Shiva®

LanRover VPN Gateway Site Planning Guide

900-0834-00
Revision A1
June 1998

Software Licensing

Shiva Corporation Software License Agreement

If you do not agree to the terms and conditions of this license agreement, return the product, together with your receipt, to your dealer within 10 days and your money will be refunded. All returned software must be unused and in its protective packaging.

By purchasing a Shiva remote access server, you have been granted a limited, non-exclusive license to use the Software and Documentation on the terms set forth in this License Agreement. Shiva Corporation or its Suppliers ("Shiva") retains ownership of these copies of the Software and Documentation. These copies of the Software and Documentation are licensed to you according to the following terms:

You may:

- Use the Software with any appropriate Shiva product.
- Make a copy of the Software on another diskette for back-up purposes only.
- Transfer the Software to another party, if the other party agrees to the terms and conditions of this License Agreement and completes and returns a Registration Card to Shiva. If you transfer the Software to any other party, you must transfer all copies and the Documentation to such party.

The license of the Software and Documentation is limited.

You may not:

- Make copies of any of the Documentation or of the Software except as expressly set forth above.
- Alter, modify, or adapt the Software or Documentation, including translating, decompiling, disassembling, creating derivative works, or merging the Software with other software.
- Rent, sublicense, assign, or otherwise transfer any interest in any of the Software or Documentation except as set forth above.
- Modify or erase any copyright, trademark, or property rights notice on any medium containing the Software or Documentation or copy or reproduce any of the Software or Documentation with all of Shiva's copyright, trademark, or property rights notices.

The License is effective until terminated. You may terminate it at any time by destroying all copies of the Software you have and mailing your original Software diskette(s) and the Documentation to Shiva. The License and your right to use the Software will automatically terminate upon your failure to comply with any provision of this License Agreement. You agree upon such termination to destroy all copies of the Software you have and to mail your original Software diskette(s) and the Documentation to Shiva.

Shiva retains all right, title, and interest in the Software and Documentation except for the limited license contained herein. The Software and Documentation are protected by the copyright laws of the United States. There are severe penalties, civil and criminal, for copyright infringement. Nothing in this License Agreement constitutes a waiver of Shiva’s rights under the copyright laws of the United States or any other law.

Media and Documentation Warranty

Shiva Corporation Limited Warranty On Media And Documentation

Shiva Corporation (“Shiva”) warrants the media on which the Software is distributed and the Documentation against defects in materials and workmanship for a period of 90 days from the date of original retail purchase. During the warranty period, Shiva will replace defective media or documentation at no additional cost, provided you return it during the warranty period, transportation charges prepaid, to Shiva. You must attach your name, address and telephone number, a description of the problem(s), and a dated proof-of-purchase for warranty service.

This warranty is limited to the original purchaser of the product and is not transferable unless otherwise agreed by Shiva in writing. This warranty does not apply if the product: has been damaged by accident, abuse, misuse or misapplication; has been modified without written permission by Shiva; or if any Shiva serial number has been removed or defaced.

UNDER NO CIRCUMSTANCES SHALL SHIVA’S LIABILITY ARISING OUT OF OR IN CONNECTION WITH THE PRODUCT OR THE USE OF, OR INABILITY TO USE, THE PRODUCT IN TORT (INCLUDING NEGLIGENCE), OR OTHERWISE, EXCEED THE PURCHASE PRICE OF THE PRODUCT. EXCEPT AS SET FORTH ABOVE, SHIVA MAKES NO WARRANTIES OR REPRESENTATIONS, EITHER EXPRESSED OR IMPLIED, WITH RESPECT TO THE PRODUCT, ITS QUALITY, PERFORMANCE, MERCHANTABILITY, OR FITNESS IN FOR A PARTICULAR PURPOSE.

ANY IMPLIED WARRANTIES ARE LIMITED IN DURATION TO ONE YEAR FROM THE DATE OF ORIGINAL PURCHASE OF THE PRODUCT.

THIS WARRANTY AND REMEDIES SET FORTH ABOVE ARE EXCLUSIVE AND IN LIEU OF ALL OTHERS, ORAL OR WRITTEN, EXPRESSED OR IMPLIED. No Shiva dealer, agent, or employee is authorized to make any modification, extension, or addition to this warranty.

SHIVA IS NOT RESPONSIBLE FOR SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES RESULTING FROM ANY BREACH OF WARRANTY, OR UNDER ANY LEGAL THEORY, INCLUDING LOST PROFITS, DOWNTIME, GOODWILL, DAMAGE TO OR REPLACEMENT OF EQUIPMENT OR PROPERTY, OR ANY COST OF RECOVERING, REPROGRAMMING, OR REPRODUCING ANY PROGRAM OR DATA STORED IN OR USED WITH SHIVA PRODUCTS.

Some states do not allow the exclusion of implied warranties or liability for incidental or consequential damages, so the above limitation or exclusion may not apply to you. This warranty gives you specific legal rights, and you may also have other rights which vary from state to state.

Proprietary and Trademark Information

This information is supplied without representation or warranty of any kind. Shiva Corporation assumes no responsibility and shall have no liability of any kind arising from supply or use of this publication or any material contained herein.

The information contained herein is proprietary to Shiva Corporation and/or its vendors, and its use or disclosure is subject to the restrictions stated in the standard Shiva Corporation license terms and conditions or the appropriate third-party sublicense agreement.

Mention of third-party products is for informational purposes only and constitutes neither an endorsement nor a recommendation. Shiva Corporation assumes no responsibility with regard to the performance of these products.

Shiva, *Shiva with design* (the Company logo), LanRover, LanRover Access Switch, LanRover/T PLUS, LanRover/PLUS, LanRover/E PLUS, NetModem, NetModem/E, AirSoft, EtherGate, Hublet, NetBridge, NetSerial, ShivaPPP, Telebridge, WebRover, and PowerBurst are registered trademarks of Shiva Corporation. CableRover, PowerSurf, PRIRover, Provision Plus, Shiva LanConnect, LanRover XP16, LanRover D56, ShivaPPP Intranet, Smart Detect, Tariff Management, ShivaRemote, ShivaPort, DIAT, ISSAK, Remote-Centric, Shiva Access Viewer, Shiva AccessPort, Shiva AccessPort Monitor, Shiva Dial-In SDK, ShivOS, Shiva Net Manager, Shiva Net Manager for UNIX, VantagePath Access Concentrator, and Access by Shiva are trademarks of Shiva Corporation.

Apple, AppleTalk, and Macintosh are registered trademarks of Apple Computer, Inc. Apple Remote Access is a trademark of Apple Computer, Inc. Microsoft, Windows, and MS-DOS are registered trademarks of Microsoft Corporation. NetWare and UNIX are registered trademarks of Novell Inc. Hayes is a registered trademark of Hayes Microcomputer Products, Inc. Ethernet is a trademark of Xerox Corporation. Token Ring is a registered trademark of International Business Machines Corporation.

Shiva Corporation
28 Crosby Drive
Bedford, Massachusetts 01730

Shiva Support Services

Overview

The following section lists all of the support services currently available from Shiva, and is intended for network administrators or remote users. The details of all available support options are explained, including a limited time, free support feature, and extended service contracts.

Reference Information

The following topics are described in this Support information:

- ShivaTechnical Support
- Finding Shiva’s Latest Technical Information
- Shiva Support Services (North America)
- Support Services (International)
- Information We Require From You

Shiva Technical Support

Shiva’s goal is to ensure that all customers are successful installing and using their Shiva remote access solution. Your purchase entitles you access to technical information through Shiva’s electronic services

Shiva works closely with its Premium VARs, system integrators, and OEM partners to provide customers with a wide variety of support options. Shiva offers the following fee-based services:

- “Shiva Response” telephone support, technology protection, on-site, and consulting services
- Technical training courses

If you did not purchase a service contract with your Shiva remote access solutions, you will need to determine how you will support your Shiva remote access solution on an ongoing basis. This involves deciding which people in your organization need to be trained to install and maintain your solution. It also means that you need to select the company you will contact when you have a problem that your staff cannot resolve.

The best approach is to enter into a support contract for the services you want to have available. Technical support for Shiva products is available from a wide selection of reseller partners worldwide. Shiva also offers a variety of cost effective technical support solutions, including service contracts and “per incident” telephone support. Background information on Shiva’s support services follows.

Finding Shiva’s Latest Technical Information

Check the following online services for the latest technical information, frequently-asked questions, and file updates.

Shiva FAX-on-Demand Server *	800-370-6917 781-687-1900
Shiva World Wide Web Server	www.Shiva.com
Shiva FTP Server	ftp.Shiva.com

* File updates not available on this service.

Shiva Support Services (North America)

End Users experiencing problems dialing in to or out of a Shiva product should contact their system administrator or internal help desk.

System Administrators experiencing problems with the installation or operation of their Shiva product should contact their service provider (as described above).

For the name of your nearest Shiva service provider or information about Shiva’s fee-based technical support offerings (see below), contact Shiva pre-sales at 1-800-97-Shiva.

Service Options: Shiva encourages customers to set up a support relationship with a Premium VAR, Shiva, or other service provider before a problem occurs. Serviced available from Shiva are listed in the table that follows.

Shiva Response Information	Technical telephone support, software upgrade, and hardware maintenance contracts. Call 1-800-97-Shiva. (1-800-977-4482)
Shiva on Demand	Telephone support available on a “per-incident” basis. All major credit cards accepted. Call 1-800-522-0824.
Shiva Technical Training	Shiva Remote Access; Shiva Professional. Call 781-687-1810 for more information.

Shiva Support Services (International)

End Users experiencing problems dialing into or out of a Shiva product should contact their system administrator or internal help desk.

System Administrators experiencing problems with the installation or operation of their Shiva product should contact their service provider.

For the name of your nearest Shiva service provider or for information about Shiva's technical support offerings, contact Shiva in the United Kingdom at 01-73-477-1055.

Service Options: Shiva encourages customers to set up a support relationship with a Premium VAR, Shiva, or other service provider before a problem occurs.

Information We Require From You

Include the following information when leaving electronic mail or placing a phone call for support.

General	*Product Serial Number. *Shiva Model Name/Type.
Hardware Information	*Type of Computer (exact make, model, and operating system). Network Cabling (Ethernet 10Base-5, 10Base-2, 10Base-T; Token Ring 4 Mbit, 16 Mbit; LocalTalk). *Modem Specifics (exact make, model, and baud rate). If using a LanRover , include both remote modem and modem attached to the LanRover.

Software Information	*Shiva remote access server image/ firmware version (launch Shiva Net Manager, select the remote access server in the Device list, then choose Get Info from the Info menu). *Dial-In Version PC Users: Launch ShivaRemote Connect and choose About from the Help menu. Macintosh Users: Report the version of ARA (LanRover/Shiva remote access server 3.5 or higher users only) or the Shiva Dial-In you are using. *Dial-Out Version PC Users: Check version of ShivaCOM.DRV under Windows or ShivaCOM.EXE under DOS. Macintosh Users: Check version of the Shiva Config control panel.
Related Software and Versions	When contacting Shiva please provide a detailed description of your support request.

* Items that are required to answer most support requests on first contact.

Contents

Planning Information

Network Topology

Your Network Infrastructure

Planning Information

Planning Information

The Site Planning topics below prepare you to install the LanRover VPN Gateway. Depending on your organizations networking needs and the applications you will run using the LanRover VPN Gateway, you will also have to provide specific information regarding your own existing corporate network. You will have to make the following planning decisions regarding the following:

- Determine a VPN Solution
- Determine a Service Provider
- Determine a Level of Security
- Determine Port Numbers
- Determine Data Rates
- Determine User Classifications
- Determine Geographic Regions

Determine a VPN Solution

There are two basic VPN architectural choices:

- Service provider independent
- Service provider dependent

The starting point of the VPN tunnel is what differentiates the two. In determining which Internet Service Provider (ISP) solution to use, you must compare both VPN solutions and weigh the advantages to your organization.

Service Provider Independent

With a service provider independent architecture, a VPN-enabled client creates a tunnel through the public network to a corporate network. To accomplish this, the client establishes a PPP connection to a local Internet Service Provider (ISP) for Internet access. The client then establishes a session through the Internet to the corporate network. The client then creates a tunnel to carry data.

The advantage of this architecture is that it can use any Point-of-Presence (POP) in the world that has Internet access. Each client on this connection must be VPN-enabled, which could prove to be costly for a large number of remote clients.

Service Provider Dependent

With a service provider dependent architecture, the corporation purchases access from a single ISP. The user dials into the local POP with a PPP client, and the tunnel is established at the POP. The client can use any PPP client, such as Microsoft's Dial-up Networking. This solution is limited by the number of VPN-enabled POPs.

Because the VPN encryption does not occur until the data reaches the POP, the data stream between the remote PC and the POP is unprotected. This solution may not be practical where sensitive data is critical.

Determine a Service Provider

For a VPN connection, the biggest VPN benefit can also be the most problematic, if the ISP you select is not carefully researched. Selection of an ISP should be a number one priority when using a LanRover VPN Gateway solution. A proven ISP will assist, support, and in most cases, actually include the setup of the connection as part of their services. This should reduce the hourly cost of the setup for network administrators.

Think of the LanRover VPN Gateway as an internet service. It is only as fast as the slowest connection between the user and the server. Choose an ISP for its capacity and ability to support the number of users to which your organization expects to need connections. It is important to evaluate the ISP based on your company's needs, and not some abstract criteria. If it is critical that users access the corporate network, then an ISP with a low user to dial-up line ratio should be chosen. An ISP whose has a primary business focus would have its peak times from 8 a.m. to 5 p.m. weekdays, while an ISP specializing in home users would see peaks in the evening and weekends. Try to select an ISP that will match your organizations particular needs.

You should choose the same ISP for the corporate network and its satellites. If your international remote offices are out of your ISP's area, try to select an ISP with a large backbone (such as Sprint, GTE, etc.). This will reduce the network routing problems that affect the speed of the virtual network running between the sites.

If you have a large number of roving VPN clients, look for an ISP with a strong national (or international) presence and 800 dial-up access.

Determine the Level of Security

To determine the level of security to employ on your LanRover VPN Gateway solution, you must consider a number issues that affect security:

- Authentication — With the VPN LanRover Gateway, all traffic arrives from the public Internet, so it is vital to authenticate the connection when establishing the tunnel.
- Integrity — The data packets could have been altered as it passed through the uncontrolled Internet. Integrity checking ensures that the data comes from an authenticated source.
- Privacy — Determine whether your data must be confidential. Data packets travel through the uncontrolled, public network. You can ensure privacy by using encryption.

Security Levels

Network traffic is usually segmented into at least four groups. The following levels of security begins with the least level of security:

- Level 1 — Network applications that require no security, such as web surfing, do not need authentication or encryption.
- Level 2 — The application data is not private, but it must be protected against tampering during transmission. The data requires authentication but not encryption.
- Level 3 — This data requires privacy and integrity. Both authentication and a low-level encryption are needed.
- Level 4 — This data needs maximum privacy and requires authentication and a high-level encryption.

The users security level should be negotiated when establishing the VPN connection. Network administrators require the necessary tools to pre-assign security levels.

Determine the Number of Ports

To determine the number of ports, you must consider such factors as users and their work patterns. A fair estimate to employ is to use a ratio of one port or session to ten users. Deciding on a ratio of users to ports involves a trade-off between cost and service level:

- A high ratio increases the frequency of failed connection attempts.
- A low ratio may increase equipment costs.

Remote site bandwidth and user work patterns should also be considered since they can affect the quality of service.

Determine Data Rates

As with the weakest link in a chain, the smallest bandwidth in a data path sets the limit on the data rate for a session. With Shiva VPN, the connection consists of a data stream that passes through the shared network and arrives at a corporate site multiplexed with other sessions. The bandwidth taken up by the individual data streams may vary. The data streams are limited by the indeterminate paths taken through the Internet and make it difficult to predict the number of concurrent sessions that can be supported.

User Classification

To get maximum usage from a Shiva LanRover VPN Gateway, you should classify your users. You should consider your user's applications, habits, and geographic location when implementing a VPN solution.

Mobile Business Workers

These users are business travelers or sales people who need access to the corporate network while traveling. Because they need to communicate securely on the corporate network, they should use digital certificates for authentication.

Telecommuters

These users, who work from their home, often have an expensive higher bandwidth connection such as ISDN or a cablemodem. These users remain static and do not travel about as mobile business workers, but their data requirements are similar to mobile business workers. Because they need to communicate securely on the corporate network, they should use digital certificates for authentication.

Corporate Network Users

These users are located on a corporate LAN (either at the corporate site or branch offices). They need to share resources with the corporate network. The corporate site and branch offices can be linked over the Internet by using the LanRover VPN Gateway.

Determine Geographic Regions

When determining how to integrate Shiva VPN services, you must understand how the user locations affect costs. When using Shiva VPN, remote users dial into an ISP point of presence (POP) to establish a VPN connection.

The distance to the POP determines the per-minute rates that, when multiplied by the length of access time, determine the total cost.

Remote users of the Shiva VPN Desktop can reduce the costs of a connection because they dial into an ISP rather than directly dialing the destination phone number.

Network Topology

LanRover VPN Gateway Capabilities

You must consider the many functions of the LanRover VPN Gateway when determining how to incorporate it into your network. You must first consider the nature of the applications you use and the traffic you need to support using the LanRover VPN Gateway.

Remote Access Applications

Remote users using the Shiva VPN client can:

- Dial into any local point-of-presence
- Tunnel through the Internet
- Access the corporate network securely without incurring long distance charges associated with direct dialing.

For examples on how to implement the LanRover VPN Gateway for remote access applications, see the following scenarios:

Corporate to Internet (page 2-6)

De-militarized Zone (page 2-7)

Extranet Applications

Determine the level of security you need in running your company's extranet applications. Using the Shiva VPN product suite, you can authorize your business partner's access to information you specify on your network, while restricting their access to other data and applications.

For examples on how to implement the LanRover VPN Gateway for extranet applications, see the following scenarios:

Untrusted Network (page 2-3)

De-militarized Zone (page 2-7)

Additional Firewall and Tunnel Functionality (page 2-10)

Adding a LanRover VPN Gateway to an Existing Firewall Infrastructure (page 2-11)

Intranet Applications

Determine if you need the LanRover VPN Gateway for connecting remote locations. You can connect central sites with mobile users and branch offices over the Internet.

For examples on how to implement the LanRover VPN Gateway for intranet applications, see the following scenarios:

Trusted Network (page 2-4)

Corporate to Internet (page 2-6)

Firewall Applications

Determine if you will use the LanRover VPN Gateway to construct a firewall, replace your existing firewall, or keep your existing firewall.

For examples on how to implement the LanRover VPN Gateway for firewall applications, see the following scenarios:

Untrusted Network (page 2-3)

Corporate to Internet (page 2-6)

De-militarized Zone (page 2-7)

Behind an Existing Firewall (page 2-9)

Additional Firewall and Tunnel Functionality (page 2-10)

Adding a LanRover VPN Gateway to an Existing Firewall Infrastructure (page 2-11)

Internal Applications (page 2-13)

Internal Applications

Determine whether you need to use the LanRover VPN Gateway to handle applications across or within a LAN.

For an example on how to implement the LanRover VPN Gateway for internal applications, see the following scenario:

Internal Applications (page 2-13)

Untrusted Network

An untrusted network means that users on each LAN want their communications to be protected and authenticated but they do not want to grant unrestricted access to each other's networks. For example, Company A and Company B may be competitors that need to share certain information with each other (such as standards), but do not want to give each other access to any other information.

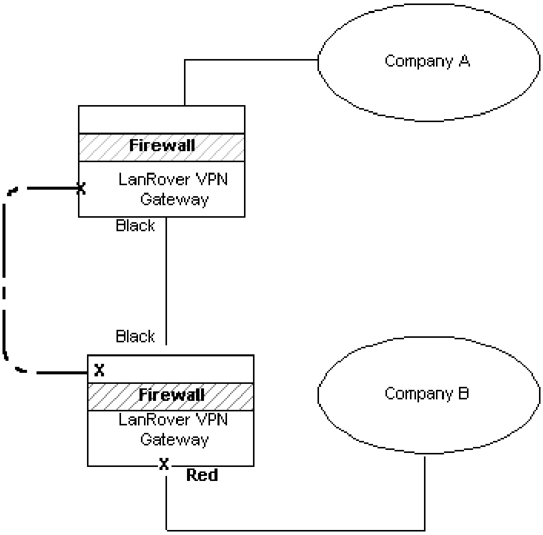

Figure: LAN-to-LAN Tunnel for an Untrusted Network

This scenario shows you a tunnel between Company A and Company B. Both companies have a LanRover VPN Gateway attached, with firewall functionality enabled on both ends.

The tunnel endpoints both terminate on the black (untrusted) side of the LanRover VPN Gateways. Therefore, traffic going from Company A to Company B must first exit Company A's firewall, then be permitted to go through Company B's firewall. Of course, traffic going from Company B to Company A must first be permitted to exit the Company B network and then be permitted to enter the Company A network.

Trusted Network

This scenario shows two networks from the same company — the Corporate Headquarters and a Branch office. The tunnel is configured red to red, making this network trusted. A trusted network means that users on each LAN can access all resources on the other LAN, or that both LANs assume that the other LAN is secure (no hackers can get in).

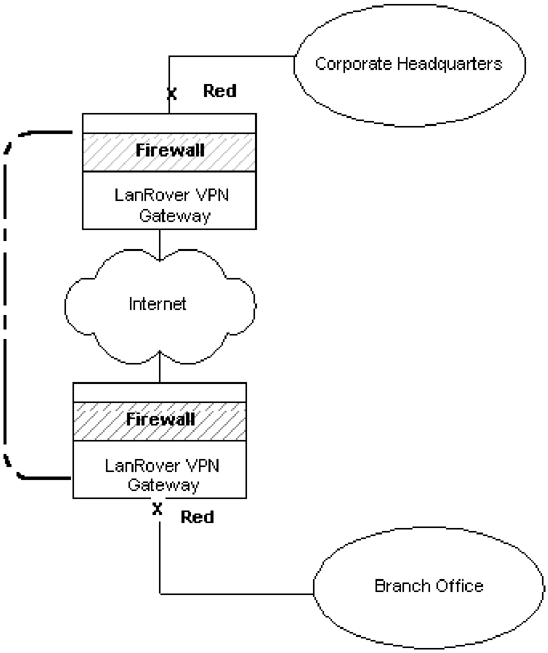

Figure: LAN-to-LAN Tunnel for a Trusted Network

The tunnel originates on the red side and terminates on the red side. Traffic coming from Corporate Headquarters goes through the encrypted VPN tunnel to get to the Branch Office, bypassing any firewall functions. Similarly, traffic originating from the Branch Office can get to Corporate Headquarters without going through the firewall.

Note that although there is no firewall functionality applied to the tunnel traffic, all traffic is still encrypted within the VPN tunnel. There is also still firewall capability against an Internet attack.

Corporate to Internet

In this scenario, there are two types of users that need to access the Corporate Network's Web or Email server: a regular Internet user, and a remote employee(s) running the Shiva VPN Client.

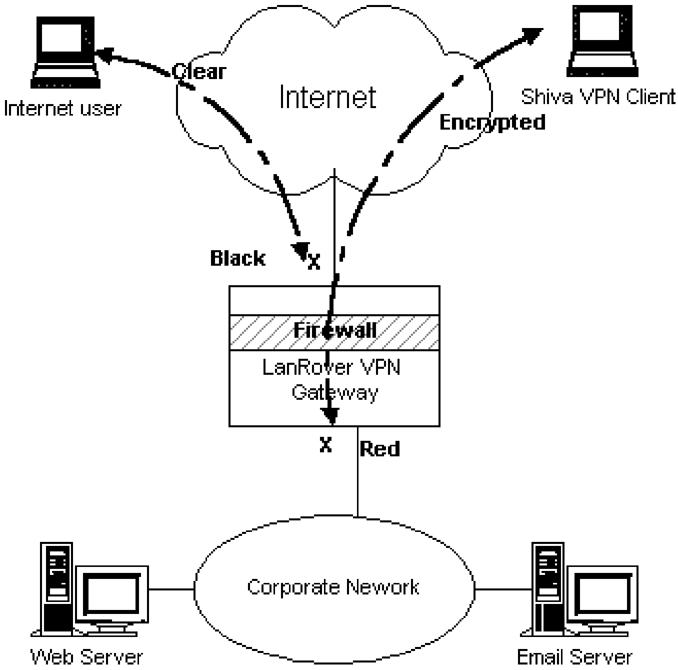

Figure: A Single User Tunnel to the Corporate Network

In the example above, the Internet user and the remote user running the Shiva VPN client pass through the Internet. The difference between the two is that the Internet user is usually restricted to a specific application (such as a Web server) or a specific machine. Any Internet user that wants to access the corporate network enters on the black side, and must go through the firewall.

The remote user using the Shiva VPN Client enters on the black side and has unrestricted access to the corporate network because that user's tunnel terminates on the red side.

A firewall rule with no (or some) restrictions is often set up so that everyone on the corporate network can get to the Internet.

De-militarized Zone

In this scenario, two LanRover VPN Gateways are set up between the corporate network and the Internet. The De-militarized zone is an intermediary zone from which certain services (such as Web or mail) are offered.

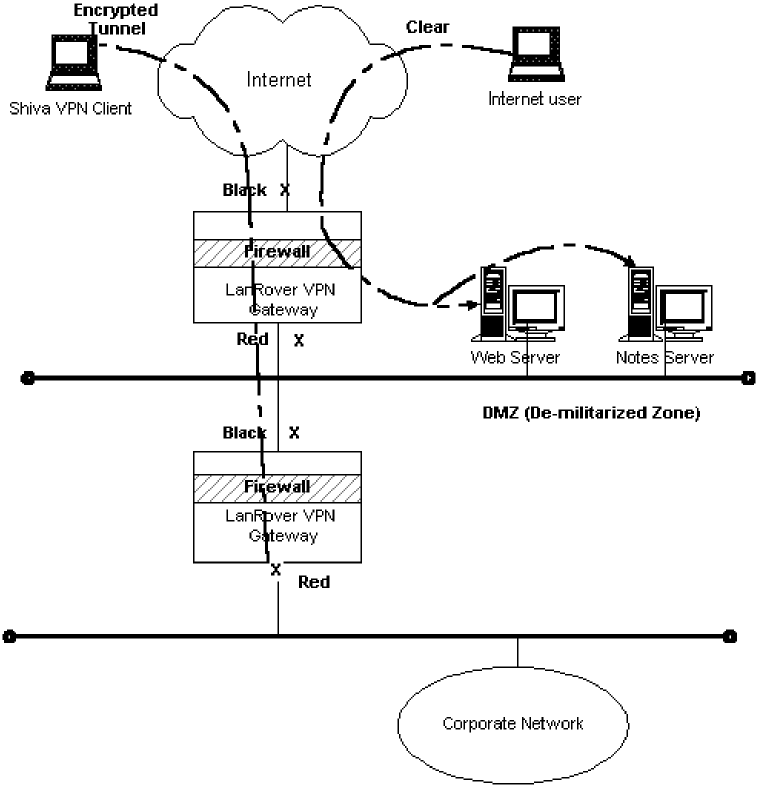

Figure: Secure Corporate Network and De-Militarized Zone

In this example, the LanRover VPN Gateway closest to the Internet, serves as a pure firewall that protects the DMZ from the Internet. The other LanRover VPN Gateway serves as a firewall (protecting the corporate network from the DMZ) and a VPN tunnel server for remote users running the Shiva VPN Client software.

This configuration protects the corporate network from a compromising an application running on a device on the DMZ. For example, if a hacker discovered a way to get into your Web server, the only devices the hacker can be access are those on the DMZ.

Shiva VPN Client users have granted controlled, authenticated access to the corporate network.

Behind an Existing Firewall

In this scenario, a corporation added a LanRover VPN Gateway behind an existing third party firewall because they are communicating with a customer/supplier through this firewall.

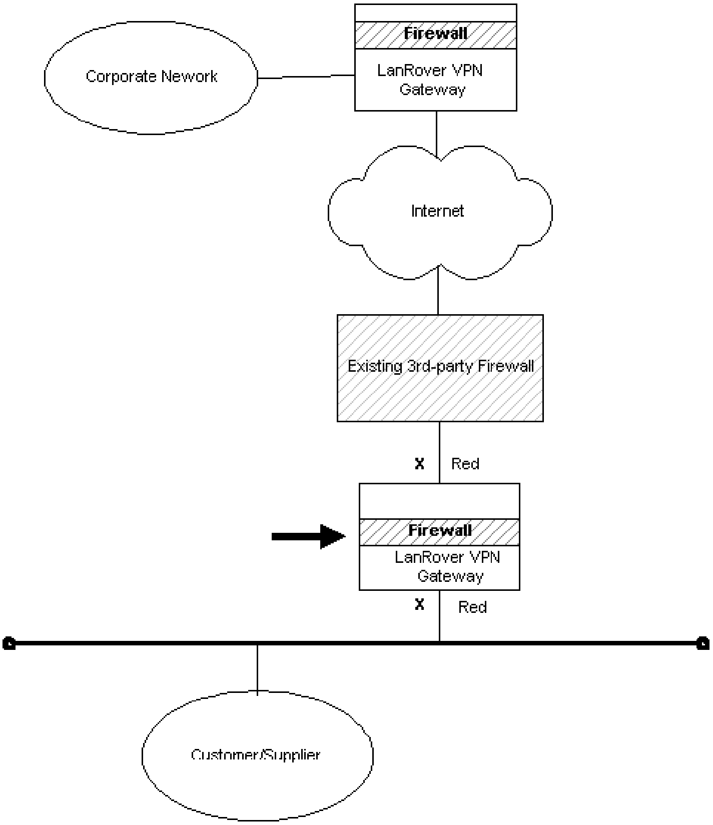

Figure: LanRover VPN Gateway and an Existing Third-party Firewall

Instead, they have set up a LanRover VPN Gateway to sit behind the existing third-party firewall. This LanRover VPN Gateway does not need any firewall functions enabled. It serves the tunnel traffic and transmits all traffic to the Customer/Supplier network through it.

An advantage to putting the LanRover VPN Gateway behind the third-party firewall is that there are no routing issues.

Additional Firewall and Tunnel Functionality

In this scenario, a corporation has added a LanRover VPN Gateway next to an existing third party firewall because they are communicating with a customer/supplier through this firewall.

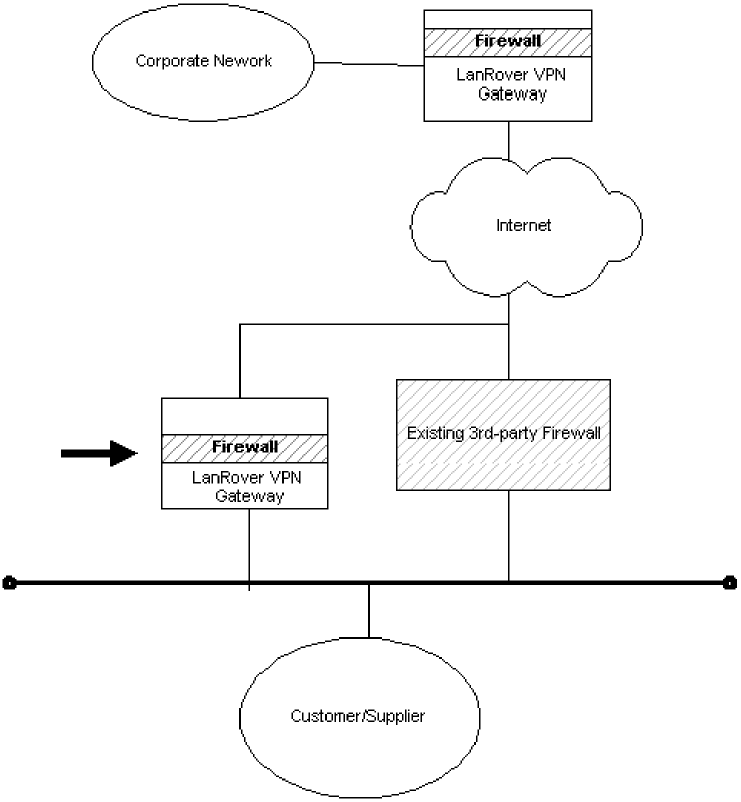

Figure: Two Firewalls and Two Paths out of the Network

This allows the customer/supplier to have two firewalls and two paths out of their network. The LanRover VPN Gateway only handles tunnel traffic between the customer/supplier network and the corporate network; it enables firewall functions and bypasses the existing third-party firewall. The existing third-party firewall is used for all other traffic.

Adding a LanRover VPN Gateway to an Existing Firewall Infrastructure

In this scenario, a corporation has decided to put a LanRover VPN Gateway in place, but they are communicating with a customer/ supplier that has a third-party firewall that they do not want to remove from their network.

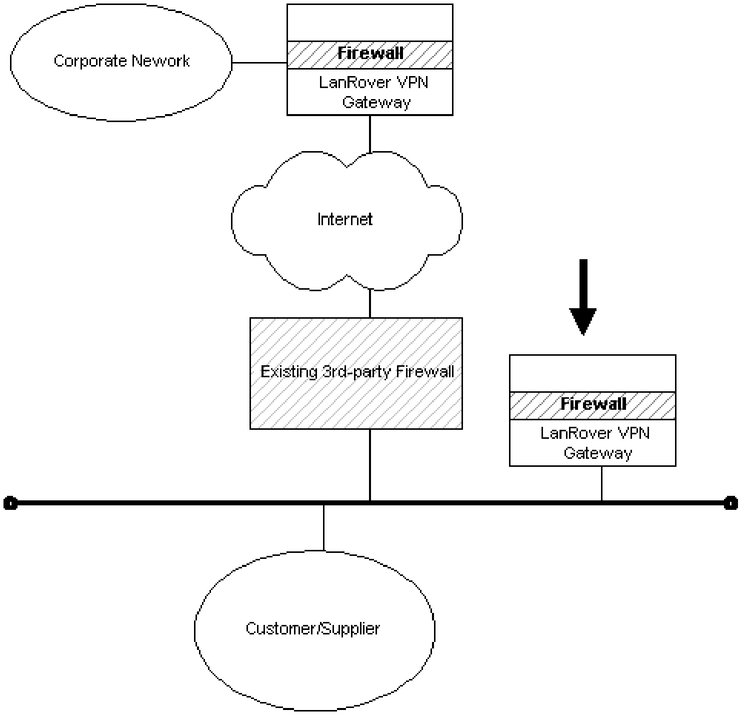

Figure: LAN-to-LAN Tunnel from Corporate to Customer/ Supplier

Instead, the LanRover VPN Gateway is placed on the customer/ supplier network to handle traffic from the corporate network. In this scenario, no firewall functions are enabled on the LanRover VPN Gateway; instead, the LanRover VPN Gateway handles encryption/ decryption of packets through the tunnel from the corporate network to the customer/supplier network.

Advantages to this setup are that it:

- Does not affect the customer/supplier’s existing infrastructure
- Is totally transparent to end users
- Is secure - there is only one path out of the network so all access control is in one place

Internal Applications

This scenario shows a LanRover VPN Gateway between the corporate network and a separate, secure network within the company. For example, the secure network may be for the Accounting department which accesses accounts payable, accounts receivable, and compensation information on the servers.

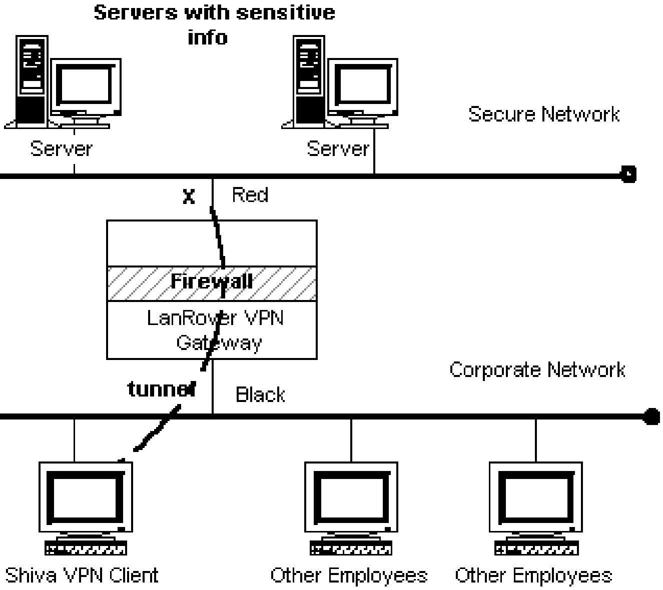

Figure: Secure Network within the Company

An Accounting department employee can access the servers on the secure network through the tunnel. Any other employee however, cannot.

This is a secure solution for internal applications. Even if the servers were set up only for access by Accounting employees, an employee with a Sniffer or network analyzer could still see the data if secure tunnels are not used. Using the Shiva VPN client ensures that the data is encrypted through the tunnel and is therefore secure.

Your Network Infrastructure

Your Network Infrastructure

To help you install the LanRover VPN Gateway, you need to complete the following checklists:

- The Router Checklists requires you to provide the router(s) manufacturer, model, and operating system. Also you need to specify each router's IP address and subnet mask.
- The Firewall Checklists help you to determine whether to implement the LanRover VPN Gateway as your firewall or keep your existing firewall. If you use your current one, you need to provide the firewall's manufacturer, type, and version. Also you need to specify the IP addresses and server information.
- The Internal Network Checklists helps you gather the IP information for your internal network. Also you need to identify the physical nature of your network. Specify the protocols that run on your network.
- The Authentication Checklists helps you to determine which method of authentication to use. If you are going to use the Certificate Authority, you will have to provide an IP address and a subnet mask.
- The Contact Information checklists are for the individuals who will be responsible for running the LanRover VPN Gateway product suite.
- The Port Combinations table dictates the ports you will use depending upon which protocols you support on your corporate network.

Router Checklists

The checklist tables below are intended to assist you with the installation of the LanRover VPN Gateway product suite into your existing network infrastructure. The checklists pertains to information about the external router that connects your network to the Internet.

- Router Classification
- IP Addresses and Subnet Masks
- Identify Your Router Information
- Filter Information

Router Classification

If you are using your own external router, specify the following information.

Router Manufacturer	Router Model	Operating System and Version Currently Used

IP Addresses and Subnet Masks for the LanRover VPN Gateway

Assign the IP addresses and subnet masks to the LanRover VPN Gateway you plan to use as a router. If you plan to use the LanRover VPN Gateway for a bridge, assign the same IP address and subnet mask to both interfaces.

Interface	IP Address	Subnet Mask
E0		
E1		

External Router Information

Specify your router's IP addresses and subnet masks.

Interface	IP Address	Subnet Mask
Internal		
External		
Additional Interface 1		
Additional Interface 2		

Filter Information

Determine if your existing router has filters. Do you plan to apply the filters to the incoming and outgoing traffic in the LanRover VPN Gateway?

Yes	No

Firewall Checklists

The checklist tables below are intended to assist you with the installation of the LanRover VPN Gateway product suite into your existing network infrastructure. These checklists prepare you to set up your corporate firewall.

Outbound Firewall Rules

Determine who and what applications need to go from the LanRover VPN Gateway to the Internet.

Who Can Go Out and What They Can Do?			
Users	**IP Address**	**Subnet Mask**	**Applications (FTP, HTTP, Telnet, POP, etc.)**

Where Can They Go?		
Users	**IP Address**	**Subnet Mask**

Firewall Rules:

- Determine who can go out (by their IP addresses and subnet masks).
- Determine what they can do. If they are unrestricted, they can do it all (http; ftp, etc.).
- Determine where they can go (by their IP addresses and subnet masks). If they are unrestricted, their IP address and subnet mask is 0.0.0.0.

Inbound Firewall Rules

Determine who and what applications may pass through the LanRover VPN Gateway from the Internet.

Who Can Come In and What They Can Do?			
Users	**IP Address**	**Subnet Mask**	**Applications (FTP, HTTP, Telnet, POP, etc.)**

Where Can They Go?		
Users	**IP Address**	**Subnet Mask**

Firewall Rules:

- Determine who can come in (by their user names or IP addresses and subnet masks).
- Determine what they can do (http; ftp, etc.).
- Determine where they can go (by their IP addresses and subnet masks).

Using An Existing Firewall

If you are using an existing firewall, specify information about it into the following table.

Firewall Manufacturer	Firewall Type	Firewall Version

Can your current firewall pass UDP traffic?

Yes	No

Firewall Interface Addresses

Specify the IP addresses of the interfaces on your existing firewall.

Interface	IP Address
Internal	
External	
Additional 1	
Additional 2	

Verify Adding a Rule

Depending on the location of your firewall on the corporate network, you must choose one of the following scenarios.

Scenario	Need Rules
Behind an Existing Firewall	yes
Additional Firewall and Tunnel Functionality	no
Adding A LanRover VPN Gateway to an Existing Firewall Infrastructure	yes

Internal Network Checklists

The checklist tables below are intended to assist you with the installation of the LanRover VPN Gateway product suite into your existing network infrastructure. These checklists pertain to how traffic is routed through your internal network.

Your Internal Default Router

Determine if your current network topology includes an internal default router. If yes, specify the IP address and subnet mask.

IP Address	Subnet Mask

Identify Your LAN

Determine the physical nature of your LAN, and the types of cables and connectors used on your network:

- 10BaseT/UTP
- 100BaseTX/UTP
- 10Base2/thick Ethernet (you need to buy a transceiver to interface correctly)
- 10Base5/thin Ethernet (you need to buy a transceiver to interface correctly)

The LanRover VPN Gateway includes two RJ-45 UTP female connections.

Internal Network IP Information

Specify the IP addresses and subnet masks of your internal network.

IP Addresses	**Subnet Masks**

Network Protocols

Specify the protocols you run on your network.

Protocols	**Yes**	**No**
TCP/IP		
IPX/SPX		
NETBUEI		
AppleTalk		
Other		

Authentication Checklists

The checklist tables below are intended to assist you with the installation of the LanRover VPN Gateway product suite into your existing network infrastructure. To set up authentication for the LanRover VPN Gateway, you need to complete the complete the following checklists:

- Authentication Type
- IP Address for Certificate Authority

Authentication Type

Determine which authentication methods to use. You may employ a combination of authentication applications for remote users and site-to-site connections. If you use a 3rd party authentication method, specify the version number.

Security Type	**Version**	Remote Users	**Site-to-Site**
Certificate Authority	NA		
Challenge Phrases	NA		
SecurID			
SAM			
RADIUS			
NT Domain			
Other 1			
Other 2			

IP Address for Certificate Authority

If you are using the Certificate Authority:

- Specify a name for the Certificate Authority. It can contain from 1 to 64 characters (no spaces). For example, AcmeCorp-CA.
- Assign an IP address for the Certificate Authority.

Certificate Authority Name	IP Address

Contact Information

For the successful installation and maintenance of the LanRover VPN Gateway Suite on your network, you should assign individuals from your organization to oversee the different aspects of the installation. Assign the following professionals who have the job-specific skills necessary to manage their part of the infrastructure.

- Gateway Contact
- MIS Contact
- Firewall Contact

Gateway Contact

The gateway contact, a person fully trained by Shiva to manage the LanRover VPN Gateway, monitors the VPN LanRover Gateway's syslog and overall functionality. This individual is responsible for resolving technical problems with the LanRover VPN Gateway. If unable to resolve a problem, the contact person should first call the ISP. If the problem cannot be corrected by the ISP, the contact person should then call Shiva Technical Support.

Gateway Contact Name	Phone Number	E-mail Address

MIS Contact

The MIS contact is a system administrator who is familiar with your corporate network layout.

Gateway Contact Name	Phone Number	E-mail Address

Firewall Contact

The firewall contact, an expert with firewalls and security servers, oversees the VPN Lanrover Gateway's firewall functionality. This person should know how to configure any existing firewalls on the corporate network.

Gateway Contact Name	Phone Number	E-mail Address

Port Combinations

The following protocol and port combinations must be opened through any firewall that is in front of a LanRover VPN Gateway.

Protocol	Destination Port	Source Port	Actions
UDP	In: 2233 Out: 2233	All All	These data packets are encrypted. They must be allowed through the firewall and should be directed to the encryptor and no other destination address.
UDP	In: 10025 Out: 10025	All All	These packets are encrypted management packets between the VPN manager and the LanRover VPN Gateway. You should not open this firewall rule unless the VPN Manager is running outside the firewall.
UDP	In: 10026 Out: 10026	All All	These are encrypted statistics packets bound for the Shiva VPN Manager. You should not open this firewall rule unless the VPN Manager is running outside the firewall.
UDP	In: 10027 Out: 10027	All All	These packets are certificate requests packets between the Certificate Authority (CA) server and a LanRover VPN Gateway or a Shiva client.

TCP	In: 10027 Out: 10027	All All	These packets are encrypted packet commands between the Certificate Authority server and Certificate Authority client. You should not open this firewall unless the CA client is running outside the firewall. Not recommended.
TCP	In: 10028	10028	These packets are encrypted broadcast data between from the Certificate Authority server and the Certificate Authority client. You should not open this firewall unless the CA client is running outside the firewall. Not recommended.

Before You Contact Technical Support

The list below describes what information you should have ready before calling Shiva Technical Support for your LanRover VPN Gateway. You should also have this information ready if a Shiva field engineer comes to your site.

IP Addresses and Subnet Masks

Make sure you have a detailed network diagram showing the subnets and their IP addresses on either side of the LanRover VPN Gateway including:

- Internet router
- Existing firewalls
- Internal router

Make sure that all IP addresses and subnet masks are clearly marked on the diagram.

Router Configuration

Specify the make and model of your existing routers and include the router configuration information detailing the following:

- Packet filtering rules
- Network address translation
- Routing protocols

Firewall Configuration

Specify the make, model, and version number of any existing firewalls and include the firewall configuration information detailing the existing set of:

- Packet filtering rules
- Proxies
- Network address translation

Default Gateway

Make sure you know the default gateway of the internal network.

Default Gateway Contacts

Have the contact names, phone numbers, and availability for your organization's in-house technical support personnel responsible for:

- System administration of the corporate network
- The existing corporate firewall and security
- The routers on either side of the LanRover VPN Gateway