ACADEMICIA: An International Multidisciplinary Research Journal
ISSN: 2249-7137 Vol. 12, Issue 04, April 2022 SJIF 2022 = 8.252
A peer reviewed journal

VPN: PROBLEM RELATES WITH SECURITY OF DATA IN TUNNELING PROCESS AND REQUIREMENTS

Anubha Gaur*

*Research Scholar,
Suresh gyan Vihar University, Jaipur, INDIA
gaur.anubha@yahoo.com

DOI: 10.5958/2249-7137.2022.00356.1

ABSTRACT

VPN is a private network that provides inter-connectivity to exchange information among various entities that supports a forum of authorized users and allows them to access various network-related services. A Virtual Private Network (VPN) is the expansion of a private network that makes links for sharing or public networks like the Internet. A VPN enables a user to send data between two computers with in a network. This paper involves various issues of transferring data protocols on which a vpn depends and the infrastructure uses the tunneling process. Also underline the problems of data transferring through the tunneling process. this paper also proposed an encryption algorithm for the data security.

KEYWORDS: *VPN, Tunneling, Protocols, DES, PAP, GRE*

INTRODUCTION:

Tunneling process:

Tunneling is the process of using an internet work infrastructure for transferring data for one network over another. The data is to be transferred in the forms of frames (or packets) of another Protocol. The tunneling protocol encapsulates the packets in an additional header and it does not send the frame which it is produced by an originating node. The additional header is required for

Providing the routing information to the encapsulated payload to pass through the intermediate

Internet. Then the encapsulated packets go through between endpoints of tunnel over the internet work. This Logical path on which the encapsulated packets travel over the internet work is called a" Tunnel". When these encapsulated packets reach the destination, they are decapsulated to get the Original data. Tunneling includes the entire process encapsulation, transmission, and Encapsulation of packets.[2]

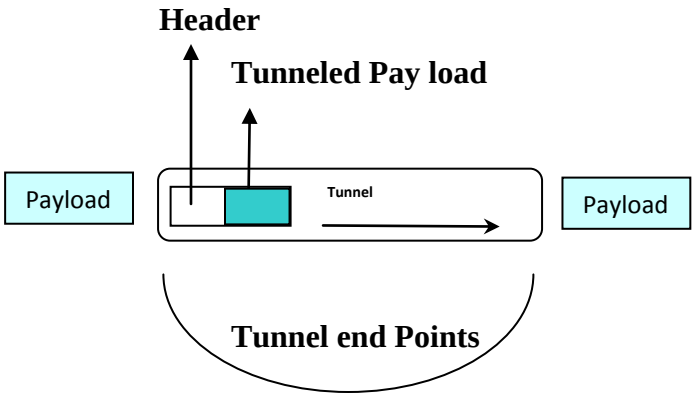


Fig-1

Security of data in tunneling process:

Generally two modes for tunneling and they are being measured by three parameters: a Security Parameter Index (SPI), security protocol Identifier and destination IP address.

The destination IP address is the IP address of the tunnel endpoint destination. The Security Parameter Index is a 32-bit number which is chosen by the tunnel endpoint destination and it has local significance only within that destination endpoint [3]. The Security protocol identifier is the protocol number for either AH (51) or ESP (50) [4].

The two modes for operating a tunnel process: (a) Transport mode and (b) Tunnel mode.

Transport mode is designed for protecting the higher-layer protocols (e.g., TCP and UDP). In tunnel mode, an IP packet becomes the payload for another IP packet. This IP packet allows the inner IP packet which has its IP header, and it relates for the encryption or other security measures, while the outer IP packet provides the data through the network. Mostly security gateways provide only tunnel mode operation, while hosts can provide both modes (tunnel and transport)

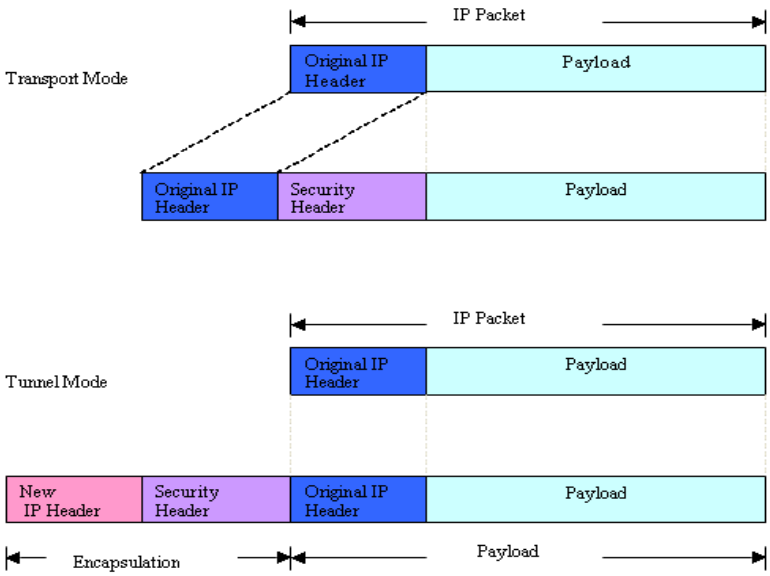


Figure:2 Transport Mode and Tunnel Mode

Various issues for the data security in tunnel process:

The data which is transferring should be safe and secure but numerous problems occur s some are as follows:

Token Card Support: At layer 2 Tunneling protocol like Extensible Authentication Protocol (EAP) hold up various methods of authentication such as one-time

Passwords, cryptographic calculators, and smart cards.[4] Layer 3 IPSec uses popular methods of

Public key certificate authentication which secure data.

Encryption of data using various algorithms:

Layer 2 tunneling protocols support data encryption Mechanisms which is based on PPP methods.

RSA/RC4 algorithm is used for encryption. Layer 3 tunneling protocols can use similar methods like, IPSec. It uses generally, DES, 3DES, Blowfish, RC5 algorithms for encryption.

Key generate Management: AT Layer 2 initial key generate while transferring data which is usually relies on user authentication. IPSec generate a common key during the IKE exchange, and timely its refresh.

Authentication of the data at user level:

Various Tunneling protocols at level 2 and level 3 apply authentications schemes.

Layer 2 which is corresponds to data link layer, tunneling protocols uses the user authentication schemes which use frames using EAP method. Many Layer 3 which is corresponds to the Network layer & use packets; tunneling schemes generally uses that the tunneled endpoints are identified and authenticated before the tunnel is established and it encapsulate the data.

OBJECTIVES OF THE STUDY:

1. To study the security issues related to the tunneling.

2. To identify the problems of data security.

- To analyze the security technique in tunneling.

- To study about the tunneling process.

- To know whether these techniques are secure or not.

REVIEW OF LITERATURE:

Authentication means certification of accessing data. VPN connection uses the same authentication Mechanisms like PPP connections, such as:

□ □ Extensible Authentication Protocol (EAP)

□ □ Challenge Handshake Protocol (CHAP)

□ □ Shiva Password Authentication Protocol (SPAP), and

□ □ Password Authentication Protocol (PAP)

Generic Routing Encapsulation (GRE):

The GRE Protocol that is Generic Routing Encapsulation is used for encapsulation of data on one network layer protocol over another network layer protocol. for the security purpose the payload in the tunneling is first encapsulated in a GRE packet, which has possibly includes the route. Then Resulting GRE packet encapsulated in some other protocol and then forwarded. In this way the data is secure and it decrypted at another end so the authencity is maintained.

Password Authentication Protocol (PAP):

Password Authentication Protocol (PAP) provides a method for 2 Way communication handshake methods for establishing its identity. This is one of the best methods of user authentication.

Types of Tunneling:

Tunnels can be created in various ways:

1 NAS-initiated tunneling:

NAS-initiated tunneling is also referred to as compulsory tunneling, which enables users to dial to Network Access Servers, for establishment a tunnel to the server. The connection is in between the client of the user and the NAS establishes but this connection is not encrypted.

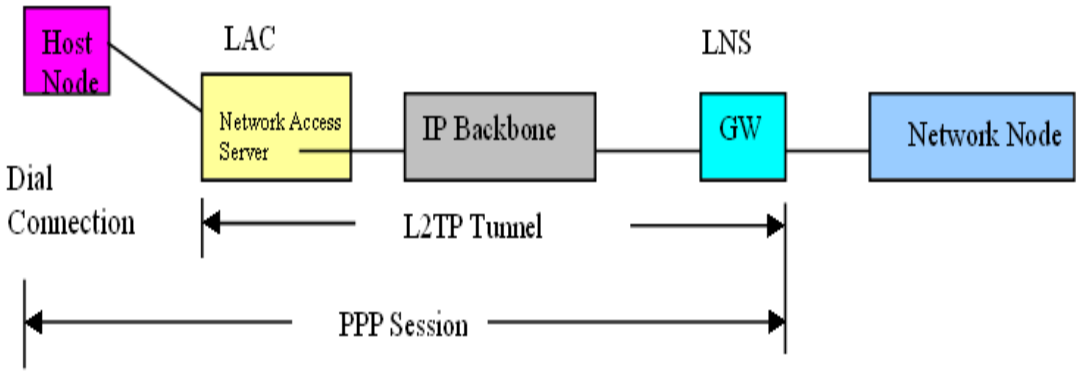


Figure: 3: Compulsory Tunneling

2. Client-initiated tunneling:

Client-initiated tunneling is also referred to as voluntary tunneling which enables clients to build up and establish encrypted tunnels to tunnel servers. It does not any intermediate NAS.

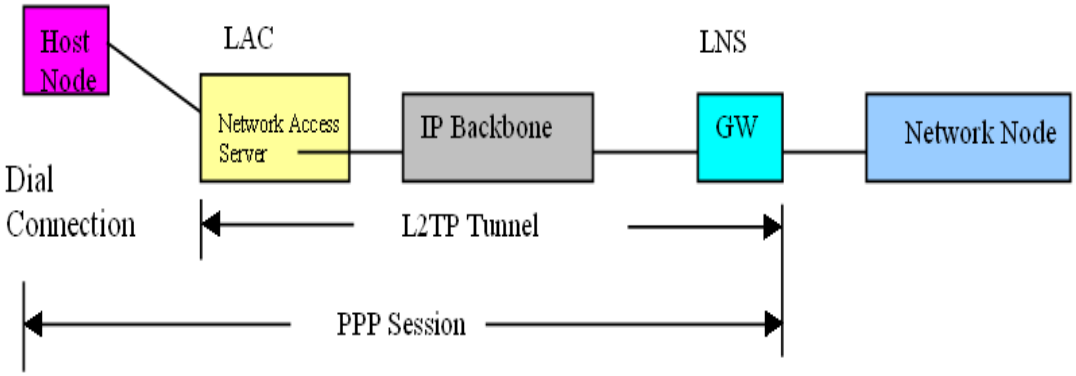


Figure: 4: Voluntary Tunneling

Note: All reference are given below

RESEARCH METHODOLOGY:

MPLS method is used to measure the availability of data transfer on client-server end. The data is being transferred on vpn network through tunneling process. While applying this method of cryptography, the data transfer rate is much better than earlier. An algorithm has following set of rules for encryption and decryption.

Cryptography	Means hiding data that can be transfer in the secret form can also be store and which is available only to the authenticated users.
Cryptosystem	It is the way of implementing cryptography .it can be hardware and software. It transforms a message to cipher text and back to plaintext
Cryptanalysis	It is the way of converting ciper text into plain text without any secret key or Breaking the encryption
Cryptology	It includes the study of both cryptography and cryptanalysis
Cipher text	it is the data in encrypted format or unreadable format
Encipher	it is the way of transforming data into an unreadable format
Decipher	it is the way of transforming data into a readable format
Plaintext	It is readable format of data, it is also referred to as clear text
Work factor	it is the Estimated time, effort, and resources necessary to break a cryptosystem

TABLE: SHOWING TERMINOLOGY OF CRYPTOGRAPHY

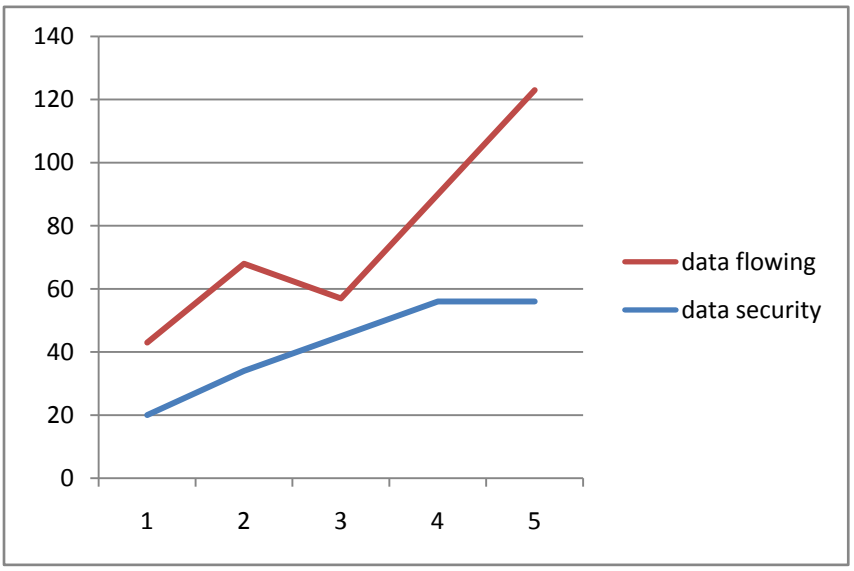
This algorithm is a probabilistic algorithm which doesn't take any input, and produces a four output (a, b c, d), where

(i) B is a positive integer such that vfxz(b, (p − 1)(q − 1)(r-1)) = value, and

(ii) A is an integer that is the product of three primes p,r,q of similar length, with p 3= q,

(iii) c is a positive integer such that a.b. d _ 1 (mod _(n)), where _(a) is the least common Multiple of (p − 1),(r-1),and (q − 1).

The algorithm produce such output that fulfill most of the condition and the graph is given for this algorithm.. The output distribution of key generation algorithm depends on the particular algorithm.



Graph: showing output of the algorithm

CONCLUSION AND FUTURE SCOPE:

On the basis of above algorithm we can conclude that all the protocols can justify but still there can be some problems along with it for the data security. It still needs some requirements and in next paper we will conclude algorithm with some more changes.

Security issues	LAYER 2 PROTOCOL	LAYER 3 PROTOCOL
RELAIBILTY	YES	YES
KEY MANAGEMENT	LESS	MUCH SECURE
ENCRYPTION	YES	YES
AGAINST ATTACKS	CAN PROTECT	YES

TABLE 1: COMPARISON OF VPN PROTOCOLS FOR SECURITY ISSUES

REFERENCES:

1. R. Boutaba, W. Ng., A. Leon-Garcia, Web-based Customer Management of VPNs, Journal of Network and Systems Management.
2. Davey, B. et al. IETF RFC3246: An Expedited Forwarding PHB. March 2002
3. Heinanen, J. et al. IETF RFC2597: Assured Forwarding PHB Group. June 1999
4. http://dmoz.org/Science/Math/Applications/Communication_Theory/Cryptography/Historical
5. D. Harkins and D. Carrel. The Internet Key Exchange (IKE). RFC 2409 (Proposed Standard), Nov. 1998.
6. S. Kent and R. Atkinson. IP authentication header. RFC 2402 (Proposed Standard), Nov. 1998.
7. S. Kent and R. Atkinson. IP encapsulating security payload. RFC 2406 (Proposed Standard), Nov. 1998.
8. S. Kent and R. Atkinson. Security architecture for the internet protocol. RFC 2401 (Proposed Standard), Nov. 1998.