

virtual

private

networks

making the right connection

dennis fowler

Virtual Private Networks

Making the Right Connection

Dennis Fowler

netWorker Magazine,
Association for Computing Machinery



MORGAN KAUFMANN PUBLISHERS, INC.
San Francisco, California

Copyrighted material

Senior Editor
Director of Production and Manufacturing
Production Editor
Editorial Assistant
Cover Design
Cover Image
Text Design
Copyeditor
Proofreader
Composition and Illustration
Indexer
Printer

Jennifer Mann
Yonie Overton
Cheri Palmer
Karyn Johnson
Ross Carron Design
© Patrick Ingrand/Tony Stone Images
Side by Side Studios
Jeff Van Bueren
Jennifer McClain
Technologies 'n Typography
Ty Koontz
Courier Corporation

Designations used by companies to distinguish their products are often claimed as trademarks or registered trademarks. In all instances where Morgan Kaufmann Publishers, Inc. is aware of a claim, the product names appear in initial capital or all capital letters. Readers, however, should contact the appropriate companies for more complete information regarding trademarks and registration.

Morgan Kaufmann Publishers, Inc.
Editorial and Sales Office
340 Pine Street, Sixth Floor
San Francisco, CA 94104-3205
USA

Telephone 415 / 392-2665
Facsimile 415 / 982-2665
Email mkp@mkp.com
WWW <http://www.mkp.com>
Order toll free 800 / 745-7323

© 1999 by Morgan Kaufmann Publishers, Inc.
All rights reserved
Printed in the United States of America

03 02 01 00 99 5 4 3 2 1

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means—electronic, mechanical, photocopying, recording, or otherwise—without the prior written permission of the publisher.

Library of Congress Cataloging-in-Publication Data

Fowler, Dennis.

Virtual private networks : making the right connection / Dennis

Fowler.

p. cm.

Includes bibliographical references.

ISBN 1-55860-575-4

1. Extranets (Computer networks) 2. Business enterprises—computer networks.

3. Internet (Computer network) 4. Computer networks—Security measures. I. Title.

TK5105.875.E87F69 1999

650'.0285'46—DC21

99-13845

CIP

“private” public networks and the extremely “public” Internet as we think of it is anything but distinct; because these network service providers are frequently also Internet service providers, the confusion is further compounded.

If you’ve done a search on the World Wide Web for the keywords virtual private network or VPN, you’ve probably even discovered that for years companies like Pacific Bell have been marketing an extended telephone service using the same terms.

Thanks to all this confusion, it can be very hard to understand exactly what qualifies as a VPN, how a VPN can be implemented, and exactly what a VPN can and cannot do for you. That’s what we’ll explain for you here.

1.1 What Is a VPN?

Very simply put, a virtual private network uses a public network’s infrastructure to make the connections among geographically dispersed nodes, instead of using cables owned or leased exclusively for one single network’s use, as is typical for a wide area network (WAN). To the user, a VPN looks just like a private network, hence the virtual in its name, even though it is sharing a web of cables with the traffic of hundreds or thousands of other users at the same time. It has all the characteristics of a private network—limited access to only authorized users, for example—even though it is sharing the same public infrastructure with other users. Another way to describe it is that a VPN is a logical local area network (LAN) that connects an organization’s geographically dispersed sites in a way that makes them all appear to be part of one single network.

There are a variety of public networks that can be employed to make a VPN’s connections, but the most prominent and most public network available is, of course, the Internet. Because the Internet is everywhere and the Internet is where most of the VPN development is taking place, and because it is, as we’ll see, the most ubiquitous and cost-effective medium for a VPN, we’ll concentrate on VPNs running over it in this book. We will devote Chapter 4 to VPNs implemented through other networking services, and we will explain the differences in detail at that time, but since the Internet is the predominant medium and the technology is essentially the same regardless of the network being used, the Internet is where we will concentrate our discussion.

To illustrate how a VPN differs from a typical WAN, let’s look at a leased-line network, as shown in Figure 1-1, and then show how a VPN differs from it. For the sake of simplicity, this is only a three-node network, a company headquarters and two branch offices linked together with three leased lines.

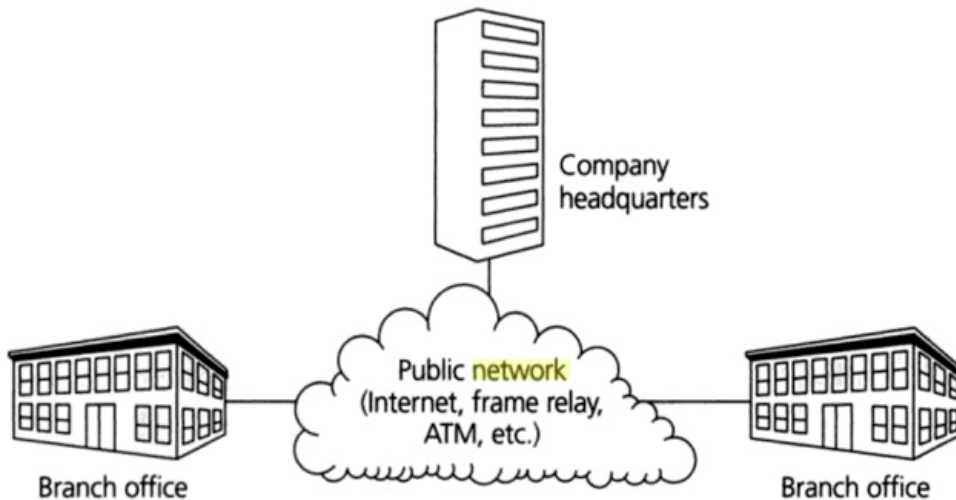


Figure 1-2 The same company using a VPN instead of leased lines.

Internet. Each office requires a single connection, most commonly a leased line and commonly referred to as a *local loop*, to the nearest public **network point of presence** (POP). That POP may be only a few feet away or it may be miles away. From that POP the data is carried by the web of connections—the cables, routers, and switches that make up the public **network**—to the POP serving the destination office, then through the local loop at that end on to their final destination.

As you can see, the connections—the local loops—between your company's offices and the public **network** are dramatically shortened. They can even be the "dry copper" connection provided by your local telephone service, perhaps an Integrated Services Digital **Network** (ISDN) connection. The costs for these short connections are correspondingly lower.

Within the cloud, however, as opposed to the leased-line design, there is no one single connection between point A and point B. Instead there is a web or matrix of cables connected by routers that the messages travel through. By using a public **network**—the Internet, for example—a **network** shared by hundreds or thousands or millions of other users, the cost of all those miles of cable is shared. We'll see further on in this chapter that this sharing can produce impressive savings.

It is also much more fail-safe than a single leased line, since a message can take any one of a number of different routes to its destination. It provides a redundancy, a safety net, that virtually guarantees that the traffic will continue to flow reasonably smoothly. If one cable is cut, the message will simply be routed automatically around the break to its destination, a service that is not generally available with a leased line.