TimeStep

The Business Case for Secure VPNs

SECURE VIRTUAL PRIVATE NETWORK SOLUTIONS

IMPORTANT NOTICE

The information in this white paper is furnished for informational use only and is subject to change without notice. TimeStep Corporation assumes no responsibility or liability for any errors or inaccuracies that may appear in this document.

Trademarks

Written and designed at:
TimeStep Corporation
362 Terry Fox Drive
Kanata, Ontario K2K 2P5
Phone: (613) 599-3610
Fax: (613) 599-3617

Rev. No. VPN2.1—March 1999

Executive summary

As the only communications vehicle with worldwide connectivity, the Internet is full of business potential. To take advantage of this potential, businesses need to find ways to take the Internet beyond web sites and e-mail. Secure virtual private network (VPN) solutions are the key to this evolution.

Secure VPNs allow corporations to send proprietary and confidential information over the Internet, confident that it will travel safely – unseen, unchanged, uncopied, and intact. Secure VPNs provide this security through the implementation of authentication, access control, confidentiality, and data integrity.

Three of the greatest opportunities for conducting business communications over the Internet exist with intranets, extranets, and remote access. When these applications are deployed over the Internet, the operational cost savings are very favorable, the return on investment is in the hundreds of percent, and the payback period is measured in months, not years. Beyond the cost savings, however, there are several other benefits to be gained through implementing secure VPNs, including:

- scalability
- flexibility
- global connectivity
- better user support

TimeStep®'s PERMIT® Enterprise is a complete solution offering seamless network security. It offers both hardware and software components to allow businesses to benefit from managing multiple secure VPN groups comprising of thousands of simultaneous sessions or millions of nodes. The PERMIT Enterprise secure VPN solution is:

- fully scalable
- standards-based for interoperability
- integrated with a public key infrastructure (PKI)
- centrally managed
- fully flexible
- transparent to the user

PERMIT Enterprise unlocks the business potential of the Internet.

Contents

Introduction

To survive in today's competitive global marketplace, businesses must have an Internet presence.

Right now, most companies use the Internet to provide basic information to customers, employees, and associates via e-mail and web sites. However, the Internet presents countless other opportunities to gain a strategic advantage. Businesses must find new ways to use the Internet for business communications or risk being left behind. Organizations that use the Internet's global infrastructure to its fullest potential will have the competitive edge.

Two concerns make businesses hesitate to use the Internet for business communications: reliability and security. On the reliability front, service providers are rapidly dealing with quality of service (QoS) concerns. They are implementing high speed, low cost Internet access services while eliminating down times. On the security front, secure VPN technology has now matured to the stage where it can offer businesses everything they need to use the Internet for communicating safely. Some service providers are also offering redundancy to ensure the best route for your data.

This paper looks at how secure VPN technology makes secure business communications over the Internet a reality. Secure VPNs not only reduce the costs of enterprise-wide communication, but also provide flexibility for easy change and growth, and simplify global interconnectivity. This paper explores two of the more compelling applications for Internet business communications: branch office connectivity and remote access.

Issues with business communications over the Internet

Concerns about security and the Internet's quality of service (QoS) have made businesses hesitant to use the Internet to send confidential and proprietary data to customers, employees, and associates.

To address concerns about quality of service, service providers offer service level agreements guaranteeing bandwidth capacity, utilization options, latency, and reliability for their customers. New technologies such as Resource Reservation Protocol (RSVP) will also allow service providers to address QoS problems. To further improve their offering, service providers will invest $7 billion by the year 2001 to beef up IP networks so that most will have backbones which rival the performance and reliability of today's frame relay WANs.

While service providers were addressing the QoS issue, the security of Internet communications remained a concern…until now. When businesses communicate over the Internet they need to guarantee that their data is safe. Secure VPN technology provides this guarantee.

What is a secure virtual private network?

Secure VPNs allow corporations to transform the Internet into an extension of their own private network. By creating a secure VPN, corporations can send proprietary and confidential information over the Internet confident that it will travel safely. Secure VPN technology allows businesses to create intranets to communicate securely with branch offices and remote employees, as well as extranets to communicate securely with trading partners.

There are four critical functions of VPN technology that ensure security for your data:

- **Authentication —** X.509 digital certificates ensure that data is coming from the source it claims to come from
- **Access control —** directory-based policy management restricts users from gaining admission to certain parts of the network
- **Confidentiality —** data encryption prevents anyone from reading your data as it travels across the Internet
- **Data integrity —** cryptographic checksums ensure that no one tampers with data as it travels across the Internet

Frame relay basics

A fully meshed network is a network in which every office communicates with every other office. Often when using private lines, corporations will use a hub and spoke model for branch office communications, in order to lower costs. With a hub and spoke model, all branch office communications go through a central office. Branch offices do not communicate directly with each other.

Each branch office must lease a local loop from a Local Exchange Carrier (LEC). The local loop serves to connect the branch office to a frame relay network leased from an Inter-Exchange Carrier (IXC) or RBOC.

Frame relay is a packet-based technology, that does not allocate bandwidth until the beginning of data transmission. Instead, the IXC or RBOC defines a permanent virtual circuit (PVC) between two corporate sites over a shared frame relay network, and allocates bandwidth as required.

Since many users may share the network, the required bandwidth may not always be available. However, frame relay vendors can offer a committed information rate (CIR) — a minimum guaranteed throughput over the PVC.

Business case for secure Internet communications

There are several compelling arguments for using VPNs to create corporate intranets. The most compelling of these arguments is the cost savings that organizations can enjoy by implementing VPNs. However, there are other strong reasons for implementing VPNs, such as ease of management and flexibility. The two business cases presented below outline the many benefits of conducting branch office communications and remote access over the Internet.

Branch office connectivity

Traditionally, branch offices have had to employ costly private lines to connect to the corporate network. For some it has proved too expensive to attempt. The following business case illustrates how VPNs dramatically lower the costs associated with branch office communications.

This business case is a cost comparison between the following two scenarios:

Private line scenario

- a five office, fully meshed network within the United States (see Figure 1)
- private frame relay network with T1 port speeds at all sites
- a committed information rate (CIR) of one-half of port speed (768 Kbps) is assumed (see *Frame relay basics* side bar for more details).

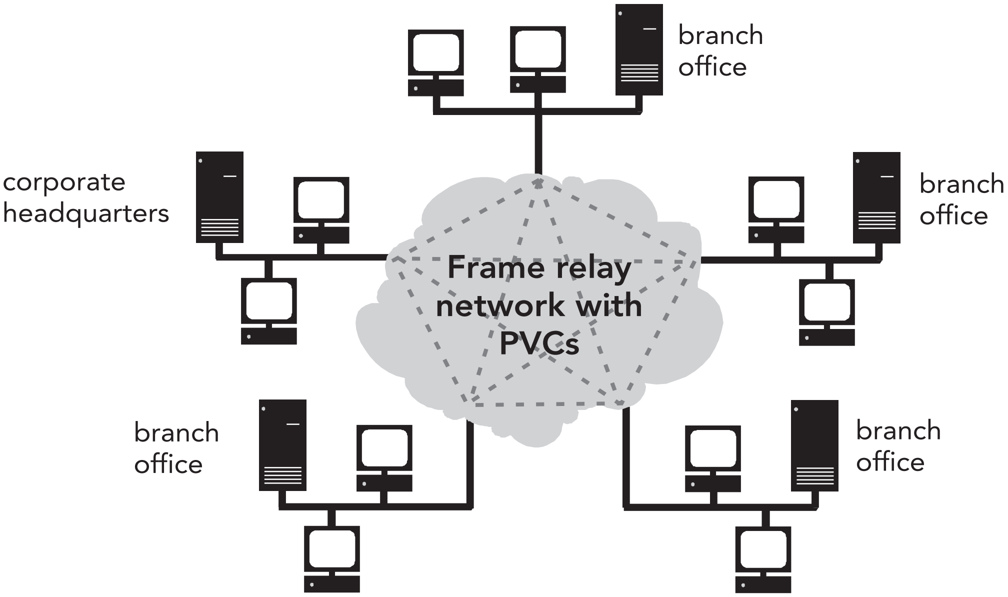


Figure 1: Private line branch office scenario

Internet scenario

- a five office, fully meshed network within the United States (see Figure 2)
- virtual private network with frame relay Internet access at T1 port speeds at all sites

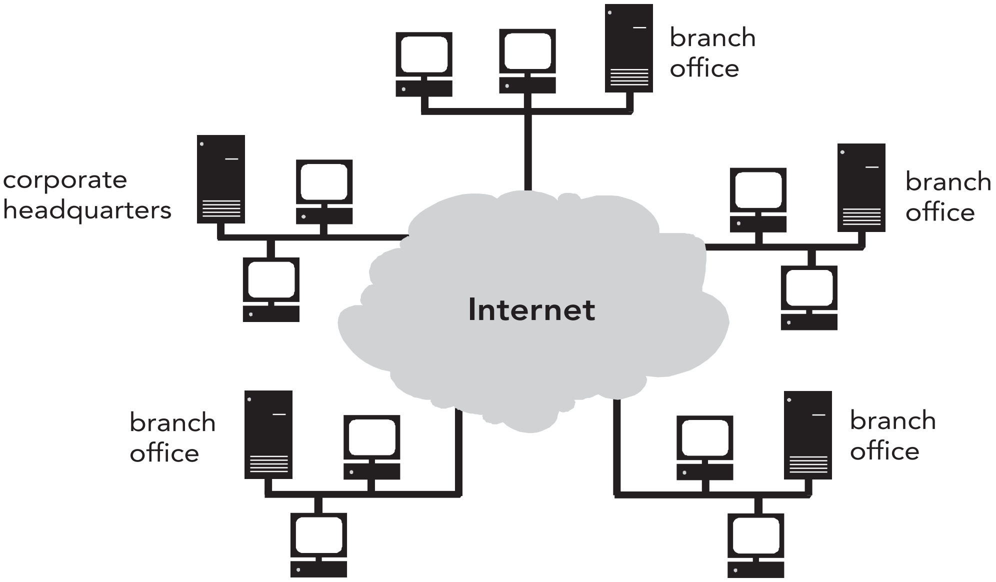


Figure 2: Internet branch office scenario

Cost model

Costing for both the branch office and remote access cases is based on the assumption that all networks are newly-created and do not take advantage of existing infrastructure such as T1 ports. Pricing does not take into consideration any kind of discounts that may be provided for level of usage or length of commitment. The formula used to calculate pay back period is:

Pay back period = Capital Cost of Internet Scenario/(Operational Costs of alternative scenario - Operational Costs of Internet Scenario)

Return on investment (ROI) is calculated based on one year's operational cost savings.

ROI = [12(Monthly Operational Cost Savings) - Capital Cost of Internet Scenario]/Capital Cost of Internet Scenario

The cost comparison between the private line and Internet options demonstrates the strength of the case for conducting branch office communications over the Internet (see Table 1). The monthly operational costs for the private line scenario are $28,500, whereas the monthly operational costs for the Internet scenario are only $13,025. The Internet scenario results in 54% operational cost savings over the private line scenario, and a capital investment pay back period of just 4.0 months. This translates into a 201% return on investment during the first year of implementation (see *Costing model* side bar for more details).

Private line scenario				**Internet scenario**			
Item	Qty	Unit cost	Extended cost	Item	Qty	Unit cost	Extended cost
Capital Costs				**Capital Costs**			
Routers*	5	$1,950	$9,750	Routers*	5	$1,950	$9,750
CSU/DSU*	5	$995	$4,975	CSU/DSU*	5	$995	$4,975
T-1 installations**	5	$300	$1,500	T-1 start up*	5	$3,000	$15,000
				PERMIT/Director Suite	1	$11,995	$11,995
				PERMIT/Gate 2520	5	$3,995	$19,975
Total capital costs			**$16,225**	**Total capital costs**			**$61,695**
Monthly operating costs				**Monthly operating costs**			
T-1 ports**	5	2,200	$11,000	T-1 Ports*	5	$1,905	$9,525
PVCs**	10	$1,400	$14,000	Local Loops***	5	$700	$3,500
Local Loops***	5	$700	$3,500				
Total monthly operating costs			**$28,500**	**Total monthly operating costs**			**$13,025**

*Prices from UUNet (August 1998).

**Average frame relay cost from AT&T, MCI, and Sprint. Taken from *"Using The Internet For The Corporate Virtual Private Network: Overview of Costs, Flexibility, and Management"* Mark Winther, Analyst, 1998.

***Average local loop cost (varies by region).

Table 1: Cost comparison between private line and Internet scenario

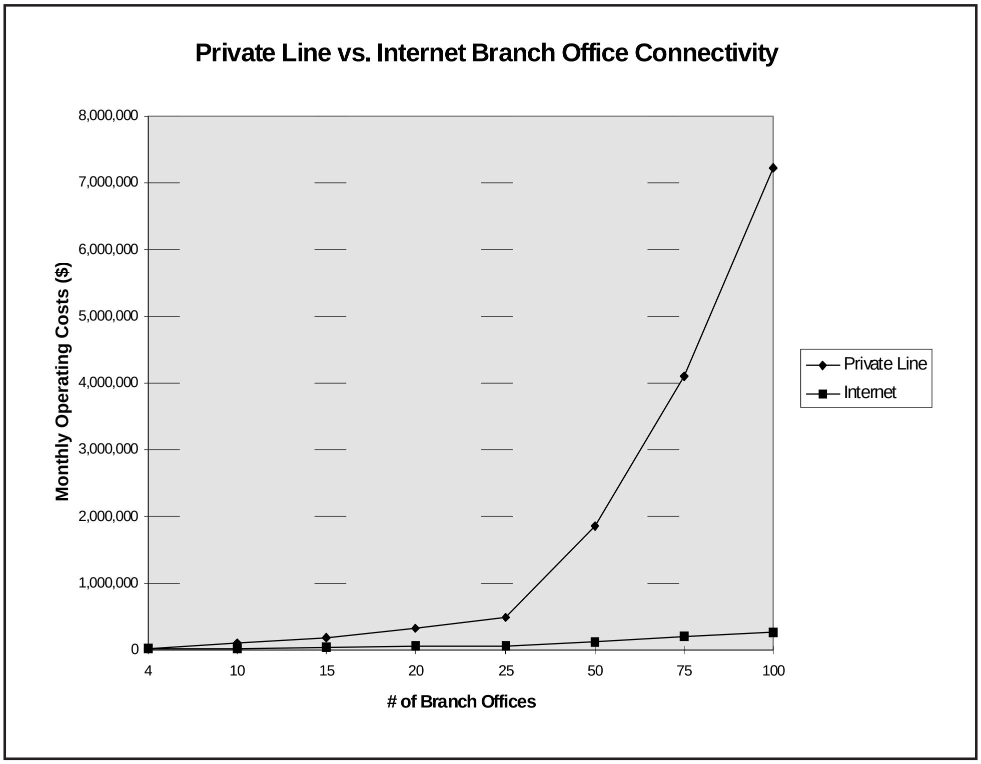
% Operational Cost Savings = 54%
Pay Back Period = 4.0 months
ROI (for first year) = 201%

VPN savings grow with your network

When costs associated with each scenario are scaled to larger networks, the cost savings continue to grow for the Internet scenario (see Figure 3). Costs for the private line scenario rise steeply between 25 and 100 branch offices, whereas the Internet curve is almost flat.

The difference is that costs associated with private line networks are not linearly related to the number of branch offices, because a PVC must be added for each office to which the new office will be connected. However, with Internet communications, adding a new office to the network simply requires you to connect the office to the Internet, rather than connecting it to every other office.

Therefore, the larger the wide-area network, the larger the savings gained by using the Internet.



*Based on full pricing (no discounting).

Figure 3: Private line vs. Internet branch office connectivity

Other benefits

Aside from direct cost savings, there are several other reasons for moving branch office communications to the Internet:

- **Flexibility —** the Internet brings a degree of flexibility to corporate communications that has never before been available. Corporations can add branch offices to their network simply by setting up Internet access. The low access price enables corporations to connect branch offices to their network that previously had no access at all. And the Internet provides instant access to global trading partners and customers as well.
- **Central management —** for a fully-meshed branch office network, private lines can be a nightmare. You must manage lines between each of the offices. For a 10-site network, you must manage 45 PVCs. For a 150 site network you need 11,175 PVCs. With the Internet, however, you need only provide each office with Internet access — you do not need to manage individual lines.
- **Global connectivity —** as the economy continues to become more global, corporate networks need to grow beyond North American borders. The fiber infrastructure for quality private lines is simply unavailable in many countries. The Internet, on the other hand, is ideal for international connectivity. The Internet Protocol (IP) can run over any communications infrastructure.

Remote Access

The need for remote access facilities is growing at an exceptional rate, as the demands of telecommuters, support personnel, and road warriors grow. Infonetics Research Inc. reports the percentages of employees accessing corporate networks remotely is growing: the number of mobile workers grows 114% by 2000 and the number of telecommuters grows 154% by 2000. This will result in 62 million remote access users (mobile workers, telecommuters, and day extenders) worldwide by 2001. (Source: User Plans for VPN Products and Services, April 1998).

Traditional, corporate-administered remote access facilities with dial-up modem lines will not be able to keep up with such demands. This growth is introducing two major problems: 1) costs are spiraling out of control, and 2) management is becoming increasingly complex.

Costs spiraling out of control

The costs associated with remote access include:

- long distance charges
- the payroll of remote access administrators
- the capital expenditures on remote access equipment

All these costs are growing considerably as demand for remote access increases. In essence, corporations are becoming service providers for their employees, and are bearing the enormous expense associated with this.

Ever-increasing management complexity

Remote access requires intense user support and a lot of network management time, due in part to the poor reliability of remote access facilities. As the number of remote access users increases, the human resources required for management and support grow well beyond what the typical IT department can provide.

The following business case is a cost comparison between direct dial-up and Internet remote access. We compare two scenarios:

Direct dial-up remote access scenario:

- the corporation has 100 remote users
- users connect to the local area network for an average of one hour per day (20 hours per month)
- users dial into the network over long distance lines and incur toll charges

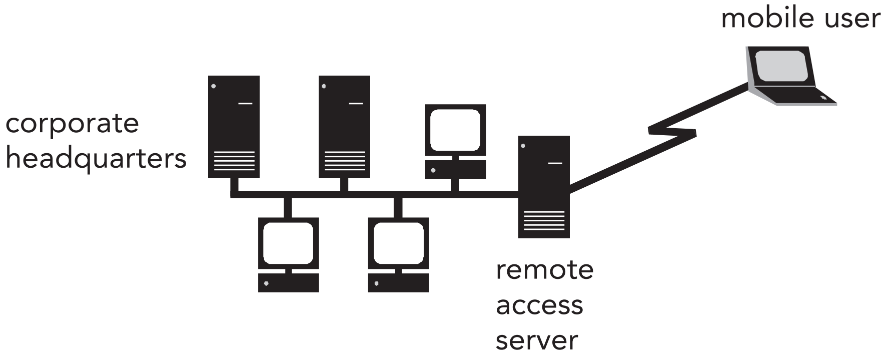


Figure 4: Dial-Up Remote Access Scenario

Internet remote access scenario:

- the corporation has 100 remote users
- users connect to the local area network for an average of one hour per day (20 hours per month)
- users dial into a local network service provider (NSP) point of presence (POP) and connect to the LAN over the Internet
- the corporation outsources the management of remote access facilities to a NSP, in order to take advantage of the service provider's economies of scale

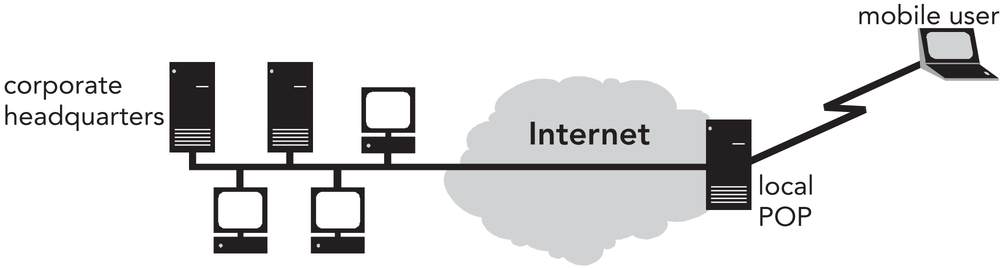


Figure 5: Internet remote access scenario

The cost comparison between direct dial-up and using the Internet demonstrates the advantages of conducting remote access over the Internet (see Table 2). The Internet scenario results in 62% operational cost savings when compared with the private line scenario, resulting in a capital investment pay back period of just 2.8 months. This translates into a 336.3% return on investment during the first year of implementation (see *Costing model* sidebar for more details).

Direct dial-up scenario				Internet scenario			
Item	Qty	Unit cost	Extended cost	Item	Qty	Unit cost	Extended cost
Capital Costs				**Capital Costs**			
Terminal server[*] (cost is per port)	13	$550	$7,150	T-1 line start up costs[**]	1	$3,000	$3,000
				CSU/DSU[**]	1	$995	$995
				Router[**]	1	$1,950	$1,950
				PERMIT/Connect	1	$14,395	$14,395
Total capital costs			**$7,150**	**Total capital costs**			**$20,340**
Monthly operating costs				**Monthly operating costs**			
Long distance charges[***]	2000	$6	$12,000	ISP charges[**]	100	$20	$2,000
				T-1 line[**]	1	$1,905	$1,905
				Local loop[****]	1	$700	$700
Total monthly operating costs			**$12,000**	**Total monthly operating costs**			**$4,605**

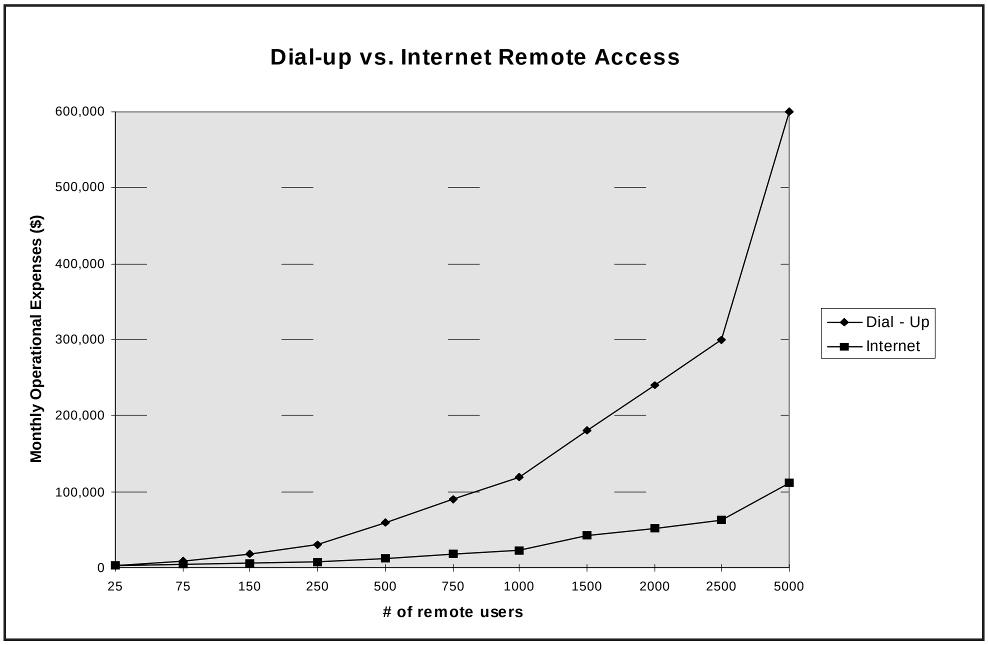
* Average industry cost.
**Price from UUNet (August 1998).
***Price from MCI (August 1997).
**** Average local loop cost (varies region to region).

Table 2: Cost comparison between dial-up and Internet scenario

% Operational Cost Savings = 62%
Pay Back Period = 2.8 months
ROI (for first year) = 336.3%

Savings grow as you add users

When you scale the costs associated with each scenario to organizations with a larger number of remote access users the margin of cost savings grows steadily. The only additional operational costs incurred when a remote access user is added under the Internet scenario is the $20 per month NSP account charge. In contrast in the direct dial-up scenario, adding a user costs an additional $120 per month in toll charges. These toll charges become significant in a large pool of users (see Figure 6).



*Based on full pricing (no discounting).
**For greater than 1000 users, pricing of port a corporate site changes from T1 to burstable T3 speed.

Figure 6: Dial-up vs. Internet remote access

Other benefits

Outsourcing corporate remote access to a service provider has several other advantages besides cost savings, including:

- **Central management —** transfer of remote access management issues outside of the corporation to service providers. It is now the service provider's responsibility to provide maintenance for your remote access facilities. This results in lower HR costs, as the number of system administrator hours spent on remote access decreases.
- **Ignore technology obsolescence —** the risk of technology obsolescence moves outside the corporation to the service providers. Remote access over the Internet allows your users to utilize a variety of access technologies, including ISDN and modems. As new high speed access technologies emerge, such as DSL, cable modem, and cellular, your organization will be able to take advantage of them without capital investment in equipment. The service providers bear the majority of capital costs for switching technologies.
- **Scalability —** as demand for remote access increases within your organization, you will have no need to buy and install more ports. It is simply a matter of ordering new access accounts from your service provider.
- **Better user support —** with direct dial-up remote access, user support falls on the shoulders of IT. In many cases it is simply not feasible to provide round the clock support for users. However, with remote access outsourced to a NSP, the burden of 7x24 support falls to them.

TimeStep's secure VPN solution

TimeStep's PERMIT Enterprise product suite offers corporations a complete IPSec-compliant secure VPN solution for corporate intranets, extranets, and Internet remote access. Designed for large-scale business communications, PERMIT Enterprise is scalable, standards-based, and integrates Entrust's public key infrastructure (PKI) while its directory-based policy management enables organizations to create and manage multiple secure VPNs. With PERMIT Enterprise, corporations can realize the cost benefits of using the Internet for business communications without worrying about information security (see Figure 7).

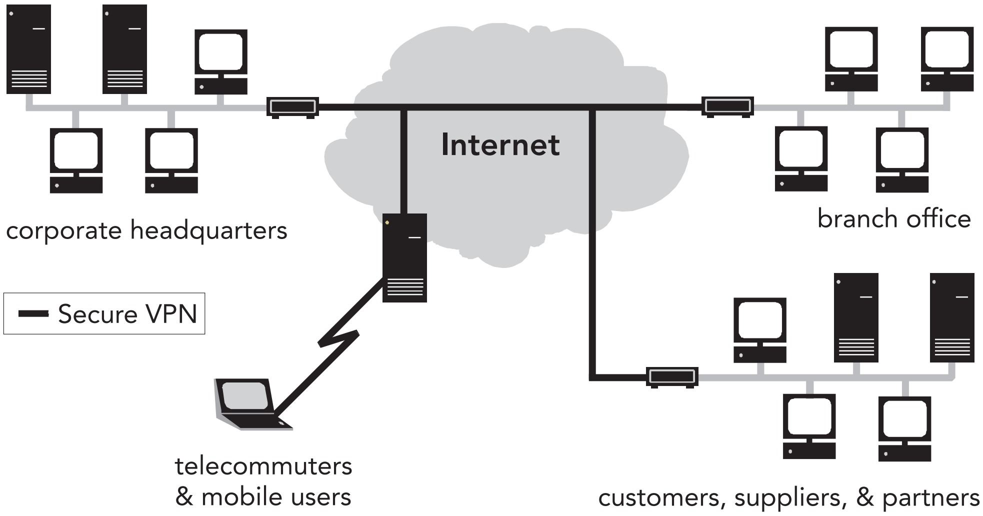


Figure 7: Secure intranet, extranet, and Internet remote access

Key benefits of PERMIT Enterprise

PERMIT Enterprise offers you

- **manageability**—PERMIT Enterprise's comprehensive system consolidates management of secure VPN, access control, and authentication to reduce the cost and complexity of network security administration. Provisioning of gateways and clients makes large-scale deployments quick and easy.
- **extensibility**—PERMIT Enterprise's integrated public key infrastructures (PKIs) and X.500 directories enable you to manage digital certificates and VPN policy for thousands of nodes and clients. This ensures a flexible and scalable solution that grows along with your business.

- **network performance and reliability**—TimeStep's hardware-based encryption allows your VPN to run at wire-rate performance. And our fully dedicated VPN gateways are robust and reliable.
- **interoperable**—TimeStep is the first vendor with both hardware gateways and a software clients that are certified by the International Computer Security Association (ICSA) as IPSec-compliant. Our PERMIT Enterprise product suite is architected as an open standard-based solution that supports LDAP-compliant X.500 directories, X.509v3 certificates, PKIX certificate management, and PKCS11 PC card token or smart cards.
- **cost-efficient network**—TimeStep's PERMIT Enterprise solution is easy to implement and maintain. As an independent hardware device it fits into any existing network infrastructures. And its client software is seamless, fully transparent to users and applications.

PERMIT Enterprise product suite

The PERMIT Enterprise product suite consists of the PERMIT/Gate™, PERMIT/Client™, and PERMIT/Director™ suite.

PERMIT/Gate 2520, 4520, and 7520

The PERMIT/Gate is a tamper-resistant gateway that secures data communications for intranets, extranets, and Internet remote access.

PERMIT/Config™, a software that allows you to manage multiple gateways from any point on your secure VPN, is a feature of the PERMIT/Gate product family.

PERMIT/Gate supports

- IPSec-compliant protocol negotiation and tunneling
- hundreds of simultaneous TCP/IP secure sessions
- a full spectrum of encryption and authentication algorithms
- remote configuration by PERMIT/Config

The PERMIT/Gate series are two port Ethernet devices with various performance characteristics depending on the application and bandwidth requirements of your networks.

PERMIT/Gate	Bandwidth	Number of simultaneous users	Applications
PERMIT/Gate 2520	4 Mbps	500	Branch office and remote access: T1/E1
PERMIT/Gate 4520	10 Mbps	500	Corporate, large branch office, and remote access: Enternet
PERMIT/Gate 7520	70Mbps	2000	High bandwidth and remote access: T3 and Fast Ethernet

PERMIT/Client

The PERMIT/Client software secures network traffic for a workstation and is ideal for Internet remote access by telecommuters and business travelers. PERMIT/Client supports IPSec tunneling and transport modes for PPP, Ethernet, Token Ring, cable modem, xDSL, and ISDN connections. The PERMIT/Client runs on Win 95, Win 98, Win NT, and Mac OS platforms. Optional two-factor user authentication support is available with any Entrust-Ready™ PC card token or smart card.

PERMIT/Client also supports

- Virtual Tunneling, including tunneling to an internal DNS
- any IPSec-compliant authentication and encryption scheme

PERMIT/Director suite

The PERMIT/Director suite contains the software applications used to manage the people and resources protected by PERMIT Enterprise products within your secure VPN. Assigning users and resources to different groups gives you the ability to maintain multiple secure VPN partitions. This allows you to control who communicates with whom, using which level of IPSec encryption and authentication. The PERMIT/Director suite includes PERMIT/Director, Entrust/Manager™, and Entrust/Directory™.

Conclusion

The key advantage the Internet has over other communication media is that it is the only medium to offer worldwide connectivity. As the economy becomes more and more global, it is imperative that businesses have the ability to communicate on an international scale. Whether it be opening a branch office in India, enabling your sales force to connect to your network from the road, or setting up a trading relationship with a supplier half-way around the world, the Internet is the only solution.

Secure VPN technology is the key to unlocking the business potential of the Internet. When businesses communicate over the Internet they need to guarantee that their data is safe from prying eyes, that it has not been altered in transit and that they can positively identify the users with whom they are communicating. Secure VPNs provide this guarantee.

Conducting branch office communications and remote access over the Internet brings, in addition to global connectivity, considerable cost savings over private lines and direct dial-up. The strength of the business case for moving applications such as branch office communications and remote access to the Internet is so strong that payback periods are measured in months and return on investment in the hundreds of percent.

TimeStep's PERMIT Enterprise product suite is the complete secure VPN solution for corporate intranets, extranets, and Internet remote access. PERMIT Enterprise enables your business to establish secure communication paths through the Internet. These can extend to branch offices anywhere, to remote workstation, or mobile user guaranteeing strong user authentication, encryption, and data integrity. PERMIT Enterprise enables your organization to realize the business potential of the Internet.

Glossary

CSU/DSU - Channel Service Unit/ Data Service Unit - sits on the WAN side of the router and provides a termination point for a digital signal. This device also provides loop-back tests on the communications line.

Committed Information Rate (CIR) - guaranteed minimum throughput over a packet-based network.

Data Encryption - transformation of data into unreadable, meaningless data through a cryptographic transformation using a key. Decryption is the process of reversing the unintelligible data into meaningful data using a key.

Digital Certificate - package of information, digitally signed by a trusted authority (usually referred to as a CA or Notary) which binds a public key to an owner. The package usually consists of an identifier field, a public key field, serial number (of the certificate), activation and expiry date as well as a signature field. X.509 defines a standard format for these certificates.

Frame Relay - a packet-based data transmission technique that sends bursts of data over a wide area network.

Fully-Meshed Network - a branch office network in which every office communicates with every other office.

Interexchange Carrier (IXC) - carriers that provide long distance services, such as MCI and AT&T.

Internet Protocol (IP) - basic transmission protocol of the Internet, and a common standard in corporate LANs and WANs.

Local Exchange Carrier (LEC) - telecommunications company that operates within a specific service area.

Local Loop - connection leased from a LEC that connects a customer site to an IXC's or RBOC's network.

Pay Back Period - period of time over which operational cost savings will pay back the initial capital investment.

Permanent Virtual Circuit (PVC) - a logical connection between two sites on a network, where bandwidth is allocated as required.

Resource Reservation Protocol (RSVP) - technology currently under development to address the issue of quality of service for service providers.

Secure virtual private network (secure VPN) - a secure private network using unsecured public networks as carriers. Users of the secure VPN may use their network as though it were a perfectly secure, isolated LAN, even though it is connected to unsecured public networks.

T1 Port Speed - a data transmission speed of 1.544 Mbps.

References

"User Plans for VPN Products and Services 1998." *Infonetics Research*. April 1998.

Barth, C., Callahan, P., Cho, D., Pincince, T. "Internet Remote Access." *The Forrester Report*. July 1996: volume 10, number 8.

Chan, S., Elliot, S., Hannigan, B. and Howe, C. "Intranets On The Road." *The Forrester Report*. June 1997: volume 11, number 7.

Cray, A. "Secure VPNs: Lock the Data, Unlock the Savings." *Data Communications*. May 21, 1997.

Erwin, B., Goodtree, D., McKnight, J., Smith S. "Intranets Across The WAN." *The Forrester Report*. December 1996: volume 1, number 7.

Steinke, S. "The Internet as Your WAN." *LAN Magazine*. October, 1996.

Winther, Mark. "Using The Internet For The Corporate Virtual Private Network: Overview Of Costs, Flexibility, and Management." *International Data Corporation,* 1998.

TimeStep Corporation is the leading provider of secure virtual private network (VPN) solutions for corporate intranets, extranets, and Internet remote access. Designed for large-scale business communications, TimeStep's award-winning PERMIT Enterprise product suite integrates secure VPN, access control, and authentication technologies in a single solution.

TimeStep Corporation
362 Terry Fox Drive
Kanata, Ontario
Canada K2K 2P5

TimeStep Inc.
593 Herndon Parkway
Herndon, Virginia
U.S.A. 20170

Tel: 1-800-383-8211
Fax: (613) 599-3617
www.timestep.com
info@timestep.com

62-00113-01

97-2551-01-00-B

Printed in Canada.