VSU-2000
VPNware Service Unit

User Guide

VPNet®

VPNet Technologies, Inc.

Licenses, Warranties, Copyrights, and Trademarks

THE SPECIFICATIONS REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

Licenses

Software

VPNet Technologies, Inc. (“VPNet”) and its suppliers grant to Customer (“Customer”) a non-exclusive and non-transferable license to use VSU VPNos™ (“Software”) in object code form on a single VPNware VSU device owned or leased by Customer.

Customer may make one (1) archival copy of the Software provided Customer affixes to such all copyright, confidentiality and proprietary notices that appear on the original. EXCEPT AS EXPRESSLY AUTHORIZED ABOVE, CUSTOMER SHALL NOT: COPY, IN WHOLE OR IN PART, SOFTWARE OR DOCUMENTATION; MODIFY THE SOFTWARE; REVERSE COMPILE OR REVERSE ASSEMBLE ALL OR ANY PORTION OF THE SOFTWARE; OR RENT, LEASE, DISTRIBUTE, OR CREATE DERIVATIVE WORKS OF THE SOFTWARE.

Customer agrees that aspects of the licensed materials, including the specific design and structure of individual programs, constitute trade secrets and/or copyrighted material of VPNet. Customer agrees not to disclose, provide, or otherwise make available such trade secrets or copyrighted material in any form to any third party without the prior written consent of VPNet. Customer agrees to implement reasonable security measures to protect such trade secrets and copyrighted material. Title to Software and documentation shall remain solely with VPNet.

The license is effective until terminated. Customer may terminate this License at any time by destroying all copies of Software including any documentation. This License will terminate immediately without notice from VPNet if Customer must destroy all copies of Software.

Software, including technical data, is subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Customer agrees to comply strictly with all such regulations and acknowledges that it has the responsibility obtain licenses to export, re-export, or import Software.

This License shall be governed by and construed in accordance with the laws of the State of California, United States of America, as if performed wholly within the state and without giving effect to the principles of conflict of law. If any portion hereof is found to be void or unenforceable, the remaining provisions of this License shall remain in full force and effect. This license constitutes the entire License between the parties with respect to the use of the Software.

Restricted Rights – VPNet’s software is provided to non-DOD agencies with RESTRICTED RIGHTS and its supporting documentation is provided with LIMITED RIGHTS. Use, duplication, or disclosure by the Government is subject to the restrictions set forth in subparagraph ‘C’ of the Commercial Computer Software – Restricted Rights clause at FAR 52.227-19. In the vent the sale is to a DOD agency, the government’s rights in software, supporting documentation and technical data are governed by the restrictions in the Technical Data Commercial Items clause DFARS 252.227-7015 and DFARS 227.7202.

Limited Warranty

Hardware

VPNet Technologies, Inc. (“VPNet”) warrants that for a period of one (1) year from the date of shipment from VPNet that the Hardware will be free from defects in material and workmanship under normal use. This limited warranty extends only to Customer as the original purchaser. Customer’s exclusive remedy and the entire liability of VPNet and its suppliers under this limited warranty will be, at VPNet or its service center's option, repair or replacement within ten (10) business days or refund of the Hardware if returned to the party supplying the Hardware to Customer, freight and insurance prepaid. VPNet replacement parts used in Hardware repair may be new or equivalent to new.

Restrictions. This warranty does not apply if the product (a) has been altered, except by VPNet (b) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by VPNet, (c) has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident, or (d) is used in ultra hazardous activities.

DISCLAIMER OF WARRANTY. EXCEPT AS SPECIFIED IN THIS WARRANTY, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE EXTENT ALLOWED BY APPLICABLE LAW.

IN NO EVENT WILL VPNET OR ITS SUPPLIERS BE LIABLE FOR ANY LOST REVENUE, PROFIT, OR DATA, OR FOR SPECIAL INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY ARISING OUT OF THE USE OF OR INABILITY TO USE THE PRODUCT EVEN IF VPNET OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event shall VPNet's or its suppliers’ liability to Customer, whether in contract, tort (including negligence), or otherwise, exceed the price paid by Customer. The foregoing limitations shall apply even if the above-stated warranty fails of its essential purpose.

Software

VPNet warrants that for a period of ninety (90) days from the date of shipment from VPNet: (i) the media on which the Software is furnished will be free of defects in materials and workmanship under normal use; and (ii) the Software substantially conforms to its published specifications. Except for the foregoing, the Software is provided AS IS. This limited warranty extends only to Customer as the original licensee. Customer’s exclusive remedy and the entire liability of VPNet and its suppliers under this limited warranty will be, at VPNet or its service center’s option, repair, replacement, or refund of the Software if reported (or, upon request, returned) to the party supplying the Software to Customer. In no event does VPNet warrant that the Software is error free or that Customer will be able to operate the Software without problems or interruptions.

Restrictions. This warranty does not apply if the product (a) has been altered, except by VPNet, (b) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by VPNet, (c) has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident, or (d) is used in ultra hazardous activities.

DISCLAIMER OF WARRANTY. EXCEPT AS SPECIFIED IN THIS WARRANTY, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE, ARE HERBY EXCLUDED TO THE EXTENT ALLOWED BY APPLICABLE LAW.

IN NO EVENT WILL VPNET OR ITS SUPPLIES BE LIABLE FOR ANY LOST REVENUE, PROFIT, OR DATA, OR FOR SPECIAL INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGRADLESS OF THE THEORY OF

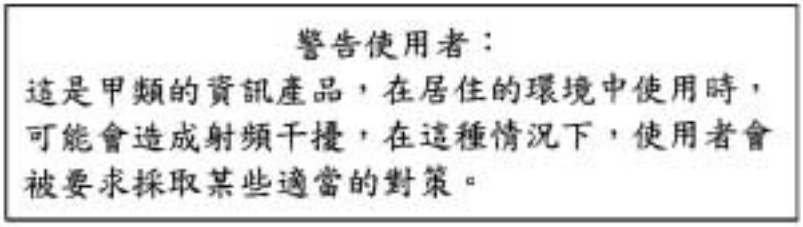
LIABILITY ARISING OUT OF THE USE OF OR INABILITY TO USE THE PRODUCT EVEN IF VPNET OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event shall VPNet's or its suppliers' liability to Customer, whether in contract, tort (including negligence), or otherwise, exceed the price paid by the Customer. The foregoing limitations shall apply even if the above-stated warranty fails of its essential purpose.

VPNware, VSU-1200, VSU-1100, VSU-1000, VSU-10, VPNmanager, VPNremote, VPLink, and VPNet are trade marks belonging to VPNet Technologies, Inc. MD5 Message Digest Algorithm Copyright RSA Security, Inc. All other product names mentioned in this manual are trademarks or registered trademarks of their respective manufacturers.

Compliance

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

BMSI (Chinese Warning Label)



Hardware, including technical data, is subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Customer agrees to comply strictly with all such regulations and acknowledges that it has the responsibility to obtain licenses to export, re-export, or import hardware.

Trademarks

VSU, VPNmanager, VPNremote, VPLink, VPNos, and VPNet are trademarks belonging to VPNet Technologies, Inc. MD5 Message Digest Algorithm copyright RSA Data Security, Inc. All other product names mentioned in this manual are trademarks or registered trademarks of their respective manufacturers.

Copyright

January 2001
P/N 09-0045-02

Table of Contents

Preface

This user guide provides installation and configuration information for the VSU-2000 VPNware Service Unit (VSU).

How This Guide Is Organized

Chapter 1, *Introduction*, includes a functional overview of the VSU-2000 and its major components along with site requirements for safe installation and operation of the VSU-2000.

Chapter 2, *Installing the VSU-2000*, provides instructions for physical installation, including placement and connection to the network. Procedures for mounting the VSU-2000 in an equipment rack are also included in this chapter.

Chapter 3, *Preparing the VSU-2000 for Configuration*, provides instructions for setting up VSU-2000 addressing and enabling remote connectivity for using the VPNmanager, VPNet's VPN network management application.

Appendix A, *Specifications*, documents physical, environmental, electrical, and compliance specifications, as well as additional features.

Appendix B, *10/100BASE-T UTP Crossover Cable Pinouts*, provides pinouts for VSU-2000 crossover cabling between the VSU-2000 and a router.

Change History

Version	Date	Changes
09-0045-01	August 2000	Initial Release
09-0045-02	January 2001	Chapter 3 - Modified VSU Quick Setup section, Added FIPS Mode and General Firmware Upgrade Imformation

Product Registration

To register the VSU-2000, navigate to `http://www.vpnet.com` on the World Wide Web.

Contacting Technical Support

Technical support is available to registered users of the VSU-2000.

- Voice: 1-888-VPNET-88 (within U.S.) or +1 408-404-1400 (outside U.S.)
- FAX: +1 408-404-1414
- Email: `support@vpnet.com`
- World Wide Web: `http://www.vpnet.com`

Chapter 1 Introduction

Functional Overview

The VSU-2000 is a VPN gateway to create virtual private networks (VPNs) within a small to medium sized business/branch office. Designed to provide the convenience of a virtual private network gateway and a firewall all in one compact rack-mountable enclosure, the VSU-2000 provides a cost-effective solution to quick and easy VPN deployment.

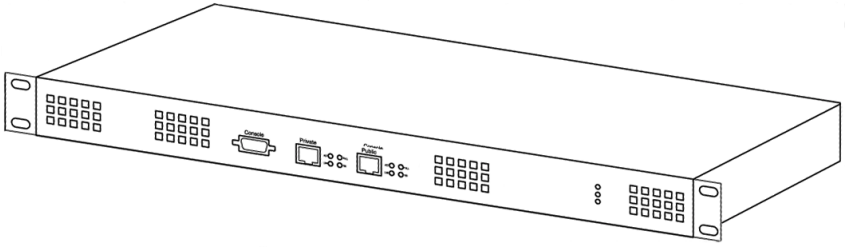


Figure 1-1 The VSU-2000

Like other gateways in the VPNware family, the VSU-2000 adds compression, encryption, authentication, and key management to public network data links to ensure privacy and integrity of corporate data, and to enable the efficient and secure operation of virtual private networks (VPNs). It is designed to perform complex operations, in real time, without compromising network performance, and in many cases can actually increase data throughput. The VSU-2000 supports up to 1000 simultaneous tunnels.

The VSU-2000 supports a full suite of VPN services including: ICSA-certified IPSec-based encryption, data compression, packet and user authentication, IKE and SKIP key management, Network Address Translation (NAT), routing, and a network firewall (packet filtering).

Security

The VSU-2000 provides data stream privacy by employing cryptographic algorithms and keys powerful enough for the most sensitive business communications. The VSU-2000 supports 56-bit DES and 168-bit 3DES encryption, as well as the ISAKMP and SKIP key management standards.

Data authenticity is assured by using MD5™ or SHA-1 hashing algorithms to reject altered or forged packets. All security mechanisms employed by the VSU-2000 conform to Internet Engineering Task Force RFCs, in order to provide interoperability and broaden the use of VPN technology.

Performance

The VSU-2000 supports IP over 10BASE-T or 100BASE-T local area networks (LANs). When packets are encrypted and authenticated according to IPSec protocol guidelines, additional bytes—in the form of IPSec headers—must be added to packets. In many cases, the additional packet overhead imposes a performance penalty in return for security. The extra bytes tend to lengthen packets and reduce the throughput (measured in packets per second). Of even greater impact is the tendency for packets lengthened by IPSec headers to be fragmented by network routers, causing further reductions in performance and additional latency. Real-time compression performed by the VSU-2000 eliminates packet fragmentation and produces fewer, smaller packets, which can significantly enhance network throughput and performance.

Plug-and-Play Installation

The VSU-2000 can be placed anywhere in a 10/100BASE-T LAN to provide VPN functionality. Native support for IP ensures that the VSU-2000 interoperates transparently with the broadest range of intranet and other network applications.

The graphical VPNmanager™ (available separately) network management application steps network managers through the setup process and allows them to configure a VPN in minutes. The VPNmanager also supports extensive facilities for VPN monitoring and troubleshooting, and for establishing multi-company

extranets. The VSU-2000 provides support for the RADIUS protocol, enabling VPNs that support hundreds of remote users and a variety of mechanisms for remote user authentication.

VSU-2000 Components

Each of the major VSU-2000 components are shown in Figures 1-2 and 1-3.

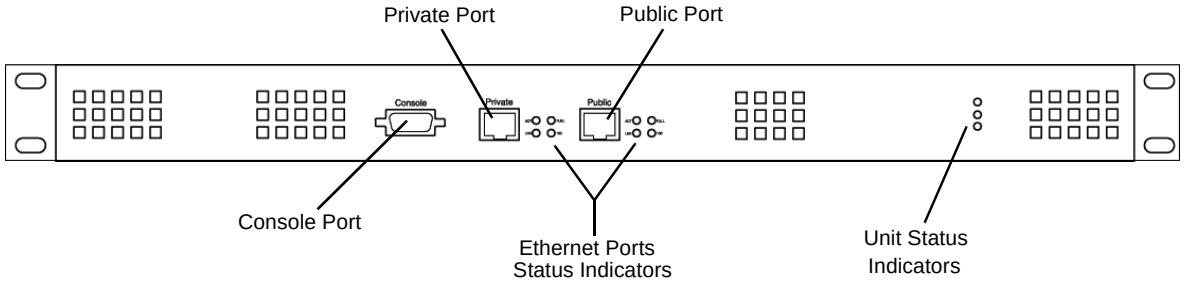


Figure 1-2 VSU-2000 Front Panel

Figure 1-3 VSU-2000 Back Panel

Ethernet Ports

The VSU-2000 includes two 10/100BASE-T Ethernet ports. One port is designated as the public (encrypted) interface and the other port is designated as the private (unencrypted) interface.

NOTE: *The VSU-2000 is enclosed in a tamper-evident case that meets U.S. NIST FIPS 140-1 Level Physical Security and may be replaced only by an authorized service technician.*

Status Indicators

The status indication LEDs on each of the two Ethernet ports and the Unit Status Indicators are defined in Figure 1-4.

When LAN traffic is detected on the public port, the LAN status indicator will blink. When VPN traffic is detected on the private port, the VPN status indicator will blink. The rate at which the LAN and VPN status indicators blink is the result of the rate of traffic detected on each port. The ON status indicator remains lit to indicate the unit is powered up.

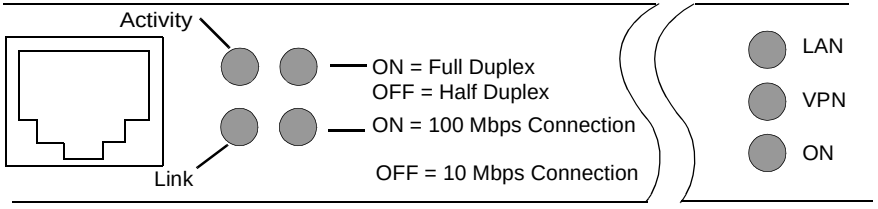


Figure 1-4 VSU-2000 Status Indicators

General Site Requirements

This section describes the requirements your site must meet for safe installation and operation of your system. Ensure that your site is properly prepared before beginning installation.

Environmental Requirements

The VSU-2000 is intended for use in a normal office or data room environment. For more extreme conditions, verify that temperature, humidity, and power conditions meet the specifications indicated in Table 1-1.

Table 1-1 Environmental Requirements

Item	Operating Specification
Temperature	32° to 104° F, 0° to 40°C
Relative Humidity	5-90%, non-condensing
Altitude	0-12,000 feet, 0-3,660 meters
Voltage	85-264 VAC

Table 1-1 Environmental Requirements

Item	Operating Specification
Input Frequency	47-440 Hz
AC input current	1 Amp Maximum

Additional VSU-2000 specifications are included in Appendix A.

Site Power Considerations

Check the power at your site to ensure that you are receiving “clean” power (free of spikes and noise). Install a power conditioner if necessary.

WARNING: *This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that a fuse or circuit breaker no larger than 120 VAC, 15A U.S. (240 VAC, 10A international) is used on the phase conductor (all current-carrying conductors).*

Required Equipment

The VSU-2000 shipping carton contains:

Quantity	Part Description
1	VSU-2000 VPN Service Unit
1	VSU-2000 VPN Service Unit User Guide
1	UTP Crossover Cable (for connection to a router)
1	Null Modem Cable (for connection to the VSU Console port)
1	Power cord (110V) or Power cord (230V)
1	Rack mount kit including two mounting brackets and screws for attaching the brackets to the VSU-2000. Screws required to mount the unit to the rack must be provided by the customer.
4	Rubber feet for desktop installations

To install and use the VSU-2000 in a typical network, the customer must supply:

- Router providing connectivity to a WAN such as the Internet
- 10/100BASE-T Ethernet hub, router, or switch providing connectivity to a LAN

- An asynchronous ASCII terminal supporting RS-232 or a PC running terminal emulation software to provide initial IP configuration (IP address, subnet mask, default router)
- PC workstation running VPNmanager software to configure the VSU-2000 in the VPN

Configuring Equipment Racks

The VSU-2000 can be placed on a desktop, shelf, or mounted in a standard 19-inch equipment rack. The location of the unit and the layout of your equipment rack or wiring room are extremely important for proper system operation. Equipment placed too close together, inadequate ventilation, and inaccessible panels can cause system malfunctions and shutdowns, as well as make system maintenance difficult.

The following information will help you plan an acceptable equipment rack configuration.

- Enclosed racks must have adequate ventilation. Ensure that the rack is not overly congested because each unit generates heat. An enclosed rack should have louvered sides and a fan to provide cooling air.
- When mounting a chassis in an open rack, ensure that the rack frame does not block the ventilation grates. If the chassis is installed on slides, check the position of the chassis when it is seated all the way into the rack.
- In an enclosed rack with a ventilation fan in the top, excessive heat generated by equipment near the bottom of the rack can be drawn upward and into the ventilation grates of the equipment above it in the rack. Ensure that you provide adequate ventilation for equipment at the bottom of the rack.

Instructions for rack mounting are provided in the section “Rackmount Installation” on page 2-1.

Chapter 2 Installing the VSU-2000

Rackmount Installation

The VSU-2000 ships with a VSU rackmount bracket kit, which includes two L-shaped brackets that attach to the sides of the VSU-2000 and to the front of a standard 19-inch equipment rack. Referring to Figure 2-1, perform the following procedure to install the VSU-2000 to a standard 19-inch equipment rack:

1. From one side of the VSU-2000, remove the two front side screws.
2. Using the flat-head screws, provided with the bracket, attach the bracket to the VSU-2000.
3. Repeat previous steps to attach the bracket on the other side of the VSU-2000.
4. Install the VSU-2000 into a standard 19-inch rack.

NOTE: *Rack screws are not provided with the VSU.*

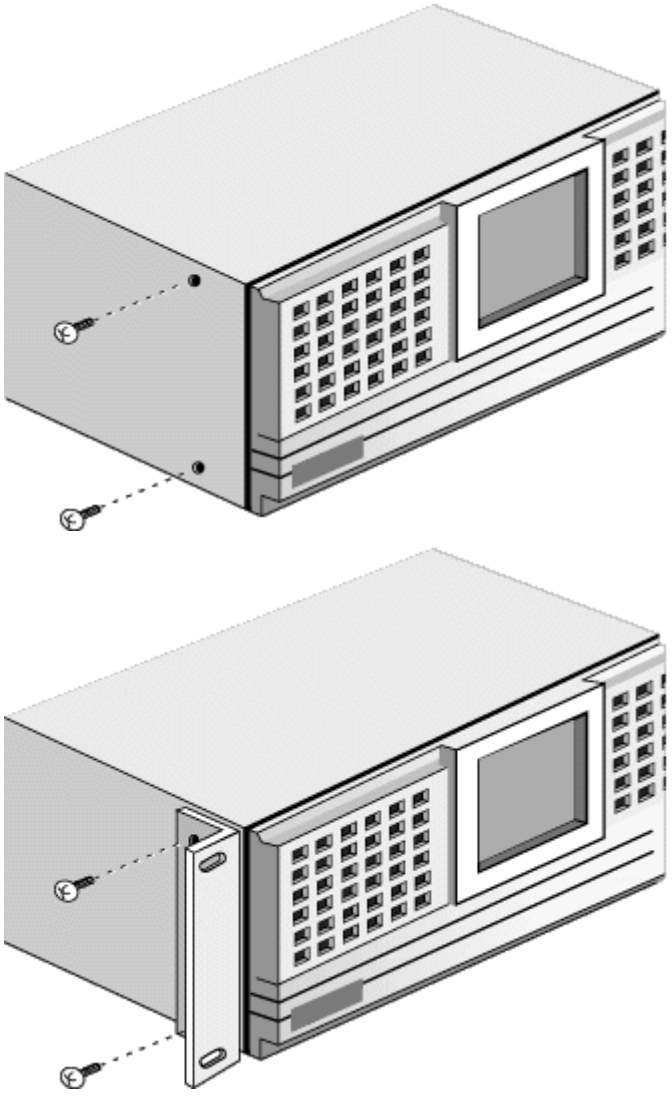


Figure 2-1 Installing the Rackmount Brackets

Connecting the VSU-2000 to the Network

Figure 2-2 shows a typical network using the VSU-2000.

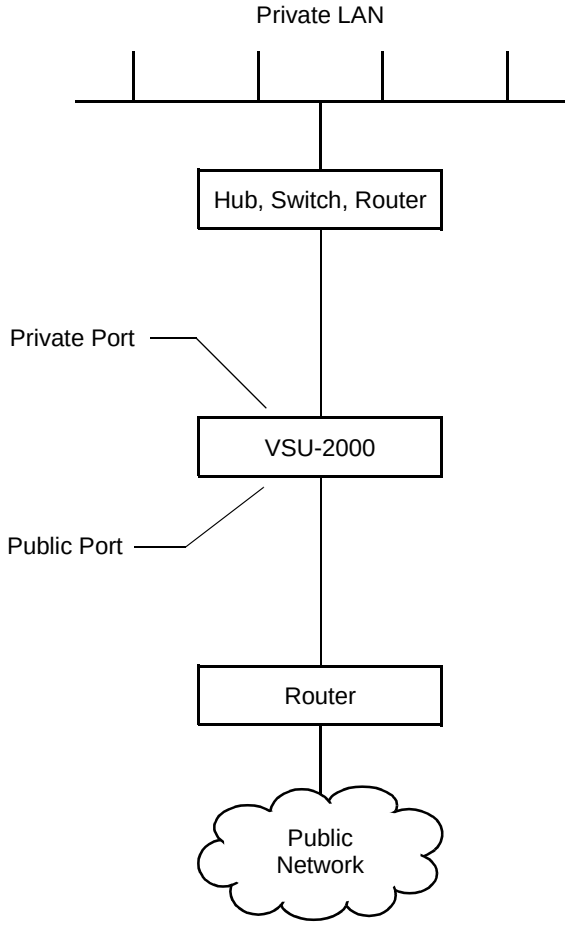


Figure 2-2 Typical VSU-2000 Hardware Installation

The VSU-2000 front panel is shown in Figure 2-3.

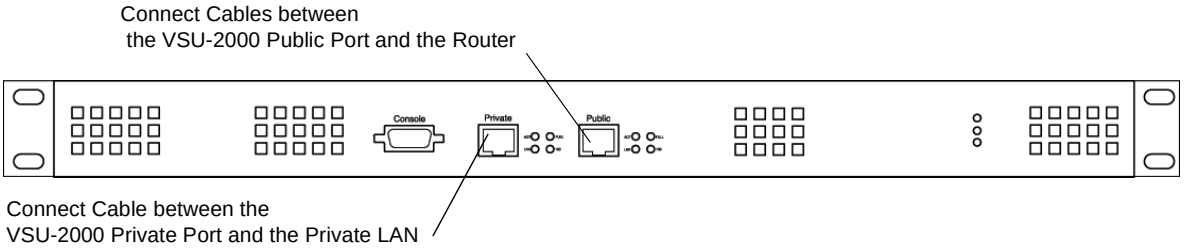


Figure 2-3 VSU-2000 Front Panel Connectors

The console port accepts an RS-232 DB-9 connection from an asynchronous ASCII terminal or a PC running terminal emulation software. The connection requires a null modem cable, which is supplied.

The communication settings for a terminal or PC connected to the console port are provided in Table 2-1.

Table 2-1 Terminal Settings

Parameter	Setting
Baud	9600
Data Bits	8
Stop bits	1
Parity	None
Flow control	Hardware (RTS/CTS)

The two Ethernet ports are 10/100BASE-T compliant host ports. They accept category 5 UTP cabling terminated in an RJ-45 connector per IEEE 802.3 requirements for 10/100BASE-T. The Ethernet ports do not provide a cross-over function; therefore a cross-over cable, (provided with the unit), is required when connecting the VSU-2000 public port directly to a router.

Perform the following steps to install the VSU-2000 in a typical LAN:

1. Connect the VSU-2000 to the router on the public (encrypted) side of the LAN using the supplied UTP crossover cable.

2. Connect the VSU-2000 to the private (unencrypted) side of the LAN.

   Using a standard straight-through 10/100BASE-T UTP cable, connect one of its RJ-45 connectors to the VSU-2000 private port and the second one to the hub or switch on the private LAN.

3. Connect an asynchronous ASCII terminal or PC running terminal emulation software to the VSU-2000 console port using the RS-232 null modem cable that came with the VSU-2000.

   The terminal's communications parameters should be set to 9600 baud, 8 data bits, 1 stop bit, no parity, and RTS/CTS hardware flow control.

4. Connect the AC power cable then power on the VSU-2000 and proceed to *Chapter 3, Preparing the VSU-2000 for Configuration.*

Chapter 3 Preparing the VSU-2000 for Configuration

Preparation

Before the VSU-2000 can be incorporated into a Virtual Private Network (VPN), it must be configured through the VPNmanager. However, to enable communication between the VPNmanager and the VSU-2000, you must first assign an IP address, subnet mask, and default route to the VSU-2000.

This chapter describes how to set up the VSU-2000 addressing and remote connectivity capabilities in preparation for remote configuration using the VPNmanager software. This preliminary configuration is performed using a terminal (or a PC running terminal emulation software) connected to the RS-232 console port.

The following procedure assumes that the VSU-2000 has been physically installed on the network, according to the instructions provided in Chapter 2

Configuration

Beginning with VPNware 3.1, the following information is configured through the VSU console Quick Setup:

- The VSU's IP address and mask.
- The VSU's secondary IP address and mask (Optional).
- The VSU's default route.
- The VSU console password. Beginning with VPNware 3.1, if you forget this password and need console access, it can be changed through the VPNmanager's Configuration console. Select the VSU Advanced Action tab, then the Reset Password dialog box.

- The SuperUser name. This is the name that is authorized to perform any kind of configuration request on a VSU. This name is provided by the VPNmanager administrator the first time the VSU is added into the VPNmanager database. The SuperUser name is case sensitive.
- The SuperUser password. This password authenticates the SuperUser name. The SuperUser password is case sensitive. If the VPN administrator forgets the SuperUser password, the VSU may still be reconfigured through the VSU console Quick Setup menu as long the administrator has access to the VSU console and knows the VSU console password.
- Configuration of blocking mode. This involves selecting one of three filtering choices according to your organization's security policy:

  Permit all non-VPN traffic - When checked (default), all non VPN traffic is allowed to pass through the VSU.

  Deny all IP non-VPN traffic - When checked, all non-IP traffic is passed through the VSU. All non-VPN IP traffic is dropped except for the following: ICMP, IGMP, GGP, EGP, IGP, DGP, EIGRP, and OSPF. ***NOTE:*** *This mode should be used when the VSU dedicated to VPN traffic and is the only device between the private and the public networks.*

  Deny all non-VPN traffic - When checked, all non-VPN traffic is prevented from passing through the VSU. This mode blocks non-IP traffic and non-VPN IP traffic including broadcast traffic (e.g. ARPs), IP-multicast traffic (e.g. OSPF updates) and other traffic containing routing information. ***NOTE:*** *This mode should be used when the VSU is dedicated to VPN traffic and is in parallel with another device (such as a router or firewall) that will enforce the network's non-VPN traffic policy. This mode should not be used when the VSU is the only path between network devices and a router with which those devices need to communicate.*
- Setting the unit to run in FIPs-compliant mode or not.
- The current time and date.

  NOTE: *Each of these items are preserved over firmware upgrades.*

When the VSU-2000 is powered on for the first time, the terminal screen should display the initial power on bootup screen shown in Figure 3-1.

```
VPNet Service Unit Model XXXX 3DES ENCRYPTION
Runtime System version x.x.xx, x/xx/2000
Copyright (C) 1996-2000 VPNet Technologies, Inc. All Rights
Reserved.

 -- Month Day 2000, 17:06:01 --ethernet0: MAC Address
00:60:a1:00:23:f9
ethernet1: MAC Address 00:60:a1:00:23:fa
ethernet2: MAC Address 00:60:a1:00:16:9a
ethernet3: MAC Address 00:60:a1:00:16:9b

Checking Non Volatile RAM integrity... OK

Checking Configuration Database... OK
Checking Certificate Database... OK
Calibrating CPU performance monitor... OK
Power/Cooling subsystems Monitor initializing...
Power Subsystem is Good.
Cooling Subsystem Good.
...Done.

VPNet Technologies - VSU XXXX 3DES ENCRYPTION - Main  Menu

  1) Configuration
  2) Statistics
  3) Utilities
  4) Logout
  5) Quick Setup

  Your choice [1-5]:
```

Figure 3-1 Initial Power On Bootup Screen for VSU

Preconfigure the VSU-2000 to communicate with the VPNmanager using the Quick Setup menu selection as described below:

1. From the Main Menu, select `5) Quick Setup.`

```
VPNet Technologies - VSU XXXX- Main Menu

  1) Configuration
  2) Statistics
  3) Utilities
  4) Logout
  5) Quick Setup

  Your choice [1-5]: 5
```

You will be prompted for the information required to set up the VSU. To accept the current value and go to the next prompt, press Return.

2. Enter the IP address and netmask assigned to the VSU.

NOTE: *The Secondary IP address and mask are optional.*

```
IP address: 192.0.2.1    Mask: 255.255.255.0

IP address: 210.1.18.135
IP mask: 255.255.255.0
Do you want a secondary IP address on this unit? [yn] y

Secondary IP address:     Secondary Mask: 255.0.0.0

Secondary IP address: 10.0.0.1
Secondary IP mask: 255.255.255.0
```

3. Enter the default route for this VSU.

```
Default Route is not configured.
Enter Default Route: 210.1.18.1
```

Typically, the default route is the IP address of the gateway router that provides an IP route between the VSU-2000 and the public network (e.g., Internet).

4. To prevent unauthorized users from accessing the VSU-2000 through the console port, enter and confirm the new VSU console password.

```
VSU Console password may be up to 31 characters.
Enter new VSU console password: ******
Confirm new VSU console password: ******
```

CAUTION: *Do not forget this password. As a security measure, the only way to bypass an unknown console password is to return the VSU-2000 to the factory at the customer's expense.*

The password may be up to 31 characters in length and is case-sensitive. Once the password is set, it must be entered to gain future access to the VSU console.

Pressing Return without typing anything at the "Enter new VSU console password" and "Confirm new VSU console password" prompts will set the VSU console password to empty (no password required).

5. A superuser name and password is required to allow the Network Administrator to initially configure this VSU through the VPNmanager application.

```
This VSU's superuser name is: "root". Change superuser name?
[yn] y

This VSU's superuser name may be up to 31 characters.
Enter new superuser name: superuser

This VSU's superuser password may be up to 31 characters.
Enter new superuser password: ******
Confirm new superuser password: ******
```

Press Return or enter "n" to leave the superuser name at its default value of root, or enter "y" to change the superuser name.

Both the superuser name and password may be up to 31 characters and are case-sensitive. The name and password will be required later when first setting up the VSU through the VPNmanager application. After the VSU has been initially set up, the VSU may use the VPNmanager Directory Server to authenticate a configuration request, at the Network Administrator's option.

```
Non-VPN traffic mode: non-VPN traffic is currently
forwarded.

Non-VPN Traffic Configuration Menu

  1) Permit all non-VPN traffic
  2) Deny IP non-VPN traffic only
  3) Deny all non-VPN traffic
  P) Previous menu

  Your choice [1-3]:
```

6. Select a traffic mode from the Traffic Configuration Menu.

   Permit all non-VPN traffic - When checked (default), all non VPN traffic is allowed to pass through the VSU.

   Deny all IP non-VPN traffic - When checked, all non-IP traffic is passed through the VSU.

   Deny all non-VPN traffic - When checked, all non-VPN traffic is prevented from passing through the VSU.

   For additional information regarding traffic modes, see page 3-2.

```
Do you want this unit to run in FIPs-compliant mode? [yn] y
```

7. Enter “n” if you do not want the VSU to run in FIPs-compliant mode. If you answer “n”, the code skips to the date and time configuration. Go to Step 7.

   Enter “y” if you want the VSU to run in FIPs-compliant mode. If you answer “y”, answer the following configuration questions. For more information regarding FIPS, see “FIPS Mode” on page 3-8.

```
FIPs-compilant mode may only be disabled via VPNmanager.
Please confirm that you want this unit to run in FIPs-
compilant mode. [yn] y
```

8. Enter the current date and time.

```
Date: 3-9-2000
Enter date [MM-DD-YYYY]:

Time: 13:51:53
Enter time [HH:MM:SS]:
```

This date and time setting are primarily used to ensure accurate timestamps when logging events. When changing either the date or time, all three parts of the date (MM-DD-YYYY) or time (HH:MM:SS) must be entered. A 24-hour clock is used when setting the time. For example, 13:00:00 is equivalent to 1:00 PM.

9. Reboot the VSU-2000.

```
Reboot is required to complete Quick Setup. Reboot Now? [yn]
y
```

Your VSU-2000 is now prepared for configuration by using the VPNmanager. The VSU initially passes all traffic between its Public and Private ports. This would be a good time to verify connectivity by pinging the VSU from public and private machines, and by passing traffic between public and private machines.

Proceed to the *VPNmanager Administrator Guide* to continue configuring your VSU.

FIPS Mode

FIPS (Federal Information Processing Standards) Mode forces the VSU to operate in a FIPS 140-1 Level 2 compliant mode. It is recommended that this mode only be used if your organization's policy requires FIPS 140-1 Level 2 certification for cryptographic devices.

Note that in the FIPS mode (as dictated by the FIPS 140-1 requirements specification), the following are NOT supported:

- SKIP VPNs
- VPNremote 2.5x Clients
- Any encryption algorithm other than DES or 3DES
- Any authentication algorithm other than SHA-1

General Firmware Upgrade Information

Configuration Items Left to the VPNmanager

The following items are likely to be configured by most administrators, but are left to VPNmanager or other VSU console menu items to keep the Quick Setup menu minimal:

- LDAP servers used to authenticate VPNmanager console users.
- Disable a VSU's SuperUser account.

Flushing the configuration on VPNware 3.1

In the event you flush the configuration (via VSU console menu item Configuration->Flush Configuration) on a VSU running VPNware 3.1 the following occurs:

- The superuser name will be "root".
- There will be no superuser password.
- If a VSU console password is configured, it will be preserved.
- The secondary IP address will be empty.
- The blocking mode will be set to forward all non-VPN traffic.

APPENDIX A *Specifications*

Packet Encryption

- DES encryption (56-bit key)
- Triple DES (EDE-CBC) encryption (168-bit key)
- Weak and semi-weak keys are automatically discarded

Packet Authentication

- Keyed MD5™ AH Message Digest Algorithm (RFC 1321)
- HMAC-MD5 and HMAC SHA-1 (RFC 2104)

User Authentication

- RADIUS servers (Ascend Access Control™, Security Dynamics ACE/Server Access Manager, BaySecure™ Access Control, Funk Steel Belted RADIUS Server)
- CHAP and PAP
- SecurID™ tokens
- x.509v3 digital certificates
- Smart Cards
- LDAP

Compression

- Stac™ Lempel-Ziv hardware data compression

Key Management

- IKE: Key updates configurable starting from 60 seconds (RFC 2409)
- SKIP: Keys updated every 30 seconds
- All packet, traffic, and authenticating keys automatically generated

Firewall Integration

- Bypass mode for non-VPN traffic
- Network (packet filtering) firewall

Network Address Translation (NAT)

- Supports static, dynamic, and port mapping
- Reverse address translation for dynamic IP clients

Protocol Support

- IEEE 802.3, Ethernet
- Full IPSec compliance: RFC 2401, 2402, 2403, 2404, 2405, 2406, 2407, 2408, 2409, 2410, 2412, 2451, IPSec Key Management using SKIP or IKE. (Tunnel and transport modes supported.)

Digital Certificates

- X.509v3 for management and IPSec communication
- Compatible with certificates generated by VeriSign, GTE Cybertrust, Entrust, Frontier Technologies, Baltimore, Netscape, Microsoft, and Thawte

System Management

- Configuration via Java-based VPNmanager™
- Monitoring from any application with SNMPv1 via VSU-2000 MIB
- Configuration traffic secured through SSL
- Secure software download for system upgrades
- Syslog event and usage logging

VPNremote Client Support

- VPNremote Client Software for Windows 95/98/NT

Compatibility

- Fully compatible with all other VPNware Service Units and VPNremote Client Software for Windows 95/98/NT (using transport or tunnel mode)
- ICSA-certified IPSec

Dimensions

- 17.0" W x 16.0" D x 1.75" H (43.2 cm x 38.0 cm x 4.4 cm)
- 1U high
- 19" rack mountable

Weight

- 7.5 lbs. (2.79 Kg)

Physical Security

- Tamper-evident enclosure (FIPS 140-1 Level 2 compliant)

LAN Interface

- Two 10/100BASE-T Ethernet ports

Management Interfaces

- RS-232 and Ethernet

Software Upgrade

- Via built-in flash RAM

Power Requirements

- 100/240 VAC
- Input frequency: 50 to 60 Hz
- AC input current: 1 Amp
- Internal Battery (End user non-serviceable part): **CAUTION:** Danger of explosion if memory backup battery is incorrectly replaced. Replace only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.

Operating Environment

- Temperature: 32° to 104° F, 0 to 40°C
- Relative Humidity: 5 to 90% (non-condensing)
- Altitude: 0-12,000 feet, 3660 meters

Safety Certification

- UL, CSA, CE, CB Scheme

EMI/RFI

- FCC Part 15, Class A, CISPR 22/85A
- VCCI

APPENDIX B

10/100BASE-T UTP Crossover Cable Pinouts

The 10/100BASE-T UTP Crossover Cable defined below is provided with the VSU-2000.

Signal Name	Male RJ-45	Male RJ-45
TX+	1	3
TX-	2	6
RX+	3	1
RX-	6	2

VSU Acronyms

CBC – Cipher Block Chaining encryption

DES – Data Encryption Standard encryption

DNS – Domain Name Server (a distributed database system used to map host names to IP addresses and vice versa)

DCE – Data Communication Equipment

DSU/CSU – Data Service Unit/Channel Service Unit

DTE – Data Terminal Equipment

ECB – Electronic Code Book encryption

HDLC – High-level Data Link Control

ISAKMP – Internet Security Association Key Management Protocol

IPSEC – Internet Protocol SECurity

MD5 – Message Digest Algorithm

PPP – Point to Point Protocol

RADIUS – Remote Authentication Dial-In User Server

RFC – Request For Comment

SHA – Secure Hash Algorithm

SKIP – Simple Key Management for Internet Protocol

SNMP – Simple Network Management Protocol

SSL – Secure Socket Layer

TCP/IP – Transmission Control Protocol / Internet Protocol

URL – Uniform Resource Locator

UTP – Unshielded Twisted Pair

VPN – Virtual Private Network

VSU – VPN Service Unit

Index