



MAKING THE INTERNET  
WORK FOR YOU

---

# IP Virtual Private Networks (IP VPNs)

*The smarter way to extend your enterprise network securely, easily and affordably*

---

**Sify Limited**

Tidel Park, II Floor,  
4, Canal Bank Road, Taramani,  
Chennai - 600 113.  
INDIA.  
Tel.: +91 44 22540 770  
eMail: [esbmarketing@sifycorp.com](mailto:esbmarketing@sifycorp.com)

*A White Paper from Sify Enterprise Solutions.*

*January 2003.*

Copyrights, Sify Limited. 2003

## TABLE OF CONTENTS

---

Executive Summary .....	Page 3
Extending Your Enterprise Network .....	Page 4
IP VPNs Demystified .....	Page 5
IP VPNs: As Secure As It Gets .....	Page 6
Boost Your Workforce Productivity and Supply Chain Efficiencies .....	Page 7
Choose The Right Service Provider .....	Page 8
Conclusion .....	Page 9

*This white paper addresses the topic of Internet Protocol based Virtual Private Networks (IP VPNs) and describes their business benefits to large and medium sized enterprises in India.*

*This paper covers a number of areas starting with an explanation of how IP VPNs work, why they are secure and their technological and cost advantages over legacy networks. The paper also briefly describes the SecureConnect™ series of IP VPN solutions from Sify.*

*Finally, this white paper is not meant to be a design guide but is intended for the CXO & senior management audience involved in technology management decisions.*

*Comments and inquiries on the subject can be forwarded to:  
**[esbmarketing@sifycorp.com](mailto:esbmarketing@sifycorp.com)**.*

## EXECUTIVE SUMMARY

*The cost, complexity and tedious nature of legacy Wide Area Network (WAN) technologies has hindered companies from extending the network to include remote sites, traveling employees, telecommuting employees and business partners such as suppliers, distributors or dealers.*

*IP VPNs have overcome the problems of heritage networks by offering a secure, scalable and reliable way to extend your network by using a shared IP network of a service provider like Sify.*

*IP VPNs offer an opportunity to save up to 45% of the total cost of ownership (TCO) when compared to a private line network.*

*When choosing a service provider, it is important to understand the depth of expertise that the provider brings in the arena of data networking services.*

## TERMINOLOGY INDEX

IP - Internet Protocol  
 VPN - Virtual Private Network  
 ATM - Asynchronous Transfer Mode  
 PVC - Permanent Virtual Circuits  
 DES - Data Encryption Standards  
 IPSec - Internet Protocol Security  
 L2TP - Layer 2 Tunelling Protocol  
 PoP - Points of Presence  
 GSR - Gigabit Switch Router  
 WAN - Wide Area Network  
 TCO - Total Cost of Ownership  
 IDC - International Data Corporation

Given the cutthroat nature of competition today, enterprises worldwide are constantly looking for means to cut costs, reduce capital expenditure as well as boost revenues. Enterprise Resource Planning, Customer Relationship Management and Supply Chain Management are some of the areas where companies have deployed enterprise wide mission critical applications, which in turn require robust and reliable networks to maximize productivity and efficiency.

The cost, complexity and tedious nature of legacy Wide Area Network (WAN) technologies such as ATM, Frame Relay and Private Networks (using leased lines) has hindered companies from extending the network to include remote sites, traveling employees, telecommuting employees and business partners such as suppliers, distributors or dealers. IP VPNs have overcome the problems of heritage networks by offering a secure, scalable and reliable way to extend your network by using a shared IP network of a service provider like Sify. IP VPNs have emerged strongly as a compelling alternative to legacy networks as evidenced by a large and growing end user base all around the world.

IP VPNs have built-in mechanisms that encrypt and encapsulate data within tunnels before sending it through the network, which make the data transmission highly secure. An added level of protection can be built in by deploying authentication methods that make use of digital certification technologies. By deploying secure IP VPNs in conjunction with digital certification services offered by an independent Certification Authority such as Safescrypt™, customers can not only connect their business partners to their corporate extranet, but can also conduct legally valid electronic transactions over the network in a highly secure manner.

Best of all, IP VPNs offer the enterprise customer an opportunity to save up to 50% of the total cost of ownership when compared to a private network with similar redundancy and any-to-any connectivity. The savings for a company with a large number of geographically dispersed locations can easily run into crores of rupees.

When choosing a service provider, it is important to understand the depth of expertise that the provider brings in the arena of data networking services. While telecom carriers tend to be broad generalists offering both voice and data services, it is likely that a data networking services "specialist" such as Sify will be better equipped to handle the rigors imposed on the network by your mission critical data applications. The track record of the vendor, certifications such as ISO 9001 as well as evidence of customer focus are strong indicators of the service provider's real ability to deliver on promises made during the selling phase.

Today's competitive environment calls for companies of all sizes to maximize productivity in order to grow revenue, cut costs, enhance customer satisfaction, boost bottom lines and survive economic slowdowns. It is the fittest who survive. To stay ahead, enterprises are deploying various mission critical applications from Enterprise Resource Planning (ERP) through Customer Relationship Management (CRM) to Supply Chain Management (SCM). With these mission critical applications requiring robust and secure network connectivity, networks today are the lifeline of a business. The evolution of internetworking technologies clearly has clearly been a key contributor to the vastly improved efficiencies within organizations. Networking is in. And it is here to stay.

In the battle for business supremacy and at times even survival, remote offices, mobility of employees, an extended supply chain and global reach have become key competitive advantages across industries. The actual location of employees, offices, factories and warehouses has become secondary because the internetworking technologies help to connect people and business processes in ways unimagined until a few years back.

On one hand, increased connectivity within the enterprise offers tremendous advantages and flexibility. But on the other hand, it also requires unassailable network security. Transmitting sensitive data across a public network such as the internet and allowing transactions to take place over an intranet or extranet is not without risk. If an unauthorized party disrupts or damages the corporate network or intercepts key files, the results can be costly.

#### THE DILEMMA OF LEGACY NETWORKS

A comparison of Wide Area Network (WAN) options across private lines, ATM, Frame Relay, and IP VPNs shows that while private networks are secure, they are also complex, cumbersome to set up and manage, and costly to maintain. And they are not usually flexible or scalable. Private networks, by design, are limited. Because a given private line links only two sites of a single customer in a point-to-point fashion (no one else can use that capacity), they deliver a secure but expensive and rigid solution. There is no way to connect a third site and have all sites interconnected in an any-to-any fashion without requiring each site to maintain leased line connections to each of the other sites. Further, users have to pay the same amount whether they run traffic for three hours or 24 hours a day.

Frame Relay or ATM networks are efficient when it comes to stable traffic patterns in a spoke-to-hub design. They work best where traffic flow is steady and predictable from the remote sites to the central

#### EXTENDING YOUR ENTERPRISE NETWORK

---

location. These approaches involve setting a permanent virtual circuit between each spoke and hub. Setting up numerous Permanent Virtual Circuits (PVCs) is costly and justifiable only if the PVC is expected to see high utilization. Consequently, these networks also tend to be complex, cumbersome and costly. Moreover, supporting IP along with legacy would mean higher overheads. Hence, the migration from legacy to IP in the entire network has to be a one-time event, and cannot be done piecemeal.

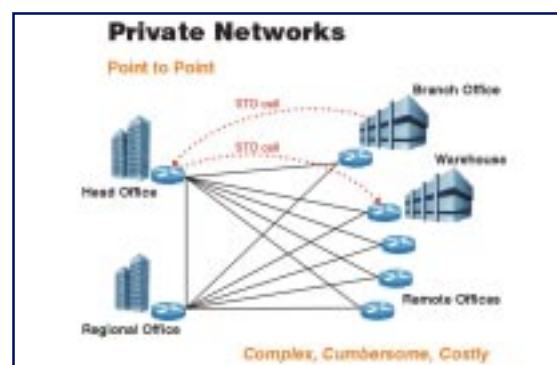
Simply stated, costs of legacy networks increase disproportionately as the complexity of the network increases. In contrast, IP-based networks are more efficient for mesh networks, where traffic flows in a many-to-many pattern. IP-based networks do not require PVCs, and users need not set up and adjust PVCs between communicating points. IP-based VPNs give the freedom and flexibility to scale a business quickly, easily, and cost-effectively.

Historically, the high cost and complexity of legacy networks based on private lines, Frame Relay or ATM hindered enterprises from fully extending their corporate networks to include remote sites, traveling employees or business partners such as suppliers, distributors or dealers. Today, the shackles have been removed and IP VPNs have emerged strongly as a compelling alternative for corporations who are looking to reap the rewards of a fully connected enterprise. Furthermore, concerns about the security of IP VPNs have been dispelled by the adoption of advanced techniques to ensure that IP VPNs are as secure as private line networks.

## IP VPNs DEMYSTIFIED

**I**P Virtual Private Networks (IP VPNs) are private partitioned networks that reside on and transport data over either a public network like the Internet or the managed IP network of a service provider like Sify. IP VPNs combine the security of a private network with the scalability and pervasiveness of the Internet. IP VPNs use shared facilities under software control that provide the appearance, functions, and benefits of a private network, including security, continuous availability and reliability.

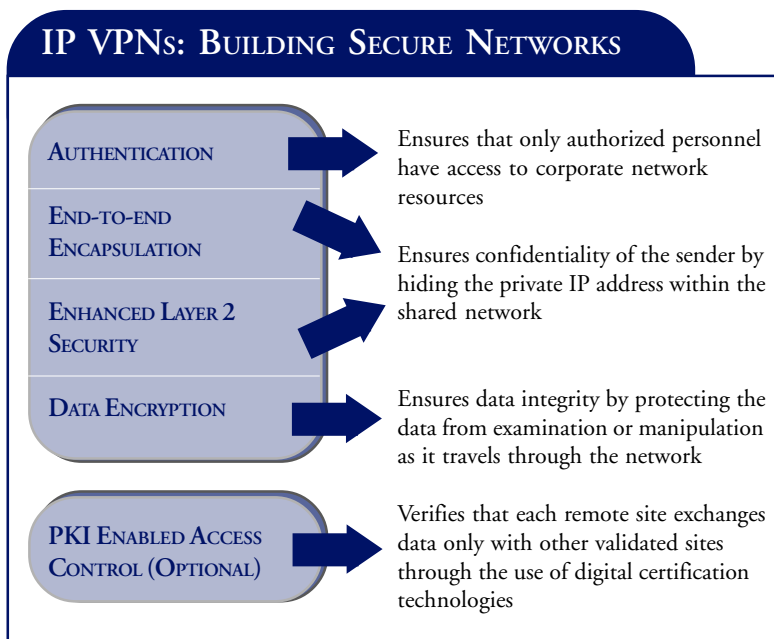
IP VPNs have built-in mechanisms to ensure that data traveling over the shared IP infrastructure is as secure as in the case of private networks. IP VPNs include measures for packet encapsulation (tunneling), encryption, and authentication to ensure that sensitive data reaches its destination without tampering by unauthorized parties. When customers choose IP VPN services from a provider like Sify, their data is routed through SifyNet, Sify's managed IP network which ensures that the data is not exposed to all and sundry, as would be the case with an public internet based VPN.



**IP VPNS: AS SECURE AS IT GETS**

What makes an IP Virtual Private Network “private” is a tunnel that is created during a VPN session. The term “tunnel” implies some sort of a fixed path through a network. But, that is not the case. Since your traffic is IP-based, it is likely that your VPN packets might take different paths through the network. What makes the IP VPN transmission a tunnel is the fact that only the recipients at the other end of your transmission can see inside your protective encryption shell. Tunneling technology encrypts and encapsulates your own network protocols (which may be other than IP) within IP. While IP Security (IPSec) and Layer 2 Tunneling Protocol (L2TP) are two widely used tunneling methods, IPSec has emerged as the technology of choice among IP VPN users today.

Encryption is a technique used to scramble and unscramble information. The VPN gateway at the sending location encrypts the information before sending it through the tunnel over the Internet. The VPN gateway at the receiving location decrypts the information back into clear-text. The industry has published well-known and well-tested encryption algorithms, such as the popular Data Encryption Standard (DES), which uses a 56 bit key. Since the encryption algorithms are standardized and known to all, they require the use of keys to make the data secure. DES has been developed even further with its 3DES (“triple-DES”) system that encrypts information multiple times. Triple DES uses the technique of encrypting, decrypting, and encrypting (EDE) increases the key length from 56 bits to 168 bits, making it extremely difficult for hackers to break through.



Further, if you establish a policy of periodically changing your keys, you will make it virtually impossible for any trespasser to break into the network.

The life span of a key is called a crypto-period. At the end of this period, keys expire. Since it was noticed that frequent change in keys actually increases the risk of disclosure, another ingenious method was designed which uses what are called symmetrical and asymmetrical keys. The use of symmetrical keys involves using the same key at each end of the tunnel to encrypt and decrypt information. Symmetrical keys are akin to “shared secrets”. The logistics of managing these keys is complicated because they are hard to distribute, given that the keys have to be kept confidential. Commonly used methods of distribution of symmetrical keys are manual and involve using paper, removable media, or hardware docking. Asymmetrical keys are more complicated to design, but logistically easier to manage. Asymmetrical keys allow information to be encrypted with one key and decrypted with a different key. The two keys used in this scenario are referred to as private and public keys.

The design, distribution and verification of public and private keys forms the fundamental premise for Sify’s digital certification services offered through its subsidiary and an independent certification vendor, Safescrypt. With optional digital certification services from Sify, enterprises can exchange vital business data or conduct electronic transactions with business partners. Digitally certified and validated transactions are legally valid and enjoy the protection provided by the most advanced security techniques available today.

Make no mistake. Constant and diligent security monitoring is as integral to IP VPN security as any of the mechanisms described above. Because IP VPNs may be used to connect small offices or remote sites, companies need to make sure they have a comprehensive policy and security solution, including firewalls and virus-scanning software, in place right from the start.

### **BOOST YOUR WORKFORCE PRODUCTIVITY AND SUPPLY CHAIN EFFICIENCIES**

Whether they are enabling secure access for employees in a branch office or for remote sites or for traveling salespersons or for business partners, companies using IP VPNs benefit greatly by expanding their employees’ ability to remain productive, no matter where they are located in the world. Because of this, IP VPNs have quickly become the latest standard in remote access to the corporate network.

In fact, the Yankee Group reports that 79% of U.S. companies with at least 500 employees and two sites use VPN solutions to provide secure access to traveling employees. 63% use them to ensure secure site-to-site connections, and 50% use them to provide network access to customers and partners. "IP VPN is a highly effective tool for a company that has offices and people geographically dispersed," says the Yankee Group. "It extends the corporate

“ 79% OF U.S. COMPANIES WITH AT LEAST 500 EMPLOYEES AND TWO SITES USE VPN SOLUTIONS TO PROVIDE SECURE ACCESS TO TRAVELING EMPLOYEES. 63% USE THEM TO ENSURE SECURE SITE-TO-SITE CONNECTIONS, AND 50% USE THEM TO PROVIDE NETWORK ACCESS TO CUSTOMERS AND PARTNERS ”

Yankee Group, 2001

network." In a Gartner survey, almost 90% of the companies in the US surveyed reported cost savings from switching to a VPN solution, primarily due to lower connectivity charges. On average, the companies surveyed by Gartner realized a 54% return on investment on their VPN investments over 18 months. "(IP) VPNs have emerged as a viable alternative to point-to-point communication and dedicated lines," says The Aberdeen Group. "They're an attractive solution for managing people and data."

SecureConnect™ is a line of IP VPN solutions from Sify, aimed at large and medium sized enterprises. They enable them to connect employees and business partners who may be anywhere in the world to the corporate intranet or extranet in a secure and reliable manner. The end user or site connects to SifyNet, Sify's managed IP network by either dialing up into the network or through a permanent, "always on" fixed connection.

SifyNet is a fully meshed national network, which provides 100 percent coverage of India – the largest reach of any service provider in India. The network comprises 54 Points-of-Presence (PoPs), built using Cisco Gigabit Switch Routers (GSRs) to ensure a high performance Tier 1 backbone.

A high level of redundancy has been designed into the network by employing sophisticated methods such Hot Standby Router

## SECURECONNECT™ IP VPN SOLUTIONS FROM SIFY



protocol (to protect against equipment failure) as well as by leasing fiber from multiple carriers in all the regions (to protect against physical infrastructure failure).

Sify uses the "best-of-breed" approach in its approach to selecting physical infrastructure providers thereby exploiting regional strengths and coverage of multiple carriers, without being burdened by their deficiencies.

### REDUCE YOUR TOTAL COST OF OWNERSHIP

It is now widely accepted that IP VPNs lower the costs of extending an enterprise network to reach a geographically dispersed end-user base, be it employees or business partners.

IP VPNs lower the Total Cost of Ownership (TCO) by requiring lower performance routing equipment at the customer premise, and by eliminating the need for costly long distance calls through the use of a shared IP backbone. Studies performed by Sify in comparing the TCO for a private line network with that of an IP VPN based network reveal that enterprises can reap savings of up to 45% by deploying IP VPNs for their WAN connectivity needs. The savings for a large Indian enterprise with hundreds or thousands of geographically dispersed locations can run into several crores. By outsourcing the management of the network to Sify, customers can free up their resources to focus on the core competencies of their business.

### CHOOSE THE RIGHT SERVICE PROVIDER

The Indian enterprise customer has a variety of choices today, when it comes to choosing a service provider. Service providers can be broadly categorized as telecom carriers and data networking services providers. Telcos tend to be broad generalists with a wide variety of offerings ranging from voice to data. In contrast, Sify specializes in data oriented offerings to the market place, built around world class customer service, deep technical and commercial expertise, a strong process orientation, an ability to constantly innovate as well as advanced project management skills. Sify has a track record in pioneering the IP revolution in India by being the first to bring a number of leading edge, enterprise-class IP based services to the market, starting with building India's first native IP network in 1996.

Telcos typically tend to focus on voice services, and it is likely that data services will be viewed as "yet another" offering in their portfolio. On the other hand, data networking services specialists such as Sify, who are likely to be better equipped and positioned to handle the networking needs imposed by the mission critical data applications of your enterprise. IDC in its latest report on the India IP VPN market in India described Sify thus :

“SIFY SEEMS TO BE THE CLEAR LEADER IN THE IP VPN SPACE. THE ONLY ISP WHICH HAS BOTH THE EXPERIENCE AND EXPERTISE TO HANDLE THE VPN NEEDS OF CORPORATES. IT HAS THE LARGEST MARKET SHARE AND COMMANDS THE HIGHEST RESPECT OF ITS SERVICES FROM ITS CLIENTS”

*International Data Corporation, 2001*

Further, the capabilities of the service provider in security design and deployment, customer premise equipment management and application management has to be taken into consideration when choosing an outsourcing partner ■