MANAGEMENT WHITE PAPER

THE VIRTUAL PRIVATE NETWORK

SECURITY IS THE KEY

SafeNet™

Introduction

The Internet – the fastest growing network in the world. The Internet is growing so fast that at the current growth rate everyone on the planet could be connected to the Internet within the next twenty years. What will the Internet look like in the future? Will it still be a network composed of surfers, browsers, hackers, and shoppers? Or, will businesses and governments use the Internet as the global backbone for commerce?

Today, the Internet is used mainly for Email and Web Browsing. In reality, corporations are adding Internet access for such activities. However, this access is still in addition to the corporate backbone network. What if corporations could use the Internet *as* the corporate backbone network? What if, instead of needing a dedicated line between New York and Tokyo, you could have local access in the USA and local access in Japan and create a network that offers the same performance, reliability, and security as a dedicated line at a much lower cost?

Using the Internet *as* the corporate backbone instead of having the Internet in addition to the corporate backbone is called a Virtual Private Network (VPN). A Virtual Private Network is a network that operates through a public network, such as the Internet, and is accessed only by individuals or groups who "subscribe" to that VPN. The combination of a private network operating via a larger, public network is analogous to a private "tunnel" that goes through the Internet. This paper describes how Information Resource Engineering's SafeNet/Enterprise products enable a VPN through implementation of world leading Internet security and security management.

Why Internet Security?

When evaluating a VPN, there are four fundamental issues that must be addressed: cost, performance, reliability, and security. Of these four, security is the gating factor because unless security issues are resolved, it doesn't matter how inexpensive, fast, and reliable the Internet becomes, without adequate security, the risks will outweigh the benefits and result in limited growth. One can use the Internet to send files between companies today; however, without proper security, no matter what the level of performance, cost, or reliability, the information and the corporation are open to attack.

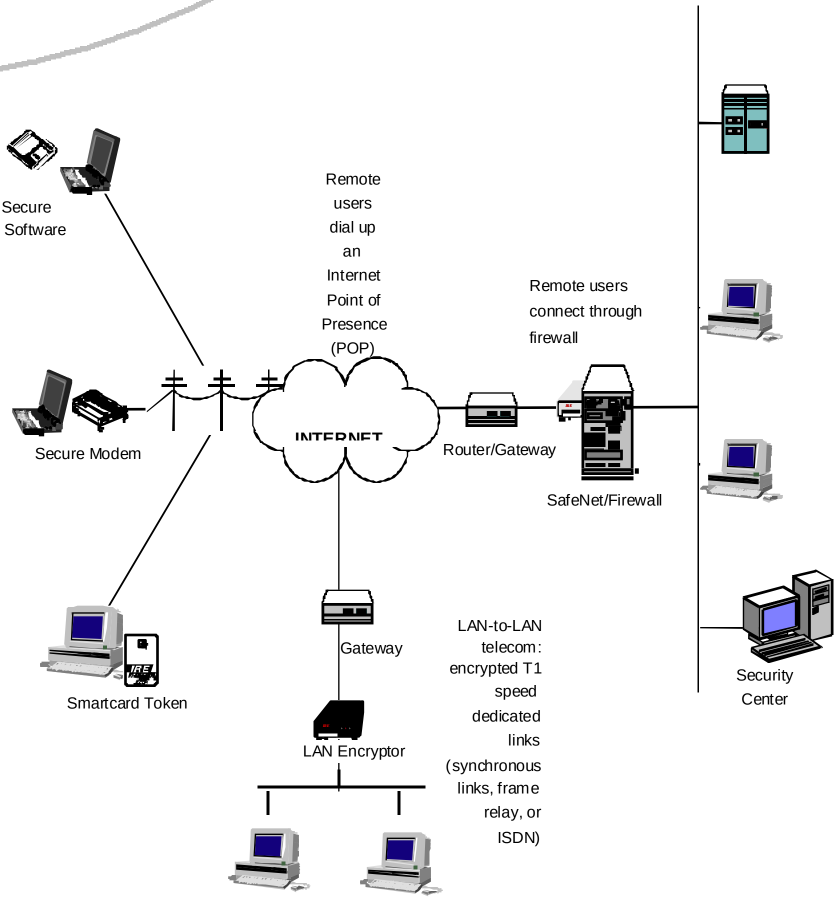
The reason for this vulnerability to attack is that the Internet is the most open network in the world. Information Services (IS) managers understand that as soon as they open the corporate network to the Internet they are opening themselves up to serious security risks. A VPN requires these managers to go one step further and not just open up their networks but to actually *shift* their corporate resources to the Internet. Information Resource Engineering provides a level of security that allows IS managers to shift from having a corporate backbone *and* Internet access to using the Internet *as* the corporate backbone network.

In addition to security, there are significant Quality of Service (QOS) issues with regard to the Internet. Quality of Service refers to the service agreement offered by an Internet Service Provider (ISP) to a client that guarantees a certain level of performance.

The Concept of Virtual Private Network

The Virtual Private Network (VPN) is a concept that has been around for many years in the voice networking world. In the mid-1980s large carriers offered VPNs for voice services so that companies could have the appearance of a private voice network while actually sharing the resources of a much larger network. This concept is now being applied to the data world, to the same effect. Essentially, a VPN is a data network that appears to be "private" but which uses the resources of a much larger data network. The Internet is an ideal platform on which to create a VPN. Figure 1.0 depicts a typical implementation of Information Resource Engineering's SafeNet/Enterprise products to create a VPN.

Example of VPN


Secure Software
Remote users dial up an Internet Point of Presence (POP)
Remote users connect through firewall
Secure Modem
INTERNET
Router/Gateway
SafeNet/Firewall
Gateway
LAN-to-LAN telecom: encrypted T1 speed dedicated links (synchronous links, frame relay, or ISDN)
Smartcard Token
LAN Encryptor
Security Center

What are the drivers for the VPN? From an intuitive standpoint, it makes sense to use the scope and scale of the Internet for corporate communications. However, why would a company want to risk transmitting sensitive data across the Internet? There are three fundamental reasons for building a VPN: cost, flexibility, and network transition.

First, cost is a critical driver in any networking decision. There are some very interesting dynamics in today's Internet networking arena:

- ♦ Significant savings can be realized by switching to the Internet. Studies in the United States indicate that switching to a VPN from either a frame relay network or leased lines can result in a 50% savings on communications charges. When international connections are involved, the savings can be significantly higher. These savings make a VPN a strategic business decision for the corporation. However, security must be implemented correctly or the savings in communications costs will be offset by the potentially higher cost of ineffective security.
- ♦ Most networking options are either distance sensitive or usage sensitive. For example, leased line networks are priced based on line rate and line distance. Frame relay is priced based on line speed, throughput (Committed Information Rate - CIR), and number of connections (Permanent Virtual Connections - PVC). Finally, X.25 is priced based upon line speed and class of service.
- ♦ The Internet, for the most part, is priced based upon access speed. This means that it costs the same to send a packet of information from New York to Boston as it does from New York to Tokyo. This fact is one of the core drivers behind the economics of VPNs.
- ♦ In the United States the Internet Service Provider (ISP) market is extremely competitive. This competition is quickly driving Internet access charges down to near commodity rates. Low access charges mean that the Internet is inexpensive to access but highly congested because of flat rate prices. The ISPs want to differentiate their services in the market, and one of the ways to do this is to increase value-added services such as VPNs.

A second issue involving VPNs is flexibility. As the global economy becomes more competitive, and corporations depend more frequently on digital communications, the need to communicate quickly with multiple partners becomes paramount. Corporations are not only interested in connecting their own operations via the "corporate network," they are also concerned with connecting partners and customers as extensions of their corporate network.

Today, companies may extend their corporate networks to partners and customers via leased lines, frame relay networks, and/or X.25. All three of these technologies require long lead times for the carriers (particularly in second and third world nations) to provide access to corporate partners and customers. As stated before, the Internet is the most accessible network in the world, but many times, dedicated lines cannot be provided if Internet access is available. As a result, in some areas the Internet is the only option.

Finally, the Internet provides a platform for networks in transition. The Internet is the network of the future, and many companies are considering a transition to the Internet from their current networking topologies. Information Resource Engineering sees the Internet as a logical transition from current X.25 or leased line networks. With current router technology, it is possible to transition the underlying network protocol from leased lines to frame relay to Internet without having to replace equipment.

These dynamics, particularly in the United States, create an incentive for the ISPs to provide VPN service and for customers to ask for VPN services. This is a win-win opportunity; one that Information Resource Engineering is helping customers explore today.

Internet Security

Implementing a VPN requires an understanding of the risks associated with the Internet. The Internet by its nature, is an open environment. Based upon technology and concepts from the 1970s, the Internet was originally developed to be a research network where the need for access and availability far outweighed the need for privacy and authenticity. The Internet was developed by an elite group of researchers for an elite group of researchers. Unfortunately, (or fortunately, depending on whether you are one of the elite researchers), times have changed. Now the Internet is faced with demands for higher level security traditionally found only in private networks. Security is critical because without it, the Internet will never achieve its potential to become the commerce highway of the future.

There are different ways to implement a secure VPN. Information Resource Engineering advocates complete VPN security offerings based on the Internet Engineering Task Force (IETF) IP-Security (IPSEC) specifications. The assumption is that the VPN should offer an equal or greater level of security than the corporation has today. A higher level of security requires a very thorough implementation.

Implement a Security Policy - The First Step in Prevention

Attacks can come from both within a VPN as well as from outside a VPN. For example, in a well-publicized series of attacks on a Fortune 100 customer, the most successful attacks were not through the Firewall, but through fax servers and remote modems on users' desk tops where default passwords had not been changed. Through these "back doors," the hackers (a paid group organized by the company being attacked) were able to break into every major computer system in the corporation.

To prepare for (and prevent) an attack, he first step a company should implement a security policy. Surprisingly, this simple step is overlooked by most companies in the US and, most likely, throughout in the world. For example, in a survey of Fortune 500 companies in the US, approximately 20% had no security policy at all. Further, a Japanese survey revealed that nearly 35% of the 100 corporations surveyed gave no consideration at all to data security.

A security policy is a road map that defines which assets need to be protected, possible weaknesses in the organization, and how to correct weaknesses and protect targeted assets. If this plan does not exist, it is impossible to know what assets need to be protected and how to best protect them.

Protecting VPN Data Where's the Risk?

For a VPN, the most critical assets are the corporate resources that are exposed to the Internet, the data that is transported across the Internet, and the identity of the source of the data. Within a corporation, one generally trusts the source of data, given that the employee who sent the data is probably sitting at an assigned space within the corporate building. However, on the Internet one can receive data from sources anywhere in the world, and there is no way to verify the location from which the data originated.

There are hundreds of security attacks on the Internet today. The most popular type is a spoofing attack where the source address is changed so that it looks like the data came from a different source. This is analogous to putting a false return address on letters you mail. Other types of attack include the replay attack, where packets are recorded and resent; the tailgate attack, where packets are put onto the end of a valid stream of packets; and the remote management attack, which attacks the firewall.

Firewalls Are Not Enough

It is generally accepted that a firewall is the required solution to the problem of Internet security. For VPNs, a firewall-only solution is inadequate for the following reasons:

- Firewalls cannot prevent changes to data that may occur as a packet moves across the Internet. A basic firewall cannot prevent a spoofing attack, nor can it determine whether data has been changed along the way. In addition, other types of attack, such as replay and tailgating, will go right through a firewall.

- Firewalls offer some level of encryption, and this capability is improving. Today, most VPN implementations are either non-standard, have a negative impact on the performance of a firewall, or require that the firewall must be upgraded to a more expensive workstation.
- Firewalls are susceptible to remote management attacks. Firewalls are generally devices that have a management port for configuration and monitoring. In many cases, this port is a point of attack for hackers who try to access the firewall configuration database and make changes that allow a hacker to penetrate the firewall.
- Most firewalls today are based upon non-secure operating systems. Some firewalls have received ITSEC (UK) and NCSA (US) certification for secure operating systems, but the majority do not have these certifications. A non-secure operating system opens the firewall software to the possibility of a break in through the operating system. As a result, the integrity of the firewall itself is compromised.

The Defense - How to Move Data Across the Internet Securely

Before data can be moved across the Internet securely (enabling a VPN), four fundamental questions must be answered:

- How do you keep information private?
- How do you know that the data sent is the data received?
- How do you know the source of the data?
- How do you control the system?

If there are solutions to these four questions, then a VPN is feasible. If however, any of these questions are not fully answered, there will be a hole in the security of the VPN making a successful implementation impossible. The following section discusses each question and the technology required to answer the question.

How Do You Keep Information Private?

The technology needed to keep information private is encryption. There are many different algorithms for encryption, and they all have different strengths and weaknesses. For example, in Pacific Rim nations there are many “favorite” algorithms in use today. These algorithms include FEAL, Misty, DES, RSA, MD5, and many others. Regardless of the algorithm, there are three aspects that must be considered: key length, strength of the algorithm and width of processor. Most people are aware of the key length, and that is the only aspect of strength on which they focus. However, though increasing key length does increase strength, it is not a good indication of total strength. The choice of algorithm and strength is a very hot topic, and Information Resource Engineering is intimately involved in the establishment of policies and procedures for encryption standards.

The most important aspect of encryption selection for a VPN is to choose an international standard encryption algorithm. There are three reasons why an international standard algorithm is important: testing, interoperability, and liability. First, standard algorithms go through extreme testing, known as vetting. These algorithms are developed by cryptography experts from around the world and are the most tested algorithms commercially available today. Second, the Internet, by its nature, demands high levels of interoperability. This interoperability is for communication between different countries, different companies, and different vendors' products. Acceptance of an international standard is the best guarantee of interoperability beyond the borders of a country. Finally, there is high liability with encryption. What happens if the encryption is broken? What is the liability? This issue is of great importance, and today there are no International liability standards for encryption. In fact, in many countries there are no limitations of liability for implementation of an encryption system. However, in the future limited liability will have to be addressed regarding the expansion of Internet services. For example, in the United States the use of standards based systems for financial transactions help protect against liability for losses. Under the Uniform Commercial Code:[1]

> " ...a payment order is effective as the order of the customer, whether or not authorized, if (i) the security procedure is a commercially reasonable method of providing security against unauthorized payment orders...The issue of whether a particular procedure is commercially reasonable is a question of law. Whether the receiving bank complied is a question of fact. It is appropriate to make the finding concerning commercial reasonability a matter of law because security procedures are likely to be standardized in the banking industry...The effect of Section 4A-202(b) is to place the risk of loss on the customer if an unauthorized payment order is accepted by the receiving bank in compliance with a commercially reasonable security procedure..."

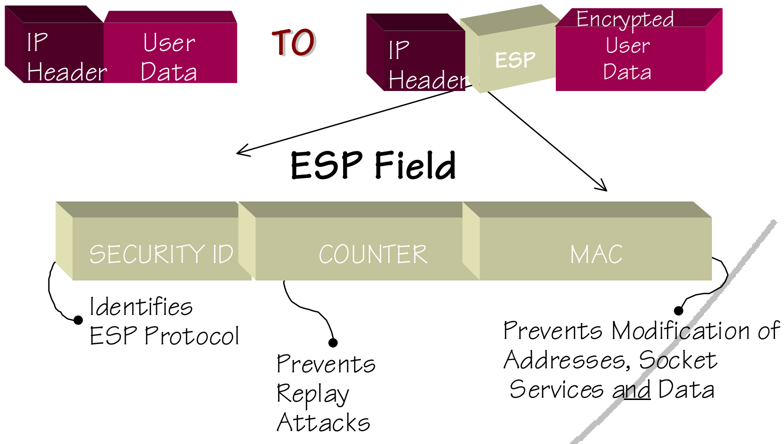
Today, use of the American National Standards Institute (ANSI) X9 based standards, developed under the auspices of the American Banking Association, is the best way to ensure "commercially reasonable" security.

How Do You Know the Data Sent is the Data Received?

Packets of information traveling across the Internet are susceptible to being "grabbed" and modified. As mentioned earlier, the simplest modification is the spoofing attack where the source address is modified. A more complex attack involves changing the actual data that is inside the packet. The way to protect data, regardless of the means of attack, is via packet authentication.

The Internet Engineering Task Force (IETF) has defined a standard way that packets can be protected as they traverse the Internet. This standard is the Encapsulated Security Payload (ESP). The purpose of this standard is to prevent the packet from being tampered with as it moves across the Internet. All ESPs are not the same however. Some consist of a transform only, indicating that the packet is encrypted. More sophisticated ESPs, such as the one implemented by Information Resource Engineering, contain a counter (to prevent "replay" attacks) and a Message Authentication Code (MAC). The MAC uses an encryption process to create an authentication code that prevents a hacker from modifying any data in your packet, including the source address field.

Encapsulated Security Payload



How Do You Know the Source of the Data?

Once you know that the transmission of data was secure, and that the data sent was not modified, you need to determine the identity of the sender. The process for identifying the sender is called user authentication. User authentication (UA), like packet authentication and encryption, can take many forms. The simplest form of UA is the password. Unfortunately, passwords are easy to break and provide limited security. The type of UA that must be invoked for clear authentication is called "two-factor" authentication where there is something "the user has" and something "the user knows." An example of this would be the use of a PIN number and a user token (smart card, random number generator, etc.).

There are a number of authentication systems on the market today. Some use a token with a random number generator that is in synchronization with a host process. Others use a challenge/response system, and still others use a simple password entry. Most systems today are designed for non-Internet use. In other words, these systems are designed for users who are connected via dial-up or dedicated connections. In these more traditional applications the transmission of data is relatively secure given the closed nature of Public Switch Telephone Networks (PSTN) and leased line networks. The Internet, however, introduces much greater risk to these systems. For example, someone can "sniff" the session with the authentication host and gain the password for the user. Even with tokens that change numbers frequently there is still a risk that someone will "grab" the password number off the Internet and log on to the host while the password number is still valid.

What is required for secure Internet and a secure VPN is what is called a "one-time password" system in which the password never transits the Internet, and the user is authenticated for *every* secure session that takes place on the Internet.

There are different standards for user authentication (UA), and they are summarized in the table that follows. The bottom-line is that UA is a critical part of VPN security and must not be overlooked. Information Resource Engineering implements a one-time password system based upon ANSI standards and provides the most comprehensive user authentication in the industry today.

How Do You Control the System?

Control is paramount to the success of the system. Control refers to the use of security management to operate the system. Security management includes configuration management, access management, key management, internal control management, and firewall management. Complete control is particularly critical when revoking users' privileges. If an employee leaves the company his/her privileges must be revoked immediately. Revocation is an easy task when the employee is stationed in a corporate location. However, when the employee is a telecommuter who may be connecting with the corporation through the Internet from anywhere at any time, privilege revocation becomes a more complex task.

Key Management

At the core of security management is key management. Key management at a very high level refers to the management of keys. Although many books have been written about this topic, it is important to understand that key management, or more importantly how key management is implemented, is critical to the success of a system. For example, one could have the strongest encryption available with the best user and packet authentication, but with weak key management, the entire system is compromised. Information Resource Engineering was the first company to implement a commercial key management system.

There are two generic types of key management: private (sometimes referred to as symmetric) and public. Private key is typically implemented by banks and other organizations that want to have a closed user community with complete central control. The most frequently implemented form of private key management today is the US ANSI (also ISO) standards for private key management called X9.17.

Public key is based on an open user community where keys are negotiated in the public domain based upon a public key that is stored at a certificate authority. In the United States as well as other countries, there are many Electronic Commerce (EC) projects based on public key management that are underway. The important point to remember is that public key management for the Internet, as defined by the IETF, is ISAKMP/Oakley. ISAKMP/Oakley (Internet Security Association Key Management Protocol/Oakley) will soon be ratified and accepted to be the key management protocol for VPNs that are based upon a public key architecture.

The following table summarizes five crucial business requirements and outlines the technological solutions necessary for successful implementation.

Steps for VPN Implementation

Business Requirement	Technological Solution
Keep communications private	Industry standard and proven encryption
Data arrives from legitimate source	Packet and Message authentication in real-time
User is who he/she "claims" to be	Continuous user authentication through the use of tokens and one-time passwords
The LAN is protected from the network	Firewall functionality to protect the LAN from the WAN
Management of the network, the users, and the resources	Centralized security and key management based upon industry standards including ANSI X9.17 and IETF ISAKMP-Oakley

If these five technological solutions are adhered to, a secure VPN will be implemented. If any step is overlooked, there will be a security hole in the system. Further, these solutions are specifically for the implementation of a VPN. A VPN is based upon a secure transmission between both intra- and inter-corporate users. If there is to be non-secure transmission of data, additional steps need to be taken to secure Internet communications.

Examples of an VPN

There are two examples of a VPN discussed below. One example is of a large government contractor, and the other is of a large automobile manufacturer.

A Government Contractor

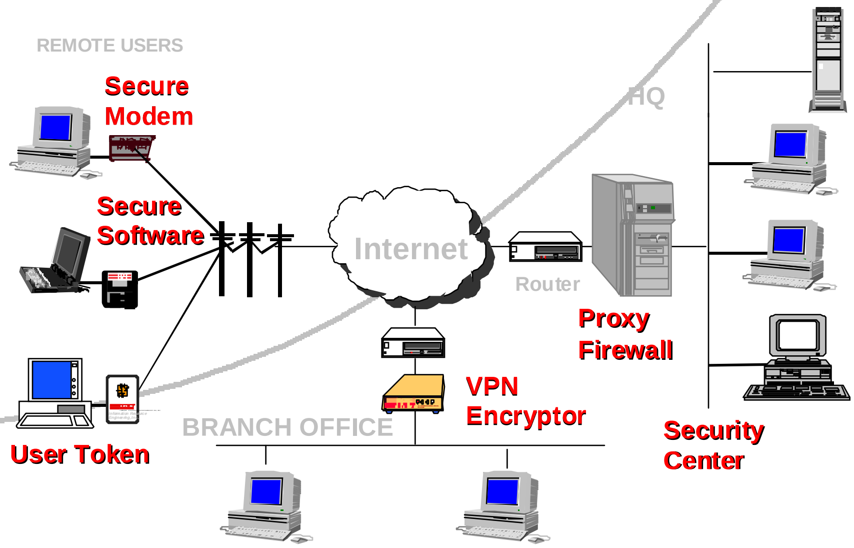
Figure 3.0 depicts a large US Government contractor. The company is based in Washington DC and has a large office in the Midwest. The contractor is using the Internet for *all* communications between its offices, remote employees, and the corporation. The salient points for this VPN example are:

- Cost Savings - This VPN results in significant savings because the cost of purchasing local Internet access is lower than the cost of dedicated lines. The company has T1 (1.544 Mbps) access at both its headquarters and remote office, and remote users use local access at speeds of up to 33.4 kbps.
- Central Security Management - This VPN has a security management workstation where the customer performs all of his/her own security management. This is a requirement of the customer's security policy that requires all security management must be performed in-house.
- Central Firewall - The company's policy is that all non-secure Internet access must be routed through the main firewall at headquarters. The VPN facilitates this requirement since all remote users are given secure "pipes" back to a central site where they can then go back through the firewall for non-secure activities. This use of the VPN results in reduced firewall expenditures and better firewall management. Of course, an employee at the office in the Midwest needs to "ride" the Internet twice if he/she wants to do

non-secure Internet work. However, given that there is high speed access, the performance of a double-connection is acceptable to users.

- Security for Traveling Executives - Remote users connect through the Internet so that wherever they are, only local access is required. As stated previously, remote users are authenticated through two-factor authentication (smart card and PIN number).
- Security and Flexibility for Temporary Workers - A Government contractor has employees who need to be on-site at Government locations for extended periods of time. Remote access via the Internet provides these employees with the most efficient and cost effective way to connect back to headquarters. Even LAN-to-LAN communication is possible through local ISP connections from various Government sites.

Contractor VPN



An Automobile Manufacturer

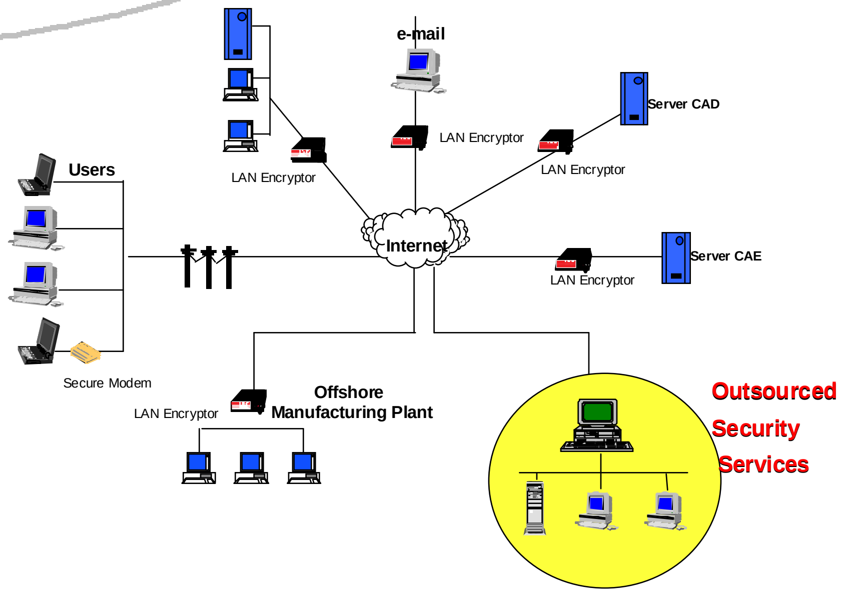
Figure 4.0 depicts a VPN for a large US-based automobile manufacturer. The example could represent any large manufacturer. The primary application of the network depicted is to connect parts suppliers with the manufacturer. The reason security is critical is because the manufacturer needs to send out highly confidential design documents so that the parts suppliers can make the parts. Sometimes parts are made two years before the actual car is assembled and released.

Before the VPN was installed, the manufacturer was operating a very expensive worldwide secure network for its suppliers, partners, and international offices. The transition to a VPN is ongoing and will be implemented in phases. The salient points of this implementation with regard to the VPN are:

- ♦ Cost - Again, cost was a major consideration when switching to a VPN was evaluated. The current secure X.25 network is extremely expensive. By switching to the Internet the manufacturer can save a significant amount over the current infrastructure. Savings are so great that the payback on VPN technology is less than one year.

- Increased Productivity - The Internet already offers higher performance in the United States than X.25 networks, and this trend will continue around the world. This manufacturer depends on moving large CAD/CAM files around the world, and every improvement in performance results in increased worker productivity.
- Increased Flexibility – Flexibility is critical to a manufacturer competing in today's competitive economy. Previously, bringing in a new supplier or design partner would require extensive planning and time. Extending a secure network onto the premises of an intended partner used to be a major undertaking. Today with the VPN, all that is required is that the partner receive a secure application (software and/or hardware) and gain local Internet access. This is another example of how the Internet is becoming the most accessible network in the world, even in Pacific Rim countries. Certainly, the connections may not offer the highest performance or reliability, but for this manufacturer, the capability to quickly get a new supplier online still offers great value.
- Partnership with Global Carrier - In this instance the manufacturer has signed an agreement with a global ISP. The ISP intends to eventually offer a guaranteed class of service for worldwide Internet connectivity.
- Outsourcing of Security Management - This manufacturer, unlike the aforementioned Government contractor, has decided to outsource the security management of the network to the global ISP.

Automobile Manufacturer VPN



As indicated, these examples are only a subset of the possibilities that a VPN. However, the examples highlight the use of security to facilitate LAN-to-LAN, remote-to-host, inter- and intra- company communications, and two options for security management.

Standards

Standards, and specifically security standards, are critical if implementation of a VPN is to be successful. For example, there are many different types of encryption available throughout Pacific Rim nations. For a corporation that only communicates within one country, implementation of a country-specific standard is acceptable. However, as soon as communication over the VPN is required outside of the country, the encryption may need to be different. Therefore, if an internationally accepted standard is implemented in the VPN, the greatest interoperability, and thus connectivity, can be achieved.

SafeNet implements ANSI (American National Standards Institute) standards for security today. These standards include X3.92 (encryption), X9.9 (message authentication), X9.26 (user authentication), and X9.17 (secret key management).

Conclusion

This paper began with a discussion about the future of the Internet. Clearly, today the Internet is the domain of Internet browsers and emailers. However, as described in this paper, there is a new possibility for the Internet - the VPN. The VPN offers an exciting next step for corporate IS managers. The VPN, if implemented correctly, can increase business efficiency, decrease costs, and increase global competitiveness. Creation of a successful VPN depends upon a successful and safe security implementation. Security implementation is our business. Information Resource Engineering provides the best security solutions in the industry. Through the implementation of SafeNet/Enterprise, numerous corporations are experiencing the advantages of a VPN today.

[i] UCC § 4A-202 (1989)