Global Information Assurance Certification Paper

GIAC Security Essentials Certification (GSEC)
Practical Assignment
Version 1.4b.
Option 1

01-April-04

Saleh Al-Rosayes

Virtual Private Network
VPN

Abstract:

The Internet as well as most packet-switching networks are based on the Internet protocol (IP). IP, however, is inherently insecure, it is relatively easy to capture IP packets that are in transit, modify and replay them without the destination host being able to detect the modifications, in addition there is no guarantee that the IP datagram originated from the source it claims to originate from.

Virtual Private Networks are a very attractive technology to address these issues, it provide secure data traffic via an unprotected private network or public network (as the Internet). The encryption of the data guarantees its confidentiality and integrity with the ability to authenticate the identity of the sender. Secure VPN with tamper-proof design gives the top security for sensitive information. Our aim in this paper to present the major components of this important technology, and how it will be used to implement encryption and authentication of data, and to describe the major factors that will seriously affect the efficiency of using such technology such as the key length and key management, we will discuss the different VPN solutions available with its major characteristics to be able to select the solution that best fit into different types of networks.

Introduction:

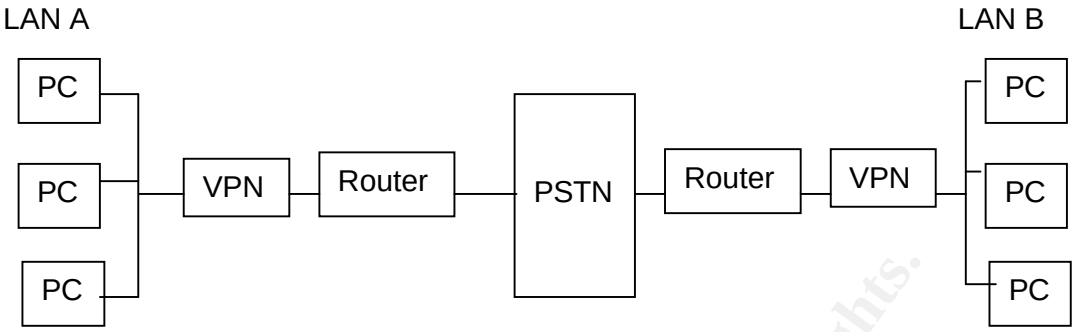
Interconnecting networks at different locations via a public network such as the internet gives the great advantages of the low cost and the wide availability. But at the same time it introduce many great challenges and risks; one of the most critical aspects is how to provide secure data exchange using the limited capabilities of most public networks.

Information can be monitored or modified on the network, it can be stolen. Viruses and Trojan horses can be imported to the local network. With the VPN (Virtual Private Network) Solution many of the security risks can be minimized.
Secure VPNs make use of tunneling and security protocols to maintain the privacy of data transactions over the Internet.

VPNs are categorized in two main types:

- Hardware VPN: This is mostly encrypting router. It has more performance, reliability and security than the software VPN. Some products also combine VPN and firewall solutions into one box.
- Software VPN: which is more flexible than the hardware VPN, but it requires more knowledge about the host operating system and the application software to be configured.

In the following figure, two networks are connected using a PSTN connection, the PSTN (Public Switched Telephone Network) connection is considered as the most available with lowest cost connection worldwide, the VPN technology is applied at the gateways of both networks, providing datagrams with the level of encryption needed before being transmitted via the public lines,



Hardware versus Software:

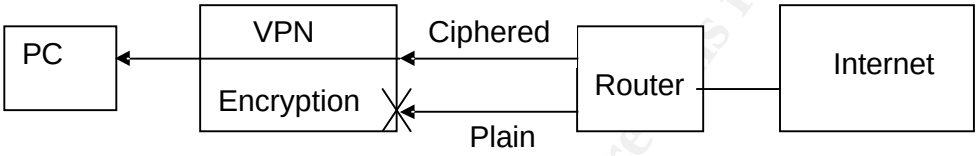
Cryptographic processes are used on a wide variety of hardware platform: On Pcs, which sometimes have encryption integrated via the software, on PC add-in cards (multi-chip security module), on single chip security modules such as smart cards and in so called “stand-alone” security devices. Where cryptographic processes are implemented solely in the software (for example on PCs), different attacks can usually be carried out. Systems with greater security need a hardware platform with a physical security module. An appropriate combination of software and hardware is required. The security module guarantees the protection of the cryptographic processes and the parameters used. The use of hardware not only increases the security of the cryptographic processes, but is crucial in running fast applications with data rates of several hundred megabits or even gigabits per second. Without a tamper-protected security module, no strong security application exists; it is the key element in the security maintenance chain. The solution is to give security applications additional protection against physical attacks. By integration all cryptographic processes and their data in a physical protected security module comparable to a safe. There, they are not only stored safely, but also run only inside the security module.

The integration of VPN services into the operating system means that IT professionals who work with these operating systems are already familiar with how to navigate these systems and do not have to worry about learning a new product. Since most VPN appliances do not integrate well with existing networks, using servers for VPN services often means greater integration with the network, particularly in the area of authentication. The issues of security, reliability, and cost stand out when evaluating a server-based VPN solution. There should be no surprise that a hardware-based VPN solution brings a greater degree of reliability and security than one built around a server operating system such as Microsoft. The same is true in the case of firewalls and routers. The cost associated with maintaining security patches and basic server administration add up on a monthly basis. Additionally, the cost of building a VPN server solution can run in excess of $2,500 once the costs of hardware and software are added. [ZDN02]
Whether you are looking at a VPN appliance, server, or managed service provider, performing proper cost/benefit analyses can be the most important

step in a successful VPN solution.

VPN Encryption

The idea of VPN Encryption is to protect all information transmitted from the trusted network via an untrusted network (internet). It also protects the access to the trusted network and hides the network structure and applications, when intercepted on the untrusted network.
The whole data packet, including the IP addresses, the data type and the data itself, will be ciphered. The datagram will be sent to the internet with new station specific addresses. This prevents analysis and modification of the data sent via the network. Only ciphered packets are allowed to enter into the trusted local area network. This prevents hacker accessing the local network.



The good encryption is done by a hardware encryption module and software according to ESP (IP Encapsulation Security Payload) and header. [RFC95]
At least two cipher units are connected through the public or private network over secure tunnels. Each tunnel uses a different communication key. All tunnel traffic (IP Datagram) is encrypted using ESP (IP Encapsulation Security Payload) extension header and a hardware encryption chip. [RFC95]
Since the header of the IP packet is also encrypted, all relevant data are hidden, not only the payload of an IP packet. These data, for example, the IP addresses of the sender and the recipient, are additionally protected in order not to disclose any topology information of the trusted area.
The use of encryption adds some additional overhead to a session. Most VPN units, whether hardware or software VPNs will be able to process encryption for connection up to 10baseT speeds. On a lower speed connection like a modem, VPN processing is much faster than delays of limited bandwidth. Often Performance is affected more by packet loss and latency on bad Internet connections than by the encryption overhead.
Virtually all of the common encryption technologies can be used in a VPN. Most of VPN vendors give the user a choice. VPN vendors support a number of different authentication techniques and products such as Kerberos, tokens, and software and hardware based dynamic passwords.

IP and Network Technology

The IP layer is basically independent of the network technology that is used to transport the data. The physical interfaces in use on the trusted and untrusted sides are irrelevant to the IP layer. In the VPN hardware all products use the same physical network technology on both sides (trusted and untrusted site). The VPN machine is a device that forwards IP packets from one interface to the other (such a device is usually called a router or a gateway). The system

selects the right tunnel depending on the destination address.

Tunnels

Two VPN devices are connected over secure tunnels via the Internet or Intranet. Each individual tunnel is ciphered with a separate communication key. The tunnel table stores the destination address and SPI (Security Parameter Index) reference of the tunnel and the actual status of the tunnel. Each entry of the tunnel table is used to define one tunnel.

Tunneling Protocols:

- Point-to-Point tunneling Protocol (PPTP) working at layer 2 of the OSI model. It is widely used for remote access connections.
- Layer2 Tunneling Protocol (L2TP) working at layer 2 of the OSI model. It is considered as an improvement of L2F (Cisco Product) and PPTP by combining best features for both to create new standard L2TP. It is for tunneling PPP sessions across variety of network protocols such as IP, ATM or Frame relay. L2TP can build tunnels without encryption but this is simply will not be a VPN because it is not protected
- IP Security Protocol (IPSec) working at layer 3 of the OSI model. It can be used as a complete VPN protocol solution, or it can be used as the encryption scheme within PPTP or L2TP. It provides authentication and encryption over the internet.
  - IPSec suite consists of:
    1. Authentication Header (AH) provides authentication integrity and anti-replay protection for both the IP header and the data payload. It does not provide confidentiality.
    2. Encapsulation Security Payload (ESP) provides confidentiality and authentication. Data is encrypted before it is transmitted.
    3. Security Association (SA) a Security Association is a relationship between two VPN Encryption units that describes how they communicate securely with each other. A Security Parameter Index (SPI) uniquely distinguishes each SA from other SAs. A Security Association is normally one-way. An authenticated communications session between two VPN units uses two SPIs (one in each direction –SPI_{RX} and SPI_{TX}). The combination of a particular SPI and a particular Destination Address uniquely identifies the Security Association. The sending unit uses the Destination Address to select an appropriate Security Association (SPI value). The receiving unit uses the combination of SPI value and Destination Address to distinguish the correct association.

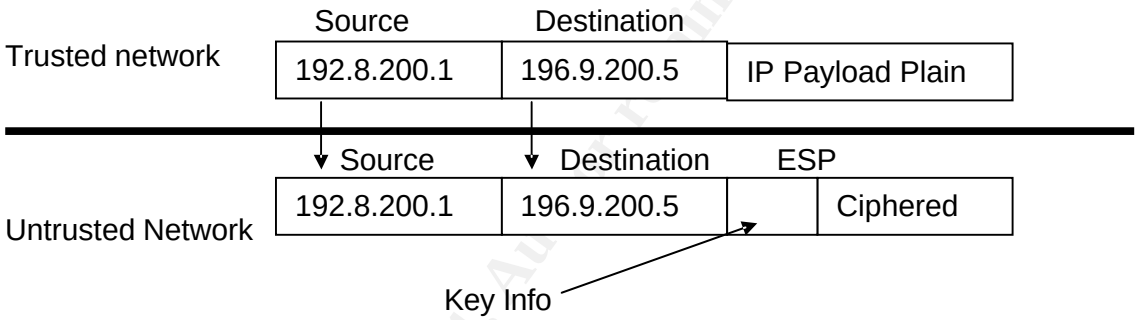
Secure Encapsulation of IP Data

IP Encapsulation Security Payload (ESP) describes two methods for using encryption to generate the confidentiality of data sent via the internet (or via a private IP network): Tunnel Mode and Transport Mode. (ESP has been assigned Protocol Number 50).[RFC95]:

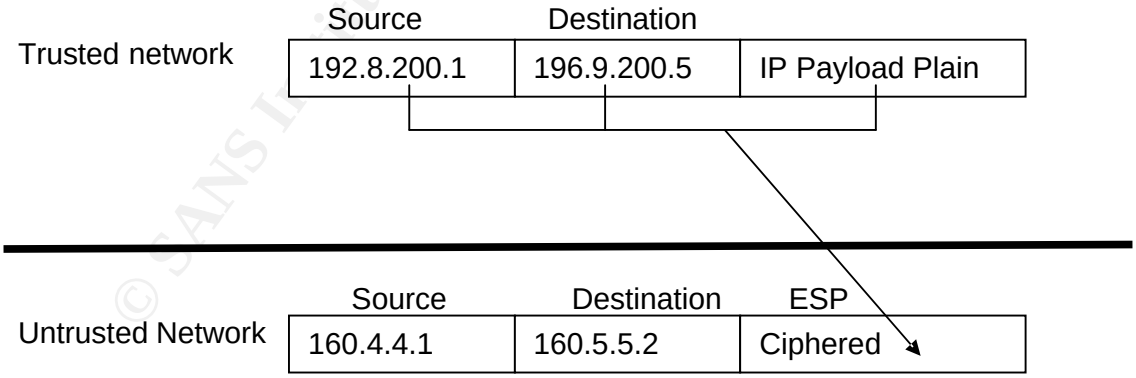
- In Tunnel Mode ESP, the original IP datagram is placed in the encrypted portion of the Encapsulating Security Payload and that entire ESP frame is placed within a datagram having unencrypted IP headers. The information in the unencrypted IP headers is used to route the secure datagram from origin to destination. An unencrypted IP Routing Header might be included between the IP Header and the Encapsulating Security Payload.

- In Transport Mode ESP, the ESP header is inserted into the IP datagram immediately prior to the transport-layer protocol header (e.g., TCP, UDP, or ICMP). In this mode bandwidth is conserved because there are no encrypted IP headers or IP options.

Transport Mode:



Tunnel Mode:



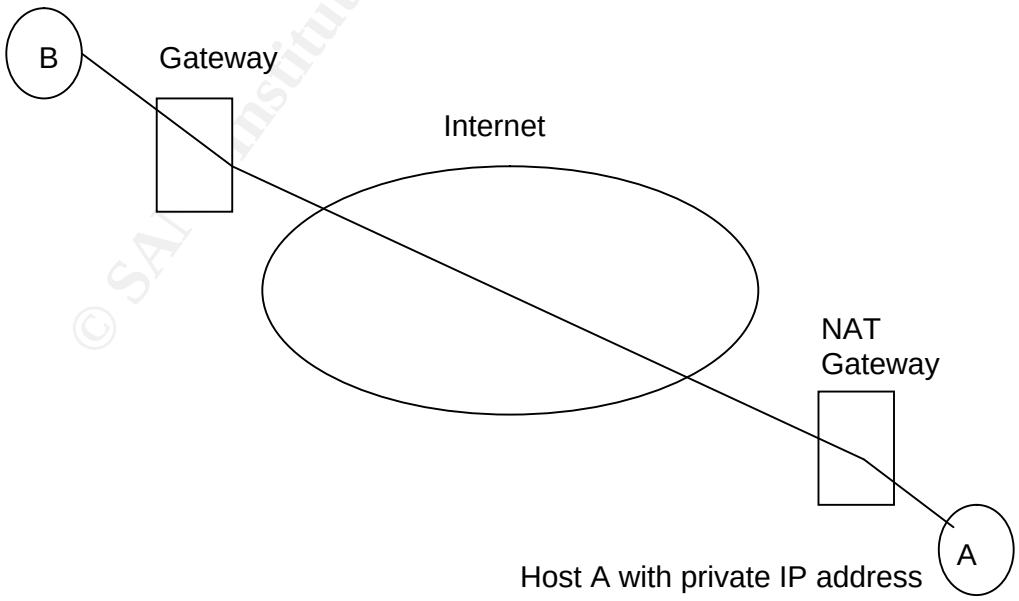
The idea behind tunnel is that the entire packet from a trusted network is encrypted and put in a new IP packet that has the address of a cipher system on another trusted network (and, if needed, the way to route the packet to this system). When the packet arrives at the remote end of the "tunnel", its contents is decrypted and the original packet is sent on the remote trusted network. When Tunnel Mode is used, hosts on trusted networks are hidden from hosts

on the public network. Routing information need not be exchanged between the trusted networks and the public network. In general, Tunnel Mode offers more flexibility and more security, but is more complex to configure than the Transport Mode. Tunnel Mode has the ability to hide the router, network and host addresses in the trusted network from the untrusted network. The own network map thus remains concealed from the unsecured public network. The tunnel traffic (IP datagram) is encrypted with a hardware cipher module according to ESP and header. [CIS00]

Integrity of IP Data

Authentication Header (AH) protocol provides connectionless integrity, data origin authentication, and an anti-replay protection service. However, AH does not provide any confidential services: it does not encrypt the packets it protects. AH's role is to provide strong cryptographic authentication for IP traffic to ensure that packets that are tampered with will be detected.
AH uses authentication codes to authenticate the IP datagram, this code is an algorithm that takes a message of any arbitrary length, and a cryptographic key, and produces a fixed-length output called a message digest or fingerprint, AH header that contains the message digest will be added to the IP datagram to give the destination system the ability to check the data integrity, the location of the AH header depends on the mode of operation of AH:

- AH Transport Mode: AH header is inserted after the IP header but before any transport layer protocol, or before any other IPSec protocol header, that result that AH authenticate the entire IP header. Therefore, there are limitations to the use of AH in transport mode. The following figure illustrates a case in which AH transport mode authentication cannot be employed.



in this scenario host A is using private IP address, and such addresses are nonroutable: routers on public networks typically do no route packets with private IP Addresses, packets sent to the internet from such hosts needs to pass through a NAT (network Address translation) gateway before leaving the source network. NAT gateways replace private IP address in the source address fields of headers in outbound packets with an assigned public IP address, and since AH authentication is enabled, when packets arrive at host B, the AH integrity check will fail because the message digest that B computes will be different from that which host A computed. [IPS01]

- AH Tunnel Mode: AH header is inserted before the original IP header and a new IP header is inserted in front of the AH. Tunnel mode is more useful when employed with ESP; ESP encrypts IP datagrams. In order for routers to route packets to their destinations, they need certain information in IP header. The new IP headers inserted on the packets are accessible by routers, but the inner IP headers are protected. [RFC98]

IP Address and Secure VPN:

IP address is fundamental components of a secure VPN. They are used for routing packets and determine which Security Association is used to encrypt and decrypt payloads. It is necessary to address the special routing issues needed to support a VPN device participating in a secure VPN, so the VPN device is able to build a tunnel that is used to securely exchange routing protocol packets so that it can acquire routing information concerning the various trusted networks in the secure VPN.

VPN Security:

The primary purpose of VPN is to secure the data transmitted over untrusted network. To achieve this goal, a VPN unit must guarantee the following factors

- Data encryption, data transferred unreadable
- Data integrity, i.e. data has not been modified during transmission.
- User Authentication, only authorized users can go through VPN.
- Access control which restricts unauthorized access to the network.

Any VPN user who handles extremely sensitive information has little choice but to take direct responsibility for security. The solution is called Secure VPN with tamper-proof design. Secure means that the information transmitted between the sender and the recipient is made unreadable for third parties by means of encryption regardless of what path it takes through the network. “Tamper-proof” means that all cryptographic process takes place in a special protected hardware module. This guarantee top security for sensitive information at all time.

Authentication:

In general, user authentication is based on answers of three questions what you know, what you have and what you are. VPN data link layer authentication protocol includes:

- Password Authentication Protocol(PAP).It uses a clear text authentication so it is a weak authentication way.
- Challenge Handshake Authentication Protocol (CHAP). It dos not transmit the actual password, it is more secure than PAP.
- Shiva Password Authentication Protocol (SPAP). It is used in mixed environments that support the Shiva Local Area Network Rover software.
- Extensible Authentication Protocol – Transaction Level Security (EAP-TLS). It is a Microsoft protocol of a strong authentication way that uses public-key certificates.

Encryption Techniques

- Symmetric encryption methods:

With symmetric techniques, the same key is used for ciphering and deciphering. Both the sender and the recipient must know the key. Security is only guaranteed if the key can be secret from third parties. Symmetric methods include Triple DES (Data Encryption Standard) and AES (Advanced Encryption Standard).

- Asymmetric encryption methods:

With asymmetric techniques, two different keys are used, one Public key for ciphering, and one Private for deciphering. Both keys are produced by the recipient as a pair, with the public key being made public, and the private key being kept secret. Any one can use the public key to encrypt messages in such a way that they can only decrypted by the holder of the associated private key. The advantage of asymmetric process over the symmetric process is that no secret keys have to be distributed. Typical representatives of asymmetric methods are Diffe-Hellman and RSA (Ronald Rivest, Adi Shamir and Leonard Adleman).

Key Size (Length):

The key size is the length of the encryption key in bits. Bits are just 1's and 0's. For example the bit representation of 99 is 1100011. Therefore 99 in binary form is 7 bits long. It was proved that with the enough computing power it is possible to crack a short key, for example in 1997, RSA Laboratories issued a challenge with a reward of $10,000 to find the DES key of a ciphertext that was preceded by a known block of text, which contained the phrase "the unknown message is:" A project headed by Roche Verse-an independent consultant-which involved over 70,000 computer systems linked over the Internet, to find the correct DES key in approximately 96 days [RSA97]. In July 1998, a machine built by the Electronic Frontier Foundation (EFF), cracked DES in less than 3 days [EFF98].

In the field of cryptography, the greatest emphasis is on key length, it dominates the agenda when considering the main cryptographic issues. The longer the key length, the harder it is for an attacker to break it. But key length whether in symmetric or asymmetric ciphering processes is only one part of the whole issue. An overall perspective must also include in addition to the algorithms and mechanisms used are the platform on which the cryptographic processes are running, and its protection. Equal importance must be given to the physical protection of the cryptographic units.
Data is transmitted securely in a VPN using industry standard IPsec tunneling, encryption services using DES and 3DES and MD5 and SHA-1 for message authentication. IPsec creates private tunnel through the Internet, connecting the trusted VPN networks. Unauthorized access to the information is prevented by the encryption and authentication services which are applied.
Encryption systems depend on two mechanisms to guarantee data confidentiality. The encryption algorithm provides the mathematical rules that convert the plain text message to a random cipher text message. The algorithm provides steps for converting the plain text message with an encryption key. The key length for a secure cryptographic algorithm should be long enough that it will be infeasible to use hundreds of thousands of computers working in parallel to break it.

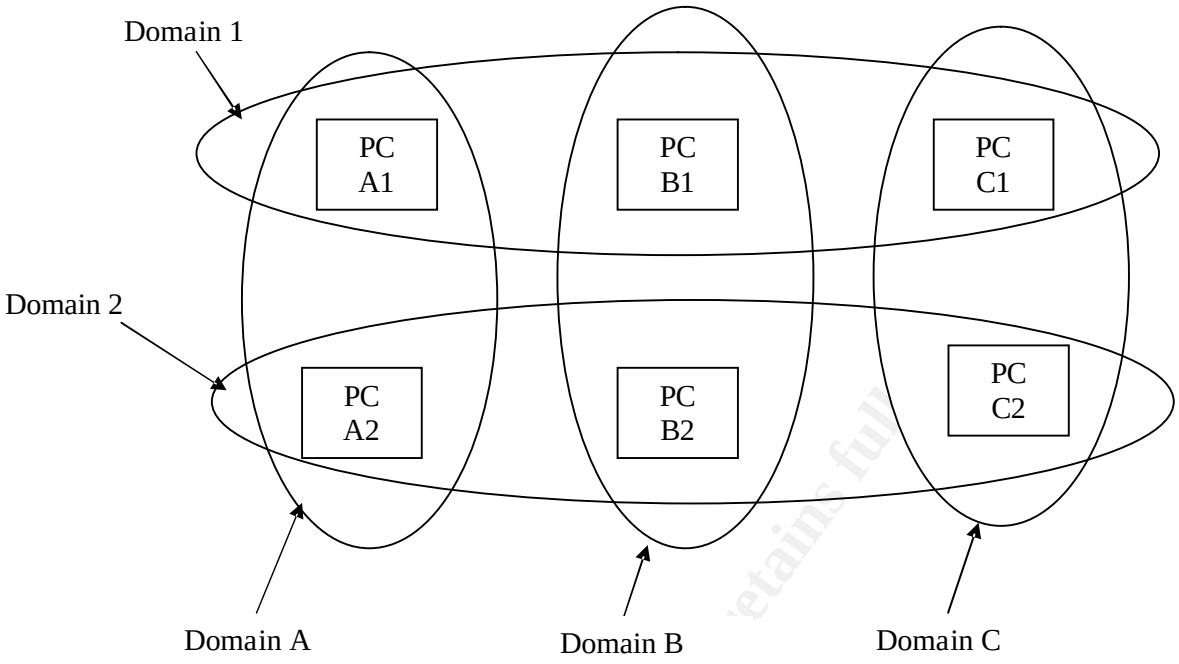
Key Management:

In VPN networks, security is always based on combination of several factors. Of these, key management is one of the most important, because much depends on it both with regard to system security and in relation to uninterrupted functioning at high capacity utilization.
As the network keeps getting larger, the demands on key management also grow. The distribution of the keys can be done either online or offline. Online distribution which is done electronically via secure link and scheduled periodically depends on the user requirements according to the information sensitivity. Let say as example for some networks it may be once a year for other it may be every day and so on. Offline distribution means it is distributed manually then it is entered using keypad or smart card according to the VPN product vendor procedure.
The purpose is to make sure that keys used in cryptosystem stays confidential, and to find the most secure way of distribution, trust should be guaranteed between all systems, once the key is compromised, the trust is no longer available, and the complete cryptosystem is not trusted.

Multi-Key Architecture:

The important step to get more flexibility based on different requirements is implementing a Multi-key architecture. Multi-key architecture allows the use of several communication keys simultaneously in the system. This has a lot of benefits such as:

- Exclusive communication links can be created which means that several user groups use a term like “communication domain” each other in different hierarchies.
- The time of Key exchange minimized.



Security Management:

Security management is to plan information security, implement it, and subject it to constant monitoring. The chosen protective measures are based on physical security, organizational security as example definition of work processes or logical categories such as use of cryptography.
Information Security Management is a sub-task of Security Management, with focus on information. IT security and computer security management concern the tools that are used to process the information.
Security Management is necessary in order to co-ordinate the cipher process used by the encryption units in the network. This involves:

- Providing each unit with the cryptographic data (algorithm parameter and cipher keys) necessary to fulfill its role in the network.
- Ensuring communication units are fully cipher-compatible at all times.
- Maintaining the secrecy of the cryptographic data during generation and distribution to the units.

With information security, an organization is able to maintain the confidentiality, integrity and availability of information. Integrity means the correctness and completeness of information but also the secure identification (authentication) of the producer of the information.

Value of information: To successfully guarantee information security, first we have to assign a value to the information based on three classifications of information “public”, ”confidential” and “secret”. To classify the information correctly, a risk assessment is very useful. The risk assessment is followed by

risk management, where protective measures are defined on the basis of the earlier risk assessment for the particular type of information. The selected safeguards are based on main three categories:

- Organizational category, such as policies, definition of work processes, training, etc.
- Physical category, such as safes locked doors with rule of access, break-proof glass, fire detection, etc.
- Logical category, such as encryption access control for IT systems, anti-virus software, etc.

Risk management also includes accessing the remaining risks after the safeguards have been implemented. No way to eliminate all risks, because of the cost and time factors. Information security management is an ongoing task. It is very important to make a periodic review of the results from risk assessment, as well as the risk management, taking account of newly identified vulnerabilities. The cost and the impact of the security measures on the work process should also be reviewed periodically. The successful implementation of information security management depends on various different factors. These includes drawing up security policies according to the organization's objectives, taking account of the organization's culture, clear support at all levels of management, clear instruction and training in security both at management level and employment level and ,not least, balanced security measures which should not seriously hinder the work processes.

VPN and Firewall:

Placing a VPN unit in parallel to an existing firewall requires no changes to an existing firewall infrastructure, but also this will means that is there two entry points to the trusted network. On most VPN units all non-VPN traffic is blocked which minimize security risk. Placing a VPN unit in front of a firewall, this will terminate secure traffic in a public zone. This will open a large hole in the firewall since there will be a certain group of IP addresses assigned to users for access. An advantage for this way that the firewall will control destination traffic, but really most VPN units can do this. This way more suitable for trading partner connectivity versus remote access users. Placing a VPN unit behind an existing firewall require some changes to the firewall. The firewall should be able to pass the VPN traffic.

VPN Setup:

What is vital for security is that the setting up of the VPN always involves working with hardware-based encryption. This allows using complex, user-specific algorithms of astronomical variety. And this in turn gives the option of creating differently structure closed user group with different degrees of user authority within the network. All users are identified within user groups. Unauthorized or intrusion is not possible. Pure software solutions can never meet these requirements, so hardware-based normally more secure.

VPN Tests:

To confirm that is any VPN system secure and satisfy an organization requirement, many testing should be applied on it. Testing routine can be categorized as follows:
Penetration Tests:
Ensure the VPN console is protected against unauthorized access. Ensure the remote management link is encrypted (secure) or it can be disabled. Ensure that VPN unit built in tamper-proof design. Ensure that a VPN unit does not pass unknown traffic. Crypto Tests: Check if tunnels can be negotiated using dynamic and static keys. Check if all data traffic through tunnel is encrypted. Check encrypted data against obvious patterns, repeated patterns and weaknesses. Try to change encrypted data contents and be sure that these data can not pass VPN unit. Management: Local management console must be secure against unauthorized access by applying full authentication. For remote administration beside the full authentication, the link also must be secure (encrypted). Services: Check the VPN system if it can support all typical services that may an organization needs such as: HTTP, SNMP, FTP, DNS, ICMP, POP3 and general file and print traffic and depends on the organization requirements certify for this point.
Configuration: The VPN unit can be easily configured from scratch or not? Is there any default security profiles configured as security levels: Plain (unsecured), secure and top secret.
Further tests have been done to evaluate different VPN solution, throughput and latency time are major factors when selecting a VPN solution whether it is a hardware or software, for testing results review reference [CSM96]

Conclusion:

Virtual Private Networks, (VPNs), are presently one of the most important segments in the technology arena for some very exciting reasons. Enhanced management and security functionality of the data networks and users as well as potentially enormous cost savings, are just a couple of the many benefits of integrating a VPN. Many data intensive enterprises such as electrical distributors, with several branch offices and partners to communicate with, are rapidly moving toward integrating VPN technology.

VPN's allow you to use the public Internet to securely connect remote offices and remote employees at a fraction of the cost of dedicated, private telephone lines, such as frame relay. There are two major uses for VPNs. The first is to connect two or more geographically separated networks, such as those at a main office and a remote branch office. The second is to allow employees or authorized users to access a network from a remote PC, such as a traveling laptop or home computer. Both of these uses involve providing authorized users with access to protected network resources.

References:

[RSA97]

RSA Data Security Inc., “Government Encryption Standard Takes a Fall.” RSA Data Press Release, June 17, 1997.

[EFF98]

http://www.eff.org/descracker.html

[IPS01]

IPSec Securing VPNs, Carlton R. Davis, “RSA Press, 2001”

[RFC95]

http://www.faqs.org/rfcs/rfc1827.html

[RFC98]

http://www.faqs.org/rfcs/rfc2402.html

[ZDN02]

http://insight.zdnet.co.uk/hardware/servers/0,39020445,2110554-2,00.htm

[CIS00]

http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns142/networking_solutions_white_paper09186a0080117919.shtml

[CSM96]

http://www.csm.ornl.gov/~dunigan/vpnperf.html