

## VIRTUAL PRIVATE NETWORKS: AN OVERVIEW FROM THE SECURITY PERSPECTIVE

Ali Ahmed Ali

[ali@cu.edu.eg](mailto:ali@cu.edu.eg)

Tarek Abd El-Mageed

[tarek@cu.edu.eg](mailto:tarek@cu.edu.eg)

Salwa Al Gamal

[Salwa\\_elgamal@menanet.net](mailto:Salwa_elgamal@menanet.net)

*Faculty of Computers and Information, Computer Science Department, Cairo University, Egypt.*

Khalid Mostafa

[kelsayed@ntgclarity.com](mailto:kelsayed@ntgclarity.com)

*Faculty of Computers and Information, Information Technology Department, Cairo University, Egypt.*

### **Abstract:**

The Internet has graduated from simple sharing of e-mail to business-critical applications that involve incredible amounts of private information. The need to protect sensitive data over an entrusted medium has led to the creation of Virtual Private Networks (VPN). VPNs allow corporations of all sizes to move away from expensive and static private line facilities to the flexible Internet. A Virtual Private Network is the extension of private network that encompasses links across shared or public networks like the Internet. With VPN data can be sent between two computers across shared or public network that emulates a point-to-point link. Packets that are sent using VPN if intercepted on the shared or public network are indecipherable without the encryption keys. A VPN is a private data network that makes use of public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures.

This paper is devoted as an overview of VPNs from the security perspective. The currently used technologies behind securing and maintaining a VPN, benefits and drawbacks are also covered. A proposed technique for remote user authentication and Security Association agreement on the application level. Another proposed technique for session key generation and exchange.

**Keywords:** Internet Protocol Security Protocol (IPSEC), Layer 2 Forwarding (L2F), Layer 2 Tunneling Protocol (L2TP), Point-to-Point Tunneling Protocol (PPTP), Virtual Private Network (VPN).

## 1 INTRODUCTION

A VPN is said to be secured if it does provide tunneling, encryption, authentication, access control over any public channel. Several other standards and protocols can provide tunneling of data, but not all of them implement encryption and authentication. The term VPN is a widely encompassing acronym that represents many communication standards. For the purposes of this paper, all references are made to secure VPNs and the IPsec's implementation to provide security in the form of encryption and authentication.

In 1994, the Internet Architecture Board (IAB) issued a report on "Security in the Internet Architecture" RFC-(1636). The report expressed the general consensus that the Internet needs more and better security due to the inherent security weaknesses in the TCP/IP protocol suite, and it identified key areas for security improvements. The IAB also mandated that the same security functions become an integral part of the next generation of the IP protocol, IPv6 from the beginning, this evolving standard will be compatible with future generations of IP and network communication technology [1].

VPN started in 1995 with the AIAG (Automotive Industry Action Group), a non-profit association of North American vehicle manufacturers and suppliers, and their creation of the ANX (Automotive Network exchange) project. The project was spawned to fulfill a need for a TCP/IP network comprised of trading partners, certified service providers, and network exchange points. The requirement demanded efficient and secure electronic communication among subscribers, with only a single connection over unsecured channels. As this technology grew, it became recognized as a solution for any organization wishing to provide secure communications with partners, clients, or any remote network. However, its growth and acceptance had been stymied by the lack of standards and by product support issues [1]. Nowadays, the market adoption of VPN has grown enormously as an alternative to private networks. Much of this is due to performance improvements and the enhancement of the set of standards. VPN connections must be possible between two or more of any types of systems. This can be further defined in three groups Client to Gateway; Gateway to Gateway; and Client to Client. This process of broad communication support is only

possible through detailed standards. IPSec (IP Security Protocol) is an ever growing standard for providing encrypted communications over IP. Its acceptance and robustness has fortified the IPSec as the VPN technology standard for the foreseeable future. There are several RFCs that define IPSec and currently there are over 40 Internet Engineering Task Force (IETF) RFC drafts that address various aspects of the standard's flexibility and growth.

Many definitions exist for a VPN, but the following may be the closest ones: -

1. Virtual private networks (VPNs) allow two or more parties to communicate securely over a public network [3].
2. Connectivity deployed on a shared infrastructure with the same policies and 'performance' as a private network [1].
3. A combination of tunneling, encryption, authentication, access control, and auditing technologies and services used to carry traffic over internet, a managed IP network or a provider's backbone [2].

This paper is organized into six sections an introduction to know what the VPN is; a survey on the current used VPN technologies; discussing the components of a VPN and the used techniques for keeping track their objectives; how to establish an IPSec VPN; benefits and drawbacks of VPN; and at last a conclusion.

## **2 VPN TECHNOLOGIES**

Four different protocols have been suggested for creating VPNs over the Internet: point-to-point tunneling protocol (PPTP), layer-2 forwarding (L2F), layer-2 tunneling protocol (L2TP), and IP security protocol (IPSec). One reason for the number of protocols is that, for some companies, a VPN is a substitute for remote-access servers, allowing mobile users and branch offices to dial into the protected corporate network via their local ISP. For others, a VPN may consist of traffic traveling in secure tunnels over the Internet between protected LANs. The protocols that have been developed for VPNs reflect this dichotomy. PPTP, L2F, and L2TP are largely aimed at dial-up VPNs, while IPSec's main focus has been LAN-to-LAN solutions. One of the first protocols deployed for VPNs was PPTP. It has been a widely deployed solution for dial-in VPNs since Microsoft included support for it in RRAS for Windows NT Server 4.0 and offered a PPTP client in a service pack for Windows 95. Microsoft's inclusion of a PPTP client in Windows 98 practically ensures its continued use for the next few years, although it is not likely that PPTP will become a formal standard endorsed by any of the

standards bodies (like the Internet Engineering Task Force [IETF]). The most commonly used protocol for remote access to the Internet is point-to-point protocol (PPP). PPTP builds on the functionality of PPP to provide remote access that can be tunneled through the Internet to a destination site. As currently implemented, PPTP encapsulates PPP packets using a modified version of the generic routing encapsulation (GRE) protocol, which gives PPTP the flexibility of handling protocols other than IP, such as Internet packet exchange (IPX) and network basic input/output system extended user interface (NetBEUI). Because of its dependence on PPP, PPTP relies on the authentication mechanisms within PPP, namely password authentication protocol (PAP) and CHAP. Because there is a strong tie between PPTP and Windows NT, an enhanced version of CHAP, MS-CHAP, is also used, which utilizes information within NT domains for security. Similarly, PPTP can use PPP to encrypt data, but Microsoft has also incorporated a stronger encryption method called Microsoft point-to-point encryption (MPPE) for use with PPTP. Aside from the relative simplicity of client support for PPTP, one of the protocol's main advantages is that PPTP is designed to run at open systems interconnection (OSI) Layer 2, or the link layer, as opposed to IPsec, which runs at Layer 3. By supporting data communications at Layer 2, PPTP can transmit protocols other than IP over its tunnels. PPTP does have some limitations. For example, it does not provide strong encryption for protecting data nor does it support any token-based methods for authenticating users. Provider-based VPNs come in two fundamentally different types, layer two (L2VPN) and layer three (L3VPN) VPNs. They target different customer segments, where customer control and flexibility are traded against customer simplicity and maintainability [4]. Table 2.1 summarizes the different VPN technologies points of weakness and strength.

*Table 2.1 Current VPN Technologies Comparison*

<b>Technology</b>	<b>Strength</b>	<b>Weakness</b>
<b>IPSec</b>	<ul style="list-style-type: none"> <li>• Standards track Protocol.</li> <li>• Works independently of higher-level applications.</li> <li>• Built as a part of IPV6.</li> <li>• Allows for network address hiding without network address translation</li> </ul>	<ul style="list-style-type: none"> <li>• No user management.</li> <li>• No production interoperability among vendors.</li> <li>• Little desktop support.</li> <li>• Not standardized</li> </ul>

	<ul style="list-style-type: none"> <li>• Will accommodate developing cryptographic techniques.</li> </ul>	
<b>Firewall</b>	<ul style="list-style-type: none"> <li>• Currently manages security parameters, including access and accounting.</li> <li>• Offers a common interface for altering tunneling rules.</li> <li>• Usually provides user access control lists and converses with remote clients.</li> </ul>	<ul style="list-style-type: none"> <li>• Software only encryption may curtail firewall performance.</li> <li>• Presents a single point of failure.</li> <li>• Requires careful modification of an established rule base when adding VPN rules.</li> </ul>
<b>PPTP</b>	<ul style="list-style-type: none"> <li>• Runs from windows NT and Windows95.</li> <li>• Accommodates end-to-end and server-to-server tunneling.</li> <li>• Popular value-added feature for remote access.</li> <li>• Use existing windows user domains for authentication.</li> <li>• Provides multi-protocol capability.</li> </ul>	<ul style="list-style-type: none"> <li>• Does not provide data encryption from remote-access server.</li> <li>• Uses only RSA and RC-4 encryption algorithms.</li> </ul>
<b>L2F</b>	<ul style="list-style-type: none"> <li>• Enables multi-protocol tunneling.</li> <li>• Widely supported by many vendors.</li> </ul>	<ul style="list-style-type: none"> <li>• No encryption.</li> <li>• Weak user authentication.</li> <li>• No tunnel flow control.</li> </ul>
<b>L2TP</b>	<ul style="list-style-type: none"> <li>• Combine PPTP and L2F.</li> <li>• Needs only a packet-based network to run over X.25 and frame relay.</li> </ul>	<ul style="list-style-type: none"> <li>• No LAN-to-LAN configuration.</li> <li>• Not multi-protocol.</li> </ul>

### 3 COMPONENTS OF A VPN

VPNs functions to ensure security for data:

- (1) **Confidentiality**-preventing anyone from reading or copying data as it travels across the internet.
- (2) **Authentication**-ensuring that the data originates at the source that it claims.

- (3) Is often provided by Encryption/Decryption.
- (4) **Access Control**-restricting unauthorized users from gaining admission to the network.
- (5) **Data Integrity**-ensuring that no one tempers with data as it travels across the internet.

The main components of a VPN are *Encryption, authentication, and Key management*.

VPNs are built around a number of standardized cryptographic technologies to provide confidentiality, data integrity, and authentication. For example, IPSec VPN uses [5]:

1. Diffie-Hellman key exchanges to deliver secret keys between peers on a public net.
2. public-key cryptography for signing Diffie-Hellman exchanges, to guarantee the identities of the two parties and avoid man-in-the-middle attacks.
3. data encryption standard (DES) and other bulk encryption algorithms for encrypting data.
4. keyed hash algorithms (HMAC, MD5, SHA) for authenticating packets.
5. Digital certificates for validating public keys.

There are two different approaches for securing the internet application coupled security which provides authentication and encryption closely coupled to the secured application, and network coupled security which resides in the network layer and provides authentication and encryption for a whole end system. The second approach is taken by the IP Security Protocol (IPSEC) working group of the Internet Engineering Task Force(IETF). Application-layer VPNs are implemented in software. As a result, software VPNs are inexpensive to implement [6]. This paper will not only take the second approach to secure the communication, but also will extend the idea to involve the application coupled security and will propose new techniques for such purpose[7].

### 3.1 Encryption

Sending private data over public network is a matter of confidentiality; sender must ensure that its data being transmitted is securely traversed from a node to another without knowing its original content. The component that provides the confidentiality in a VPN is Encryption.

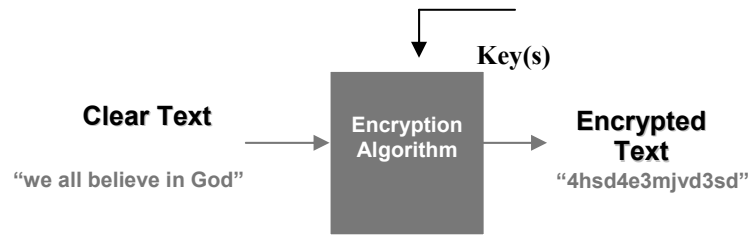


Figure 3.1.1 Encryption Process

Many encryption techniques may be used to provide Confidentiality but before illustrating them a look has to be taken on the basic techniques of encryption.

### 3.1.1 Symmetric Encryption [8]

1. Same key used to encrypt and decrypt message.
2. Faster than asymmetric encryption.
3. Used by IPSec to encrypt actual message data.
4. Examples: DES, 3DES, RC5, Rijndael.

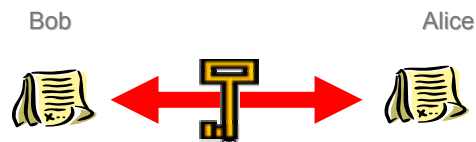


Figure 3.1.1.1 Symmetric Cipher Process

### 3.1.2 Asymmetric Encryption [8]

1. Different keys used to encrypt and decrypt message (One public, one private).
2. Provides non-repudiation of message or message integrity.
3. Examples include RSA, FFS.



Figure 3.1.2.1 Asymmetric Cipher Process

Many encryption algorithms may be used to secure the transmission of the messages over the public channel, it depends on the level of security a user seeks for, almost all vendors of VPNs are agreed to provide DES and

3DES as mandatory algorithms for encrypting messages, CAST128, and BLOWFISH to be extra installed algorithms. This issues a problem of INCOMPATIBILITY because cross-vendors VPN can't communicate easily since the absence of standards. If a symmetric key encryption is used a gain and a drawback are exist, the gain is its high performance in encrypting/decrypting messages and its weakness is if one gets the secret key that one can fail all the system since the symmetric technique uses the same key(s) for both encryption and decryption. Consider encrypting messages with RSA technique with a key length of 2048-bit key it would be beneficial for being more secured, though it will take time in encrypting messages.

## 3.2 Authentication

The authentications methods can be applied to a VPN are [9]:

- Pre-shared secret, it is no more than a password that each peer has configured and identified with the others. The most common form of authentication currently used for VPNs, it requires very little configuration time and does not need a separate infrastructure. It is too simple to manage and may be simple to be hacked.
- Digital signature, Various Security Association state information is hashed together with a key and the initiator signs the results. The initiator has the opportunity to send its certificates to the responder along with the signed hash, allowing the responder to validate the signature.

The responder must go through a rigid procedure to validate the certificate: -

1. Check the type of the certificate, if it is used or not for signing.
  2. Verifying the certificates dates.
  3. Integrity check.
  4. Determining if the issuer is a trusted entity.
- Public Key Encryption, The digital signature may seem like Public Key Encryption but DS is the encryption of a hash with a private key but in the PK the recipient uses the public key of the sender to confirm or deny the sender's claim.

In the following section a new authentication algorithm will be proposed for peers on a VPN network.

$C_i$	Client # i
$ID_{C_i}$	Client # i ID
AList	A list of all currently authenticated Users
$pub_{C_i}$	Client # i public Key
$Prv_{C_1}$	Client # i private Key
$Pub_{Server}$	Server Public Key
$Prv_{Server}$	Server Private Key
X	A well known value agreed upon between server and its clients
$IP_{C_i}$	Client # i IP address
SA	Security Association a contract between two communicating parties
V	Random Number generated by Server
Ticket	$E_{Pub_{C_1}}(ID_{C_1}, IP_{C_2}, SA)$

When client 1 is seeking for a secure communication channel with client 2, client 1 must be authenticated first and this is done through the previous technique. Our proposed technique is not only an authentication technique but also a SA generation and exchange technique. The whole process can be accomplished in at most 2 exchanges, i.e. 4 messages pass. C1 first will send ID of it and the ID of C2 to the server; the server will now generate SA for the incoming communication then will check if C1 is already authorized then sending stopping the authentication process and only send SA for both parties C1 and C2. if C1 is not authenticated yet the server generates a random variable  $v$  encrypt it with the public key of C1 and send the result to C1. C1 in return decrypts the Message and gets  $v$  adding a well-known value  $\Delta$  and to get  $p$  then encrypt it with public key of Server and sends it back again to server. The server decrypts the message to get the  $p$  then checks if the value  $p = v + \Delta$  then C1 is an authorized client then the server sends C1 the IP of C2 to start exchanging messages and the SA which will hold the security parameters. The SA will be sent to C2 as well. and if the check does not hold this means an unauthorized access is detected.

An important issue must be discussed here why the server sends to C1 its ID –IDC1- again?

If a man-in-the middle captured the ticket - EPubC1(IDC1, IPC2, SA)- can he send data to IPC2 ? Obviously yes but what if the ticket - of that Client - will be sent with messages? Surely, the server then can check for the ID of the ticket and the sender's ID if they are the same so it is ok and if not it will detect an intruder. And this is a great benefit for such an algorithm.

### 3.3 Key Management

A vital topic when establishing a VPN is how could the clients of that VPN generate, exchange and destroy the used session keys – the keys used in encryption and decryption.

One way to achieve that by the Keys Management Center – KMC -. The Implementation is a matter of answering the question of installing identical copies of KMC at each client –distributed KMC- or only one copy at the Host –centralized KMC.

The main issue here is the process of generating the session's keys. Two techniques can be applied her:

- a) The HOST generates  $n$  session keys and installs them into the client KMC.
- b) When two peers want to communicate, the initiator sends a cookie to the responder; this cookie contains the session key encrypted by the responder's public key.

The first solution is easier and applicable for infrequent communication. The second solution can take place efficiently when peers make frequent sessions of communication and require frequent keys. A new scheme for generating and exchanging session keys designed for VPNs by the second solution will be now proposed.

The following technique in figure 4 assumes that having  $n$  key generator or length  $m$ - these key generators may be random source generator or linear feedback shift register- the output of  $n$  keys will be multiplexed through a bit multiplexer to generate only one key  $k$ . This key is encrypted by the responder public key to generate  $k_e$  then sent to the responder. The responder then decrypt the key  $k_e$  and gets  $k$  and may now send an acknowledgment to the initiator, now the two peers agree on the same session key  $k$  in only one message exchange. This technique is a quite simple and can be embedded at any VPN application regardless the used network protocol.

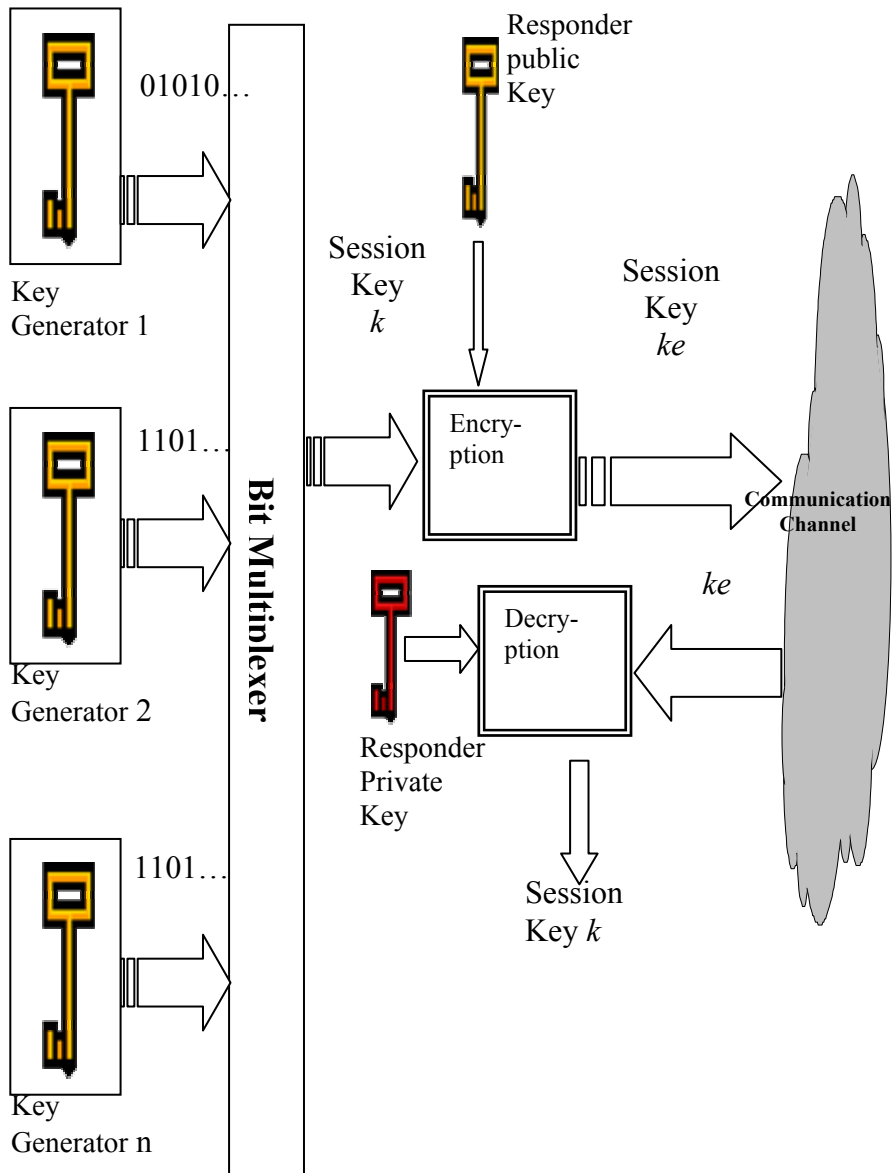


Figure 3.3.1 A Proposed Techniques for Key Generation and Exchange among VPN peers

## 4 ESTABLISHING A VPN

Now the components of a VPN have been defined, it is necessary to discuss the form that they create when combined. To be IPsec compliant the most emergent technology in this field, four implementation types are required of the VPN. Each type is merely a combination of options and protocols with varying SA control. The VPNs, shown in Figure 4.1, can use either security protocol.

In Example A figure 4.1 [1], two hosts can establish secure peer communications over the Internet. Example B figures 4.1 a typical gateway-to-gateway VPN with the VPN terminating at the gateways is illustrated to provide connectivity for internal hosts. Example C figure 4.1 combines Examples A and B to allow secure communications from host to host in an existing gateway-to-gateway VPN.

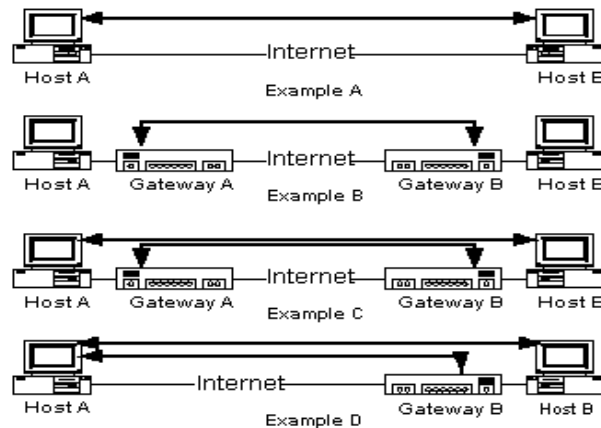


Figure 4.1 IPsec VPN construction

Example D figure 4.1 details the situation when a remote host connects to an ISP, receives an IP address, then establishes a VPN with the destination network's gateway. A tunnel is established to the gateway, and then a tunnel or transport mode communication is established to the internal system. In this example, it is necessary for the remote system to apply the transport header prior to the tunnel header. Also, it will be necessary for the gateway to allow IPsec connectivity and key management protocols from the Internet to the internal system.

## 5 FURTHER DISCUSSIONS

As getting familiar to a VPN, its basic functions, components and terminologies, a discussion in this Section of the advantages/benefits and the disadvantages/drawbacks of obtaining a VPN is held. Table 5.1 shows the idea.

*Table 5.1 VPN advantages and disadvantages*

<b>Advantages</b>	<b>Disadvantages</b>
More Flexibility, since it Leverage ISP point of presence and Uses multiple connection types (cable, DSL, T1, T3, ..)	VPNs require an in-depth understanding of public network security issues and proper deployment of precautions.
More Scalability, since one can Add new sites or users quickly and Scales bandwidth to meet demand.	The availability and performance of an organization's wide-area VPN (over the Internet in particular) depends on factors largely outside of their control.
Lower cost, since it Reduces the framed relay/leased line costs and the extra Equipments Costs.	A Compatibility problem different vendors products with the absence of STANDARDS will not work properly together.

## 6 CONCLUSION

VPNs allow corporations of all sizes to move away from expensive and static private line facilities to the flexible Internet. A Virtual Private Network is the extension of private network that encompasses links across shared or public networks like the Internet. A Compatibility problem arose from the existence of different vendors' supplies different VPN products with the absence of STANDARDS will not work properly together. The standardization process has to include used cryptographic algorithms, used authentication techniques and used key management strategies.

In this paper we have introduced the VPN, discussing and comparing the current technologies beyond building a VPN. We also have shown the components of any VPN, scanning what is meant by confidentiality in VPN. We have scanned the authentication scheme and we have proposed a new technique for remote user authentication and SA

exchange. We have illustrated how session keys can be kept, and have suggested a simple key generation and exchange protocol. We also have discussed the different examples for establishing an IPSec VPN. And finally, we have shown the benefits and drawbacks of establishing a VPN.

## **7 REFERENCES**

[1] Jim Tiller (2000), IPSec Virtual Private Networks: A Technical Review, Lucent Technology Inc.

[2] Philip Giunta (2000), Virtual Private Networks: An Overview, Lucent Technology Inc.

[3] J.P. McGregor, R.B. Lee (2000), Performance impact of data compression on virtual private network transactions, 25th Annual IEEE Conference on Local Computer Networks (LCN'00), November 08 – 10, Tampa, Florida.

[4] Gustav Rosenbaum (September 2003), William Lau and Sanjay Jha Recent Directions in Virtual Private Network Solutions, IEEE International Conference on networks(ICON2003), Sydney, Australia.(accepted).

[5] Roger Younglove (December 2000), Virtual Private Networks – How They Work. Computing & Control Engineering Journal, 11(6):260–262.

[6] C. Javier Castro Pena and Joseph Evans (2000), Performance Evaluation of Software Virtual Private Networks (VPN). In Annual IEEE Conference on Local Computer Networks, pages 522–523. IEEE.

[7] J. Zhou kent Ridge (2000), Further analysis of the Internet Key Exchange Protocol, Digital Labs Computer Communications, 23-1606-1612.

[8]William Stallings (2003), Cryptography and Network Security, Pearson Education Inc.

[9] James S. Tiller (2001), A Technical Guide to IPSec Virtual Private Networks, AUERBACH publications.