Understanding Secure Virtual Private Networking

Understanding Virtual Private Networks

Introduction

The Internet has revolutionised communication by providing platform independent global electronic mail together with access to unimaginable amounts of online information via the World Wide Web. Consumers using dial connections to send and receive email and to access online information fuelled the second phase of Internet growth. Now the Internet is entering a new phase of growth and is being used as a viable and widely available transport mechanism for mission critical business solutions. It has always been possible to use the Internet to provide communication between geographically separate networks and computer systems such as the early university networks. Only recently has it been possible to use the Internet to provide secure and *private* communication between business systems.

The fact that in certain parts of the world it is far easier to obtain an Internet connection than it is to get an international or even national point to point leased line, has led many companies to explore the use of secure communication through the Internet. Interest in Virtual Private Networks or VPN's has reached the point where in 1997 the worldwide market for VPN's was an estimated $200Million and is predicted to grow to almost $12Billion by the year 2001.

Why should there be such dramatic growth in the deployment of VPN's? The answer is easy, VPN's can significantly reduce expenditure on fixed costs. By implementing VPN technology it becomes possible to economically connect intra office networks, provide secure cost effective remote access and provide all company locations secure access to the same key internal resources. In addition it is possible for a manufacturer to provide links to strategic suppliers and for example, to allow stock or product design information to be exchanged without the worry that the information might be stolen or copied as it traverses the public networks. It is possible to provide the same connectivity using technologies such as Leased Lines, ISDN and Frame Relay, but they are more difficult to manage, less secure and more expensive

What is a VPN

Virtual Private Networks (VPN's) allow you to establish secure data communications between multiple networks or network devices using insecure public networks such as the Internet or public Frame Relay networks as the underlying infrastructure. It can be argued that VPN security is significantly better than that provided by dedicated connections such as leased lines or Frame Relay networks because VPN's use encryption to scramble data and ensure that for all intents and purposes it is impossible for a third party to unscramble it. Other users who share the same network and malevolent users who would seek to steal information cannot access the data without the appropriate keys to decrypt scrambled data packets.

Flexibility and Cost Savings

VPN's also offer incredible flexibility and potentially massive cost savings because of their ability to connect between geographically separated end points by using the Internet. The cost savings are achieved by connecting to an Internet Service Provider (ISP) at each network location and by encrypting the data that passes through the public Internet. This means that rather than paying for international leased lines between say, London and Johannesburg, you pay for a local connection to your ISP at each end of the connection and use the Internet connections between the ISP's. Figure 1 shows a network in London connected to a network in Johannesburg using dedicated leased lines. Contrast this with the VPN equivalent shown in Figure 2.

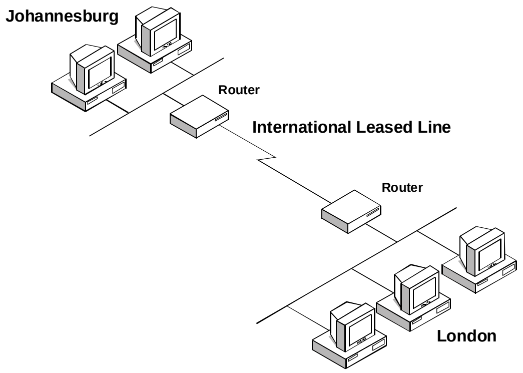


Figure 1

A 128Kbps leased line connection between London and Johannesburg could cost as much as $230,000 per year[1]. Figure 2 shows how using local connections to an ISP and the Nokia IP400 can provide the same connectivity using a secure, reliable connection through the Internet. Although additional equipment is required to provide the VPN functionality, the savings made on the recurring line charges more than pay for any additional start up costs. Typically a local ISP connection at each end of the link would cost less than $20,000 per year representing a saving of at least $190,000 in annual network charges.

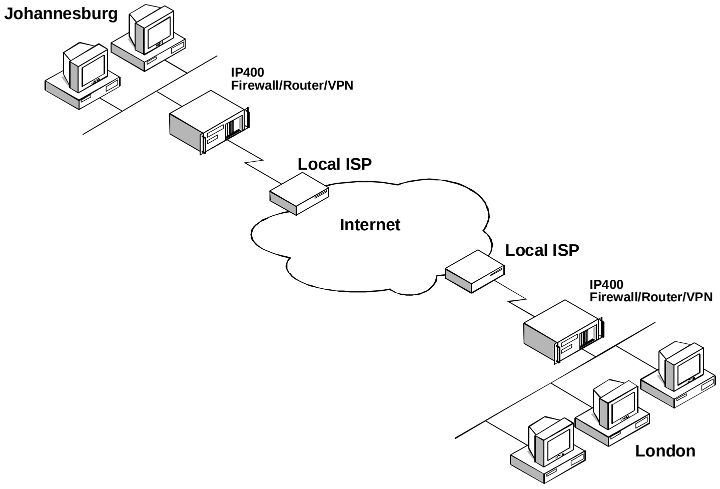


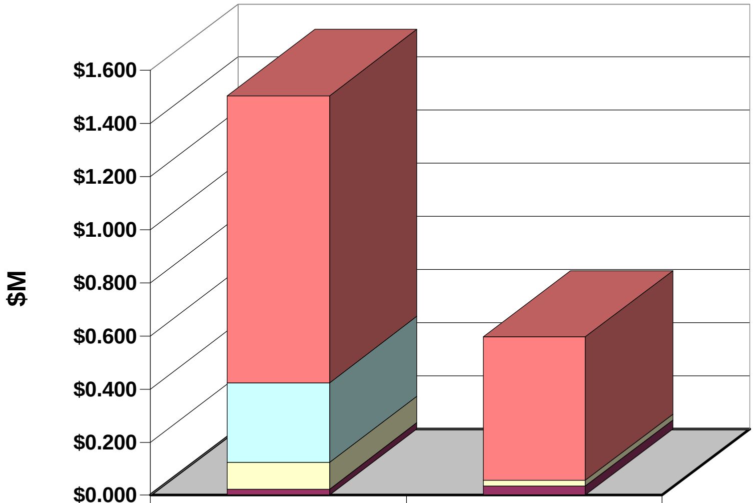
Figure 2

These savings are typical and are given for a single link between London and Johannesburg. The cost savings between other International locations can be even more attractive. For example a dedicated 256Kbps Link from New York to Tokyo could cost as much as $370,000 per year, by using VPN's savings of at least $300,000 can be made in annually recurring charges.

Using the Internet as a direct replacement for other more traditional forms of connectivity such as leased lines, ISDN and Frame Relay is becoming a compelling financial argument. Combining the cost savings with the additional flexibility and new services that can also be implemented and VPN's become a business decision that is difficult to ignore. Common uses for VPN's include the ability to provide connectivity between manufacturers and suppliers and to provide low cost Inter site communication for services that do not require absolute bandwidth

[1] Source - Grid Technologies.

guarantees. These kinds of networks have become known as Extranets because they extend the reach of corporate networks and allow connections between manufacturers and suppliers that may have been prohibitive using conventional networks. In a recent study, Forrester Research compared the cost of connecting 1000 users with Remote Access Servers (RAS) and conventional office equipment with the cost of connecting the same users through the Internet using VPN technology. The results demonstrated that over $900 per year per user, *close to $1M per year in total* could be saved. Figure 3 details these findings.



	Traditional Remote Access Costs ($M)	VPN Costs ($M)
🟥 Phone/ISP charges	$1.080	$0.540
□ User Support	$0.300	$0.000
🟨 Capital Expense	$0.100	$0.022
🟪 T1 Lines	$0.024	$0.034
🟦 Total	$1.5	$0.59

Source Forrester Research Inc.

Figure 3 Annual cost to Support 1000 users

Companies planning to use the Internet for corporate traffic tend to be concerned about performance. This is a genuine concern because it is not yet possible to provide end-to-end guarantees with respect to reliability, delay and bandwidth. However, the good news is that Quality of Service is an issue that is being addressed by a number of the Internet Engineering Task Force (IETF) working groups[i]. Many ISP's are global organisations and have their own high bandwidth backbones. For connections that remain within their domains, many Service Providers are able to offer performance guarantees through Service Level Agreements (SLA's). Bandwidth management and Quality of Service are also facilities offered by the IP 400 which can manage bandwidth used by network applications at the ingress and egress points of a public network and can control end-to-end bandwidth on private networks.

In addition to the VPN functionality we have discussed, VPN's can also provide authenticated access to corporate resources for local, remote and mobile users. The Internet is still used as the secure transport mechanism, but users are authenticated to ensure that they are who they claim to be. Once a user has been authenticated, it is possible to limit the users access rights - essential when working with contractors, external suppliers, e-commerce applications and when dealing with any secure information.

A typical example of mobile user authentication might be an international sales person. Rather than using expensive international calls over the public telephone network, they make cheaper local calls to an in country ISP, establish a secure path over the Internet and are authenticated at the corporate site.

Figure 4 shows a mobile user who has established a secure connection through the Internet. Software on the users machine interacts with the Nokia IP400 to ensure that data remains secure and at the same time validates the users access to the corporate systems.

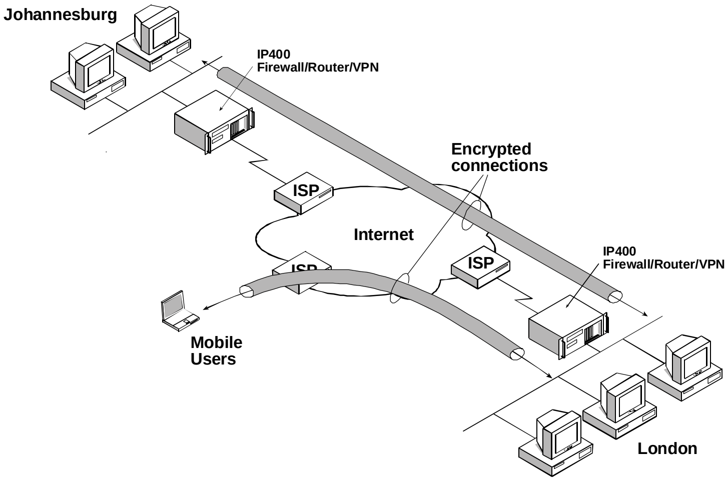


Figure 4

The same software that is used to provide authentication for the mobile users can also be used to control access to corporate resources for both remote and local users. In fact a network wide security policy can be implemented permitting users access to only those systems to which they have been granted access, regardless of where in the organisation they are connected. This allows complete security to be implemented for fixed, roaming and mobile users with minimum work and considerable cost benefits.

Elements of a VPN

From the previous discussion it can be seen that a number of essential features are required in order to implement a secure and reliable VPN.

1. It is necessary to ensure that all data passing over public networks is secure and passes integrity checks. Integrity checks affirm that the data has not been tampered with in transit.
2. Local, Remote and mobile users must be authenticated to ensure that they are who they claim to be.
3. Users should only be given access to those systems that they need to have access to.

These key elements of a VPN and how they can be realised are described below.

Link Encryption and integrity

To ensure that data passed between sites and over public networks remains secure a variety of different techniques may be used. Various tunnelling schemes are in use and these tend to wrap the original data (including headers) inside another data frame. Although many tunnelling schemes use some form of authentication, most do not encrypt the original data. Once a hacker has gained access to the data, there is nothing to stop them reading the plain text and stealing the information. The most secure method of sending data over a public network such as the Internet is to use a device that can provide robust link encryption between the various locations such as the Nokia IP 400 family. The use of encryption guarantees that even if a third party does capture part or all of the datastream, the message cannot be read because data is scrambled using secure encryption mechanisms.

A number of different encryption methods have to be used in order to cater for the restrictions various national governments place on its use. The most well known scheme is DES (Data Encryption Standard) originally developed by IBM in the USA.

Most encryption schemes are only as strong as the key length. If I can guess the key used to encrypt the original data, I can apply the key to the encrypted data and extract the original message. The importance of key length can best be illustrated by an example; some time ago my boss received a promotional piece of junkmail. This one was slightly different because he was sent a locked moneybox, locked by a combination lock that he didn't have the combination to. The company promised to call at the end of the week with the combination to the lock. If, when the box was finally opened, it contained a lucky number he would have won the prize. All he had to do was answer a few simple questions and presto he gets given the combination.

Our team couldn't wait until the end of the week, so one day when he was at lunch, we each took a turn at entering the correct combination. This lock had three rings and so there were potentially 1000 different combinations (000-999). We managed 1 combination every 5 seconds and cracked the code after only 35 minutes. It was then easy to substitute the enclosed promotion for one that promised a vacation to the Bahamas. This of course caused concern for the promotional company and problems for us when we confessed to our little "joke". The important thing to note about encryption keys is that the longer the key length, the harder it is to guess the key. At 5 seconds per combination it would have taken one and a half-hours to check every possible sequence. If there had been 5 rings there would have been 100,000 combinations a daunting 138 hours to check every possible sequence.

IBM originally proposed DES with a 112 bit key to the National Bureau of Standards, after discussions with the National Security Agency (NSA) a US government department, IBM agreed to reduce the key length to 56 bits. In theory the reduced key length makes DES encrypted data easier to crack, but to do so you need enormous computing power and plenty of time. The US government regards encryption as a strategic security issue and has banned the export of products that use a 56-bit key. Therefore products exported from the US that use DES make use of a 40-bit key. Of course, products developed outside of the US that use DES are not subject to US export restrictions. If you would like further information on cryptography, Bruce Schneier[ii] has produced what has become the de facto cryptography reference.

Encrypting data ensures that it remains private when sent over public networks. It also guarantees the authenticity and integrity of the data. The only way that sending and receiving parties can encrypt and decrypt the data is if they have access to the each other's keys and can be sure that the other party is whom they claim to be. This way you know who the data is from and that it cannot have been tampered with en-route.

Authentication

So now we have this nice secure encrypted path over the Internet between two or more sites. We may even be linking external contractors to corporate information systems. How then do we ensure that users are who they say they are and only allow them to access the systems we want them to? We could use usernames and passwords, but these are usually easy to guess and easy to steal or borrow. There are many industry standard authentication schemes such as Radius and SecurID and these schemes typically use a two part user authentication mechanism. The user must know something such as a PIN code and must have something such as a token. Without both parts of this system, a user is not allowed access to the network. The token part is usually a small credit card like device that generates a unique code valid for a very short period of time. The user enters the code from the Token together with a PIN code known only to the user and is then uniquely identified to the system. This prevents the shortcomings of most username/password schemes because without the unique code from the token the PIN code is useless.

Controlling Access to Resources

There are many different types of VPN product available, most simply provide encryption of the traffic as it traverses a public network. Of course, this is a great way of protecting private data; however, encryption is only part of the story and does not take into account access control. Without adequate access controls all users of a secure link have access to the same network resources. For a manufacturer providing links to suppliers, the manufacturer should ensure that a given supplier has limited access to the applications and information that they need and nothing more.

By combining access control with user authentication and link encryption we can be reasonably sure that the data is secure, it came from a known source, the users are whom they claim to be and they are only allowed access to the systems that they are authorised to use.

The Nokia VPN Solution

The IP400 Series from Nokia is the industry's best-performing and most flexible integrated firewall/router. Ideally suited to provide secure Internet connectivity, the IP400 Series combines high-performance IP routing with a complete implementation of the Check Point Firewall-1 enterprise security suite. Check Point is the market leader in Firewall solutions, commanding over 44% market share[2]. The Nokia IP400 Series is the only networking platform to support the complete FireWall-1 version 3.0 feature set including Check Point's award-winning FireWall-1 inspection module, integrated network address translation, authentication, encryption (enabling VPN support), firewall synchronisation and server load-balancing.

Products such as the IP400 Series and Check Point Firewall-1 make it easy to establish network wide security policies with single console control of a security domain. The IP400 allows fully redundant high performance installations that eliminate the need for multiple boxes each performing a discrete function. The IP400 and Firewall-1 provide Encryption, High Availability, Authentication, Routing and Management in a single easy to use package.

In conjunction with Firewall-1, the IP400 Series supports the use of different encryption schemes to different destinations over a single Internet connection. This allows 56 bit DES to be used inside the USA and 40 bit DES on links to or in other countries such as Japan. Check Points proprietary FWZ (40bit) can be used on links to countries that do not allow the use of DES. A single platform makes management and support far easier. One product with a single user interface

[2] International Data Corp 1997

rather than separate products each with their own management systems, key management systems, user interfaces, training and support requirements.

High Availability

The combination of Firewall synch, VRRP and high performance routing has enabled Nokia to deliver a unique High Availability platform. Most high availability solutions are simple hot standby solutions that require expensive duplicate software and hardware to stand idle until the main firewall fails. The IP440 solution allows multiple active firewalls to share the traffic load and at the same time provide a highly resilient solution. The use of load balancing routing protocols such as OSPF and BGP enables multiple redundant links to the Internet/Intranet to be used. Single or multiple service providers can be used and apart from additional IP440's, no extra hardware or software is required to enable HA solutions.

Summary

Implementing a VPN does not have to be an all or nothing scenario. It is possible to gradually migrate to a VPN on a link by link basis and to run VPN links in parallel to conventional leased line connections. It is even possible to use VPN's as a fallback should conventional network connections fail. One of the most compelling reasons to use a VPN has to be the cost savings that can be realised. Payback is usually measured in months rather than years and the added flexibility and control provide a company independence from the rigid structures of normal network suppliers.

A typical VPN user might have the need to connect multiple locations that would normally use dedicated or switched network connections, might have a geographically diverse network including both national and International locations and would have applications that do not have specific bandwidth and latency requirements.

The Internet is a global resource with connections available in practically every country. VPN's offer the user a highly flexible and managed way of building corporate networks allowing users to make adds, changes and deletions almost instantly and permitting remote locations and even suppliers to be completely integrated with corporate security policies. This can all be managed via a simple easy to use Graphical User Interface from a single location or console and with connections between sites being assigned on a temporary or permanent basis.

The VPN's described in this document combine Encryption, Authentication, Access Control, Traffic Management, Routing and High Availability into a single cost effective platform. Previous VPN implementations were cumbersome to administer and had clumsy or insecure key management schemes.

Careful cost management and tight fiscal controls demand that any solution offering equivalent connectivity, higher security and lower costs should be closely examined. The cost savings that can be achieved by using VPN's are potentially very large providing payback in weeks or month.

The combination of ease of use, cost savings and security make VPN's difficult to ignore. These elements, combined with the experience and expertise of Nokia make a compelling argument for change.

If you would like to find out more about the Nokia IP400 family and how we can help you with your VPN requirements, please visit our web site at http://www.iprg.nokia.com or contact us at one of the addresses below.

[i] Differentiated Services Working Group http://diffserv.lcs.mit.edu/

[ii] Applied Cryptography Second Edition – Bruce Schneier. Wiley ISBN 0-471-11709-9

NOKIA IP - WORLDWIDE HEADQUARTERS
232 Java Drive
Sunnyvale, CA 94089
USA
Phone: +1 408-990-2000
Fax: +1 408-743-5675
Email: sales@ **iprg.nokia.com**

NOKIA IP - EMEA HEADQUARTERS
2 Heathrow Boulevard, 284 Bath Rd.
Heathrow, Middlesex UB7 0DQ
England
Phone: +44-(0)181-564-3900
Fax: +44-(0)181-564-3939
Email: Euro-sales@ **iprg.nokia.com**

Visit us on the Web: http://www.iprg.nokia.com