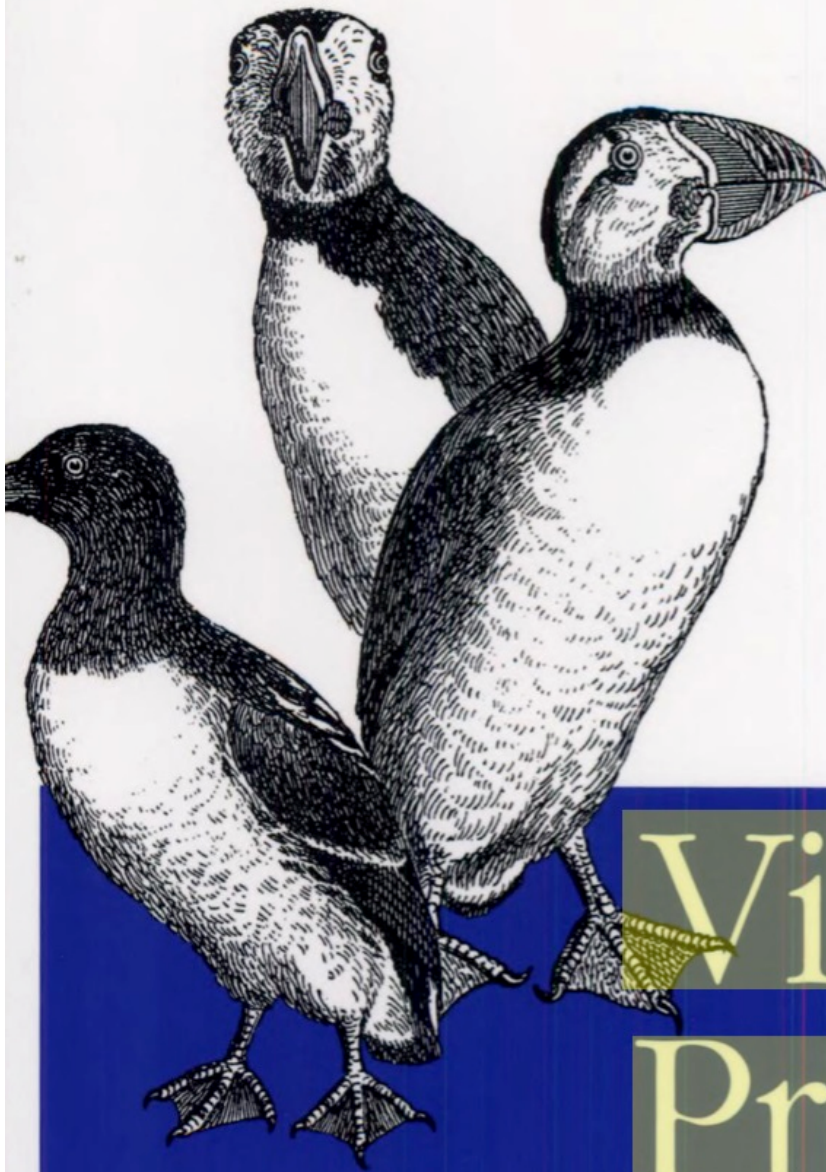


Turning the Internet Into
Your *Private Network*

2nd Edition



Virtual Private Networks

O'REILLY®

Charlie Scott, Paul Wolfe & Mike Erwin

Copyrighted material

Virtual Private Networks, Second Edition

by Charlie Scott, Paul Wolfe, and Mike Erwin

Copyright © 1999, 1998 O'Reilly & Associates, Inc. All rights reserved.
Printed in the United States of America.

Published by O'Reilly & Associates, Inc., 101 Morris Street, Sebastopol, CA 95472.

Editor: Andy Oram

Production Editor: Jane Ellin

Printing History:

March 1998:	First Edition.
January 1999:	Second Edition.

Nutshell Handbook, the Nutshell Handbook logo, and the O'Reilly logo are registered trademarks of O'Reilly & Associates, Inc. Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this book, and O'Reilly & Associates, Inc. was aware of a trademark claim, the designations have been printed in caps or initial caps.

The association between the image of puffins and the topic of **virtual private** networks is a trademark of O'Reilly & Associates, Inc.

While every precaution has been taken in the preparation of this book, the publisher assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained herein.



This book is printed on acid-free paper with 85% recycled content, 15% post-consumer waste. O'Reilly & Associates is committed to using paper with the highest recycled content available consistent with high quality.

ISBN: 1-56592-529-7

[6/99]

We'll go into detail about the power, politics, and use of various encryption techniques in Chapter 2.

Tunneling

Many VPN packages use tunneling to create a private network, including several that we review in this book: the AltaVista Tunnel, the Point-to-Point Tunneling Protocol (PPTP), the Layer 2 Forwarding Protocol, and IPSec's tunnel mode. VPNs allow you to connect to a remote network over the Internet, which is an IP network. The fact is, though, that many corporate LANs don't exclusively use IP (although the trend is moving in that direction). Networks with Windows NT servers, for instance, might use NetBEUI, while Novell servers use IPX. Tunneling allows you to encapsulate a packet within a packet to accommodate incompatible protocols. The packet within the packet could be of the same protocol or of a completely foreign one. For example, tunneling can be used to send IPX packets over the Internet so that a user can connect to an IPX-only Novell server remotely.

With tunneling you can also encapsulate an IP packet within another IP packet. This means you can send packets with arbitrary source and destination addresses across the Internet within a packet that has Internet-routable source and destination addresses. The practical upshot of this is that you can use the reserved (not Internet-routable) IP address space set aside by the Internet Assigned Numbers Authority (IANA) for private networks on your LAN, and still access your hosts across the Internet. We will look at how and why you would do this in later chapters.

Other standards that many VPN devices use are X.509 certificates, the Lightweight Directory Access Protocol (LDAP), and RADIUS for authentication.

VPN Solutions

A VPN is a conglomerate of useful technologies that originally were assembled by hand. Now the networking companies and ISPs have realized the value of a VPN and are offering products that do the hard work for you. In addition, there is an assortment of free software available on the Internet (usually for Unix systems) that can be used to create a VPN. In this book, we're going to look at some of the commercial and free solutions in detail. Which one you choose for your network will depend on the resources available to you, the platforms you run, your network topology, the time you wish to spend installing and configuring the software, and whether or not you want commercial-level support. We can't cover every vendor and product in this book; they change too quickly. Instead, we offer guidelines you can use on all networks and details on a few stable products that