Site to Site Open VPN

Nagi Ishag Mohammed[1], Nadia El Fadil Hamid[2]

[1]College of Computer Science, Mashreq University, Khartoum, Sudan
[2]Faculty of Human & Technological Development, Omdurman Ahlia University, Khartoum, Sudan

Abstract - *Site to site VPN is the VPN connection established between two VPN gateways that reside in two different networks over the Internet, so that both networks computers can exchange data securely. There is no VPN client needed on user computers. The VPN connection will be established between both VPN gateways. Both VPN gateways will encrypt and decrypt the communication data to ensure the security and integrity of data.[1,2,3].*

The site to site VPN can be supported by IPsec tunnel mode, PPTP, L2TP over IPSec tunneling protocols.

Key Words: B2B: Business to Business, B2C: Business to Customer, ISP: Internet Service Provider, LAN: Local Area Network, VPN: Virtual Private Network, WAN: Wide Area Network.

1. INTRODUCTION

A virtual private network (VPN) is the extension of a private network that encompasses links across shared or public networks like the Internet. With a VPN, data can be exchanged between two computers across a shared or public networking a manner that emulates a point-to-point private link (such as along whole T-Carrier-based wide area network [WAN] link).

Virtual private networking is the act of creating and configuring a private network.

To emulate a point-to-point link, data is encapsulated, or wrapped, with in headers that provide routing information, which allows the data to traverse the shared or public network to reach its endpoint.

To emulate a private link, the data is encrypted for confidentiality; Packets that are intercepted on the shared or public network are indecipherable without the encryption keys.

The logical link over which the private data is encapsulated and encrypted is a VPN connection.

Users working at home or on the road can use VPN connections to establish a remote access connection to an organization server by using the infrastructure provided by a public network such as the Internet From the user's perspective, the VPN connection is a point-to-point connection between the computer (the VPN client) and an organization's server (the VPN server). The exact infrastructure of the shared or public network is irrelevant because it appears logically as if the data is sent over a dedicated private link. Organizations can also use VPN connections to establish site-to-site connections with geographically separate offices or with other organizations over a public network such as the Internet while maintaining secure communications. With both remote access and site-to-site connections, an organization can use VPN connections to trade long-distance dial-up or leased lines for local dial-up or leased lines to an Internet service provider (ISP).[5].

2. THE PROBLEM:

- Network data protection how to keep all network communications secure between two sites over an unsecured Internet.
- Expensive cost of private circuits (leased lines).
- Non-safety-the-shelf software, specifically in security applications.
- Closed source VPN such as IPSEC VPN contains too many options to be configured and administered securely by non-expert personnel, it also operates in kernel space providing the opportunity for catastrophic failure.
- Traditional IPSec implementations required a great deal of kernel code, complicating cross-platform porting efforts.
- SSL is not design for site-to-site VPNs. SSL provides access to web-based applications from any location with a Web browser and an internet connection.

3. Objectives:

- To help alleviate and minimize the administrative workload, through the implementation of an alternative method of authentication to Different network can safely grant network access to each other's through a secure site to site VPN Tunneling.
- To make a secure connection between Different sites.
- Saving cost on lease lines for remote users using public network. This is very important if many members of an organization need to connect outside the local area network.

- To design an open source simple, secure, and fast site to site VPN that neither suffer from complexity of IPSec VPN nor just works on browser.

4. VPN Background:

Virtual private networking is the collection of technologies applied to a public network the Internet to provide solutions for private networking needs. VPNs use obfuscation through secure tunnels, rather than physical separation, to keep communications private.

Protection of private corporate information is of utmost importance when designing an information infrastructure. However, the separate private networking

Solutions are expensive and cannot be updated quickly to adapt to changes in business requirements. The Internet, on the other hand, is inexpensive but does not by itself ensure privacy.

There are, in general, two ways to make a conversation private: **physical separation**, where only the intended audience can access the signal, and **obfuscation**, where even though many might detect the signal only the intended audience can understand the message. When the communication happens in a public medium, obfuscation is the only solution. For businesses in particular, the Internet is rapidly becoming the communications medium of choice. Yet conducting business requires private communications, and the Internet is a public medium.

Everyone who access to the internet may gain access to data of everyone, and between them lie a tremendous amount of "unwelcome" third parties that want to steal information from others for good, or even control other computers for illegal use.[4]

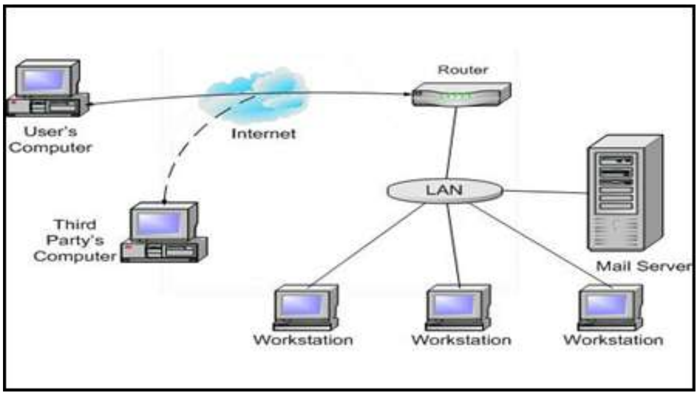


Fig -1 Third parties can use their computers to track the dataflow between user and internal network.

Here comes the problem: how to keep the data flow between the user computer and internal network secure from others and so VPN?

4. INTRODUCTION TO VPN:

The terms VPN, which stands for Virtual Private Network, is introduced to provide a secure connection between remote computers to local area network (LAN) through internet to gain access to internal computer's resources. Data between two ends are encrypted before transmission, making others impossible to interpret the content even they can track the data flow in the connection (Figure 2).

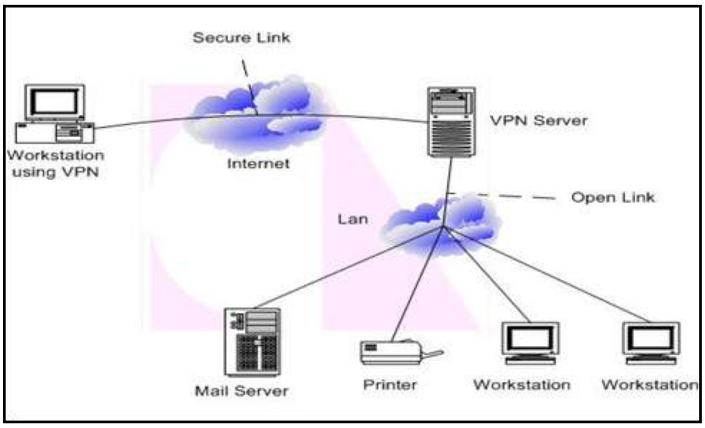


Fig-2 VPN connection between remote computer and VPN server.

In a virtual private network (VPN), various networking technologies are applied toward the goal of providing private communications within the public Internet infrastructure.

A VPN is a concept composed of two parts: a virtual network overlaid on top of the ubiquitous interconnection of the Internet and a private network for confidential communications and exclusive usage. In VPNs, "virtual" implies that there is no physical network infrastructure dedicated to the private network. Instead, a single physical network infrastructure is shared among various logical networks. For example, you can use the same network access circuit to access the Internet, to connect different corporate sites, and to connect to another business's network. This virtual network allows the construction of additional logical networks by changing device configuration only. This approach is faster to deploy and is less costly than employing dedicated physical infrastructures.

Perhaps even more important is the "private" aspect of the VPN. The very purpose of a private network is to keep the data—and sometimes even the act of communicating the data—confidential so that it can be received only by the intended audience. This privacy ensures that advantages you gain by using a public infrastructure do not come at the expense of data security.

The aim of VPNs is to use the public Internet to enable private communication to be conducted securely and reliably across the globe.[6,7].

4.2 VPN MOTIVATION:

4.2.1 Ubiquitous coverage:

Adding new destinations to a private network means adding new circuits. Thus, the coverage of a private network is limited. The Internet, on the other hand, is a vast interconnection of heterogeneous networks. Any host connected to a network that is connected to the Internet is in turn connected to any other host connected to a network connected to the Internet.

4.2.2 Scalability:

As an organization grows and more companies must be added to the network, the number of leased lines required increases dramatically. Four branch offices require six lines for full connectivity; five offices require ten lines, and so on. Mathematicians call this phenomenon a **combinatorial explosion**, and in a traditional WAN this explosion limits the flexibility for growth. VPNs that utilize the Internet avoid this problem by simply tapping into the geographically-distributed access already available.

4.2.3 Cost reduction:

Another advantage gained by using an Internet-based VPN is cost reduction based on the system's economy of scale. Simply put, it eliminates the need to purchase and maintain several special-purpose infrastructures to serve the different types of communication needs within a corporation.

Cost Reduction had done in 3 ways:

One way a VPN lowers costs is by eliminating the need for expensive long-distance leased lines. With VPNs, an organization needs only a relatively short dedicated connection to the service provider. This connection could be a local leased line (much less expensive than a long-distance one), or it could be a local broadband connection such as DSL service. Another way VPNs reduce costs is by lessening the need for long-distance telephone charges for remote access. Recall that to provide remote access service, VPN clients need only call into the nearest service provider's access point. A third, more subtle way that VPNs may lower costs is through offloading of the support burden. With VPNs, the service provider rather than the organization must support dial-up access for example. Service providers can in theory charge much less for their support than it costs a company internally because the public provider's cost is shared amongst potentially thousands of customers.

4.2.4 Security:

VPNs use cryptographic technology to provide data confidentiality and integrity for the data in transit. Authentication and access control restrict access to corporate network resources and services.

4.2.5 E-Commerce:

More and more business is being conducted using the Internet. Electronic commerce is not only a major new method of retailing merchandise (called "B2C" for business-to-consumer e-commerce), but it is also a way for businesses to trade goods and services among themselves (called "B2B" for business-to-business e-commerce). Interconnectivity of businesses is essential, and the Internet is the logical choice for the interconnection technology. E-commerce must be secure. Private networks use physical separation for security, but it is impractical to have a separate infrastructure for each customer or B2B partner. A public infrastructure is more flexible but lacks security. VPNs provide both interconnectivity and security (2).

4.3 ADVANTAGES OF USING VPN:

1. Cost is saving on lease lines for remote users using public network. This is very important if many members of an organization need to connect outside the local area network.

2. Enable high speed remote user to securely connect though public network.

3. No workload on monitoring direct access data links of remote users

4.4 FIELDS WHERE VPN USED:

1. Banking (especially E-banking service).

2. Some public service of the government.

3. Commercial (like E-commercial, E-shopping, etc).

4. Educational use.

4.5 TUNNELING TECHNOLOGY:

Tunneling is a method to transfer data from one endpoint to another through a network (internet). A tunneling protocol encapsulates one protocol or a session into another. It can transport a network protocol through a network which could not support it. The data (frames or packets) that sent from one endpoint is added with an additional header. The additional header provides routing information so that the encapsulated data can be transferred to the other endpoint.

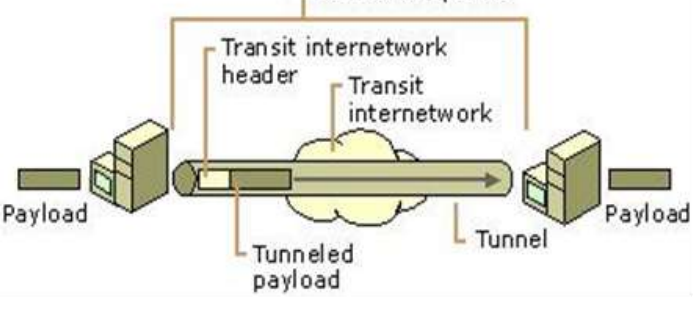


Fig-3 Tunneling model

The tunnel client and the tunnel server must use the same tunneling protocol, when they establish a tunnel.

4.6 TUNNELING PROTOCOLS:

4.6.1 IP security (IPSec) protocol:

IPSec tunnel mode encrypts IP packets, and encapsulates them into an IP header before sending them across internet or a corporate IP network. IPSec functions at the network layer (layer 3 of OSI model), and it supports both IPv4 and IPv6. IPSec contains several cryptographic protocols: Encapsulating Security Payload (ESP), Authentication Header (AH) and Internet Key Exchange (IKE). ESP and AH secure packets flows by providing authentication, data confidentiality (only provided by ESP) and message integrity.IPSec can be used to protect both UDP and TCP protocols, and it’s flexible. These are all contributed by working on layer 3, but that also increases its complexity and processing overhead.

4.6.2 Layer 2 Tunneling Protocol (L2TP):

L2TP carries PPP (Point to Point Protocol) frames and acts as a data link layer protocol for tunneling between two endpoints. It utilizes two kinds of messages, data messages and control messages. The figure below shows the structure of L2TP.

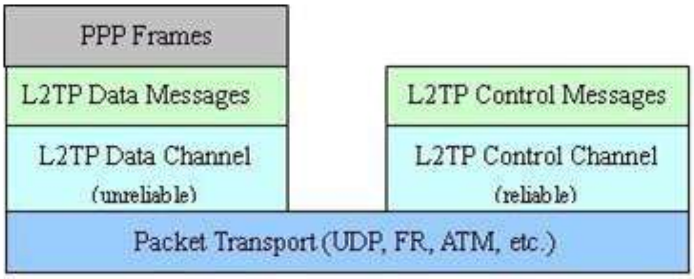


Fig-4 shows L2TP structure.

PPP frames are encapsulated by a Packed Transport (UDP, FR, ATM, etc.), then passed over an unreliable Data Channel. The control messages are sent through a reliable Control Channel.L2TP does not provide confidentially authentication. Nested protocols which are running within each session is needed to realize reliability and security. IPSec is often used to support L2TP to provide confidentiality, authentication and integrity, and this combination is known as L2TP/IPSec.

4.6.3 Point-to-Point tunneling protocol (PPTP):

PPTP works on layer 2. It encrypts and encapsulates the PPP frame in an IP header, which is sent across the internet or a corporate IP network.[3,4]

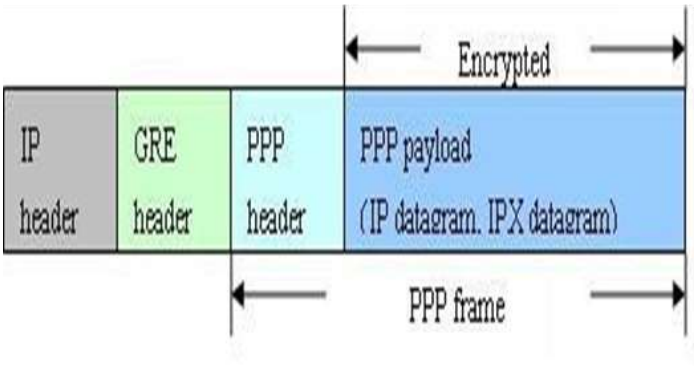


Fig-5 Structure of a PPTP packet.

4.7 VPN TYPES:

4.7.1 Remote Access VPN:

Here, VPN is "client initiated”. It’s intended for remote users that need to Connect to their corporate LAN from various points of connections. It is intended for salesmen equipped with laptops and telecommuters that will connect intermittently from vary diverse locations (homes, hotels, conference halls..).

The key factor here is flexibility, as performance and bandwidth are usually minimal and less of an issue. More than encryption, authentication will be the main security concern

4.7.2 Site to Site Intranet VPN:

This type of VPN is "client transparent". It is usually implemented for networks within a common network infrastructure but across various physical locations. For instance, several buildings may be connected to a data center, or a common mainframe application that they can access securely through private lines. Those VPNs need to be especially secure with strong encryption and meet strict performance and bandwidth requirements. They must remain easily upgradeable, since many users may be added to the load down the road (additional locations or Applications).

4.7.3 Site to Site Extranet VPN:

In this case VPN uses the Internet as main backbone. It usually addresses a wider scale of users and locations, enabling customers, suppliers and branch offices to access corporate resources across various network architectures. They rely on VPN standards such as IPSec to ensure maximum compatibility while trying not to overly compromise security (3).

4.8 Open VPN:

The project is created in 2002 by James Yonan and is continuing to improve all the time.Open VPN is an open source tool used to build site-to-site VPNs with the SSL/TLS protocol or with pre-share keys. It has the role to securely tunnel the data through a single TCP/UDP port over an unsecured network such as Internet and thus establish VPNs.

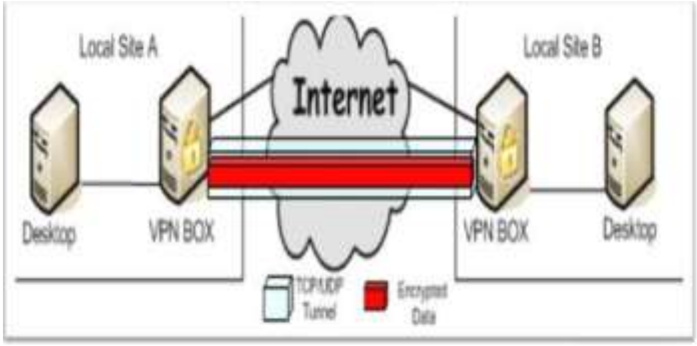


Fig-6 shows Open VPN structure.

Open VPN uses a free and open source version of SSL called OpenSSL for the encryption and authentication tasks. OpenSSL is a toolkit composed of the:

- SSL library.
- Crypto library.
- Command line tool.

The cryptography library implements a wide range of cryptographic algorithms such as:

- Symmetric algorithm: Blowfish, DES, 3DES, AES ... etc.
- Certificates: x509.
- Hash function: HMAC, MD5.[3,6,7]

5. Methodology:

5.1. How The System Works:

To describe the way the system works, it is important to know about initial TCP/IP stack, which consists of four layers**:**

1-Physical.

2-Network interface (or data link layer).

3-Internet.

4-Transport.

5-Application.

Physical Layer:

Layer 1 corresponds to basic network hardware just as layer 1 in the ISO 7-layer reference model.

Network Interface:

Layer 2 protocols specify how to organize data into frames and how a computer transmits frames over a network, similar to layer2 protocols in the ISO reference model.

Internet layer:

Layer 3 protocols specify the format of packets sent across an internet as well as mechanisms used to forward packets from one or more routers to final destination.

Transport layer:

Layer 5 protocols, like layer 5 in the ISO model, specify how to ensure reliable transfer.

Application layer:

Layer 5 corresponds to layer 6 and 7 in the ISO model, each layer 5 protocol specifies how one application uses an internet. The following figure illustrates how these layers work with each other to provide communication services between two devices using TCP protocol:

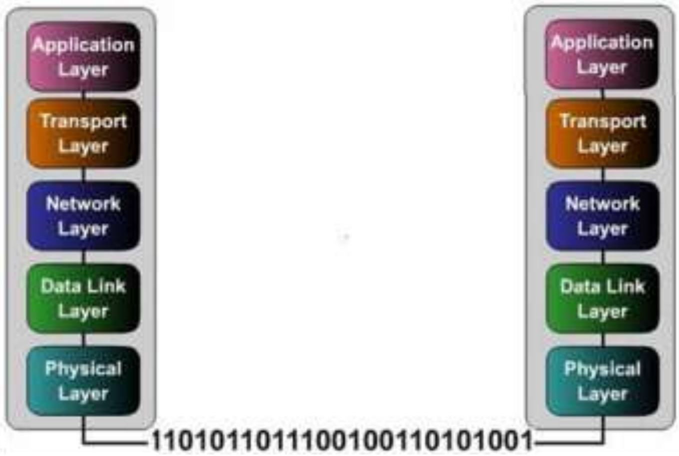


Fig-6 shows TCP/IP layers.

5.2. SOCKET

Details of TCP/IP stack figure (4.1) do not performed by the user because the operating system is doing this process and hides it from end users.To simulate this system (TCP/IP stack) network programming must be used.Some networks provide file transfer service, when user needs a file gets it by just clicking a button without knowledge of what is going on behind the scenes, to see what is going on behind the scenes a SOCKET is used.

Is the end point to transfer data between two devices, there is a group of sockets that is used in the process of data transfer, namely:

5.2.1. Sock Stream:

Used in case of using TCP/IP protocol to transfer data according to their arranged, it's secure and provides Double-exchange of data in both directions and belongs to the family **AF_INET.**

5.2.2. Sock datagram:

Used in case of using UDP (user Data protocol) to transfer data ,It's fast and not secure, belongs to the family **AF_INET,** and can be used with the family **PF_PACKET** when using the function SEND ().

5.2.3. Raw Socket:

Raw mode is basically there to allow bypass some of the way that computer handles TCP/IP. Rather than going through the normal layers of encapsulation/den capsulation that the TCP/IP stack on the kernel does, just pass the packet to the application that needs it. A **raw socket** is a socket that allows direct sending and receiving of network packets by applications, bypassing all encapsulation in the networking software of the operating system. Usually raw sockets receive packets inclusive of the header, as opposed to standard sockets which receive just the packet payload without headers.

5.2.4. Sock SeQPacket:

It's provides a contact organizer of the data, reliability, possibility of double contact, and simultaneous connection.

5.2.5. Sock_RDM:

Provides a secure connection with datagram, but does not guarantee the order of the data.

Since this system is interested in time and passes data between two or more different networks, it is required to have a device (Router) responsible from passing data through data link layer by using raw socket without intervention of the operating system.

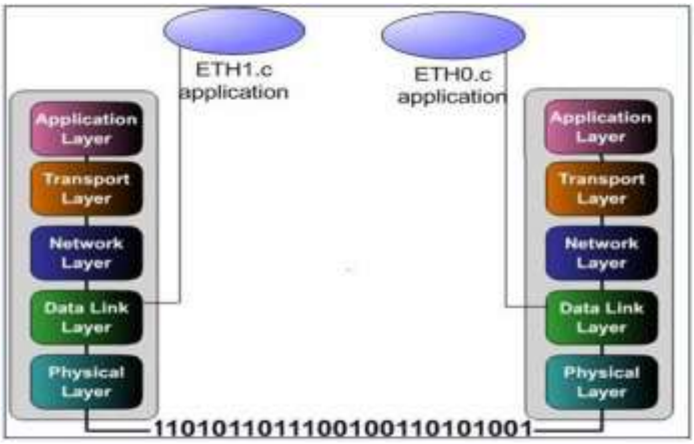


Fig-7 shows how to deal a socket with packets.

5.3 Sending processes:

5.3.1 The process of receiving packets:

1. Create a Raw Socket.

2. Set interface you want to sniff on in promiscuous mode.

3. Bind Raw socket to this interface.

4. Receive packets on the socket (All packets received will be complete with all headers and data).

5.3.2 Processing received packets:

1. Extract Ethernet header from received packet.

2. Encrypt all the rest of the packet.

5.3.3 The process of injecting packet onto network:

1. Create a raw socket.

2. Bind socket to the interface you want to send packets onto.

3. Create a TCP packet.

4. Encapsulates an encrypted packet within TCP packet (Tunneling).

5. Send the packet through raw socket to the other router.

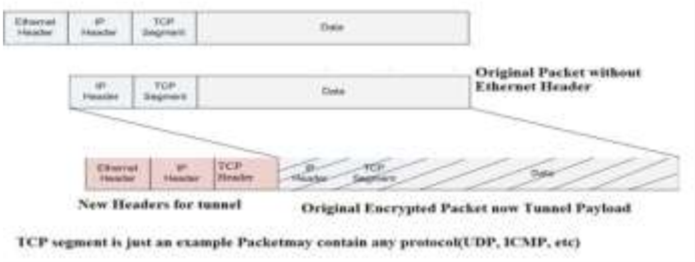

Ethernet Header
IP Header
TCP Segment
Data
IP Header
TCP Segment
Data
Original Packet without Ethernet Header
Ethernet Header
IP Header
TCP Header
IP Header
TCP Segment
Data
New Headers for tunnel
Original Encrypted Packet now Tunnel Payload
TCP segment is just an example Packetmay contain any protocol(UDP, ICMP, etc)

Fig-8 shows the processes of packet in the sending side

5.3.4. Receiving processes:

5.3.4.1. The process of receiving packets:

1. Create a Raw Socket.

2. Set interface you want to sniff on in promiscuous mode.

3. Bind Raw socket to this interface.

4. Receive packets on the socket (All packets received will be complete with all headers and data).

5.3.4.2 Processing received packets:

1. Extract original packet from encapsulating packet.

2. Decrypt the whole packet.

3. Make ARP command with destination IP header exists in original packet to bring the intended recipient MAC.

4. Create Ethernet header with router's MAC as source Ethernet header and intended recipient MAC as destination MACheader.

5. Concatenate Ethernet header with decrypted packet.

5.3.4.3. The process of injecting packet onto network:

1. Create a raw socket.

2. Bind socket to the interface you want to send packets.

3. Send the packet through raw socket to intended recipient.

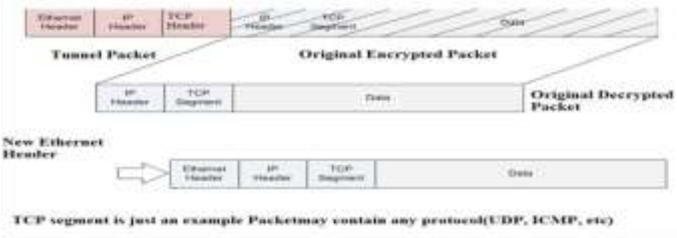


Fig-9 shows the processes of packet in the receiving side.

To Forward packets, two sockets are used, each socket connected to specific NIC by bind function, Where one socket is allocated to receive packets from the NIC that linked it, and passes the packets after processing them through the other socket connected to other NIC which is used to pass packets to receiver, thus Forwarding process have been done in one direction. To make Forwarding in opposite direction, also two sockets are used the same way as was mentioned previously. Making four sockets working in a single program leads to loss of packets and complicate sending and receiving process. Because of this complication and possibility of packets being lost, the program was subdivided into two sub processes each containing two sockets one of them completing the process of reception and processing packets and passes them in to other direction via other socket, as well as the other program make the forwarding in opposite direction, that means each program containing four sockets two for sending and two for receiving.

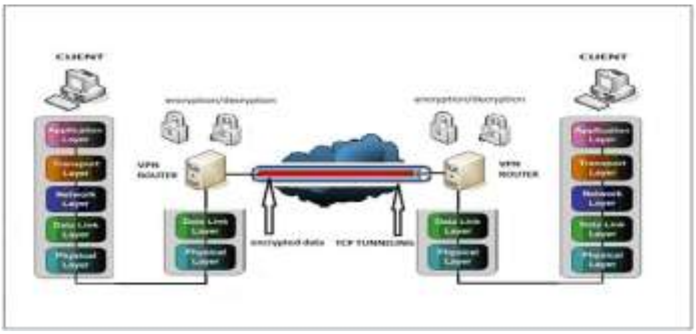


Fig-10 shows the processes of encryption/decryption and tunneling.

6. Results and Recommendations:

6.1 RESULTS:

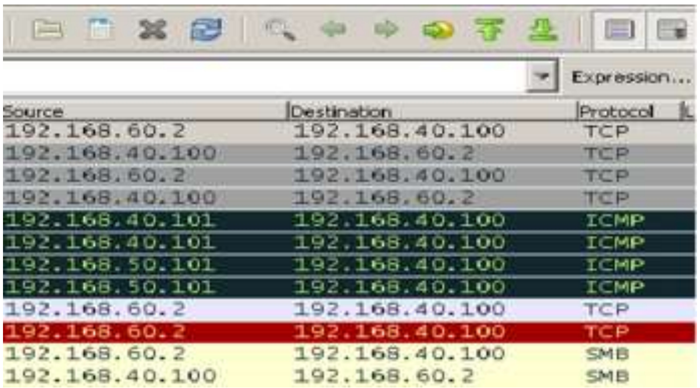
6.2 Tasting the project using wire sharke:

1. Shared folder

2. Web server

3. Remote desktop connecting

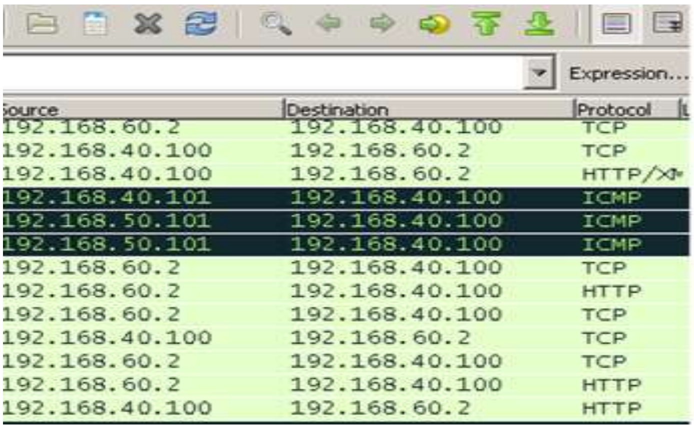
6.3 Connecting to get the shared folder from other network:



Source	Destination	Protocol
192.168.60.2	192.168.40.100	TCP
192.168.40.100	192.168.60.2	TCP
192.168.60.2	192.168.40.100	TCP
192.168.40.100	192.168.60.2	TCP
192.168.40.101	192.168.40.100	ICMP
192.168.40.101	192.168.40.100	ICMP
192.168.50.101	192.168.40.100	ICMP
192.168.50.101	192.168.40.100	ICMP
192.168.60.2	192.168.40.100	TCP
192.168.60.2	192.168.40.100	TCP
192.168.60.2	192.168.40.100	SMB
192.168.40.100	192.168.60.2	SMB

Fig-11 show the connection to get the shared folder

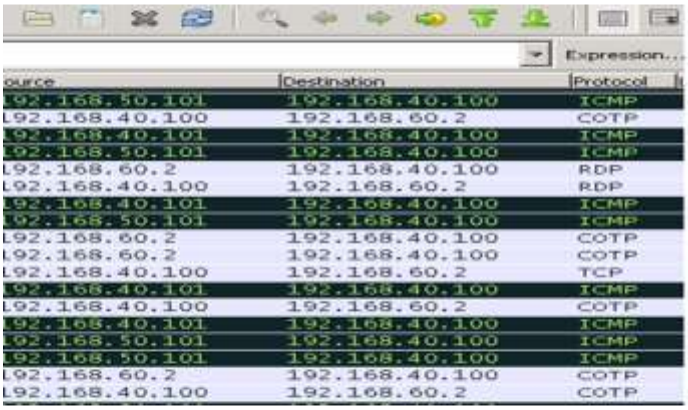
6.4 Connecting to the web server from the other site:



Source	Destination	Protocol
192.168.60.2	192.168.40.100	TCP
192.168.40.100	192.168.60.2	TCP
192.168.40.100	192.168.60.2	HTTP/X
192.168.40.101	192.168.40.100	ICMP
192.168.50.101	192.168.40.100	ICMP
192.168.50.101	192.168.40.100	ICMP
192.168.60.2	192.168.40.100	TCP
192.168.60.2	192.168.40.100	HTTP
192.168.60.2	192.168.40.100	TCP
192.168.40.100	192.168.60.2	TCP
192.168.60.2	192.168.40.100	TCP
192.168.60.2	192.168.40.100	HTTP
192.168.40.100	192.168.60.2	HTTP

Fig-12 show the connecting to the web server from other site

6.5 Remote desktop to the other site:



ource	Destination	Protocol
192.168.50.101	192.168.40.100	ICMP
192.168.40.100	192.168.60.2	COTP
192.168.40.101	192.168.40.100	ICMP
192.168.50.101	192.168.40.100	ICMP
192.168.60.2	192.168.40.100	RDP
192.168.40.100	192.168.60.2	RDP
192.168.40.101	192.168.40.100	ICMP
192.168.50.101	192.168.40.100	ICMP
192.168.60.2	192.168.40.100	COTP
192.168.60.2	192.168.40.100	COTP
192.168.40.100	192.168.60.2	TCP
192.168.40.101	192.168.40.100	ICMP
192.168.40.100	192.168.60.2	COTP
192.168.40.101	192.168.40.100	ICMP
192.168.50.101	192.168.40.100	ICMP
192.168.50.101	192.168.40.100	ICMP
192.168.60.2	192.168.40.100	COTP
192.168.40.100	192.168.60.2	COTP

Fig-13 show the remote desktop connecting

7. Recommendations:

To make this system more reliable and provide Attractive services we recommend doing some tasks we didn't achieve:

1. Development the system to run on IPV6.
2. Use real-time adaptive link compression and traffic-shaping to manage link bandwidth utilization.
3. Modify security model to protect against passive attacks.
4. Using software encryption instead of using the existing encryption software in the OpenSSL library and check.
5. Using software encryption instead of using the existing encryption software in the OpenSSL library and check. It first to make sure they are free of gaps and to ensure high degree of confidentiality and security .elaborate study of the time needed to break the encryption algorithm is done.
6. Select different algorithms for encryption.

REFERENCES

[1] Cisco, “Reference Guide A Primer for Implementing a Cisco Virtual Private Network” (Posted 28/8/2000) http://www.cisco.com/warp/public/cc/so/neso/vpn/vpne/vpn21_rg,htm

[2] Microsoft Corporation, White Paper – “Virtual Private Networking (VPN) Security” (Posted 5/01/1999) http://www.microsoft.com/NTServer/commserv/deployment/planguides/VPNSecurity.asp

[3] Microsoft Corporation, White Paper – “An Overview Virtual Private Networking” (Posted 25/6/1998) http://msdn.microsoft.com/workshop/server/feature/vpnovw.asp

[4] Check Point, “Refining the Virtual Private Network” (May 1999) http://www.checkpoint.com/products/vpn1/vpndef.html

[5] Professor Raj Jain, “Class lecture on Virtual Private Network”(23/2/01) http://www.cis.ohio-state.edu/~jain/cis788-99/h_7vpn.htm

[6] T.Bird, P.Clark, D.Farmer, S.Goldhaber, B.Hotte, E.Johnson, I.Khalil, M.Petrovic, L.Phifer, T.Weil, “VPN Information on the World Wide Web”(25/2/01) http://kubarb.phsx.ukans.edu/~tbird/vpn.html

[7] Stallion Technologies, “What is Internet-based Virtual Private Networking?” (25/2/01) http://www.stallion.com/html/solutions/vpn-overview.html

BIOGRAPHIES

Nagi Ishag Mohammed

Received the M.Sc. degree in computer science from University of Gezira in 2007 and Ph.D. in computer science from National Ribat University in 2017 respectively. He stayed in Mashreq University and University of Science and Technology as teacher of computer science from 2004 until now.

Nadia ElFadil Hamid

Received the B.Sc. degree in computer science from Al Neelain University in 2000 and M.Sc. in computer science from University of Gezira in 2006 respectively. She stayed in Al Neelain University and Omdurman Ahlia University as teacher of computer science from 2000 until now.