PRICEWATERHOUSECOOPERS

Alchemy

VPN Companies Meeting the Challenge

A Business Case for VPN Technology

Executive Summary

The business world today is increasingly dependent on communications and companies are requiring and providing more real time information in order to stay competitive. This has impacted information security programs as connections to remote employees, business partners, vendors and others have new avenues for business communications. These communications provide immediate access to a wide array of systems and business information and the need for new communications tools are required to help protect the information as it moves beyond traditional boundaries.

There has been much discussion in the press and in industry about Virtual Private Network (VPN) products and services. Like many other new technologies, the VPN market has been suffering through the standards development phases to establish the guidelines for interoperability. PricewaterhouseCoopers has established the following criteria for today's VPN products.

VPN Requirements

- Scalability
- Performance
- Reliability
- Usability
- Ease of management
- Interoperability
- Protocol support
- Seamless Integration
- Authentication
- Accounting, auditing, and logging

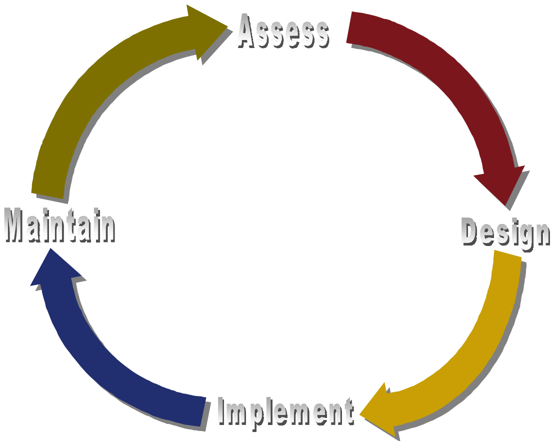
PricewaterhouseCoopers and Network Alchemy Alliance

PricewaterhouseCoopers has formed an alliance with Network Alchemy to provide global assessment, design and implementation services. The PricewaterhouseCoopers Technology Risk Services practice is skilled in providing world class security services for large national and international organizations. PricewaterhouseCoopers is excited to add the Network Alchemy products to their list of best of breed solutions based on their ability to meet the requirements of large scale VPN's.

PricewaterhouseCoopers will provide professional services in cooperation with Network Alchemy to help businesses successfully deploy VPN solutions and develop their enterprise security architecture.

- **Security Assessment**
  Assist in identifying the requirements relating to VPN solutions by evaluating the security program and architecture currently in place.
- **Security Architecture Design**
  Provide assistance in development of a VPN design for resource protection or electronic commerce applications.
- **Security Architecture Implementation**
  Assist in deployment of security architectures including VPN's to ensure a successful implementation.
- **Security Operational Services**
  Provide the necessary training and services needed to ensure that the VPN and other security solutions

stay effective for any given environment.



In addition to providing VPN specific services to organizations, PricewaterhouseCoopers provides value-added services to enhance the overall enterprise security architecture. Organizations require many other security-related solutions that work in concert with individual solutions such as VPN's. It is only after the organization understands the complete security "life cycle" that they can begin to enhance the overall security of the organization.

VPN Defined

There are many VPN products and services on the market today and a wide variety of implementations. This has created some confusion on what the term VPN actually means. This paper will attempt to define and provide clarity on VPN solutions and what their uses are in today's business.

To properly define a VPN, it will be necessary to understand a few terms and definitions. The following terms and definitions should help provide some understanding of what a VPN really is.

Virtual **-** being such in essence or effect though not formally recognized or admitted

Private **-** intended for or restricted to the use of a particular person, group, or class

Network **-** a system of computers, terminals, and databases connected by communications lines

Public network **-** A network generally accessible by many other networks where the connections to and from the network are generally not known and the entities on the network are free to join.

External network **-** A network that is not publicly accessible but may have connections to other networks that are authorized.

Internal/private network **-** A network that is primarily used by some entity and is protected from the public due to physical barriers.

Definition of a virtual private network (VPN) **–** A network utilizing encryption technology to privatize data for transmission to a trusted party.

1. It is virtual because it can use a public or a private network to transmit data
2. It is private because it uses encryption for protection of the data
3. It is a network because devices and systems are communicating on a common path

What a VPN does do

The core function a VPN provides is privatizing data from point A to point B. The VPN's primary function is to protect the data during transmission over a given network path. This privatizing of data allows the use of public networks for transmission as though they were private (virtually private). The privatizing of data through the use of a VPN can also be beneficial where information and services must be protected from disclosure, modification, unauthorized use, and interruption while traversing network segments.

What a VPN does not do

A VPN does not protect or privatize the data while it is at point A or once it arrives at point B. It can also leave information exposed while unencrypted over a given network path (internal networks before encryption device or external networks after decryption device). This point is made because a VPN only addresses one aspect of information protection but does address other issues with information that is on a disk, displayed on a screen, or printed to the local printer. Businesses must understand that there is no solution that does everything and that information security is a continuous "life cycle" involving many policies, procedures, and controls. A VPN is a great control if deployed correctly within the enterprise. Security is only as good as the weakest link. Every business must assess, design, implement and maintain their security program and understand where the risks to information assets are.

VPN business uses

Common uses of VPN technology include:

- Connecting business units at different physical locations together via a public network
- Connecting departments who transfer sensitive data together over a shared corporate backbone
- Connecting to business partners to enhance the purchasing and sales cycles
- Providing cost effective remote access for mobile employees via a public network
- Connecting confidential systems together to allow secured communications

Organizations can utilize VPN technology throughout the enterprise. When VPN technology is deployed correctly in the organization it can enable business processes that would otherwise be cost prohibitive. VPN technology can rightfully be viewed as an enabling technology that enhances the ability of the organization to achieve its' goals and objectives by increasing opportunities and revenue.

Security means more than keeping bad things from happening to you. PricewaterhouseCoopers security experts can turn security technologies, policies, and procedures into *business enablers* that will make it possible for your enterprise to maximize competitive advantage, achieve increased operating efficiency, and enhance revenues.

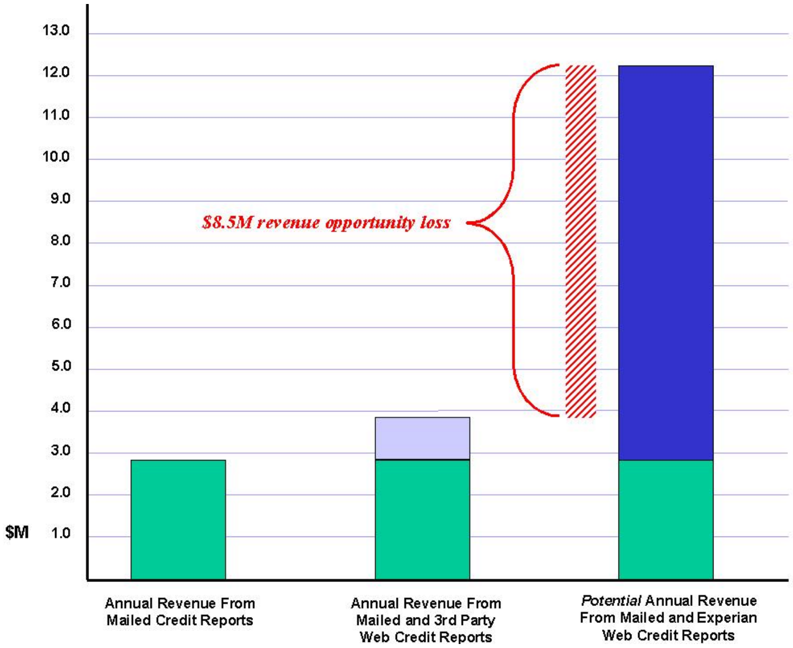
Return on Investment – Security as a Business Enabler

Here is a recent example drawn from open sources where security became the crucial factor that would allow a company to leverage the power of today's information technology into a multi-million dollar opportunity.

Credit reporting is one of the services offered by Experian Inc., a subsidiary of Great Universal Stores in the United Kingdom. Formed in 1996 out of a merger between TRW Information Systems & Services and CCN Group, Experian wanted to increase its competitive advantage over its two main challengers in this market, Equifax Inc. and Trans Union. Use of modern information technologies offered the opportunity to do so; after receiving more than 20,000 electronic-mail requests for online access to credit reports, in 1997 Experian launched a Web-based service that allowed clients to download credit reports from Experian databases across the Internet.

Once advertised, the service proved its tremendous revenue potential – over 2,000 credit report requests were received within the first 12 hours, more than triple the customary monthly rate of 30,000 hard-copy requests. At $8 per report the web service represented at least $10M in potential annual revenue. Unfortunately for Experian, within the first day of operation the system mis-routed 14 reports, sending sensitive credit information to people whom had not requested it. This was the very sort of problems that have privacy advocates and the Federal Trade Commission concerned, so Experian was forced to quickly suspend service. While they later contracted with third-party companies to provide their Web/credit report service, the demand has not represented a tenth of the potential, as the third-party providers do not have Experian's name recognition.

Experian has suffered a revenue opportunity loss of nearly $9M per annum, as shown in Figure-1 below. The cost of security in an implementation that protected information confidentiality and integrity would have been far less.



Return on Investment – Using Security to Increase Enterprise Efficiency

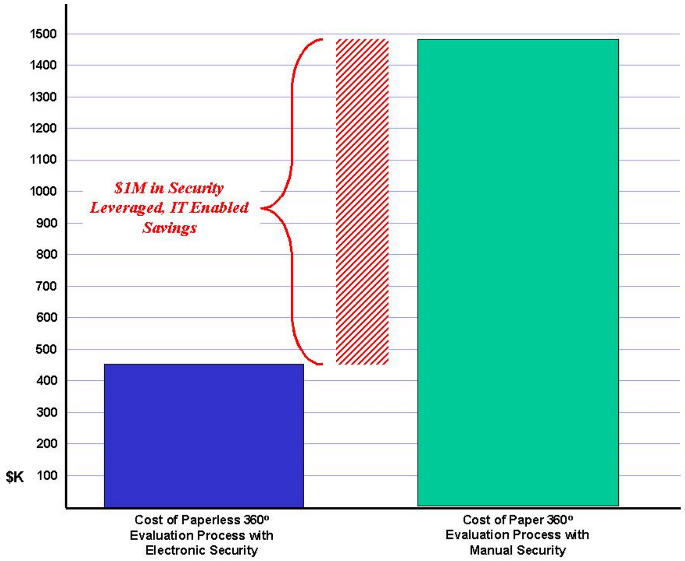
Here is a recent example where security became the fulcrum that allowed a company to leverage the power of today's information technology (IT).

A large technology company wanted to improve its employee evaluation process using a new full-circle or multi-rater assessment process. This new method was expected to help the company define corporate competencies, increase the company's focus on client service, and enable employers to align their performance with the organization's needs and to create a less hierarchical workforce. However, the multi-rater assessment process was far more complicated than the traditional appraisal process, as each employee would be rated by a body of peers and subordinates, as well as by their supervisor. Each member of individuals' appraisal teams would provide grades and comments for subsequent tabulation and read-out.

The first year the costs were high, as the entire process to distribute, enter data, tabulate results, and report was carried out manually. Obviously, the credibility and viability of the system largely depended upon maintaining confidentiality of individuals' grades of their subordinates, peers, and supervisors. As a result, a complex, labor-intensive method for secure distribution, collection, tabulation, storage, and reporting was employed, at an internal cost of nearly $1.5M.

However, in subsequent years, the process has been carried out over the company's intranet. Using this method, graders receive information, select their team, submit their grades, and receive results electronically. Security continues to be the crucial factor; the credibility of the intranet-based system rests on employees' certainty that their information remains confidential throughout the process. To assure this, access to each individual's account is protected by a their personal user ID and password, transactions are protected during transport through a combination of physical and technical protections, and all data is stored on secure media.   As shown in Figure-2 below, this one-time security investment has resulted in annual savings of over $1M in labor, productivity, postage, tabulation and storage costs.

Efficient, effective information use is a discriminator in today's business world. PricewaterhouseCoopers will show you how to use information assurance to keep your competitive edge.



Requirements of a Well Designed VPN

Scalability

Scalability is more than just throughput. Throughput is how much data a given box can handle at any one time. The problems with that we encounter are how do we grow from there. Once we reach that limit what do we do to scale. Scalability must include ways to stack boxes together to work in tandem, similar to the concept of stackable hubs. If we need more connections we just add another hub to the stack. Of course there is always a limit to how many things we can stack, but the point is that we are not limited by a single unit's performance. Scalability allows a solution to grow as the business grows and eliminates fork lift upgrades and usually provides load balancing and redundancy.
Performance

Performance is the raw throughput of a device. The VPN must be able to handle a large amount of traffic if it is going to work in the enterprise. Depending on the given scenario, a VPN should be able to process close to the input line speed that it connects to or to the line speed of the slowest link. If you are connecting a VPN device to a 100Mbps Ethernet segment but the incoming traffic is routed over a T1 then you would only need the 1.544Mbps throughput. If you were using the VPN to encrypt traffic across an internal ATM backbone then you would want the encrypted throughput to be close to 100Mbps.

Reliability

For a VPN to actually make it in the business world it must be reliable. Reliability means that it should be available at all times, like your telephone works at all times. Reliability must include redundancy features to allow automatic recovery of failed devices with limited interruption of service. As VPN solutions are adopted in the business world and begin to play a key role in the organization, reliability will be a necessary factor. Organizations are looking to use VPN technology as an enabling strategy to provide access to enterprise resources to increase opportunities and revenues while lowering the costs of providing connectivity.
Usability

The VPN needs to be very easy to use and understand. For a VPN solution to be successful the end users of the VPN should be able to use their services without realizing they are doing so. The VPN should be transparent to the user when tunnels are established and torn down. There shouldn't be any unnecessary requirements for the users to perform allowing for secured access to resources required to get their job done. increased security and efficiency allowing the workforce to meet the organizations goals and objectives. A good policy distribution system should allow the VPN to determine when to encrypt and when to send clear text information. The only requirement the user needs to notice is authentication to provide access.

Ease of Management

For a VPN product to be deployed by any medium or large enterprise, it must have a well-implemented management solution. In security products it is key to have a solid management solution to ease the burden of administration, management and reporting. The management platform must have a simple way to design security policy, an easy way to distribute that policy and an easy way to simultaneously manage a large number of devices. It should include the capability for separation of duties, distributed management consoles and fault tolerance.

Interoperability

To make complete use of a VPN product it should be interoperable with other VPN products. For a complete enterprise solution the VPN will need to allow you to communicate with business partners and others who may have deployed a different solution than you. This requires that to communicate securely you should ensure that your selection of VPN equipment be interoperable according to industry standards and protocols. This factor will enhance the ability of the organization to enable new forms of electronic commerce in the future and continue to capitalize on the cost advantages of VPN's as well as protect investment.
Protocol Support

If a VPN is truly an enterprise solution it will provide a wide range of networking protocols. These protocols ensure that you can communicate with other business partners and various forms of dial devices that may be necessary in the organization. The following protocols should be supported:

- IPSEC
- IKE
- PPTP
- L2TP
- RADIUS

Seamless Integration

For a VPN solution to fit into an organization it must integrate into the network and other systems as a complementary service. A VPN is merely privatizing data to protect information as it travels from point A to point B. The VPN device should integrate into the existing infrastructure and provide value. This additional value is only recognized fully if the solution will work with the existing remote access servers, internet connections, certificate authorities and authentication mechanisms. A solution loses value if an administrator must maintain a completely separate authentication database to provide access.

Authentication

As we start distributing data through the use of VPN technology we must realize the need for authentication. This authentication will be required at several levels. First it is required that the VPN software authenticate with the other VPN devices that it is communicating with. This requires that device A and device B have properly exchanged information (keys, certificates, etc…) to authenticate before they begin the encryption /decryption or authentication/verification of communications. Second it may be necessary (as in the case of the remote laptop users) to follow up with user authentication to ensure the person in possession of the device is who they say they are. This can be in the form of username/password, tokens, certificates, smart cards or a variety of other user access controls available. This provides an extra measure of protection to mitigate the risks of lost or stolen devices. To help with centralizing user administration, the VPN system should support third party authentication mechanisms.

Accounting, Auditing, and Logging

For any security solution to be complete, it must be able to log, account, and create audit trails. The system should log system events to help administrators identify problem areas and understand when key events have taken place. The security function will want logging enabled to review breaches in security policy, potential intrusions and other security related events. Others in the organization such as Internal audit and accounting may wish to view accounting for users, usage, and other activities. A good logging function will provide the necessary information with the ability to notify selected individuals when encountering a given event.

Understanding the Requirements to implement a VPN

Organizational Security Policy

One of the underlying requirements to implement a VPN is the overall enterprise security policies and procedures. A VPN is merely a point solution to solve a specific problem. A security policy should be identifying your need for a VPN based on the formalized risk assessment process that identified the risks to information.

Understanding business requirements

A VPN should be viewed as an enabling device to allow business communications to be achieved over public infrastructures or other insecure means. A VPN solution will help businesses provide solutions for remote employees, business partners, and other electronic commerce initiatives.
Understanding what you are protecting

Before deploying any solution businesses need to understand the problem and ensure that the solution they are deploying actually addresses that problem. A VPN only protects the information in transit from point A to point B and additional measure may need to be taken to safeguard the information once it reaches point B.

Understanding legal issues

With any encryption solution there are legal considerations to look at. Encryption import and export laws must be understood when deploying international solutions and this must be taken into account during the design phase of the solution.
Understanding integration issues

Infrastructure requirements are a big consideration when looking at deploying a VPN solution. Organizations need to understand VPN technologies as well as other technologies to integrate the solution into the network properly. A solid understanding of information security, system security, routing, and other issues must be addressed to deploy a success enterprise wide VPN solution.

Conclusion

Organizations are becoming more aware of the opportunities available to meet strategic goals and objectives by leveraging security and technology to deliver services to employees, clients and business partners. The use of VPN technology has matured to a level where it will provide organizations with a solid solution to enable new avenues to drive revenue and reduce operating costs.

PricewaterhouseCoopers has formed an alliance with Network Alchemy to provide a full range of security related services to deliver world class security solutions. This alliance combines the excellence in best of breed product development by Network Alchemy and the excellence in best of service security consulting by PricewaterhouseCoopers to deliver an incredible value to today's organizations.

About the Author:

Chris Cooper is a Manager in the Technical Risk Services Practice at PricewaterhouseCoopers, based in St. Louis, MO. Chris has more than six years of experience in information systems and information security. He has experience designing and implementing enterprise level VPN solutions for large scale clients. Chris can be contacted at ccooper@us.pwcglobal.com.

Your worlds Our people