ISSN No: - 2456- 2165

A Review :- External Authentication Approach For Virtual Private Network

Ravi Kumar Jain
M.Tech Scholar
Computer Science
Government engineering college Ajmer
ravirahul1988@gmail.com

Prakriti Trivedi
Assistant Professor
Computer science Engineering
Government engineering college Ajmer
niyuvidu@rediffmail.com

Abstract:- The OSI model is implemented for protection & security of crucial information to be accessed by hackers in the transmission process. The OSI model applies a security system like IPSec (Internet Protocol Security) incorporated in network layer & SSL (Socket Secured Layer) in transport layer. The PPTP (Point to Point Tunneling Protocol) is implemented in data link layer to develop a tunnel that is secured for exchange of data is a one way transmission and is termed as VPN (Virtual Private Network). A highly strengthened method for authentication is applied for improvising the reliability & security of VPN apart from conventional username & password technique [1]. In the last document [15] we try to suggest some procedures for producing a process of authentication that is covered in two steps in the PPTP VPN that is also termed as External Database Authentication. The main advantage of this technique is that data related to user is accumulated in a précised authentication server that is comprised of a large place or organized, structurized user data through the high level of robustness & security. So this method suggests in the elaboration to the functionality of LDAP (Lightweight Directory Access Protocol) server that is hosted in over LAN of an organization, for strengthening of process of authentication of PPTP VPN. In this document, a system of OSSEC is suggested for minimizing the time of decryption & encryption in the VPN network.

I. INTRODUCTION

Gaining remote control access is highly demanded by the persons such as directors, businessman etc. who are continuously over travelling but want to remain in contact with their organization all of the time with updated information & monitoring them in a personal network from remote areas. The security concerns must be fulfilled as it may comprise of some important data. a famous technique for achieving such goals is referred as VPN. A private network is elaborated through the public network like Internet through VPN [2]. It allows sharing the information in a public network just like they are linked to it directly. Some generally applied VPN techniques are comprised of PPTP, that functions over on port TCP 1723 [3], L2TP (Layer 2 Tunneling Protocol), SSL (Secure Socket Layer), IPSec (Internet Protocol Security). Various open source & commercial products of VPN are provided in the market with variation in their features [4]. Even, a hard effort is put over for standardization of VPNs; none of the relied technologies of VPN are counted under standards of IETF till now [5]. The initial process for establishment of a VPN connection is authentication. This process helps in determining if the user has the authorization or not. The method is followed with the login usernames & passwords in public & private computers even over the internet [6]. If the password is known, it assures that user is valid. The process of registration is completed by user itself by an allocated or self-depicted password. The user should be aware of the passwords on every use. Client must prove himself authenticated for using the services of VPN over its server. There are two techniques in which the process of authentication is completed over VPN server. It is done by either making use of credentials with the database stored locally for the users that it will be retaining (Internal Authentication) or applying the services of a précised authentication server i.e. External Authentication. The way of authentication is selected by VPN server that is not provided to client.

The authentication is considered to be a cardinal aspect for security purpose in VPN, it is highly recommended to provide strength to it as it is a two step process. Hence, in spite of a VPN server performing the VPN authentication, it is considered to be better having a précised third party authentication server that is accumulated in similar LAN structure that has the whole responsibility of accumulating the data about user in a structurized format & doing authentication in contrast to the user data.

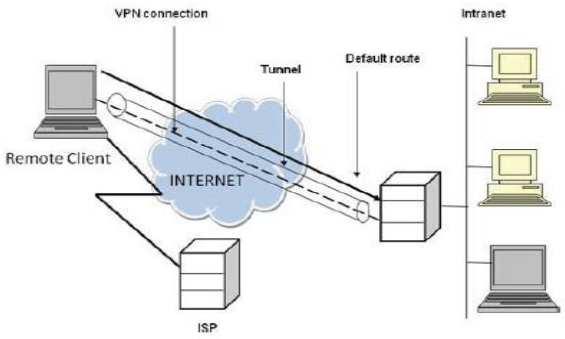

Fig.1. Remote access VPN

ISSN No: - 2456- 2165

It has some advantages like PPTP is having over VPNs even though it has some confusing problems. It can be easily accessed through VPN technique. There is no need of any certificates of computer or public key design & can be configured very easily. Even though the suggested LDAP technique is applied as a conjunction long the PPTP, it can be elaborated towards other VPNs like L2TP. A précised authentication server gives hierarchy & structure of user that can eliminate the redundancy arising because of users having similar username. Eventually it adds up some more life to the user credentials that leads to invalid login state if any attempt is done to authenticate as the time of expiration is over. The figure 1 presents the structure of linking remote client to the main branch by the internet that incorporates VPN for transmission of information in a secured manner. All of the resources of intranet can be elaborated to employees as the technique of VPN is included in an organization or their living places by making use of tunneling method in between VPN client & server.

II. RELATED WORK

An explanation was provided by Akhtar, Salim & Qadir [7] for the application of LDAP services over VPN authentication in maintenance of an instance of the entries by user in directory from where multiple clients can be authenticated rather than maintaining various copies on VPN server. By evaluating the performance of LDAP protocol mainly for the 'search ability' [8]. As per the outcomes, even the scenario of worst case performance i.e.no cache for query operation (i.e. total server search latency) is less than 8 seconds, over a shared hardware platform, that is low than the default time out of 30 seconds for major VPN protocols for authentication like CHAP. So,, there is some assurance about the assumptions made by us for using such kind of functions in the authentication process of VPN that don't generate the problems like hanging the VPN session. The present authentication process support provided externally as like the ones linked up with Active Directory authentication don't treat this issue like a 'join' function (VPN server is linked to external server) may consume more time than a minute. Though there is a requirement of proving the above provided generalization to be true in contrast on the basis of performance where as intense experiments are conducted incorporating several erroneous circumstances like hanging of server, disruption in network on the medium level of protocol. The [9] also goes in favor to the provided concept and reveals that LDAP server is not the fine solution that can be implemented as authentication process in the real-time communication systems (i.e. VPN to be considered here). The main concern is over providing support to various users as in the scenario of video conferencing. By making use of a main LDAP server for the process of authenticating application, it is more practically implemented rather than incorporating a separate authentication module in every application [10]. This online document 'Poptop MSCHAP2 ADS How-to' presents that for a VPN server that can be applied for using the services of an Active Directory server for the authentication process, it should be able to linked to latter. This mechanism has two issues [11]:

1. There is need to produce machine account for each of the VPN server with which it has to follow the process of communication.
2. Real authentication process will be executed by external server but not by VPN. Such issues can be eliminated by applying a basic LDAP service.

III. AUTHENTICATION SERVICE FRAMEWORK

These days many of the bigger organizations retain their data in a structure like a directory. Hence it is advisable to not produce the copy of similar data over a VPN server. But, it is able to directly communicate with external server in order to make contrast over credentials of client to the accumulated data. The figure 2 explains the process of authentication in two steps:

1. In between gateway server & user – The remote client transmits the data in encrypted form (MSCHAP/MSCHAPv2).

2. In between active directory server & gateway server – the received data is sent directly.

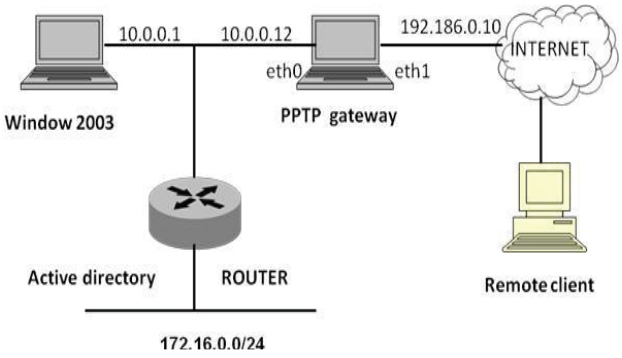

Fig.2. VPN server communication with Active Directory server

IV. PROBLEM STATEMENT

LDAP is considered to be as authentication protocol that is independent of platform & is applied externally. More number of users can go for it as they go through open source technique for a secured CPN connection. They are able to make selection of an encryption technology for authentication purpose & it is suggested for eliminating the dependency of real authentication that works over the external server that leads to minimization of selecting authentication protocol if the CHAP & PAP protocol are not provided for service based over window based directory. Hence, the process of authentication constituted over LDAP improvises the efficiency, security & robustness. Though, it also enhances the strength of authentication criteria, it is believed that security can be

ISSN No: - 2456- 2165

refurbished by improvising the communication process of server & client & selecting the string encryption & authentication protocol. As an illustration, vulnerability to some sort of attacks like replay attacks is the same in contrast to present authentication methodologies as no change is observed in the process of communication going on between the two of the VPN entries. Further, the technology presented for PPTP VPN can be elaborated to other technologies of VPN like L2TP & IPSec. It helps in securing the process of VPN to some more extent, trustworthy & robust. The protocol of LDAP works fine for decryption & encryption of user information. But there is some problem with time of decrypting & encryption in this protocol. In the last paper [15] the time of decryption & encryption was too large. It can be minimized for VPN by suggested technology.

V. PROPOSED METHODLOGY

A VPN network constituted over OSSEC is applied for minimizing the time for encryption & decryption of the network. OSSEC can help in achieving this ability. OSSEC is also referred as HIDS (host based intrusion detection system) that is a multiplatform, scalable & open source platform that works for host side. It is highly efficient associating & assessment technique that works for monitoring of window registry, centralized policy enforcement, incorporating log assessments, reorganization of root kit, checking for veracity in file, alerting in real time scenario & active reaction. It supports all major platforms like FreeBSD, Open BSD Linux, Mac OS, Windows & Solaris. OSSEC is comprised of various parts. There is a central manager provided that looks after all the things, taking data from databases, agents, system logs & devices that are agent free. The given image presents the main manager that is taking events from logs of other agents & devices remotely connected to it. If some activity is observed, execution of active responses takes place & notification is given to the admin.

Fig.3:- Architecture of OSSEC

The methodology of OSSEC HIDS is implemented as it helps in making the assessments as explained but also present various guidelines for several log formats, that makes the links more simplified. Two techniques are presented here for implementing the OSSEC.

- Local (as a single system is provided for monitoring the activities).
- Client or Server for centralized assessment.

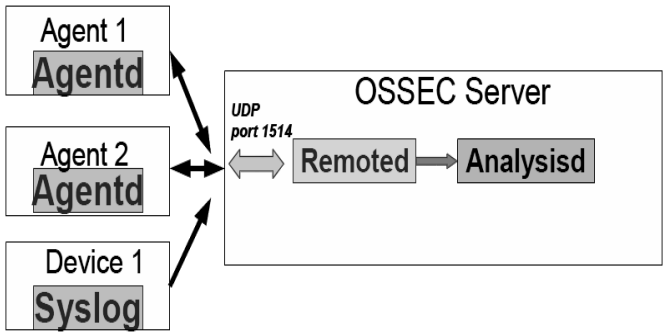

Fig 4:- Agent/Server Network Communication

VI. CONCLUSION

In this document, a technique of OSSEC server is provided for minimizing the time of encryption & decryption of VPN. OSSEC is needed for individual installations & distributed networks. The Solaris, Mac & Linux environments work fine over this technique. The performance efficiency of OSSEC & LDAP for VPN encryption & decryption technique is explained.

References

[1] Pham Ngoc Thanh, Keecheon Kim,Implementation of Open Two-Factor Authentication Service applied to Virtual Private Network, 978-1-4673- 5742- 5/13/$31.00 ©2013 IEEE.
[2] [Online]Available:http://en.wikipedia.org/wiki/Virtual_private_net work
[3] K. Hamzeh,G. Pall, W. Verthein, J. Taarud, W. Little, G. Zorn,"point to point tunneling protocol".RFC2637(July 1999).
[4] Shashank Khanvilkar and Ashfaq Khokhar, Virtual Private Networks: An Overview with Performance Evaluation**, 0163-**6804/04/$20.00 © 2004 IEEE.
[5] [Online]Available:http://www.vpnc.org/vpn-standards.html.
[6] [Online]Available:http://en.wikipedia.org/wiki/Authentication.
[7] Qadir, Salim and Akhtar,'Profile Management and Authentication using LDAP'.
[8] Xin Wang, Schulzrinne, Henning, Kandlur, Verma, 'Measurement

and Analysis of LDAP Performance'.
[9] Ahmad, Abu Saleh, 'Centralized Authentication and Speed up Approach for Clients of Multiple Multimedia Conferencing Systems Using Lightweight Directory Access Protocol'.
[10] Eli B. Cohen, 'Issues in Informing Science and Information\ Technology'.
[11]
[Online]Available:http://www.members.optushome.com.au/~wskwok/p optop_ads_howto_1.htm.
[12] M. Wahl, H. Alvestrand, J. Hodges, R. Morgan,"authentication methods for LDAP", RFC 2829 (May2000).
[13] J.Sermersheim,"lightweight directory access protocol", RFC 4511(June 2006).
[14] K. Zeilenga, Ed.," Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map".RFC 4510 (June 2006).
[15] Anupriya Shrivastava , M A Rizvi , " External Authentication Approach for Virtual Private Network using LDAP", *First International Conference on Networks & Soft Computing 2014*