Compliments of NCP

NCP Special Edition

Remote Access VPN

FOR DUMMIES®

A Wiley Brand

Learn to:

- **Apply best practices for secure remote access VPN**
- **Implement hybrid IPsec/SSL tunneling**
- **Enable central VPN client management**

Brian Underdahl
J. Hirschmann

Founded in 1986, NCP engineering has delivered innovative software that allows enterprises to overcome the complexities of creating, managing, and maintaining secure remote network access for users. NCP's award-winning IPsec/SSL VPN product line supports organizations that want to leverage the latest devices to increase staff productivity, reduce network administration, and adapt policy changes on the fly. Each solution is 100 percent interoperable with existing third-party software or hardware. The company serves 30,000-plus customers worldwide throughout the healthcare, financial, education, and government markets, as well as many Fortune 500 companies, and has established a network of technology, channel, and OEM partners.

For more information, visit www.ncp-e.com.

Remote Access VPN

FOR DUMMIES®

A Wiley Brand

NCP Special Edition

by Brian Underdahl
and
J. Hirschmann

FOR DUMMIES®
A Wiley Brand

Remote Access VPN For Dummies®, NCP Special Edition

Published by

John Wiley & Sons, Inc., 111 River St., Hoboken, NJ 07030-5774, www.wiley.com

ISBN: 978-1-118-91425-0 (pbk); ISBN: 978-1-118-91529-5 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Acquisitions, Editorial, and Vertical Websites

Project Editor: Carrie A. Johnson
Editorial Manager: Rev Mengle
Business Development Representative: Karen Hattan
Custom Publishing Project Specialist: Michael Sullivan

Introduction

Staying competitive in today's world increasingly means being connected. Organizations of all sizes need to make sure their employees have access to company resources no matter where they're located. Organizations also have to provide remote access across a multitude of devices from laptops to tablets and smartphones.

Unfortunately, simply providing remote access without considering resource security isn't an option. Your organization's resources must be protected at the same time you're enabling outside access to your systems. Balancing these two needs can be a real challenge.

About This Book

Remote Access VPN For Dummies, NCP Special Edition, is designed to help you understand how best to meet the challenges of providing a secure remote access Virtual Private Network (VPN). This book shows you what remote access VPN is, explains the core technologies involved, and looks at the current state of the art regarding remote access VPN. In addition, this book discusses remote access VPN solutions that address the typical shortcomings common to many current VPN products.

How This Book Is Organized

Remote Access VPN For Dummies, NCP Special Edition, is divided into six concise and information-packed chapters. They cover the challenges of traditional approaches to secure remote communication and describe best practices for implementing a secure remote access VPN solution that's robust and cost effective. The book is brief, so feel free to read it in full, or browse instead, using the headings as your guide to particular information.

Icons Used in This Book

This book uses the following icons to call your attention to information you may find helpful in particular ways.

The information marked by this icon is important and therefore repeated for emphasis. This way, you can easily spot noteworthy information when you refer to the book later.

This icon points out extra-helpful information.

This icon marks places where technical matters, such as VPN jargon and whatnot, are discussed. Sorry, it can't be helped, but it's intended to be helpful.

Paragraphs marked with the Warning icon call attention to common pitfalls that you may encounter.

Chapter 1

Introducing Remote Access VPN

In This Chapter

- Getting to know secure remote access VPN
- Understanding the importance of remote access VPN

Today's workforce is mobile, and the IT environment has become more heterogeneous. People need to be able to connect to the office securely so they can work from wherever they are. This chapter looks at the technology that makes such remote access possible.

Looking at Tunnels and Encryption

Virtual Private Network (VPN) technology lets you connect to a corporate network through a shared or public network (Internet) connection. The technology gets its name from the fact that a VPN connection creates a virtual private tunnel between you and the network at the other end of the connection. Essentially, you can work with any network accessible resources just as if you were actually on the premises.

The "private" part of the name means there's a link between the sites, and you access network resources in the same way as local resources. Most VPN solutions are secure so data or other traffic passing between you and the organization's network is encrypted.

Actually, the encrypted traffic could be intercepted as it passes through the Internet, but the encryption keeps the data secure so even if it's intercepted, no one can tamper with it or make use of it. See Chapter 2 for more information on how VPN traffic is protected on the Internet.

Seeing How a VPN Fits into the Big Picture

In the not too distant past, people expected that getting information took some time. If you needed to access certain reference materials, you drove down to the library and requested a book. In many cases, you had to wait for a librarian to fetch the book from some dark shelf deep within the library, or even wait until another person returned the book. Now, of course, everyone expects that whatever information is needed will be instantly available.

This expectation has also had a huge effect on how organizations do business. Customers expect quick answers, and if you can't provide them with those answers right now, plenty of vendors will be happy to grab the business away from you. This need to provide accurate information quickly means that people need to be able to access the resources on your network from wherever they may be, and this access is provided through a VPN.

Remote access VPN means that you can access the information you need without the participation of another person in the office. As a result, remote access VPN actually increases productivity and reduces staffing costs because you don't have to rely on another person who's physically located on the premises to access corporate resources, such as checking inventory levels or order status. You can easily accomplish this by using the VPN connection.

Securing Remote Access

Before remote access VPN was invented, people could use other methods such as using a modem to connect to a network. Unfortunately, these older methods typically didn't offer much security (at all) and were complex, limited, slow, and difficult to use. Even if you were able to find a telephone jack, you still had to deal with choosing all the correct connection settings, making sure you correctly entered the proper dialing sequence, and then supplying the correct username and password in order to log on to the system. In addition, depending on your location, you could rack up some extreme roaming charges.

By using an existing Internet connection, remote access VPN eliminates many of the problems remote users used to face. After all, it's pretty easy to find an Internet connection pretty much anywhere today.

Although finding an Internet connection is usually pretty easy, those connections aren't always as inexpensive or trustworthy as you may think. See Chapter 5 for information about security loopholes that a good remote access VPN solution addresses.

In addition to enabling users to use network resources remotely, remote access VPN solutions also need to take into account the fact that different users may need to be granted different access permissions and be using different types of devices. For example, in addition to Windows-based laptops or smartphones, users may have Apple products or Android tablets and smartphones. A good remote access VPN solution makes connecting any of these devices to your network both easy and secure.

Chapter 2

Getting to Know Secure VPN Solutions

In This Chapter

- Introducing IPsec and SSL VPN
- Looking at SSL VPN's missed promises
- Understanding hybrid IPsec/SSL VPN solutions

Providing employees with the ability to work effectively no matter where they may be is critical in today's competitive market. It's obvious, however, that you can't simply open the door and allow everyone to come and go freely. Instead, you need the means to provide remote access VPN that's secure and protects the organization's resources. This chapter examines the tools that help make remote access VPN a secure process.

Understanding the Evolution of IPsec and SSL VPN

Most businesses function within some sort of secured environment. Even if your only security measure is a lock on your front door, you at least are applying some

control over who can come and go into your place of business. Just as there are door locks and burglar alarms designed to provide physical safety, tools are designed to provide the necessary security to protect your assets in a remote access VPN environment. The most common solutions are *IPsec (Internet Protocol Security) VPN, SSL (Secure Sockets Layer) VPN,* or a hybrid combination of both.

IPsec is a set of methods for securing Internet-based communications by authenticating and encrypting information as it passes back and forth between two end points. IPsec is an *open standard,* meaning that its specification has been published and is available for anyone to use. IPsec VPN functions at a lower network level than SSL VPN and, because of this, is considered more secure. See Chapter 3 for information about the security benefits of IPsec.

SSL VPN is based on a different tunneling technology than IPsec and also includes a secure connection that's authenticated and encrypted. It was developed due to increasing popularity of web-based applications and the need for easy and "clientless" secure remote access to them.

Seeing How the SSL VPN Promise Fell Short

IPsec and SSL VPN are designed to provide secure communications through a shared or public network (Internet) connection. SSL VPN was introduced as an easy solution that only required a browser and didn't require administrative rights. You simply opened a secure web page and received a response from a secure web server to establish an SSL VPN tunnel.

Along with SSL VPN's ease of use also came limitations related to accessing the corporate network and important business applications because an SSL VPN only supported web-based applications — for example, Outlook web access. Remote SSL VPN users discovered they didn't have access to all the resources on the corporate network that they had while working through an actual direct network connection or through an IPsec VPN. This lack of full network access limited the usefulness of the typical SSL VPN connection.

SSL VPN continued to evolve and new modes of SSL VPN were introduced including *thin* and *fat clients*. Thin clients can be downloaded on the fly but are limited to only applications with static ports — for example, Remote Desktop Protocol (RDP) and Secure Shell (SSH). This limitation led to the introduction of fat clients that provide full network access and support for dynamic ports, such as video, but these fat clients require administrator rights for installation.

SSL VPN was introduced to ease the complexity of a client-based IPsec VPN solution that required administrator rights for client installation. However, SSL didn't deliver on this promise, leaving companies that have complex VPN environments hungry for a hybrid solution.

Arriving at Hybrid IPsec/SSL VPN Solutions

Some remote access VPN solutions today are a hybrid of IPsec/SSL VPN technologies that provide everything in one environment. For a remote access VPN solution

to meet the needs of all users throughout the organization (teleworking, field services, sales, service, suppliers, partners), parallel support of both VPN tunneling technologies, IPsec and SSL VPN, is imperative.

Both technologies have their advantages and specialties. IPsec VPN is preferred if you wish to fully integrate employees who work in and out of the office and who access a multitude of different applications, because it's harder to attack, so it's more secure. SSL VPN should be implemented when suppliers or partners only need sporadic access to a small number of specific applications (ideally web based or static ports). Consider a hybrid IPsec/SSL VPN solution if you need to provide remote access for all types of users.

Chapter 3

Uncovering the Security Benefits of IPsec VPN

In This Chapter

- Diving into remote access VPN security
- Understanding IPsec VPN security advantages

The unparalleled ability of IPsec VPN to secure data has rarely, if ever, come into question. And today, through advancements in the technology's infrastructure, IPsec VPN has become easy to use, while still retaining superior security. This chapter looks at how an IPsec VPN delivers on that promise.

Looking at Why IPsec VPN is So Secure

Perhaps the single most beneficial aspect of an IPsec VPN is its robust functionality. IPsec is a protocol suite designed for securing Internet Protocol (IP) communications, and it allows for a wider spectrum of standards-based, open protocols and authentication algorithms than SSL VPN. The basis for SSL VPN is Transport Layer Security (TLS). Because SSL VPN isn't a standard, every

vendor provides a proprietary technology. SSL VPN is browser based; it's more susceptible to common Internet threats. For example, phishing sites could be used to hijack user logon authentication.

Conversely, registered IPsec VPN users seldom have to worry about such processes being handled incorrectly or malfunctioning. High expectations are placed on mobile workers to perform their tasks as if in the office, and IPsec's ability to offer secure access to the complete network is a better choice for this type of user than SSL VPN, which offers access to just specific resources.

IPsec represents a transparent pipe to all protocols and applications, ensuring secure access to the largest number of registered devices. IPsec VPNs are capable of integrating superior security standards across a wider array of protocols, including the web-based applications that SSL VPNs are so well known for handling. With IPsec VPN, the experience for the end-user is just like you're in your own office, regardless of where around the globe you're currently located.

The implementation of an IPsec VPN was once considered extensive and labor-intensive; however, this perception is actually caused by the meticulous process inherent in making sure every end-point on the network is accounted for. In order to further increase security, the VPN software is uploaded to each designated device on an IPsec-enabled network. On the other hand, an SSL VPN is more browser-based, but unless only web proxy functionality is performed, SSL VPNs also require a client and therefore similar user client privileges on the device.

While an SSL VPN client is delivered via a browser, which eliminates the need for additional software, this also makes it more vulnerable to outside and unwanted threats that can be caused by browser hijacking — a problem preempted by IPsec VPN.

Adding Security Functions

CIO/CSOs and those in charge of information security can tie additional security functions onto IPsec clients, making malicious attacks much harder to accomplish. Examples of such additional security functions include a managed endpoint dynamic firewall, hotspot logon to keep the client secure in hostile environments, and endpoint protection policies, ensuring that the client has all the relevant security components operational at all times. When these additional security functions are combined with IPsec's exclusive nature regarding client interactions, the VPN essentially acts as a guarded gatehouse, prohibiting unwanted visitors.

To the economically minded CIO/CSO, these added security features may lead to the assumption of higher operational costs with IPsec VPN. Fortunately, recent advancements in IPsec technology have mitigated procedural overhead.

When evaluating remote access VPN solutions, look for a high degree of integration that delivers high-end security with operational efficiency and cost effectiveness. Consider whether the solution provides integrated IPsec or hybrid IPsec/SSL VPN management technology incorporating efficient control over rollout, configuration and management of the client, seamless integration into existing identity management platforms and

processes, and full automation of user provisioning. See Chapter 4 for more information on central management.

With the rise of the global workforce and the recent proliferation of mobile devices owned and operated by employees, both at home and in the office, the decision on which VPN to employ is critical. IPsec is undoubtedly the most secure, robust, and transparent network widely available to businesses.

Organizations that don't have an IPsec VPN or hybrid IPsec/SSL VPN on the table when considering remote access solutions are, ultimately, putting their data and the trust of their various stakeholders at risk.

Chapter 4

Understanding IT Department Challenges

In This Chapter

- Seeing the range of requirements
- Looking at the point solution patchwork
- Making sure you can manage clients centrally
- Finding a solution to remote access VPN challenges

Information Technology (IT) departments face a whole host of challenges in trying to provide all the computing-related services a modern organization needs. Adding remote access VPN that accommodates the needs of a broad range of users while at the same time avoiding overtaxing existing systems or budgets can seem like a huge task. This chapter looks at some of the challenges faced by an IT department in implementing remote access VPN solutions.

Meeting a Wide Range of Requirements

People use many different types of devices to access data. These different types of devices use many different flavors of operating systems, and this diversity can be a real challenge for an IT department that has been tasked with offering a remote access VPN solution for the organization's users. For example, different users may have devices with any of the following operating systems:

- Windows 32/64 bit
- Linux
- OS X and iOS
- Android
- Windows CE
- Windows Mobile/Windows Phone

Each of these different systems has different requirements and capabilities. Applications that run on one of these systems can't simply be used on most of the others. As a result, you either need experts who can create native applications for each supported device type, or you need a remote access VPN vendor whose product can provide such support.

In addition to the many different types of operating systems in use on the various devices, those devices use a number of different methods for connecting to remote access VPN solutions. For example, some of the connection methods may include the following:

- Wired Ethernet connections
- Public Wi-Fi hotspot connections
- 3G or 4G (LTE) cellular data connections

Look for a remote access VPN solution that provides support for all operating systems and various devices and that uses a common one-click logon GUI.

Consider the requirement that your remote access VPN solution supports a broad range of user abilities, too. Sure, some of your users may be quite technical, but others may have a more difficult time using technology. The best solution will be one that's easy for everyone to use.

Understanding the Point Solution Patchwork

Too often, IT departments are under pressure to provide immediate solutions to meet the needs of users. This pressure can lead to quick decision making without giving a lot of thought to the future implications of those decisions. A prime example of this process happens when executives demand that the IT department provide users with remote access VPN to meet the latest need of the day.

The evolution of a mobile workforce and lack of proper planning has often led to IT departments having to support a patchwork of remote access VPN solutions. For example, your IT department may have implemented an IPsec VPN solution from one vendor for the users who need full network functionality. And subsequently, you may have implemented a remote access VPN solution from another vendor that uses SSL VPN for other users who only need web-based access.

Make sure the solution you choose protects your investments. For example, if you change vendors you don't want to have to throw out

your existing remote access VPN solution and switch to one supported by your new vendor. Instead, look for a solution that isn't locked to one vendor and works with third-party VPN gateways.

Managing Clients Centrally

Managing a network is a complicated task for administrators because networks are complex and require a lot of attention and maintenance. As users become more dependent on mobile devices, managing all these devices and users can be overwhelming. A good way to take complexity out of the equation is to implement centralized remote access VPN management for both IPsec and SSL VPN.

With a central remote access management system, one IT administrator can easily manage the network and the users who access it. This ease results because many tasks associated with managing remote access VPN can be simplified and automated. For example, a central VPN client management solution with a single point of administration makes it possible to integrate with your existing user database (such as Active Directory) to centrally manage user configurations. Clients can be automatically configured after they're authenticated as users. A central client management solution also makes it possible to automatically deploy new clients, provide updates to existing clients, and even remove clients.

When considering remote access VPN solutions, look for the ability to centrally manage users with a single point of administration to automatically roll out clients and updates and that supports a broad range of platforms.

Looking at a VPN Client

A good VPN client automatically searches for the best available network and changes to better communication mediums as soon as they're available. This capability is known as *seamless roaming* and allows devices to automatically change between 3G/4G, Wi-Fi, and LAN networks and dynamically redirects the VPN tunnel without interrupting mobile computing sessions.

Figure 4-1 shows an example of a VPN client that has common functionality across devices.

Figure 4-1: The NCP VPN clients look similar and work the same on different types of devices.

Typical remote access VPN solutions leave connection details to the end user. Often, making such a connection can be quite confusing for users, resulting in both frustration and increased technical support costs when users contact the IT department to ask for help.

Look for a VPN client suite that includes an Internet connector and personal firewall, and is designed to plug-and-play, remove all complexity for the user and maintain reliable connections.

Chapter 5

Looking at Today's Secure Remote Access Landscape

In This Chapter

- Seeing today's patchwork
- Coping with security
- Taking control of the costs
- Understanding management's issues
- Dealing with users

Remote access VPN technology has been around in various forms for a number of years. This chapter takes a look at the current state and discusses the issues organizations must face.

Avoiding the Point Solution Conundrum

It's easy to get bogged down in a patchwork of solutions that each addresses only a single aspect of your remote access VPN needs. In this type of scenario, you end up needing to document and support a bunch of

different products at the same time. The end result is often confused and frustrated end-users, which leads to IT department headaches.

Instead of separate IPsec and SSL VPN solutions, confusing and different connection interfaces for each different type of 3G card, and different administration tools, consider a comprehensive hybrid IPsec/SSL VPN solution that incorporates one central management console and presents users with a common GUI no matter what type of device or OS is being used.

Choose a remote access VPN solution that includes central client management. Your IT staff shouldn't have to memorize the differences between client device operating systems, or VPN client GUIs. With NCP's solution, users have a similar client experience, including Path Finder and Friendly Net Detection, which greatly reduces their need to call the help desk to get network access.

Dealing with Security Loopholes

Network security is a top priority for every IT manager today. When IPsec and SSL VPN are deployed as separate point solutions, you have more endpoint security risks to consider. If you can't maintain complete, bulletproof security for all traffic between your remote users and your VPN gateway, you won't be able to ensure the security of anything on your network.

Attackers may attempt to gain access to your network in a number of ways. They may attack the remote device if there's any vulnerability, such as a missing or inadequate firewall. If your encryption is weak,

attackers may intercept data as it passes between your remote users and your network. Or they may take a more direct approach by disguising themselves as employees or entitled remote access users.

Consider a VPN client that includes a firewall to increase the level of end device security. Features to look for include location awareness, application-specific filter rules, and secure hotspot logon.

Optimizing Flexibility

Is the solution you're considering flexible enough to meet your needs as conditions change in the future? Consider a solution that's easily scalable so it can support an expanding user base.

Generally speaking, a software-based solution is more flexible and scalable than a hardware-based solution. You can easily back up, replace, or upgrade a software-based solution without having to replace expensive hardware-based components. You can also run the whole VPN solution in a virtual environment.

An important part of the flexibility equation relates to the VPN client suite and a central management console. Look for a client suite that integrates the VPN, a personal firewall, and the Internet connector into a single, one-click logon GUI. Similar to the client side, you could work with a mixture of different GUIs from different suppliers on the central side to set up remote users or operate the system. A more flexible approach is a central management console for user directory, certificates,

endpoint policy, and software rollout that provide a single point of administration. This approach provides a good overview and forms the basis for fast troubleshooting.

Reducing Costs of IT System Infrastructure

IT departments are in the unenviable position of having to control costs while providing the services necessary to enable productivity and keep the corporate network secure. Advantages do exist to providing a hybrid IPsec/SSL VPN solution (check out Chapter 2 for more info). Unfortunately, providing both IPsec and SSL VPN is often achieved by implementing two different solutions. This doubling-up of solutions increases both acquisition and support costs, which can be avoided by implementing a hybrid IPsec/SSL VPN.

Your users also need a way to connect to the Internet to initiate the remote connection, and this connection needs to be addressed if it isn't provided as part of the VPN client. A personal firewall is also required to prevent network threats. In addition, you may find that you need things like One Time Password (OTP) tokens or security certificates for user authentication. OTP tokens can be quite expensive on a per-user basis. All these extra details add up to increased purchasing, training, and end-user support expenses.

OTP tokens are part of a two-factor authentication system and can be hardware, such as a USB dongle, or software specifically assigned

to a particular computer user. Tokens generate authentication codes at fixed intervals by using a built-in clock and a factory-encoded key (or seed). The seed for each token is unique and is recorded on a secure server when the token is purchased.

To avoid the added cost of OTP tokens, look for a remote access VPN solution that can send a dynamically created, session-dependent OTP or key via a text message. This alternative method of sending the authentication key can greatly reduce the cost of a solution compared to one that uses OTP tokens and increase the level of security.

Seeing Management Headaches

Complexity and security are only two of the headaches management faces in implementing a remote access VPN solution. User training and support can be a real nightmare when you're faced with a broad base of remote users with a variety of different device types. Consider, for example, how differently the VPN connection and sign-on process would be for users of Windows-based laptops, Android smartphones, and iPads. Now, throw into that mix the possibility that those users may try to connect over a 3G or 4G connection, through a public Wi-Fi hotspot, by using a client's Ethernet port, or even from their home offices through a wireless router. Supporting all these different scenarios across a mix of remote access VPN solutions would be a real nightmare without a common one-click logon GUI.

Coping with Frustrated End Users

Consider the situation of the end-user who must navigate a confusing set of steps simply to log on to a VPN connection. Unfortunately, because each 3G card supplier has its own GUI, users see differing logon interfaces. In addition, each required click represents an opportunity for error, so the typical process of establishing a remote access VPN connection can be very frustrating for end-users.

Products such as NCP's Secure Client Suite can solve many connection issues. For example, instead of requiring end-users to wade through a maze of screens to make a connection, the NCP Secure Client Suite layers the details behind a common GUI that enables the user to log on with one click. In addition to reducing end-user frustration, this single-click logon reduces management's burden of documenting and training users on a whole bunch of differing user GUIs.

Chapter 6

Ten Reasons to Choose NCP for Your Solution

In This Chapter

- Choosing NCP for your secure remote access VPN
- Seeing a good vendor in action

If you've been reading this book straight through, you've read about what to look for and what to avoid in choosing a remote access VPN solution to suit your needs. This chapter highlights NCP's solution and tells you why it should be on your list to check out for your secure remote access needs. Take a look at this list of NCP offerings:

- **Hybrid solution flexibility:** NCP's secure remote access solution supports both IPsec and SSL VPN (covered in Chapter 2). This dual support makes it easier to provision your security policies related to your remote user types.
- **Superior security:** IPsec follows well-known standards and NCP strictly implements relevant standards. NCP is the only company singularly focused on secure remote access VPN and is

continually innovating in the areas of the VPN client suite, hybrid IPsec/SSL VPN server, and remote access VPN central management.

- **Freedom of choice regarding mobile devices, operating systems, and security gateways:** NCP provides universal support for all client operating systems and mobile devices by using a common, intuitive one-click logon GUI and the ability to use the client with all common IPsec VPN gateways, including Cisco, Juniper, Check Point, and so on. NCP helps you manage user access universally with maximum investment protection. Check out Chapter 4 for more information on these areas.
- **Central management:** NCP Secure VPN Enterprise Management is the hub of a comprehensive remote access VPN solution. It provides centrally managed IPsec/SSL VPN, client provisioning, and end-user configurations as well as personal firewall management without compromising ease of administration. NCP Secure VPN Enterprise Management works with the NCP Secure VPN Enterprise Server as well as third-party IPsec VPN gateways.
- **Single point of administration:** Integrate with your existing user database (such as Active Directory) to centrally manage user configurations. Clients will be automatically configured after users are authenticated.
- **Fast rollout and easy updates:** A quick download and simple install procedure across a broad range of device types make it easy for users to begin using the NCP client and move to new versions without further efforts.

- **Automated change management:** The NCP central management server automatically detects when the software on a client device needs updating, so users don't have to be individually informed and manually apply any needed updates.
- **Increased productivity:** The NCP universal one-click VPN client is designed to be easy to use, administer, and provide reliable connections and maintain them even while roaming between networks (seamless roaming).
- **Reduced help desk calls:** With NCP's solution, users have a similar client experience including Path Finder and Friendly Net Detection, which greatly reduces their need to call the help desk in order to access corporate resources. Check out Chapter 5 for more info.
- **Reduced documentation and training costs:** There's no need for a thick user manual covering many different possibilities because the NCP solution layers the details behind a common interface. Training costs are reduced because users only need to know to click a single button.

IPsec & SSL

Two Sides of the Same VPN Coin

IPsec and SSL VPN each have their advantages and specialties. What if there was a hybrid solution that provided both IPsec and SSL tunneling? The NCP Secure Enterprise Solution, comprised of a VPN client suite, hybrid IPsec / SSL VPN server and remote access VPN management system, fills this need. The 100% software solution was developed from the ground up to be interoperable with all major network-layer security technologies, including VPN gateways and firewalls, preventing vendor-lock pitfalls.

www.ncp-e.com

Next Generation Network
Access Technology

NCP
SECURE COMMUNICATIONS

Simplify remote access management and reduce cost

Efficiently managing remote access with limited IT resources can be overwhelming and lead to headaches. This book helps you identify the best remote access solution for your business.

- ***Discover how secure IPsec and SSL VPN have evolved and led to hybrid solutions — today's remote access landscape***
- ***Grasp the security benefits of IPsec — get more robust functionality than SSL VPN***
- ***Choose the right remote access VPN solution — look for hybrid IPsec/SSL tunneling with central management***

Open the book and find:

- **How a hybrid solution maximizes flexibility**
- **How central management increases efficiency and reduces cost**
- **IPsec VPN security functions to thwart malicious attacks**
- **How to improve IT productivity**

Go to Dummies.com®
for videos, step-by-step examples, how-to articles, or to shop!

FOR DUMMIES®
A Wiley Brand

ISBN: 978-1-118-91425-0
Not for resale