blocking (at least) IP Protocol 50 or UDP traffic between the dpfping host and the BorderGuard; attempts to establish a cryptographic connection to the BorderGuard from this point will almost certainly not work. However, this does not tell you \*where\* in the path between host and BorderGuard the blockage is taking place. To do that, you can generally use dpfping in its second form:

*dpfping -t <dest ip addr>* operates in a manner similar to the better-known traceroute utility. It generates an IP packet whose protocol type is 50 or UDP port 820. It then sends the packet out with progressively greater Times to Live, expecting to receive an ICMP Response from progressively further intermediate routers until the dpfping IP50 or UDP 820 packet is returned by the BorderGuard. This gives either the full path to the BorderGuard, or will trace the path up to the point of blockage.

If the site's policy is to block ICMP Responses (Network unreachable, Time to Live Exceeded, etc.), then the trace form of dpfping will only give you the path as far as the firewall that blocks ICMP responses. If the firewall policy permits ICMP responses to flow, but blocks ICMP probes, then the trace form of dpfping will perform its intended function.

### Directions

The utility is loaded by default into the Blue Ridge Networks VPN Client directory at installation. It can be run from this directory, or copied into another directory as needed. Start a command prompt by clicking on Start → Run, then type *cmd* and click on OK. Change to the VPN Client directory, or the directory with the utility, which is called *dpfping.exe*. Type "dpfping" at the DOS command prompt to see a list of settable parameters. The UDP Port used by the BorderGuard is generally port 820.

Type dpfping at the system prompt of that directory to get a list of the following options:

```
C:\>dpfping
dpfping <destaddr> -rncqv -c <numpkts> -s <size> -w <secs> -m <maxttl> -t
<value> -u <udpport>
```

where:

```
destaddr <hostname|ip address> address of target to reach.
-r Do a traceroute until the destination is reached.
-n Report host addresses in numeric form.
-c <numpkts> Number of packets to probe.
-w <secs> Interval in seconds between packets.
-m <maxttl> Max value of TTL in probe packet.
-q Quiet. Just reports if destination reachable or not.
-s <size> Size of DPF Ping pkt in bytes (44 - 256).
-u <udp port> UDP port number.
-v Verbose output.
-t <value> IP Packet Type of Service, 0 - 255.
```

### IP Protocol 50 Ping

The results of a check for **IP Protocol 50 access** would be similar to these:

```
C:>dpfping 158.70.146.20 -r -n -v
DPF traceroute to 158.70.146.20 [158.70.146.20], 32 hops max, 0 byte
packets.
 1 65.202.129.129 36 bytes to 65.202.129.170 10 ms
 2 65.202.129.1 36 bytes to 65.202.129.170 30 ms
 3 137.39.5.158 36 bytes to 65.202.129.170 20 ms
 4 152.63.34.114 36 bytes to 65.202.129.170 20 ms
 5 152.63.33.73 36 bytes to 65.202.129.170 20 ms
 6 152.63.38.89 36 bytes to 65.202.129.170 20 ms
 7 152.63.38.121 36 bytes to 65.202.129.170 20 ms
 8 204.255.168.174 36 bytes to 65.202.129.170 20 ms
 9 4.24.10.25 36 bytes to 65.202.129.170 30 ms
10 4.24.10.29 36 bytes to 65.202.129.170 20 ms
11 4.24.4.214 36 bytes to 65.202.129.170 20 ms
12 4.0.2.138 36 bytes to 65.202.129.170 20 ms
13 4.1.9.234 36 bytes to 65.202.129.170 30 ms
14 158.72.173.5 52 bytes to 65.202.129.170 20 ms
15 158.72.175.2 36 bytes to 65.202.129.170 30 ms
16 158.72.176.2 36 bytes to 65.202.129.170 20 ms
17 158.74.200.1 36 bytes to 65.202.129.170 30 ms
18 158.70.215.20 36 bytes to 65.202.129.170 30 ms
19 158.70.146.20 [158.70.146.20] DPF is alive.
    DPF Address = 158.70.146.20
    Received TO = 158.70.146.20
    Received FROM = 65.202.129.170
1513 ms
```

### UDP Port 820 (or other UDP Port) Ping

To check on the status of a BorderGuard using **UDP Port 820**, results would look like this:

```
C:\>dpfping 158.70.146.20 -r -n -v -u820
DPF traceroute to 158.70.146.20 [158.70.146.20], 32 hops max, 0 byte
packets.
 1 65.202.129.129:820 36 bytes to 65.202.129.170 10 ms
```

## APPENDIX B - DPFPING UTILITY

```
2 65.202.129.1:820 36 bytes to 65.202.129.170 10 ms
3 137.39.5.158:820 36 bytes to 65.202.129.170 10 ms
4 152.63.34.114:820 36 bytes to 65.202.129.170 10 ms
5 152.63.33.73:820 36 bytes to 65.202.129.170 10 ms
6 152.63.38.89:820 36 bytes to 65.202.129.170 30 ms
7 152.63.38.121:820 36 bytes to 65.202.129.170 10 ms
8 204.255.168.174:820 36 bytes to 65.202.129.170 20 ms
9 4.24.10.25:820 36 bytes to 65.202.129.170 20 ms
10 4.24.10.29:820 36 bytes to 65.202.129.170 20 ms
11 4.24.4.214:820 36 bytes to 65.202.129.170 20 ms
12 4.0.2.138:820 36 bytes to 65.202.129.170 20 ms
13 4.1.9.234:820 36 bytes to 65.202.129.170 30 ms
14 158.72.173.5:820 60 bytes to 65.202.129.170 20 ms
15 158.72.175.2:820 36 bytes to 65.202.129.170 20 ms
16 158.72.176.2:820 36 bytes to 65.202.129.170 20 ms
17 158.74.200.1:820 36 bytes to 65.202.129.170 20 ms
18 158.70.215.20:820 36 bytes to 65.202.129.170 20 ms
19 158.70.146.20:820 [158.70.146.20]:820 UDP-DPF is alive.
    DPF Address = 158.70.146.20
    Received TO = 158.70.146.20
    Received FROM = 65.202.129.170
    1512 ms
```