



***PROPOSAL FOR A SECURE VPN SOLUTION
FOR POWELL ELECTRICAL MANUFACTURING CO.***

April 27, 1999

PREPARED FOR:

SUBMITTED BY:

TimeStep Corporation
362 Terry Fox Drive
Kanata, Ontario
CANADA K2K 2P5
613-599-3610

Table of Contents

EXECUTIVE SUMMARY	2
I ABOUT TIMESTEP CORPORATION	3
A. COMPANY BACKGROUND	3
B. OUR MISSION	3
C. OUR RECENT SUCCESSES	3
D. OUR PARTNERS	5
II OUR PRODUCTS	7
THE RIGHT TECHNOLOGY: PERMIT ENTERPRISE	7
A. KEY BENEFITS OF PERMIT ENTERPRISE	8
B. INTRODUCING PERMIT ENTERPRISE	8
C. THE IMPACT OF PERMIT ENTERPRISE	11
D. PERMIT ENTERPRISE SECURE VPN APPLICATIONS	11
III PROPOSED SOLUTION	13
CENTRAL OFFICE	13
SUBSIDIARIES	13
MANAGEMENT	14
PERMIT ENTERPRISE SOLUTION	15
FAULT TOLERANCE	15
PERMIT ENTERPRISE SOLUTION WITH FAULT TOLERANCE	16
ISSUES	16
CUSTOMER SUPPORT SERVICES	17
IV PRICING	19
PERMIT ENTERPRISE SOLUTION	19
PERMIT ENTERPRISE SOLUTION WITH FAULT TOLERANCE	20

Executive Summary

In 1991, TimeStep® was founded on the premise of developing a “carrier scale” security solution for IP networks. With Newbridge® Networks Corporation as a partner, a global telecommunications giant that had partnered with over 800 customers, TimeStep set about creating extensible, standards compliant products that would address remote access, LAN-to-LAN communications, and emerging extranet opportunities. With our release of the PERMIT® Enterprise product suite, TimeStep has remained at the forefront of top-notch cryptographic solutions.

In the last year, the most powerful cryptographic algorithms have been designed into IPsec through the IETF (Internet Engineering Task Force). TimeStep not only adopted these standards, but also has participated in the RFCs that now dominate what is officially the IPsec standard.

As a leading provider of secure virtual private network (VPN) solutions, TimeStep is uniquely positioned to assist Powell Electrical Manufacturing Co. in achieving its security objectives. TimeStep looks forward to the opportunity to work with Powell Electrical Manufacturing Co. and combining the strengths of both companies.

TimeStep’s award-winning PERMIT Enterprise product suite is designed for service deployment. Our products are extensible, fully manageable, interoperable, and satisfy the four basic applications required for a true secure VPN solution: secure Internet connectivity, remote access, branch office communications, and extranets. TimeStep’s product design facilitates Powell Electrical Manufacturing Co.’s requirement for a supplier who can respond quickly and effectively to your needs. TimeStep will work closely with Powell Electrical Manufacturing Co. to demonstrate our ability to provide technical resources based upon Powell Electrical Manufacturing Co.’s selection of TimeStep’s technology.

We have carefully reviewed Powell Electrical Manufacturing Co. document and have made every effort to address all of the requirements. TimeStep stands ready to commit the time and resources necessary to meet Powell Electrical Manufacturing Co.’s requirements.

I About TimeStep Corporation

A. Company Background

Founded in 1991, TimeStep became a Newbridge Affiliate in 1994. In the past four years, TimeStep has grown from 3 to over 100 employees while broadening the customer base of its award-winning PERMIT Enterprise product suite to over 120 global customers.

TimeStep's solution is fully extensible and meets the demands of Network Service Providers (NSPs) and large enterprises deploying Internet remote access, intranets, and extranets. Producing flexible, interoperable, break-through products, TimeStep makes it safe to send information over the largest network infrastructure there is today—the Internet.

B. Our Mission

TimeStep envisions a future where all organizations will send information over networks with complete security and peace of mind. By forming alliances with customers, other network equipment vendors, and network service providers, TimeStep is leading the network security industry towards compatible secure VPN solutions.

TimeStep is also working closely with standards organizations to define emerging standards. Our PERMIT Enterprise product suite is IPsec certified by the International Computer Security Association (ICSA) as IPsec-compliant. Moreover, TimeStep is the only VPN vendor with both IPsec-certified hardware gateways and software client.

C. Our Recent Successes

TimeStep Corporation is recognized, by the industry and media, as a leader in Internet Protocol Security (IPsec)-compliant secure VPN solutions:

- ◆ **April 20, 1999**
TimeStep's PERMIT Enterprise™ Suite wins Network Magazine's 1999 VPN Product of the Year Award
- ◆ **March 23, 1999**
TimeStep's PERMIT/Gate 4520 is Well Connected Nominee

- ◆ **March 15, 1999**
3Com Licenses TimeStep's IPsec client for VPN Offering
- ◆ **March 9, 1999**
TimeStep hosts Online Seminar for World's Largest Extranet
- ◆ **March 3, 1999**
TimeStep and EXOCOM Announce Joint Partnership Offering Canadian users Industry-Leading IT Security
- ◆ **February 23, 1999**
TimeStep Wins INFOWORLD's Golden Guardian Award for Best VPN Solution of 1998
- ◆ **February 18, 1999**
Ameritech selects TimeStep to provide IPsec security for ANX service
- ◆ **December 07, 1998**
TimeStep's VPN solution selected by GTE for its VPN Advantage service offering
- ◆ **November 09, 1998XX**
TimeStep first VPN vendor to integrate ICL directory to create most scalable VPN solution in the industry
- ◆ **October 26, 1998**
TimeStep introduces PERMIT/Gate 7520 VPN box capable of supporting emerging high-speed network technologies
- ◆ **October 21, 1998**
TimeStep's high-performance VPN gateway selected as finalist in Network + Interop's Best of Show Awards
- ◆ **October 19, 1998**
TimeStep introduces new features in secure VPN solution that create the industry's most comprehensive IPsec client
- ◆ **September 14, 1998**
TimeStep attracts world-class resellers into new Reseller Partner Program
- ◆ **September 9, 1998**
Bell Emergis selects TimeStep to provide security for AutoLinux network solution
- ◆ **July 27, 1998**
TimeStep secures Macintosh remote users with the introduction of Mac IPsec client

- ◆ **May 20, 1998**
TimeStep's leading VPN products certified IPsec-compliant in first-ever ICASA-testing
- ◆ **May 12, 1998**
TimeStep's PERMIT Enterprise VPN solution wins a *Network Computing* 1998 Well-Connected Award
- ◆ **May 5, 1998**
TimeStep's first to ship IPsec-compliant turnkey remote access VPN solution with fully integrated PKI

To read the details on these announcements, visit our Press Release archive at http://www.timestep.com/press_releases/archive.htm.

D. Our Partners

At TimeStep, we believe in partnership. Strategic alliances gives us a competitive edge and a knowledge base that is second to none. Below is a partial list of our partners.

◆ **Entrust Technologies**

Entrust Technologies develops Entrust/PKI, a software security infrastructure that provides enterprise-wide encryption and digital signatures using public key cryptography.

Entrust® Technologies and TimeStep Corporation have a software-licensing agreement to embed Entrust's public-key infrastructure (PKI) technology in TimeStep's PERMIT Enterprise secure virtual private network (VPN) solution.

Entrust's PKI technology was chosen because it is the leader in its marketplace, and because it is the forerunner in defining the fundamental standard for its industry, PKIX.

Part of Entrust's appeal is its superior ability to manage certificates. Certificates authenticate users in a network and are a more secure, less expensive alternative to hardware tokens. Authentication verifies the identity of the person with whom you are communicating. Enterprise also integrates an LDAP-compliant directory to store the certificates. The Entrust/Directory is also a major contributor to the extensibility of the product. Finally, embedding Entrust's technology allows cross certification, which means that corporations can certify users from different VPNs.

◆ **RSA Data Security Inc.**

RSA Data Security Inc. is the world's "brand name" for cryptography, with over 15 million copies of its software encryption and authentication technologies installed and in use worldwide. The company develops and markets platform-independent developer's kits and end-user products, and provides comprehensive cryptographic consulting services.

TimeStep has a long-term strategic relationship with RSA which dates back to the mid 1980s. At the time, the founders of TimeStep were the key personnel within the Newbridge security group when Newbridge Networks became one of the first licensees of RSA's public key technology for the MainStreet™ TAP link encryption product. Based on that experience, TimeStep licenses RSA's BSAFE product for use within the PERMIT line of Virtual Private Networking products.

◆ **ICL**

ICL Inc. is the U.S. software marketing arm of ICL PLC and a Fujitsu subsidiary. ICL PLC is a \$4 billion global IT firm that specializes in implementing IT systems for major projects and providing innovative services to a range of industries. The company is the developer of the i500 LDAP and Enterprise Directory Server.

TimeStep Corp and ICL have forged a relationship that integrates the industry's most scalable LDAP and X.500 directory into TimeStep's IPsec VPN solution. Virtually unlimited in its capacity to handle entries, ICL's i500® will make the PERMIT Enterprise secure VPN solution the most scalable solution on the market. Because of this dramatic increase, TimeStep's PERMIT Enterprise product suite is more aligned than ever to the network service provider's requirement for a high-capacity VPN solution.

◆ **Newbridge Network Corporation**

Newbridge Network Corporation develops, manufactures and markets the MainStreet™ line of WAN networking products for T1/E1, ISDN, X.25, SONET, Frame Relay and ATM networks for the corporate and telephone service provider markets. The VIVID™ (Video, Voice, Image and Data) line of switched ATM LAN networking products delivers a fully integrated solution for switched, high-speed ATM for the campus network.

The Newbridge Affiliate Strategy

The focus of the Affiliate Strategy is to diversify into fast growing niche markets through investment in focused, aggressive start-up companies, without requiring Newbridge to defocus from its core business. In return, the Affiliates Companies provide Newbridge with a breadth of solutions that no other LAN/WAN networking vendor can match. Newbridge has created a business model that attracts highly motivated entrepreneurs and breeds successful high-tech businesses.

II Our Products

The Right Technology: PERMIT Enterprise

The PERMIT Enterprise product suite addresses a wide variety of security needs that allow you to use public networks like the Internet for secure Internet remote access, secure branch office connectivity, secure extranet connectivity with business partners, customers, and suppliers.

PERMIT Enterprise also

- ◆ provides sophisticated tunneling options, including TimeStep's unique Virtual Tunneling™ for mobile users
- ◆ provides remote configuration of the secure network
- ◆ provides an easily-expanded, modular, component architecture
- ◆ allows layered secure VPNs, with multiple groups of communicating nodes using the same hardware
- ◆ supports multiple secure VPNs

PERMIT Enterprise features:

Encryption	DES, 3-DES, RC5, CAST, Blowfish, IDEA (optional)
Authentication	Certificate-based with RSA signatures, shared secret
Integrity	HMAC-MD5, HMAC-SHA-1
Key management	IKE (formerly ISAKMP/Oakley), Diffie-Hellman
Protocol support	TCP/IP, UDP, IPSec ESP/AH, LDAPv2, PKIX
Security Standards	IPSec, IKE, X.509v3, PKIX, LDAPv2, RSA, X.500, PKCS11
Capacity	500 (2520/4520) and 2,000 (7520) simultaneous secure sessions
Performance	Gateways at 3-DES: 4Mbps (2520), 10 Mbps (4520), and 70Mbps (7520) Directories: 10 thousand nodes (Entrust), 1 million nodes (ICL)

Certifications	ICSA-IPSec ISO 9000 designed to meet FIPS-140-1
System management	PERMIT/Director (policy management) Entrust/Manager (certification authority) PERMIT/Config (remote configuration)

A. 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 client 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.

B. Introducing PERMIT Enterprise

TimeStep, a pioneer and industry leader in the secure VPN marketplace, has been developing secure VPN hardware and software solutions since 1994. TimeStep has the most experience deploying secure VPNs and was the first to integrate PKIs and X.500 directories. Our comprehensive system consolidates management of secure VPN, access control, and authentication to reduce the cost and complexity of network security administration.

Figure 1 shows a network setup including the full suite of PERMIT Enterprise products.

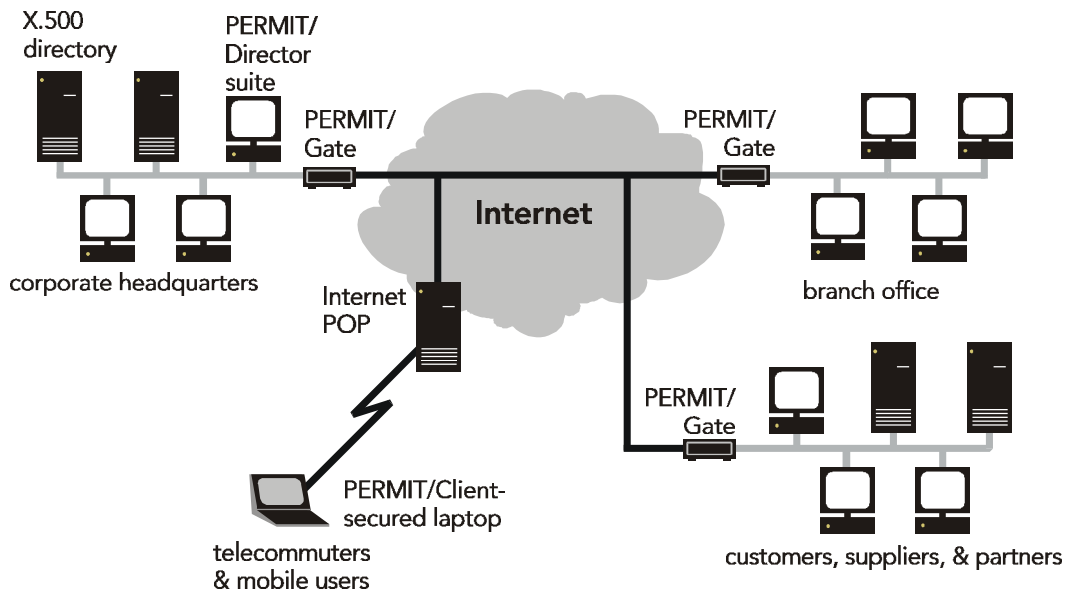


Figure 1: Secure VPN components

◆ **PERMIT/Gate 2520, 4520, and 7520**

The PERMIT/Gate is an industry-leading gateway that secures data communications for intranets, extranets, and Internet remote access.

PERMIT/Config is software that allows you to manage multiple gateways from any point on your secure VPN.

PERMIT/Gate supports:

- ◆ IPsec-compliant key negotiation and tunneling
- ◆ thousands 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	Application
PERMIT/Gate 2520	4 Mbps	500	Branch office & remote access: T1
PERMIT/Gate 4520	10 Mbps	500	Corporate, large branch office & remote access: Ethernet
PERMIT/Gate 7520	70 Mbps	2000	High bandwidth & remote access: T3, 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 or WINS
- ◆ 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. The PERMIT/Director suite includes PERMIT/Director, Entrust/Manager™, and Entrust/Directory™.

PERMIT/Director gives you sophisticated, flexible access control. With PERMIT/Director's directory-based policy, you can connect two LANs using two PERMIT/Gate 2520, 4520, or 7520 units. These LANs can then be layered and subdivided into any number of entirely discrete or partially interconnected secure VPNs. This gives you the ability to control who communicates with whom allowing you to manage multiple secure VPNs under one or more PKIs. PERMIT/Director

creates attribute certificates that define VPN membership and assembles them into desired VPN groups.

Entrust/Manager is an industry leading CA that creates and manages X.509 digital certificates. The digital certificates are used to authenticate secure VPN tunnels and tie them to actual users. Certificates and the CA concept offer a number of powerful benefits in sophisticated secure VPNs including cross-certification, for large scale implementations.

The LDAP-compliant X.500 directories: The PERMIT Enterprise secure VPN uses an LDAP-compliant directory as a public repository of certificates, both “identification” certificates generated by the CA and the attribute certificates generated by PERMIT/Director. The directory serves PERMIT/Client-protected nodes and PERMIT/Gates. Whenever communication is initiated, the PERMIT/Gate or PERMIT/Client can contact the X.500 directories to verify the following:

- ◆ a nodes’ certificate has not been revoked (by checking with the Certificate Revocation List)
- ◆ communications between the two nodes is permitted (by checking group certificates)

Using an industry-standard X.500 directory also augments possibilities for interoperability. You can configure your X.500 server to be cross-certified with other X.500 servers. This allows you to incorporate existing X.500 directories into extranets between business partners.

Entrust/Directory, the X.500 directory supplied with the PERMIT/Director suite, supports up to 5,000 records. For a solution that scales to millions of entries you can order ICL’s i500 directory.

C. The Impact of PERMIT Enterprise

The PERMIT Enterprise product line gives you unprecedented power and flexibility to build secure VPNs that are easily extensible and interoperable. PERMIT Enterprise secure VPN products can solve your internetworking problems whether you’re looking for branch office internetworking, peer to peer networking with business partners, Internet remote access solutions, or a combination of all three.

D. PERMIT Enterprise secure VPN applications

PERMIT Enterprise has three main applications—intranets, extranets, and Internet remote access. Each of these applications draws different benefits from the PERMIT Enterprise suite of products.

Intranets—cost-effective secure branch office connectivity

Branch office connectivity over the Internet is a practical, low-cost alternative to leased line wide-area networking and gives you the flexibility to connect with small or distant offices, which may not have been feasible before now. PERMIT Enterprise enables your business to establish secure communication paths through the Internet to branch offices anywhere, thus extending your corporate intranet to every corner of the world. Many organizations are taking advantage of securing communications to branch offices and suppliers around the world.

Remote access—protection for your remote users

Remote access via the Internet eliminates the capital costs and toll charges associated with private remote access facilities while allowing telecommuters to leverage off the high-speed Internet access available from an NSP. PERMIT Enterprise extends your secure corporate network over the Internet to the remote workstation or mobile user with strong user authentication, encryption, and data integrity. You eliminate costs and gain worldwide connectivity at the same time.

Extranets—vendor, customer, and collaborative networks

Networks between corporations drive the efficient operation of business-to-business commerce. As an IPSec-compliant solution, PERMIT Enterprise enables you to establish extranets with your partners, suppliers, and customers while cross-certification allows you to maintain the security of your internal network by setting and managing your own network security policy. Supply chain networks such as the Automotive Network eXchange® (ANX®) are taking advantage of secure VPNs today.

For more information on implementing a secure VPN within these applications read TimeStep's *VPN Solutions Guide*. Visit www.timestep.com in the Resource Centre under Resources to download a copy.

III Proposed Solution

In accordance with Powell Electrical Manufacturing Companies' requirements for the proposed VPN solution, we are bidding our fully IPsec compliant PERMIT Enterprise solution which consists of PERMIT/Gate, PERMIT/Client, PERMIT/Director and the Entrust® Certification Authority and Informix X.500 Database.

Central Office

For the telecommuters, mobile sales force, and executives, we propose the use of our PERMIT/Client software. The PERMIT/Client software addresses the need for a solution for Windows '95, Windows'98, Windows NT 4.0 and Macintosh for both dialup and Ethernet applications. PERMIT/Client can be used in virtual tunnel mode to allow browsing of the corporate network that would not otherwise be available with other vendors' products. Virtual Tunneling™ allows you to present yourself as a node on the subnet you are connecting to and thus use NetBios to browse the network, print, share files and access Intranet servers as though you were directly connected to the subnet. PERMIT/Client also allows those users who are dialing into different corporate sites to create and save site profiles so that they can easily change the gateway they are tunneling to and the IP address they are presenting themselves as.

It is important to note that while PERMIT/Client can easily handle the demands of the remote users, the limiting factor may be the network connections that are provided. For this reason it is suggested that possibly an ISDN, xSDL, or Cable Modem Internet connection be considered for power users such as the telecommuters.

Subsidiaries

In order to provide the necessary levels of security between the central PEMCO Houston site and the various subsidiaries throughout the network we propose placing a PERMIT/Gate 7520 (70 MEG, fully IPsec compliant gateway) in front of access point to the central site and the use of the PERMIT/Gate 2520 as the access points into the subsidiaries' networks. Placing PERMIT/Gates between the corporate backbone and the subsidiaries will not only allow you to restrict access to any networks but will also allow seamless encryption of all/some of the traffic to and from the networks.

The PERMIT/Gate 7520 was chosen because it provides the bandwidth necessary to support the eight subsidiaries plus all of the remote users who will also be connecting into the network. The PERMIT/Gate 2520 was chosen rather than the PERMIT/Gate 4520 (10 MEG, fully IPsec compliant gateway) as none of the WAN links exceed T1 speeds and rarely will 10 MEG Ethernet traffic exceed the 4Meg

throughput of the gateway. The 1520 (2 MEG, 25 connection, fully IPsec compliant gateway) was not chosen as it supports a limited number of users.

Management

In order to provide the users with confidentiality, authentication, integrity and automatic key management, we are proposing the use of the Entrust® Public Key Infrastructure (PKI). The Entrust PKI is fully integrated with the PERMIT Enterprise product line and therefore brings all the Entrust benefits with it. This includes cross-certification, LDAP-compliant X.500 directories, support for X.509v3 certificates, RSA algorithms (1024 bit signatures), support for TCP/IP, LDAP, IETF PKIX protocols, IPsec compliance, and unlimited scalability. It is also suggested that in the interests of scalability and security that the Entrust® PKI and X.500 directory services be placed on separate hardware platforms.

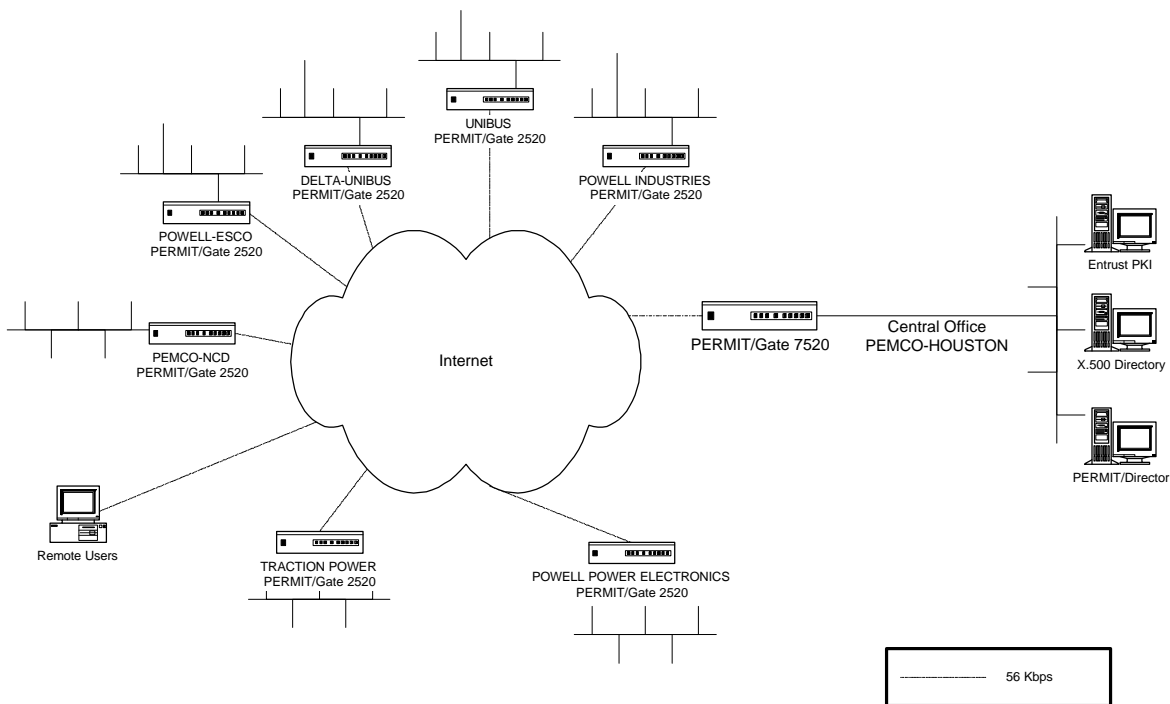
To control access to the subnets, we are proposing the use of PERMIT/Director. PERMIT/ Director is a group administration tool that establishes secure VPN access control by assigning users and resources to groups. This will allow access rights to be setup not only for the subnets but also resources on those subnets.

Through the use of PERMIT/Director group membership is assigned through the GUI. Users can either be imported directly from the X.500 directory or manually created in PERMIT/Director. In order for two network entities to set up a Secure Association through which to communicate, they must have at least one like group membership. (There is no limit on the number of groups a node can belong to nor is there a limit on the number of groups PERMIT/Director can handle.) PERMIT/Director can be administered remotely and will allow system administrators to make changes from the network at anywhere and at anytime through DCOM with the added security of doing it all through an encrypted tunnel back to the server.

In order to allow remote configuration/administration of PERMIT/Gate we propose the use of PERMIT/Config. This utility can be run from any Windows '95 or Windows NT 4.0 workstation or server and will allow complete configuration, monitoring and uploading of new software to PERMIT/Gates anywhere on the network. This application uses the HMAC hashing algorithm and a password to encrypt the communications ensuring all traffic between the GUI and the application. Therefore, it is not vulnerable to attack.

In addition to all of the above management systems PERMIT/Gate can be managed by SNMP. Statistical information can be retrieved using any of three methods: SNMP; use of PERMIT/Config to retrieve logs; setting PERMIT/Gate to "push" information to a syslog server where a standard accounting package can be used to format the data.

PERMIT Enterprise Solution



Fault Tolerance

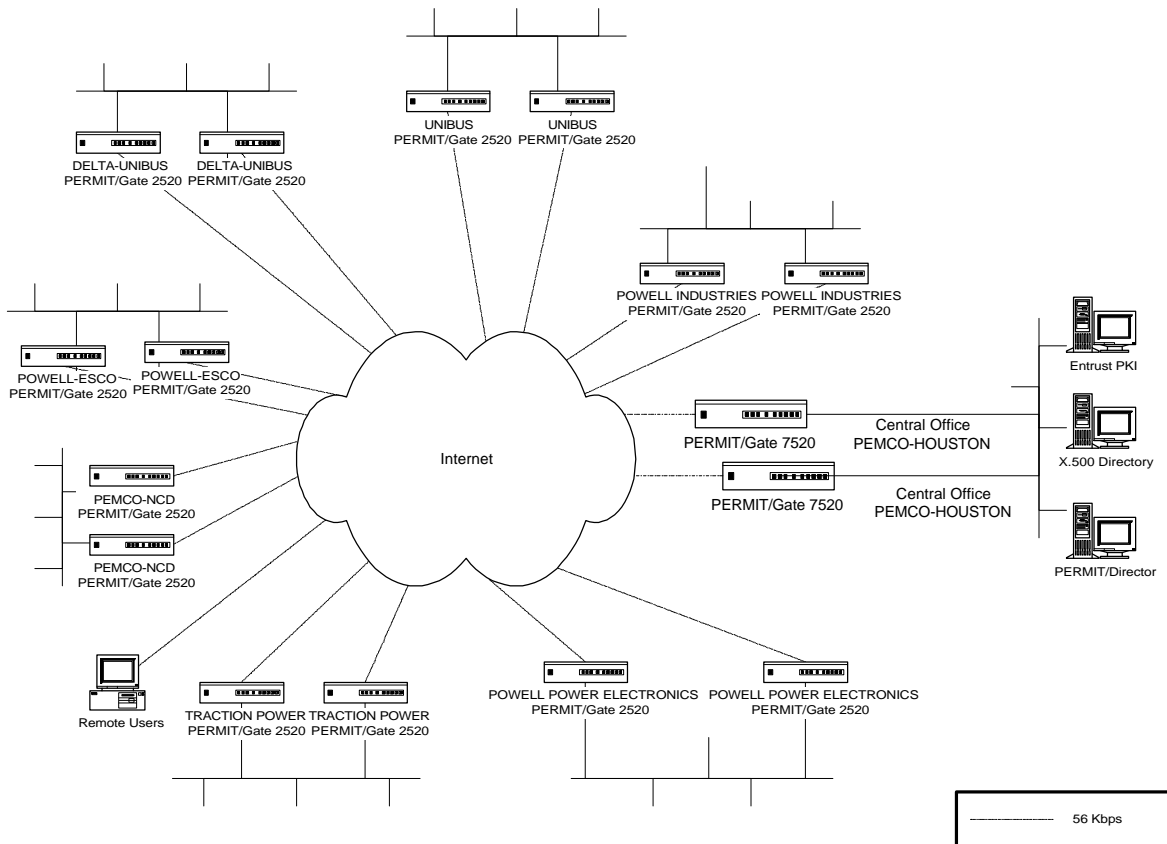
Currently PERMIT Enterprise does not directly support fault tolerant solutions in so much as user intervention is necessary. A complete hot standby solution is planned for a future release however through the use of careful planning a manual solution is available.

In order to provide fault tolerancy with your network topology it is suggested that two PERMIT/Gate 7520's be placed in parallel at the corporate site and two PERMIT/Gate 2520's be placed at each of the subsidiary sites. By using this method you have the option of either sending all the traffic between one PERMIT/Gate 7520 and a PERMIT/Gate 2520 or by setting up half of your network to point their default gateway at one PERMIT/Gate and the rest at the other. By doing this, you in effect have load sharing. In the event of a failure all that is required is to modify the default gateway on the nodes behind each PERMIT/Gate to point at the working unit.

As far as client fault tolerance is concerned, each PERMIT/Client can have multiple profiles (connection points) allowing the user to select which PERMIT/Gate they wish to connect to. In the event that you cannot get connected to one of the PERMIT/Gates that is protecting the network, the profile can be changed to the other available PERMIT/Gate on the fly.

NOTE: In order to have complete fault tolerance it is suggested that redundant links be put in between each site i.e. two 56K frame links to each site, as this is the only way to ensure that the network does not go down. Also note that a redundant PERMIT/Director suite option was not proposed because with proper backup procedures, it is our opinion, that reasonable fault tolerance can be provided.

PERMIT Enterprise Solution With Fault Tolerance



Issues

With regards to the IPX traffic on your network, all IPX must be set up on the servers to be tunneled in IP if it is to be sent through PERMIT/Gate as it supports only IP traffic in accordance with the IPSec standard.

Although there is no mention of firewalls in the description of the Powell Electrical Manufacturing Co.'s network it must be noted that any firewall must have the following ports opened:

- ◆ IP packet types 50 and 51 (decimal) to allow ESP and AH packets to pass.

- ◆ UDP port 500 for ISAKMP negotiations, port 38036 decimal to allow PERMIT Config to communicate with the gates to pass.
- ◆ If the CA and the X.500 directories are on either side of the firewall you need to open TCP port 389 (decimal) (if Entrust® default is used) for LDAP communications to the X.500 directory.
- ◆ Port 709 (decimal) (if Entrust® default is used) for communications to the Certification Authority.

Customer Support Services

TimeStep Customer Support Services offers a range of professional offerings to meet our customer needs. Services are offered from our head office located in Kanata (Ottawa), Ontario, Canada and through our offices located in Herndon, Virginia; Santa Clara, California; Dallas, Texas; London, England and Hong Kong, China.

Virtual Employee Programs

Standard and customized maintenance programs are available for all TimeStep customers and partners. Service programs are available for varying time periods—from days to months or longer.

Technical Assistance and Support Services

- ◆ 24 x 7 Telephone Assistance
- ◆ Product configuration, network analysis and installation guidance
- ◆ Maintenance Software Service
- ◆ Technical Web Support including online-product information

Annual Maintenance:

Annual maintenance fee for technical support (TAC, software upgrades, emergency equipment replacement).

Instructor-led Training (Public Course)

TimeStep offers training on a monthly basis at our headquarters located at Kanata (Ottawa), Ontario, Canada. This two day course is for the new PERMIT Enterprise administrator who is responsible for installing and maintaining their PERMIT Enterprise solution. It provides hands-on exercises where you will install, configure, and test a secure virtual private network (VPN) using Shared Secret or Entrust certificates as the authentication mechanism.

Instructor-led Training (Custom/On-site Course)

TimeStep offers customized training that can be held either at our head-quarters located at Kanata (Ottawa), Ontario, Canada or at the customer site. We can tailor our training to suit your needs.

IV Pricing

In keeping with our proposed secure VPN solution, please find below a breakdown of the pricing. Note that whenever possible bundled options were used to reduce the cost. All prices are full list. All prices are in US Dollars and do not include applicable taxes. . Standard versions support DES, 3DES, BLOWFISH, CAST and RC5.

PERMIT Enterprise Solution

Total cost: \$56,958

7 PERMIT/Gate 2520's				
PERMIT/Gate 2520 Version 1.1	Standard Version	TSHW-2520-IPSC	\$3,995 each	Two port Ethernet gateway with up to 4 Mbps throughput with IPSec Secure VPN application. Supports 500 concurrent users and includes PERMIT/Config.

1 PERMIT/Gate 7520				
PERMIT/Gate 7520 Version 1.1	Standard Version	TSHW-7520-IPSC	\$10,995 each	Two 10/100bt port Ethernet gateway supports T3 connections with IPSec Secure VPN application. Supports 2000 concurrent users and includes PERMIT/Config.

1 PERMIT/Director Suite				
PERMIT/Director Suite Version 1.1	Standard Version	TSMG-PDSU	\$11,995 each	A bundled option of PERMIT/Director, Entrust/Manager, Entrust/Directory, PERMIT/Config and a copy of the PERMIT/Client for Windows manual and software.

69 PERMIT/Clients				
PERMIT/Client with Public Key Infrastructure (PKI) authentication. PERMIT/Client option with Entrust certificate for use with a PERMIT/Director Suite or Entrust/Manager and Entrust/Directory, also supports shared secret authentication.	Standard Version	TSSW-WNDW-PKI	\$87/user	PERMIT/Client with PKI authentication (Entrust Ready) for Windows 95/98 and NT 4.0 User License (Shipment includes license agreement only).

PERMIT Enterprise Solution with Fault Tolerance

Total cost: \$95,918

14 PERMIT/Gate 2520's				
PERMIT/Gate 2520 Version 1.1	Standard Version	TSHW-2520-IPSC	\$3,995 each	Two port Ethernet gateway with up to 4 Mbps throughput with IPsec Secure VPN application. Supports 500 concurrent users and includes PERMIT/Config.

2 PERMIT/Gate 7520				
PERMIT/Gate 7520 Version 1.1	Standard Version	TSHW-7520-IPSC	\$10,995 each	Two 10/100bt port Ethernet gateway supports T3 connections with IPsec Secure VPN application. Supports 2000 concurrent users and includes PERMIT/Config.

1 PERMIT/Director Suite				
PERMIT/Director Suite Version 1.1	Standard Version	TSMG-PDSU	\$11,995 each	A bundled option of PERMIT/Director, Entrust/Manager, Entrust/Directory, PERMIT/Config and a copy of the PERMIT/Client for Windows manual and software.

69 PERMIT/Clients				
PERMIT/Client with Public Key Infrastructure (PKI) authentication. PERMIT/Client option with Entrust certificate for use with a PERMIT/Director Suite or Entrust/Manager and Entrust/Directory, also supports shared secret authentication.	Standard Version	TSSW-WNDW-PKI	\$87/user	PERMIT/Client with PKI authentication (Entrust Ready) for Windows 95/98 and NT 4.0 User License (Shipment includes license agreement only).