TIMESTEP

PERMIT Enterprise: An architectural overview

SECURE VIRTUAL PRIVATE NETWORK SOLUTIONS

IMPORTANT NOTICE

Trademarks

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

Rev. No. ARCH2.0—April 1999

Executive summary

TimeStep®'s PERMIT Enterprise™ product suite is an IPSec-compliant secure virtual private network (VPN) solution that enables businesses to communicate securely over the Internet. Using the Internet as a carrier is an extremely flexible and cost-effective alternative to other methods of building global networks.

The PERMIT Enterprise architecture was designed to be scalable, directory-enabled, and centrally managed. In fact, this architecture is used by some of the largest and most demanding telecommunications companies in the world to offer new IP VPN services.

The three main components of TimeStep's secure VPN solution are the PERMIT/Gate™ family of security gateways, PERMIT/Client™ software applications, and the PERMIT/Director™ suite management infrastructure.

The PERMIT/Gate is a tamper-resistant gateway that secures data communications for intranets, extranets, and Internet remote access. TimeStep has four different gateways to suit your network traffic needs—PERMIT/Gate 1520, 2520, 4520, and 7520, depending on your bandwidth requirements.

The PERMIT/Client software secures network traffic for a single workstation and is ideal for Internet remote access by telecommuters and business travelers.

The PERMIT/Director suite contains the software applications used to manage the people and resources protected by PERMIT Enterprise products within your secure VPN.

The three main applications for PERMIT Enterprise are intranets, extranets, and Internet remote access. PERMIT Enterprise's particular strength is its ability to support secure VPNs with many thousands of nodes and multiple VPNs.

Contents

Introduction

Before secure VPN

Five years ago, if you wanted a global network, you built it yourself.

In order to link branch offices to the corporate network, you might have leased your own high-speed lines, and bought your own multiplexors. To provide your road warriors with access to the corporate network, you installed dial-up servers and banks of modems. And you maintained them yourself. When the rush of technology forced changes, you absorbed the cost of upgrades.

Securing those networks for government and financial applications usually required expensive link encryptors (T1 or T3) to secure communications from hop to hop. In these situations remote access was out of the question unless backed by hardware encryption for dial-up applications.

If you found those networks inflexible and the costs too high, you made do with the fax and telephone, shipped magnetic media by courier, and wished for the day when safe inter-office email and file transfer might become affordable.

Secure VPN

That day is here. These factors make it possible:

- the rapid growth of the Internet to become a truly global communications medium and THE business network for business to business communications
- the maturation of secure VPN solution technologies
- the standardization of the IPSec protocol for secure VPN technology
- the introduction of Network Service Providers (NSPs) providing service level guarantees for Internet connectivity
- the constant emergence of new Internet applications
- the growing dominance of IP

With the advent of secure VPN solutions, you can use the Internet for safe, flexible, extensible, and inexpensive global corporate networking. The reach of the Internet and the quality of service improve daily. With the right network security technology, you can simply plug into this existing global network and never give another thought to building your own.

Business drivers for VPNs

Organizations are finding that secure VPNs are providing them with more and more ways to enable business communications over the Internet. The business drivers for secure VPN solutions include the:

- dramatic increase in telecommuting, branch offices, and mobile work force
- high cost of implementing and maintaining private networks
- need to interact with trading partners
- strong security required by many organizations such as government and finance

These business drivers and more make it not only feasible for businesses to deploy a secure VPN solution but cost effective as well.

(Check out TimeStep's *Business Case for Secure VPNs* for more information. **Visit www.timestep.com under Resources.**)

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
- allows 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

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. The architecture of our PERMIT Enterprise product suite is designed 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 infrastructure. And its client software is seamless—fully transparent to users and applications.

In this paper

This paper covers:

- secure VPN concepts, including IPSec, tunneling, certificates, and shared secret authentication
- the three principal applications of PERMIT Enterprise: intranets, extranets, and Internet remote access
- the PERMIT Enterprise product suite
- the overall network topology and architecture of the PERMIT Enterprise IPSec-compliant secure VPN

Secure VPN concepts

What is a secure VPN?

A secure VPN is a communications network secured by encryption and authentication and layered on existing public networks, like the Internet, or, in some cases, through a large corporate WAN.

A properly-configured secure VPN using robust encryption technology appears to internal users to be a secure, isolated office LAN or WAN running entirely over private lines. The major differences between a secure VPN and traditional private networks are real security (not just privacy), flexibility, extensibility, and cost. For secure global connectivity, secure VPNs are the only option for many companies today.

Secure VPNs are based on a number of underlying technologies:

- IPSec, the IP security standard recently established by the Internet Engineering Task Force (IETF)
- tunneling, which allows private networks to cross the Internet using unregistered IP addresses
- certification and third-party authentication through certification authorities or shared secret authentication for small secure VPNs

IPSec

The technology to implement secure VPNs has been around for only a few years, but reached a new level of maturity in early 1997 when an international working group coordinated by the IETF reached substantial agreement on the details of the IPSec protocol suite standard. This made it the first and only interoperable security standard for IP.

The standardization of the IPSec protocol suite means secure VPN can be a painless part of any existing IP network. You can use existing IP networks like the Internet as data carriers, without the security risks inherent to IP. You can link any two LANs in the world for a fraction of the cost of leased lines. Mobile sales forces can call in through a local point-of-presence (POP) anywhere in the world, saving you from having to maintain dial-up servers for direct dial-up remote access.

Better still, IPSec allows you to interoperate with partners, suppliers, and buyers that use IPSec-compliant equipment and software. If you have an IPSec-compliant secure VPN, and the people you do business with have an IPSec-compliant secure VPNs, nothing but a few configuration changes prevents you from giving each other carefully controlled access to each other’s networks.

Tunneling

Among other benefits, IPSec allows for the tunneling of private, unregistered corporate addresses over public, registered addresses such as the Internet.

Tunneling hides the unregistered address inside a packet that uses a registered IP address when the tunneled message moves onto the Internet. This not only makes it possible to use the Internet as a carrier, it also protects the identity of the user by hiding the address.

TimeStep's Virtual Tunneling allows the remote client to appear as a local user on your internal network while maintaining its Internet address for normal Internet access. This enables mobile users to login to their privately addressed corporate network securely from any ISP and surf the Internet at the same time without the overhead of Network Address Translation (NAT).

TimeStep adds to the tunneling concept, internal secure VPN descriptive machine names, by providing for domain name servers specifically for use by tunneling machines. You can even tunnel your DNS and WINS lookup requests, and resolve the machine name inside the secure VPN.

Certificates and third-party authentication

IPSec's sophisticated authentication infrastructure offers the most robust and scalable approach to authentication yet devised: certificates and certification authorities (CAs).

Using certificates allows you to delegate authentication services to industry standard CA servers, from which security administrators distribute authentication information.

IPSec CAs use industry standard LDAP-compliant database servers, such as the X.500, to store their information. CAs can then take advantage of the X.500's built-in support for distributed databases, making it easy and reliable to set up large, decentralized authentication server networks.

Certificates and VPN Policy

Attribute certificates containing secure VPN policies can also be defined for groups of users, making even complex secure VPNs involving multiple trading partners and millions of users easy and intuitive to maintain.

Attribute certificates store permissions associated with a certificate. Each user on the secure VPN has an attribute certificate associated with their name. These certificates are stored in the LDAP-compliant directory, along with the public key certificates, giving you the benefit of keeping your policy authenticated by a trusted third party.

Attribute certificates allow you to create secure VPN groups. Each member's attribute certificate lists the groups of which it is a member. As long as two attribute certificates show at least one group in common, the nodes are allowed to communicate.

Shared secret authentication for smaller secure VPNs

For smaller, less complex secure VPNs, IPSec specifies simpler 'shared secret' authentication options. Shared secrets allow you to set up the secure VPN without a certificate infrastructure by using passwords for your users.

IPSec's Internet Key Exchange (IKE) protocol now includes an extended authentication model so that existing authentication infrastructures can be supported.

The PERMIT Enterprise product suite

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. (For a description of the communications protocols that PERMIT Enterprise uses, see *PERMIT Enterprise topology and communications* in this paper.)

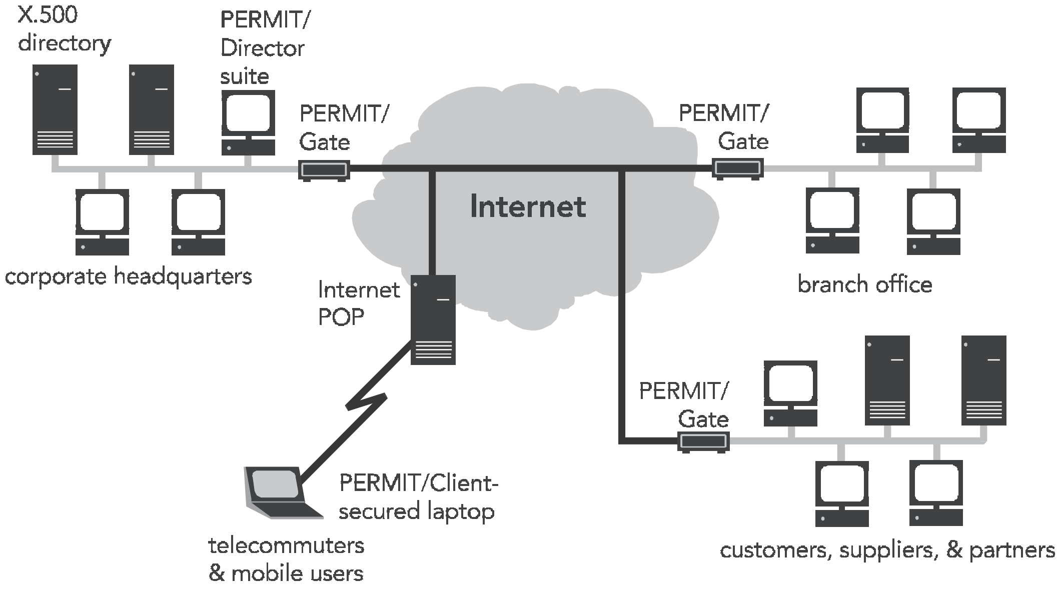


Figure 1: Secure VPN components

PERMIT/Gate 1520, 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™ is a software package 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 secure tunnels
- 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 secure tunnels	Application
PERMIT/Gate 1520	2 Mbps	25	SOHO & telecommuters: cable modems & DSL
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

Table 1: PERMIT/Gate 1520, 2520, 4520, and 7520

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 1520, 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 the ‘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 that:

- a node’s certificate has not been revoked (by checking with the Certificate Revocation List)
- communication 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, or you can order ICL’s i500 directory that scales to millions of entries.

The impact of PERMIT Enterprise

The PERMIT Enterprise product line gives you unprecedented power and flexibility to build secure VPNs that are easily scalable 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.

PERMIT Enterprise secure VPN scenarios

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.

(Check out TimeStep's *VPN Solutions Guide* for more information on implementing a secure VPN within these applications. **Visit www.timestep.com under Resources**.)

How you combine the PERMIT Enterprise components to form your secure VPN depends on what you need your secure VPN to do. The following scenarios depict some common configurations.

Scenario 1: Secure Internet remote access

Providing Internet remote access services to telecommuters and mobile users with IPSec-compliant secure VPN products has a number of distinct advantages over using traditional dial-up server solutions. It is simpler in terms of the necessary infrastructure, less expensive to maintain, completely transparent to the user and the user's applications, and more flexible. Your users can take advantage of new access technologies, such as cable modems or DSL, without you having to change equipment at the corporate site.

Here's how a network set up for Internet remote access with the PERMIT Enterprise family of IPSec-compatible products might look:

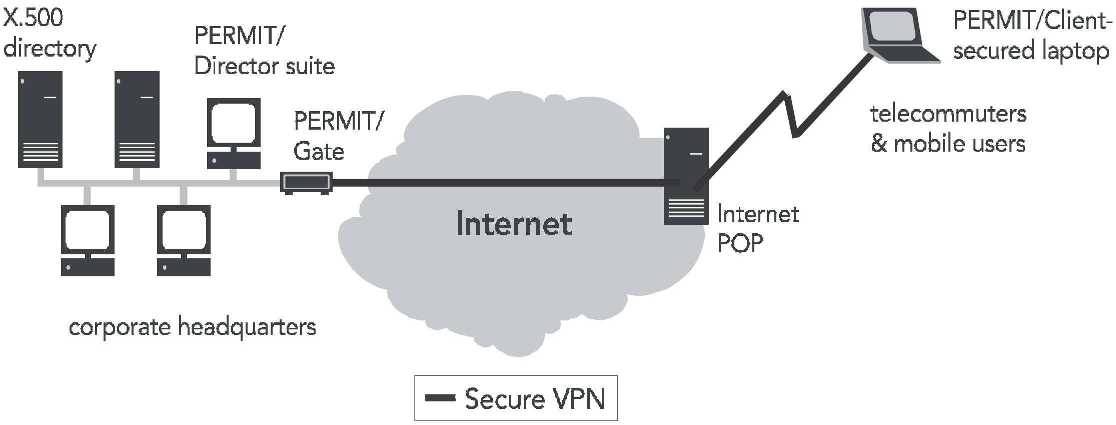


Figure 2: Certificate-based, Internet remote access secure VPN

This secure VPN uses a CA for authentication, and provides Internet remote access services. The components provide the following functions:

- The PERMIT/Gate in front of the office LAN provides secure VPN services from one end.
- PERMIT/Client installations on the telecommuters and mobile users' laptops provide the services from the other end.
- PERMIT/Director suite provides access control, dictating which nodes may communicate with which other nodes. Entrust/Manager, a component of the PERMIT/Director suite, is the CA that registers and manages certificates.
- The X.500 server stores all certificates for authentication including attribute certificates that define secure VPN group membership.

Dial in from anywhere

The ISP's Internet POP shown in the diagram could be any server, anywhere in the world. So your field agents can connect to the nearest available server, saving you long distance charges and providing a more reliable data connection.

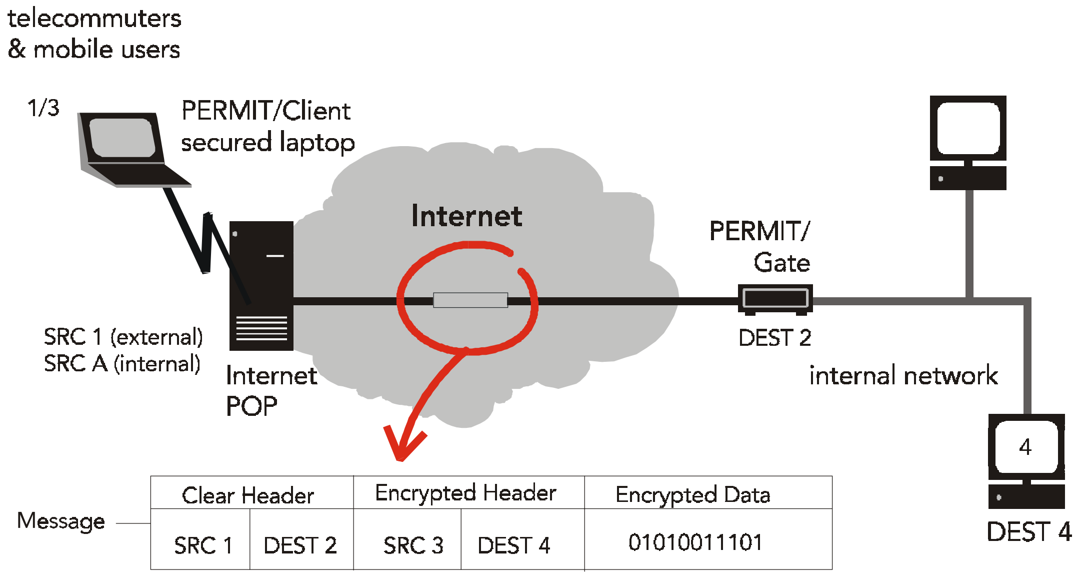
Virtual Tunneling

TimeStep's PERMIT/Client software is the first IPSec Virtual Tunneling client in the world of secure VPNs.

The diagram below shows how Virtual Tunneling allows a remote PERMIT/ Client node to use both an internal and an external address to become part of the PERMIT/Gate-protected network while surfing the Internet at the same time.

The PERMIT/Client-protected node uses an ISP-assigned public IP address (1) to surf the Internet in the clear. At the same time, the PERMIT/Client-protected node has an internal IP address (3), assigned by the PERMIT/Gate, which it uses when securely accessing the internal network behind the PERMIT/Gate. When it tries to contact a node on the protected network (4), PERMIT/Client uses two headers on its messages: a clear header and an encrypted header. The clear header is the same as in tunnel mode: source address (1) and PERMIT/Gate destination address (2).

However, in virtual tunnel mode, the encrypted header contains the internal address of the source PERMIT/Client (3) and the internal address of the destination node behind the PERMIT/Gate (4). In fact, this is true IPSec tunneling and identical to IPSec tunnel mode in a gateway to gateway scenario.



	Clear Header		Encrypted Header		Encrypted Data
Message	SRC 1	DEST 2	SRC 3	DEST 4	01010011101

Figure 3: Virtual Tunneling

For more information on tunneling, see *Tunneling in the PERMIT Enterprise secure VPN* in this paper.

Scenario 2: Branch office connectivity

Linking branch offices together via the Internet with secure VPN products can be achieved in two ways. In the simplest configuration, you could link two small branch offices with shared secret authentication. For linking more and larger branch offices, you can set up your secure VPN with a CA and enhance it with an Entrust CA and/or a PERMIT/Director.

Branch office connectivity using shared secret

In terms of scalability, shared secret secure VPNs do not provide the same level of access control that certificate-based VPNs offer. However, they do provide secure VPN services, and in a configuration with only two branch offices, as shown in Figure 4, there is no need to provide more sophisticated access control. Shared secret authentication keeps it simple. The two separate office LANs become, for the purposes of internal users, one corporate LAN with one exception; you can configure the PERMIT/Gates to restrict host access on the LAN side of the gateway.

For more information on shared secret, see *shared secret authentication* in this paper.

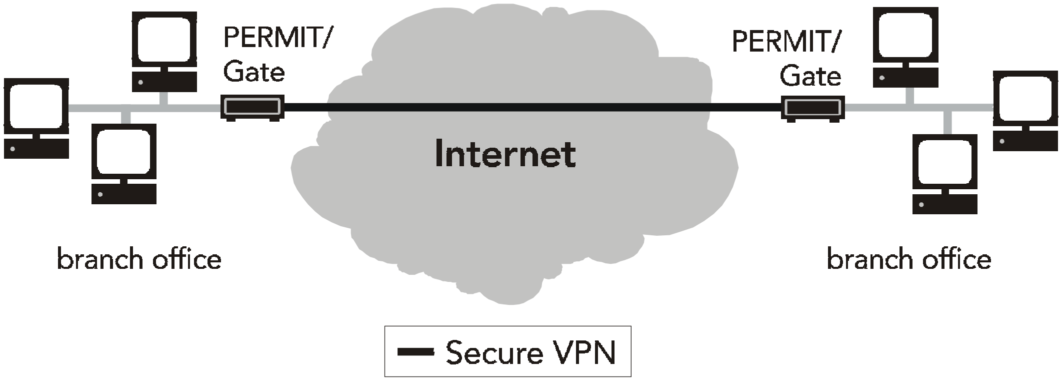


Figure 4: Shared secret branch office secure VPN

Branch office connectivity using PERMIT/Director

The configuration shown in Figure 5 supports a more complex structure. By including PERMIT/Director, you can set up secure VPN groups to control who can communicate with whom. Figure 6 illustrates this in more detail, but with trading partners rather than branch offices.

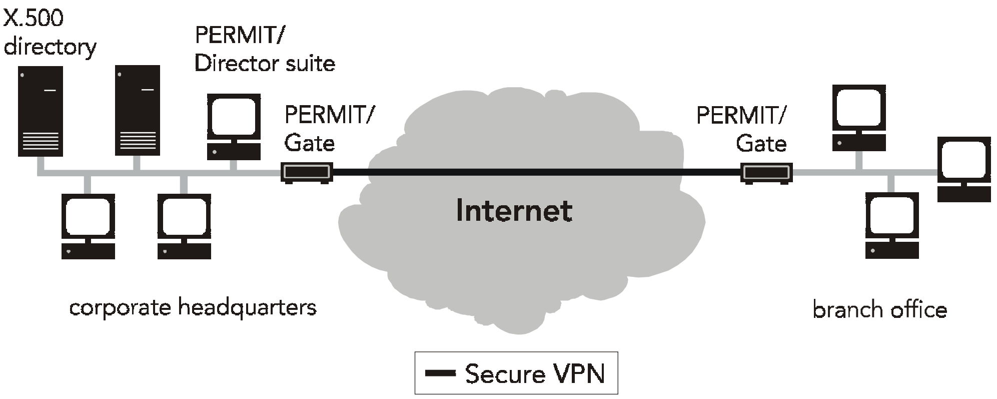


Figure 5: Branch office secure VPN with PERMIT/Director

Scenario 3: Trading partners and extranets

The interoperability that IPSec-compliance provides offers powerful advantages in complex secure VPN implementations, involving extranets between trading partners.

In the diagram below, business A is a large business with many significant trading partners (businesses B, C, and D). Each trading partner has its own network and would like access to parts of business A's LAN.

N.B. For added security, PERMIT/Director can be added to each company's network to manage PERMIT/Gates while sharing an X.500 directory.

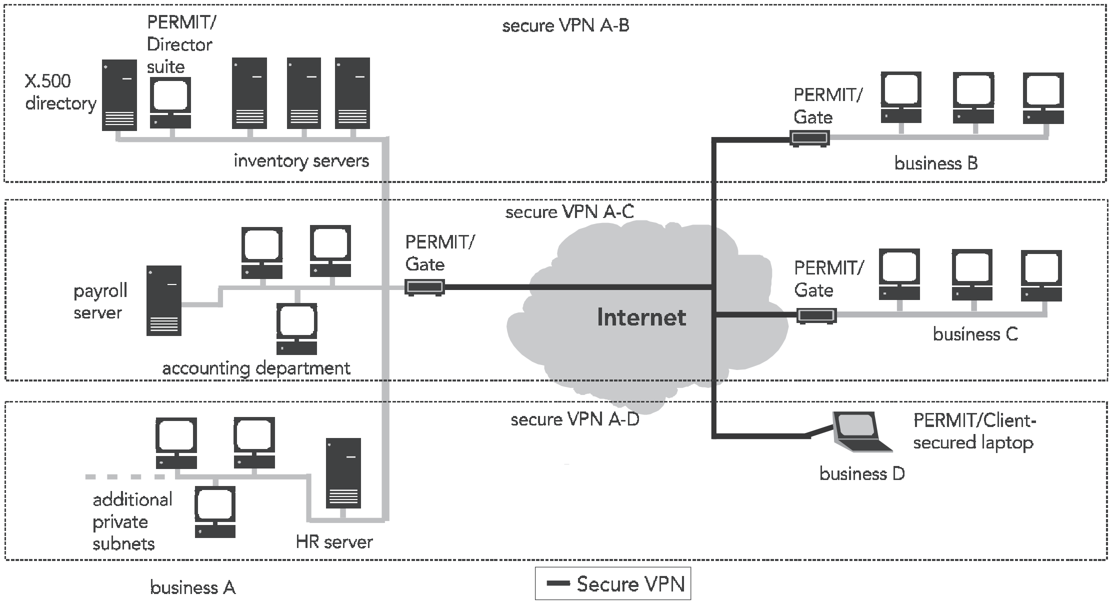


Figure 6: Certificate-based extranet secure VPN

Business B supplies business A with parts. Business A would like business B to have access to a bank of servers carrying an inventory database, so they can more easily coordinate ordering and delivery.

Business C is a payroll company that handles business A's payroll needs. Business A would like business C to have access to a server carrying employees' time sheet files as well as to a number of specific nodes in the internal accounting department.

Business D is a human resources firm responsible for much of business A's hiring. Business A wishes to give business D's consultants limited access to personnel information on their servers, so the consultants can plan their hiring ahead.

In the above configuration, the three extranet secure VPNs are defined (A-B, A-C, and A-D), and a single PERMIT/Gate negotiates all of these for business A.

The secure VPNs in this example do not overlap, though that is also possible. Nothing prevents business A from giving groups of nodes within businesses B and C access to the same server, while maintaining separation between businesses B and C, for example.

Shared X.500 servers and CAs

In this scenario there is one single X.500 server in business A's network. Neither businesses B, nor C, nor D have their own, nor do they necessarily need one. If their own networks are small enough to make it practical, they may actually use shared secret within their own secure VPNs (if they have them). However, when negotiating with nodes at business A, their PERMIT/Gates and PERMIT/Client-protected nodes can query business A's X.500 server to authenticate identities.

The multiple secure VPN alternative

However, businesses B, C, or D could also have their own CA and/or their own X.500 server. The CAs could cross-certify one another, allowing seamless authentication between the domains served by the two CAs.

Cross-certification makes possible the creation of global secure VPN networks involving many companies and many thousands of nodes (see also *cross-certification* in this paper).

PERMIT Enterprise authentication options

PERMIT Enterprise's flexible architecture allows you to use two authentication options in your secure VPN, depending on security needs and the scale of your network:

- shared secret authentication
- authentication with certificates

Authentication with shared secrets and authentication with certificates differ in conceptual complexity, the level of control over communications they allow, and the amount of additional equipment you will require to use them.

- Shared secret authentication is conceptually simpler, and requires less equipment, but offers less flexibility and can be more work to maintain.
- Certificates require additional equipment, but offer more flexibility, and are easier to maintain. Certificates make scaling secure VPNs much easier, and for that reason are more practical in larger secure VPNs, and in secure VPNs that may grow.

IPSec's Internet Key Exchange (IKE) protocol has been extended to include an extended authentication model so that existing authentication infrastructures can be supported.

Shared secret authentication

Shared secret authentication is practical in small, simple secure VPNs, in which layered security and linking with trading partners' extranets is not an issue.

With shared secret authentication, for two nodes to communicate securely through the public network, both PERMIT/Gates (or the PERMIT/Gate and PERMIT/Client, or the PERMIT/Gate and the third party IPSec-compliant security device) involved in the exchange must be configured with identical shared secrets.

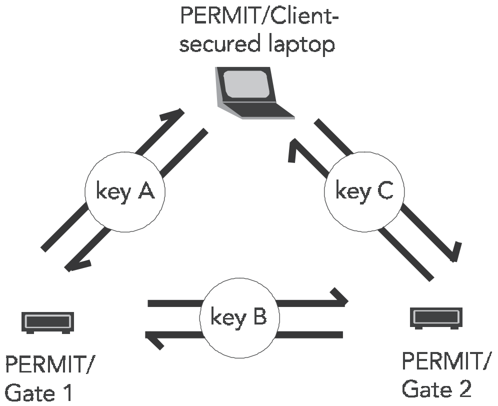


Figure 7: Three way shared secret example

With shared secret authentication, updating the shared secrets becomes more difficult as the number of nodes involved increases, as you have to distribute new secrets manually.

Authentication with certificates

With PERMIT Enterprise, the main advantages of authentication with certificates are:

- user-based certificates
- access control via secure VPN groups
- cross-certification for creating multiple secure VPNs

User-based certificates

The Entrust CA issues user-based certificates.

The advantage of user-based certificates is that they are portable. Users can store their certificates, private key data, and public key of the CA on an Entrust-Ready PC card token or smart card, carry this token with them, and log on to the network securely from any workstation running PERMIT/Client.

Access control via secure VPN groups

You can use PERMIT/Director to group certificates into secure VPN groups that are either autonomous or overlap in order to accommodate complex business situations such as those found in trading partner networks.

Attribute certificates allow you to define secure multiple VPN groups behind the same PERMIT/Gate, creating, in effect, additional secure VPNs within the same network. You can collect certified users into groups (using PERMIT/Director), and the PERMIT/Gate will ensure that only users in the same group may communicate with one another. You can use the same principle to link in a controlled fashion to trading partners’ extranets.

Imagine again that business A is a large company with a complex LAN composed of several subnets at its head office. It’s trading with three other businesses, B, C, and D, who also have LANs protected by IPSec-compliant gateways.

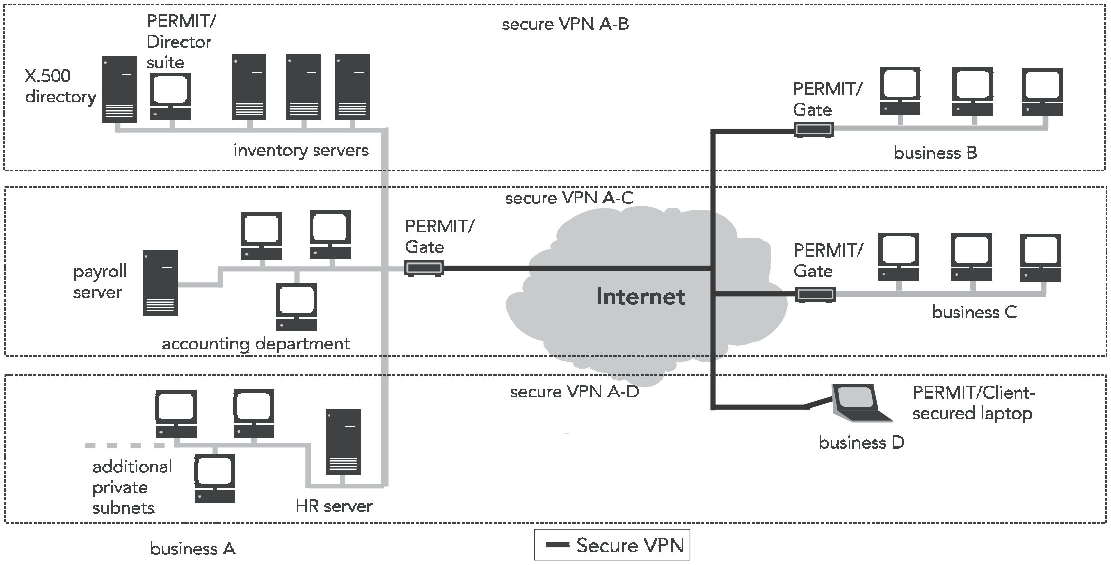


Figure 8: Extranet example

With certificates as an authentication mechanism, and using PERMIT/Director to control which node can talk to which other node, business A can define secure VPN groups within its LAN that defines with whom businesses B, C, and D can talk. In effect, the PERMIT/Gate in front of business A's LAN actually administers three entirely separate secure VPNs.

Certificates have a few other advantages over shared secret authentication. With certificates, you can set key updates to be entirely automatic. You can also easily revoke certificates to remove users or groups of users from the system, without disturbing the rest of the system.

Cross-certification for creating multiple secure VPNs

The flexible, networked architecture of X.500 servers, in which one server can refer a query to another server when necessary, makes possible a secure VPN concept called 'cross-certification'.

With cross-certification, two CAs (potentially two CAs run by two trading partners, or two departments of the same organization) create certificates certifying each other's identity. That is, CA2 would create a certificate tying CA1's public key to CA1's identity, and signed with CA2's private key. Then CA1 would create a certificate tying CA2's public key to CA2's identity, and then sign it with CA1's private key.

Once two CAs cross-certify, any node relying on CA1's certificates for authentication can now rely on CA2's certificates as well, and vice-versa.

Effectively, any node in the secure VPNs served by those two CAs can then authenticate the identity of any other node. Therefore, any two nodes in the system can communicate securely subject to access control (such as that enforced by PERMIT/Director).

Cross-certification is particularly useful for extranets in which a secure VPN is formed between many trading partners that each have their own CA.

The flexibility certificates give you ultimately translates into a significant advantage over older, more primitive approaches to authentication: certificates make the IPSec-compliant secure VPN truly, painlessly, and dramatically scalable.

With the intelligent infrastructure a good CA and an X.500 server (or network of X.500 servers) give you, you can build a secure VPN encompassing millions of nodes, and any number of groups within. And it can grow at any rate — just as you do, and just as IP networks always have.

Conclusion

Networks are an important and growing part of modern business. The power they offer people to communicate and to work together at a distance is changing the world in ways no one could have predicted mere years ago.

With the establishment of IPSec as the universal standard for network security, get ready for your world to change again—and change for the better. You can now have all the benefits IP networks offer you: their universal cross-platform compatibility, their almost organic expandable quality, and the peace of mind that comes with knowing your data is secure while it travels through them.

At TimeStep, we're committed to making this promise a reality, with meaningful implementations of these new standards that are powerful, flexible, and extensible. The scalable architecture of the PERMIT Enterprise product line is our proof of that commitment. With PERMIT Enterprise, no network is too big, and no security requirements are too complicated. Finally, your secure network can grow as your business grows.

Appendix A: Tunneling between gateways

Tunneling is a networking technique that allows secure VPN users to pass private, unregistered IP addresses safely through the public network, and to hide the IP addresses of sensitive machines from users on the public network.

For example, in Figure 10, node A behind proxy device C sends a packet to node B behind proxy device D. Proxies C and D are gateways with legal addresses on the public network. Nodes A and B are internal to the private network and may either have unregistered IP addresses or sensitive ones that the network administrator does not wish to reveal to the world.

In IPSec-compliant tunneling, a proxy device on the transmitting end of a secure VPN connection (such as the PERMIT/Gate 4520 labeled proxy C in our example) encapsulates the original IP header on a packet within the data payload, and affixes a new header to the packet. The new header contains the address of the transmitting proxy device as its source, and the address of a receiving proxy device as its target.

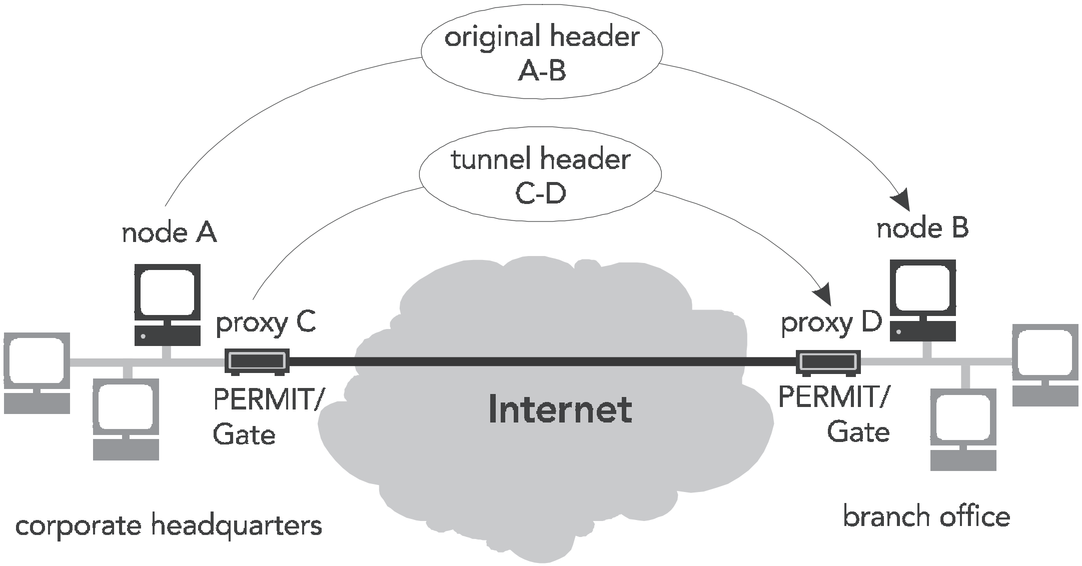


Figure 10: Tunnel example—network view

On the receiving end, a second proxy device (proxy D in our example) removes the header, extracts the original header from the data payload, and then affixes that header to the packet again.

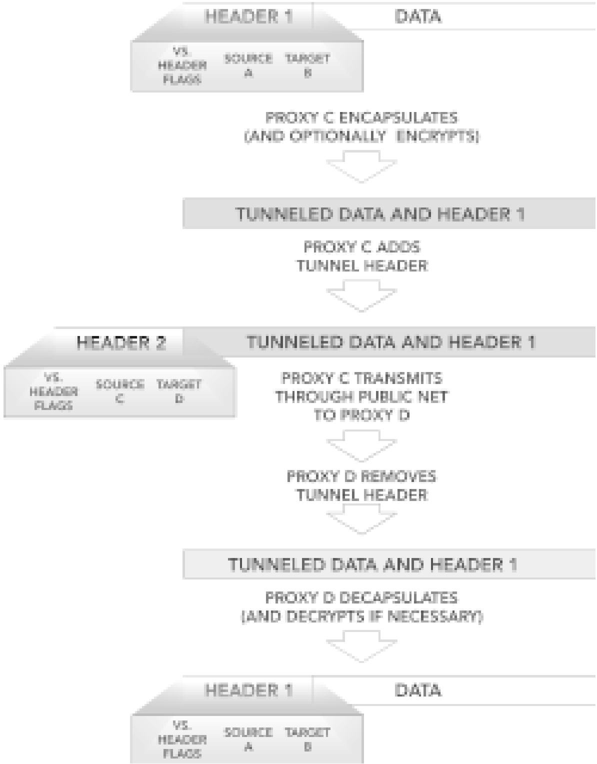

HEADER 1
DATA
VS. HEADER FLAGS
SOURCE A
TARGET B
PROXY C ENCAPSULATES (AND OPTIONALLY ENCRYPTS)
TUNNELED DATA AND HEADER 1
PROXY C ADDS TUNNEL HEADER
HEADER 2
TUNNELED DATA AND HEADER 1
VS. HEADER FLAGS
SOURCE C
TARGET D
PROXY C TRANSMITS THROUGH PUBLIC NET TO PROXY D
PROXY D REMOVES TUNNEL HEADER
TUNNELED DATA AND HEADER 1
PROXY D DECAPSULATES (AND DECRYPTS IF NECESSARY)
HEADER 1
DATA
VS. HEADER FLAGS
SOURCE A
TARGET B

Figure 11: Tunnel example—packet view

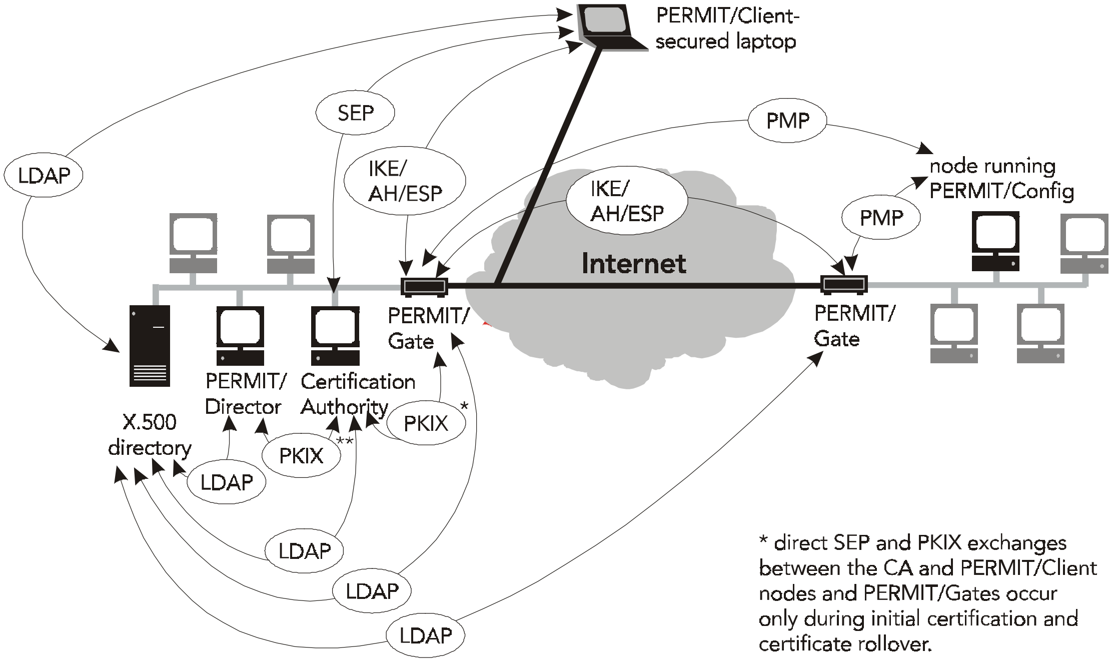
If the transmitting proxy device also encrypts the payload within which it encapsulates the original header, the end result is that at no point during transmission is the original header visible to users on the public network. Therefore, any addresses within that header (potentially both the addresses of the original sending and receiving node) are also invisible to those users. This has the following implications:

- used with encryption, tunneling defeats or weakens traffic analysis conducted in the public network on the private network, in that an observer monitoring traffic on the public network can only tell that there is traffic between the two proxy devices, not specifically which nodes within the private network at either end are communicating
- used with encryption, tunneling protects both the transmitting and receiving nodes from *any* attack from the public network, including even denial of service, since it conceals their addresses from the public network
- used with or without encryption, tunneling allows nodes with addresses that are illegal on the public network to use the public network as a data carrier

Under IPSec, and in the PERMIT Enterprise secure VPN, tunneling may be used with or without encryption, and with or without authentication. PERMIT Enterprise also offers tunneling into secure networks from mobile nodes protected by PERMIT/Client.

Appendix B: Topology and communications

The typical PERMIT Enterprise secure VPN uses a variety of communications protocols between different components at different times. The following diagram summarizes the protocols in use:



* direct SEP and PKIX exchanges between the CA and PERMIT/Client nodes and PERMIT/Gates occur only during initial certification and certificate rollover.

** the PKIX exchange between PERMIT/Director and the CA occurs only during initial certification of PERMIT/Director

Figure 9: Protocols in use

IKE/AH/ESP

IKE, Authentication Header (AH) standard, and Encapsulation Security Payload (ESP) standard, are protocols for Security Association (SA) negotiation and data exchange under IPSec.

IKE exchanges take place between IPSec peers (PERMIT/Gates, PERMIT/Client nodes, or third-party IPSec-compliant software and hardware) at the beginning of data exchange between two nodes, to establish the parameters under which data will thereafter be exchanged.

The AH standard is an IPSec header standard containing authentication data. Data passed between IKE peers is often authenticated with an AH.

The ESP standard is an IPSec payload standard containing encrypted data, and optionally, authentication data. Encrypted data passed between IPSec peers travel in an ESP.

IPSec defines tunnel mode and transport mode that uses AH and ESP transforms.

LDAP

The Lightweight Directory Access Protocol (LDAP) is the standard protocol for interfacing with X.500-compliant directories.

PERMIT/Gate and PERMIT/Client use LDAP to collect and verify, if necessary, certificates identifying other nodes (nodes other than the ones they themselves protect) from the X.500 directory, and to read 'attribute certificates' identifying VPN group membership from the X.500 directory. Group certificates identify which nodes can communicate with which other nodes, and are created and signed by PERMIT/Director.

Entrust CA uses LDAP to maintain the library of authentication certificates on the X.500 directory.

PERMIT/Director uses LDAP to maintain the library of group certificates on the X.500 directory.

PKIX

The Public Key Infrastructure X.509 (PKIX) protocol is the standard for communications with X.509-compliant certification authorities.

The PERMIT/Gate uses PKIX for communications with Entrust CA when you create new certificates to authenticate nodes protected by the PERMIT/Gate. It also uses PKIX when updating (rolling over) the certificates.

PERMIT/Director uses PKIX for communications with Entrust CA when creating its own certificate that contains the signature with which it will later issue attribute certificates for the system.

SEP

Entrust's Secure Exchange Protocol (SEP) is a proprietary protocol unique to Entrust CA and used in place of PKIX by PERMIT/Client-protected nodes for communications with Entrust CA.

The PERMIT/Client protected node uses SEP for communications with Entrust CA when creating a new certificate to authenticate the node it protects. It also uses SEP when updating (rolling over) the certificate.

PMP

TimeStep's PERMIT Management Protocol (PMP) is a proprietary protocol used between PERMIT/Config and PERMIT/Gates for configuration purposes. Whenever PERMIT/Config communicates with a PERMIT/Gate, it uses PMP.

Appendix C: Ports and protocols

Protocol	PKIX	Entrust Admin	SEP	LDAP	IKE	PMP	DCOM
Port Number (decimal)	709	710	33	389	500	38036	5000-6000
Protocol Type	TCP	TCP	TCP	TCP	UDP	TCP	TCP
PERMIT/Client			✓	✓	✓		
PERMIT/Gate	✓			✓	✓	✓	
PERMIT/Config						✓	
Entrust CA	✓	✓	✓	✓			
X.500 Directory				✓			
Entrust Admin		✓					
Directory Server	✓			✓			✓
Director Console							✓

Table 2: Ports and prototcols used to administrate the PERMIT Enterprise product suite

Protocol Numbers for IPSec encryption

ESP	50 (decimal)
AH	51 (decimal)

Appendix D: IPSec RFCs

RFCs TimeStep supports

RFC 2401: *Security Architecture for the Internet Protocol*

RFC 2402: *IP Authentication header*

RFC 2403: *The Use of HMAC-MD5-96 within ESP and AH*

RFC 2404: *The Use of HMAC-SHA-1-96 within ESP and AH*

RFC 2405: *The ESP DES-CBC Cipher Algorithm With Explicit IV*

RFC 2406: *IP Encapsulating Security Payload (ESP)*

RFC 2407: *The Internet IP Security Domain of Interpretation for ISAKMP*

RFC 2408: *Internet Security Association and Key Management Protocol (ISAKMP)*

RFC 2409: *The Internet Key Exchange (IKE)*

RFC 2410: *The NULL Encryption Algorithm and Its Use With IPSec*

RFC 2411: *IP Security Document Roadmap*

RFC 2412: *The OAKLEY Key Determination Protocol*

RFC 2451: *The ESP CBC-Mode Cipher Algorithms <<TimeStep authored>>*

Documents still in draft form (scheduled for IPSecond)

draft-ietf-ipsec-isakmp-xauth-03: *Extended Authentication Within ISAKMP/Oakley <<TimeStep authored>>*

draft-ietf-ipsec-isakmp-mode-cfg-04: *The ISAKMP Configuration Method <<TimeStep authored>>*

draft-jenkins-ipsec-rekeying-00: *IPSec Re-keying Issues <<TimeStep authored>>*

draft-ietf-ipsec-pki-req-01: *PKI Requirements for IP Security*

draft-ietf-ipsec-auth-hmac-ripemd-160-96-02: *The Use of HMAC-RIPEMD-160-96 within ESP and AH*

draft-ietf-ipsec-icmp-handle-v4-00: *IPv4 ICMP messages and IPSec security gateways*

draft-ietf-ipsec-icmp-options-00: *Options for handling ICMP messages that must be forwarded*

draft-ietf-ippcp-protocol-06: *IP Payload Compression Protocol (IPComp) <<TimeStep authored>>*

draft-ietf-ippcp-lzs-04: *IP Payload Compression Using LZS*

draft-ietf-ippcp-deflate-03: *IP Payload Compression Using DEFLATE <<TimeStep authored>>*

draft-ietf-ipsec-policy-model-00: *IPSec Policy Data Model <<TimeStep authored>>*

draft-ietf-ipsec-vpn-policy-schema-00: *An LDAP Schema for Configuration and Administration of IPSec based Virtual Private Networks (VPNs) <<TimeStep authored>>*

draft-ietf-ipsec-isakmp-hybrid-auth-01: *A Hybrid Authentication Mode for IKE*

draft-ietf-ipsec-secconf-00: *Secure Configuration of IPSec-Enabled Network Devices*

draft-ietf-ipsec-mib-02: *IPSec Monitoring MIB <<TimeStep authored>>*

draft-ietf-ipsec-sps-00: *Security Policy System*

draft-ietf-ipsec-spsl-00: *Security Policy Specification Language*

draft-simpson-desx-02: *The ESP DES-XEX3-CBC Transform*

draft-ietf-ipsec-dhless-enc-mode-00: *A DH-less encryption mode for IKE*

Glossary

AH—see **Authentication Header.**

Asymmetric encryption—an encryption scheme in which one key (the public key) and one algorithm are used to encrypt data, and another key (the private key) and another algorithm are used for decryption. The benefit of established asymmetric encryption schemes such as RSA is that you cannot easily find the private key simply from knowing the public one, and the public key can only be used for encryption, not for decryption. In practice, someone using asymmetric encryption for communication generates a public/private key pair, keeps the private key secret, and distributes the public key to anyone who wishes to communicate with them. Those with the public key can then use it to encrypt communications destined for that person, and only that person can decrypt that data. This property of asymmetric encryption schemes makes them particularly valuable in network environments. Asymmetric encryption schemes typically must use a much larger key than symmetric schemes. See also **encryption**, **symmetric decryption**.

Authentication—in cryptography, a way of proving identity. An authentication scheme typically requires a sender to perform manipulations on the data they're sending (with a **digital signature** scheme and/or a **hash function)** to prove they have certain cryptographic keys only they should know, thereby proving their identity. Authentication schemes often guarantee the integrity of the data being sent as well. See **digital signatures** and **hash functions**.

Authentication Header (AH)—part of the **IPSec protocol suite.** It is the header used in IPSec-compliant IP packets to carry authentication data (a digital signature scheme or keyed hash), thereby preventing tampering during transmission and permitting verification of the identity of the sending party.

CA—see **Certification authority.**

Certification authority (CA)—a server providing public key certificates for the purposes of authenticating communicating parties' identities. Certificate authorities and the certificates they issue allow two parties to verify one another's identities.

The CA issues a public key certificate, which contains both the identity of the communicating party, and a public key corresponding to that party's private key. The CA then signs this whole package with its own private key.

During communications, to verify the other party's identity, you contact the CA for a copy of the public key certificate authenticating that party. You check the CA's signature on the certificate against your own copy of the CA's public key, to verify the certificate's authenticity. Next, you read from the certificate what the communicating party's public key should be. Then, you verify the identity of the party with whom you're communicating by checking that the private key used to sign the message corresponds to the public key registered for that party on the certificate.

TimeStep's PERMIT/Enterprise secure VPN product suite uses Entrust CA.

Data Encryption Standard (DES)—a **symmetric encryption** algorithm certified as a standard for US government departments that use encryption. DES uses a 56 bit key, giving it a 2^{56} **keyspace**. DES has the advantage that it is easily implemented in hardware (and that chips to implement it are readily available), but the disadvantage is that, by computational standards now available, its keyspace may not be large enough for continued use. The **IPSec protocol suite**'s **ESP** protocol uses DES as the minimum fallback standard, but also supports newer schemes with larger keyspaces.

DES—see **Data Encryption Standard**.

Digital signature—a form of authentication. In digital signature schemes, persons proving their identify must encrypt transmitted data with a key only they could have, and then pass both the original data and the **ciphertext** they generate with their key to whomever wishes to verify their identity. Such schemes often offer the benefit that they protect transmitted data against alteration, since doing so would also require that the signature be changed to match it, and the key generating that signature is secret. The **PGP/Web of Trust** system, for example, uses asymmetric **RSA** keys to generate digital signatures on e-mail.

Since most encryption schemes generate ciphertext at least as long as the original **plaintext**, many digital signature schemes also use **hash functions** to reduce the amount of data that must be signed. The sending party first uses the hash to produce a shorter (usually fixed in size) piece of data, then signs this with the signature scheme. To verify, the recipient does the same hash on the data, then runs the opposite encryption operation on the signature, using either the same key as the sender should have (see **symmetric encryption**) or the complementary public key (see **asymmetric encryption**). The output should match the hash if the signature is legitimate and the message has not been altered.

The **IPSec protocol suite** uses digital signature schemes for authentication and data integrity checks throughout the protocol suites.

Encryption—a scheme in which information is rendered unreadable during transport, so that an intercepting party cannot make use of it. In encryption, readable data (the **plaintext**) is encrypted to produce an unreadable **ciphertext**. The ciphertext must then be decrypted (converting it back to the plaintext) before it can be read at the receiving end.

Modern encryption schemes typically use an algorithm and key system. The algorithm is a set of rules for what to do to the data to encrypt it. The key is a parameter—a value the algorithm uses to encrypt the data. Once a certain key has been used to encrypt data, you usually need either the same key (symmetric encryption) or a different but complementary key (asymmetric encryption) to decrypt the data. Typically the rules of the algorithm used are public, but keys used are kept secret between communicating parties, so that only they can decrypt the message.

Standard public algorithms used for encrypting data include **DES**, 3-DES, **RSA**, CAST, and Blowfish.

Encryption key—a parameter used to encrypt and decrypt data. Once data has been encrypted using a given key, either the same key (in **symmetric encryption**), or a complementary key (in **asymmetric encryption**) is then needed to decrypt it. See also **keyspace**.

Encapsulating Security Payload (ESP)—payload format used in IPSec-compliant IP packets to carry encrypted and/or authenticated data, thereby preventing sniffing (eavesdropping) on the network between communicating nodes.

Entrust CA—the CA used by the PERMIT/Enterprise secure VPN system. See **Certification authority**.

ESP—an IPSec term. See **Encapsulating Security Payload.**

Extranet—a secure VPN between trading partners.

Firewall—a traditional (non-VPN) means of ensuring security during communications between private and public networks. The firewall filters communications, forbidding certain types of access on private servers from the public network.

Hash function—a cryptography term. A hash function is a subclass of the encryption functions used to assist **digital signature schemes**, and for cryptographic **authentication** schemes in general. Hashes used for such schemes have the property that their output is of constant length, whatever the input, and that it is extremely difficult to come up with a second input message that would produce the same hash. Therefore in digital signature schemes, rather than signing the message itself, the sending party usually first runs a hash on the message and signs the output (also colloquially called the hash) thus reducing the size of the signature and the amount of data that has to be sent. Hashes may also be keyed. A keyed hash uses a parameter (a key) much like an encryption key, and precisely the same key must be used to generate the same hash from the same data. So a keyed hash can provide authentication of the sending party's identity on its own, by proving they know the appropriate key.
Keyed hashes are similar to encryption functions, except that hashes are reducing processes, so you cannot get the original data back from the hash output. You can only verify that the hash is appropriate output from that data.

A hash is both a **pseudo-random function** (PRF) and a **one-way function**.

Header (or packet header**)**—a network term referring to a portion attached to the beginning of a packet to specify the protocol level data needed to process the rest of the packet. This data can include destination addresses, which **SA rules** to use to decipher it, how to assemble it with the next packet, or which procedures to use to authenticate the packet.

See also **payload**.

IETF—see **Internet Engineering Task Force**.

IKE—part of the **IPSec protocol suite**. IKE is the current IPSec standard for **SA rules** negotiation, key management, and key exchange. IKE uses three modes—**aggressive mode**, **quick mode**, and **main mode**. IKE stands for Internet Key Exchange. IKE was formerly known as **ISAKMP/Oakley**.

IKE SA—an IPSec term referring to an SA negotiated using **IKE**, strictly for the purpose of negotiating general purpose **IPSec SA**s.

Internet Engineering Task Force (IETF)—a multinational group of people working on Internet communications technology issues at the international level. The IETF coordinates working groups, including the **IPSec working group,** developing communications standards.

Internet Key Exchange—see **IKE**.

Internet Protocol (IP)—a network term referring to the basic transmission protocol, immediately above the physical protocols (frequently Ethernet or PPP) in the Internet, and a common standard in many large corporate and academic LANs and WANs. IP is the protocol responsible for delivering **packets** to their destination. Other, higher level protocols (typically **TCP**) are responsible for actually breaking the data into appropriate chunks for transmission, and reassembling them on delivery. IP is a highly flexible scheme designed to transparently negotiate communications between networks of differing capabilities, and for highly flexible, adaptive routing. **TCP** and **UDP** are the two protocols that most commonly call on IP's services. See also **network layers**.

IP is the only IP network protocol used universally throughout the net (and this applies to the Internet) for all communications. This is one of the reasons adding security at the IP level has such value.

Internet Security Association and Key Management Protocol—see **ISAKMP**.

IP—see **Internet protocol**.

IP address—a network term referring to a 32 bit address, usually written in four bytes (e.g. 123.145.156.178), used in IP networks to identify a node on the network. Packets are routed by **IP** to the appropriate machine on the network according to the destination IP address in the packet header. Every machine on a network to which packets may be routed must have a unique **IP address**. See also **Internet protocol**, **IPv4**, and **IPv6**.

IPSec—acronym for Internet Protocol (IP) Security. See also **IPSec protocol suite**.

IPSec protocol suite—a set of industry-standard extensions to the Internet Protocol (IP)**,** adding security services developed by the IETF's IPSec working group. The suite consists of protocols for an authentication header (**AH**) assuring data integrity, an encapsulating security protocol (**ESP**) format ensuring data privacy, and a key management and exchange scheme (**IKE**).

TimeStep's PERMIT/Enterprise secure VPN product suite uses the IPSec protocol suite for security, making it interoperable with all network equipment and software compliant with the IPSec protocol suite.

IPSec SA—term specific to this paper referring to a general purpose SA used for carrying IP data. See also **IKE SA**.

IPSec working group—a subcommittee of the **Internet Engineering Task Force (IETF)** dedicated to developing security extensions for the **Internet Protocol**; designers of the **IPSec protocol suite**.

IPv4—**IP version 4**. The current standard for IP addresses and routing behavior. IPv4 addresses are 32 bits wide, and are most commonly described in four decimal-separated ordered octets (four numbers from 0-255). For example: 192.168.1.1, (which translates to 0xC0A80101 in hex) is an IP address.

IPv6—**IP version 6**. The proposed next generation standard for IP addresses, incorporating IPSec security features and other additions. IPv6 addresses are 128 bits wide—four times as long as an IPv4 address, giving an address range that is 2^{96}—or about $8x10^{28}$—times as large as that provided by IPv4. The most common expression of these (currently) is eight hexadecimal integers in the range 0x0000 to 0xFFFF, ordered and colon-separated. For example, 0001:0001:0001:0001:0001:0001:C0A8:0101 is an IPv6 address.

ISAKMP—the **Internet Security Association** and **Key Management Protocol**. A framework negotiation protocol on top of which **IKE** is designed. You may occasionally find IPSec types who refer to IKE as ISAKMP, but the terms aren't precisely interchangeable. IKE (formerly called **ISAKMP/Oakley**) is technically an instantiation of ISAKMP, adding functionality for the specific purposes of IPSec key and protocol negotiation.

ISAKMP/Oakley—obsolete term for **IKE**.

Key—a cryptography term. See **encryption key.**

Keyspace—a cryptography term. The total range (or number) of possible **encryption keys** that might be used in a given encryption scheme. Using binary keys, the key space is always two raised to the power of the length of the key. So the keyspace for a 56 bit binary key is 2^{56}, or around $7.2x10^{16}$ (about 72 million billion possible keys). See also **encryption**.

LDAP—see **Lightweight Directory Access Protocol.**

Lightweight Directory Access Protocol (LDAP)—standard protocol for communicating with X.500 directory servers.

Main mode—an IPSec term referring to the packet exchange protocol used in IKE phase one (in IKE) to negotiate an IKE SA. See also **aggressive mode**, **quick mode,** and **IKE SA**.

Network layers—network layers can be discussed in different ways. The ISO Open System Interconnection (OSI) standard, an international standard for network layering, actually specifies seven network layers. However, it's fairly common to describe IP networks as having five layers:

- the physical layer
- the data link layer
- the network (IP) layer
- the transport layer
- the application layer

The physical layer is the actual wire on which the data travels. So Ethernet cable might be the physical layer in an IP network. In other places, the physical layer might be a phone line.

The data link layer is the protocol layer that actually handles the physical layer. So for that Ethernet cable, the data link layer would be the Ethernet protocol. On the phone line, the data link layer would be the PPP protocol.

The network layer is the layer in which **IP** does its work—routing and delivering packets between **IP addresses**.

The transport layer supports a number of higher level protocols running on IP that typically provide certain types of service. **UDP**, for example, delivers data which has to get there on time or not at all, such as live video and audio. **TCP**, by contrast, delivers data that can arrive late, but which must be intact (as in binary executable files).

Finally, the application layer is the actual program using the network for communications. An e-mail client program, for example, is part of the application layer.

The network layer concept simplifies a number of logistic hurdles in building networks—primarily by breaking up big problems into smaller ones. Effectively, each layer's protocol(s) encapsulate(s) the problems encountered in delivering data at that layer, so higher levels can just rely on the lower level protocol to get the job done.

Nonce—a random number usually used either for verification purposes, or for adding randomness to cryptographic key exchanges. In **IKE** exchanges, you send the other communicating party a nonce which they then must sign with their **digital signature** and send back, so you can verify their identity.

Oakley—the mechanism of key exchange/negotiation, used in **IKE**.

One-way function—a mathematical/cryptography term. A one-way function has the often useful property that it is difficult to find what the inputs were from the output alone. A **hash** is a one-way function.

Packet—a network term. A packet is the basic unit of transmission under **IP** (and virtually all network protocols). Data streams are broken into packets (small 'buckets of data') by the transmitting machine, passed through the network in pieces by **IP**, and then reassembled at the receiving end.

You will also see the term **datagram**. A **datagram** is a unit of data, and a **packet** is the physical thing on the wire. But the terms are usually used interchangeably, and for most purposes, this is both convenient and legitimate.

Packet header—see **header**.

Payload—a network term referring to the data portion of a packet following the header. See also **packet** and **header**.

PERMIT Management Protocol (PMP)—TimeStep's proprietary protocol for communications between PERMIT/Config and PERMIT/Gates.

PGP/Web of Trust—a cryptographic authentication scheme typically used by Internet e-mail users to authenticate the identity of the sending party, and the integrity of their message. The scheme uses a variant of the **RSA** asymmetric encryption system to sign data, and a 'Web of trust' system (in which groups of users vouch for each other's identity) to exchange public keys. See **digital signatures**.

PGP stands for Pretty Good Privacy.

Phase one exchange—an **IKE** exchange used to establish the initial **IKE SA**.

Phase two exchange—an **IKE** exchange used to establish the general-purpose **IPSec SA**, or to refresh keying material either for an IPSec SA or an **IKE SA**.

Plaintext—cryptographic term for a message before **encryption** and after decryption. You encrypt the plaintext to generate the ciphertext, which you then transmit through the unsecured channel. You then decrypt the ciphertext to get back the plaintext.

PMP—see **PERMIT Management Protocol.**

PKIX—see **Public Key Infrastructure X.509 protocol**.

Protocol—a general term/network term (1) referring to a way of doing things; (2) in networking, the rules that govern how machines communicate. The **Internet protocol (IP)**, for example, defines the rules for machine addressing and for routing packets between machines in a network.

Pseudo-random function (PRF)—a mathematical/cryptography term. A pseudo-random function is a function in which a small change in the input may result in any magnitude of change in the output. Pseudo-random functions are deterministic—in that the same inputs always result in precisely the same output. However, without actually running the function, it can be difficult to know what will be the output. Random number generators and **hashes** are both pseudo-random functions.

Public Key Infrastructure X.509 (PKIX) protocol—standard protocol for communications with X.509 compliant certificate authorities, including Entrust CA.

Quick mode—an IPSec term referring to the packet exchange protocol used in IKE phase two in IKE to establish general purpose **IPSec SAs**, and to refresh keying material for **IKE SAs** or **IPSec SAs**. See also **main mode**, and **aggressive mode**.

RSA—the original and best-known asymmetric encryption scheme. RSA uses the product of two large primes as a public key, and values derived from those (secret) primes as a secret key. See **asymmetric encryption**.

SA—see **Security association.**

Security association (SA)—an agreed-upon set of encryption and authentication algorithms, keys, and protocols for communicating securely. Two nodes in a secure network communicating through the public network first agree upon the terms of a security association, and then use that security association for subsequent communications.

SA rules—in the **IPSec protocol suite**, the set of algorithms, and keys, and rules for using them in a **Security Association** (SA).

Secure Sockets Layer (SSL)—a technology developed by Netscape, and now standardized, usually used to secure HTTP traffic between a web browser and a web server. Typically the technology in use in shopping-cart applications, it secures the server and client on a session by session basis, generally using widely-publicized certificates for identity verification.

Secure virtual private network (secure VPN)—a secure private network using unsecured public networks as data carriers. The **IPSec protocol suite** provides the capability of building secure VPNs within the context of larger, unsecured public IP networks such as the Internet. Users of the secure VPN may use their network as though it were a perfectly secure, isolated LAN, even though it is directly connected to unsecured public networks.

Secure VPN—see **Secure virtual private network**.

Security gateway—a secure VPN device functioning as the gateway between the public network and a segment of the private network. TimeStep's PERMIT/Gate line of security gateways provide high speed encryption services for the nodes they protect, as well as proxy negotiation of security associations.

Secure Exchange Protocol (SEP)—an Entrust proprietary protocol used in place of PKIX by PERMIT/Client protected nodes for communications with Entrust CA.

SEP—see **Secure Exchange Protocol.**

Security Parameters Index (SPI)—an IPSec term referring to an arbitrary 32 bit number which, in concert with a destination IP address, uniquely identifies a single **SA**. The headers of IPSec packets carry an SPI, which the recipient node then uses to look up the **SA rules** for a given incoming packet. A node may reassign an SPI to a new SA after the old SA expires, provided it waits long enough that it is unlikely packets from the old SA are still percolating.

SPI—see **Security Parameters Index**.

SSL—See **Secure Sockets Layer**.

Symmetric encryption—a cryptographic term describing encryption schemes in which the same key is used both for encryption and decryption. Example **DES**.

Third-party authentication—an authentication scheme in which a trusted third party (such as a CA) vouches for the identity of the communicating parties. See also **Certification authority**.

Tunneling—secure VPN technique in which one IP header (containing the addresses for use in the private network) is encapsulated within the data payload, and a second header (containing legal addresses for use on the public network) is added outside the payload, for the purposes of routing the packet through the public network.

Transmission Control Protocol (TCP)—an IP-specific network term. A general-purpose protocol designed for carrying data of virtually any type and any size though **IP**-based networks, and the standard protocol for most general-purpose communications in the Internet. TCP is said to 'run on top of' (see **Network layers**) IP, meaning it uses IP for actual delivery and addressing of the data. TCP effectively sets up a dedicated, but temporary channel between two nodes. An e-mail client would typically use TCP for carrying messages back and forth, to and from an e-mail server. Contrast **UDP**.

UDP—see **user datagram protocol**.

User Datagram Protocol (UDP)—an IP-specific network term. A general-purpose protocol used in **IP** networks in situations in which reliable delivery is not required. Like **TCP**, UDP runs "on top of" (see **Network layers**) IP, meaning it uses IP for actual delivery and addressing of data. Internet clients use UDP principally for communications with domain name servers, in resolving Internet addresses. Real-time audio and video traffic also frequently uses UDP. **IPSec's IKE** protocol suite is based on UDP. Contrast **TCP**.

Virtual private network (VPN)—a system in which a public network is used to carry the data of a private one, usually in such a way that the distinctions between the resulting virtual network and a true private LAN or WAN are invisible to the user. Note that the term VPN by itself however does not necessarily imply that the data carried is private (i.e. unreadable by other network users), as does the term **secure virtual private network** (secure VPN). However, the term VPN commonly refers to a secure VPN.

VPN—see **virtual private network**.

Virtual Tunneling—tunneling scheme in which mobile nodes effectively receive two IP addresses and two domain name servers—a 'real' IP address and domain name server assigned by the ISP for communications with the public network (usually the Internet), and a 'virtual' IP address and domain name server for use in tunneled communications with the private network. TimeStep's PERMIT/Client software provides Virtual Tunneling. See also **Tunneling**.

X.500 server—a standard distributed database server system used for a wide range of purposes in the network world. The PERMIT/Enterprise secure VPN system uses the X.500 server to distribute public key (authentication) certificates, as well as distributing information on communications permission—including who can talk with whom within the secure VPN.

TimeStep Corporation is the most experienced 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 VPNs, 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

62-00141-00

97-2570-01-00-B

Printed in Canada.