Volume 1 , Issue 6 , September – 2016 International Journal of Innovative Science and Research Technology

ISSN No: - 2456- 2165

A Review for VPN and VPN Service Provider

Manoj Kumar Jangid
M.Tech Scholar
Information Technology
Government engineering college, Ajmer
mkjangir17@gmail.com

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

Abstract:- Virtual Private Network(VPN) is using for setup the communication in between two person at the public network. In VPN data transmission will be securely by use cryptographic algorithm and protocol., VPNs provide security services such as confidentiality, host authentication and data integrity. In this paper , we give the review for the VPN (Virtual Private Network) .

***Keywords**: VPN, Linux, Intranet, One-way delay, Throughput.*

I. INTRODUCTION

In the enterprise type of network environment, the internet and internet connection both are required. The internet connection gets expensive by the provided leased lines and frame relay trunks. For some cases, internet connection providing companies give the dial-up connection. In the dial-up connection, the speed of the internet is limit up to 53/48 KBPS. Due to high requirement of internet connection, access drive needs the internet from multiple sites. An IP-based Virtual Private Network provides the solution for the multi-user problem. Recently internet connection services providing is much easy and cheap as compare to communication lines setup and internet connection distribution. For select the VPN, there is wide range VPN are available from expensive to inexpensive. For choosing the VPN, we have to do the careful analysis so that good VPN can be selected. Secure remote access over public high-speed communication lines can help to reduce the need for costly private point-to-point telecommunication services. This secure “tunnel” communication between different sites of an organization is essential to cost effective operations of any enterprise. Recently, a trade report and study show the growing demand for VPNs as Information Technology (IT) departments are continually charged with the task of creating a secure and robust network infrastructure. A Gartner report predicts [1] that VPNs will be implemented by more than 80 percent of enterprises by the year 2007, as a form of network access control.

There is a wide variety of choices for VPN implementations, from expensive hardware devices to inexpensive open source software that can be implemented with a minimal hardware cost. Implementing the wrong type of VPN has the potential to render the inherent cost savings useless [3]. Careful analysis must be performed to determine the best type of VPN that is appropriate for enterprise implementation. This is a difficult task, since there are few independent, concrete statistics on VPN efficiency. Many vendors are reluctant to publish exact efficiency statistics for their products. This is due in part to the wide variability of VPN encryption methods, hardware implementations, and supporting infrastructures. We mention two types of methods for VPN tunneling

A. Point to Point Tunneling Protocol (PPTP, RFC263)

This kind of protocol will support to the Windows type of servers environment. It is also widely available PPTP type of tunneling protocol which is not an IETF standard. The PPTP encryption process is considered as weak encryption mechanism.

B. Layer 2 Tunnel Protocol (L2TP, RFC2661)

L2TP is an IFTP based standard protocol. It will provide Layer -2 tunnel over the IP network. L2TP protocol does not contain any encryption protocol to protect the data. It relies on IPsec to encrypt the data which is sent through the tunnel. In the protocols, IPsec/L2TP is considered as a more secure from the comparison of PPTP protocol. We select the IPsec-based VPN to protect the data.

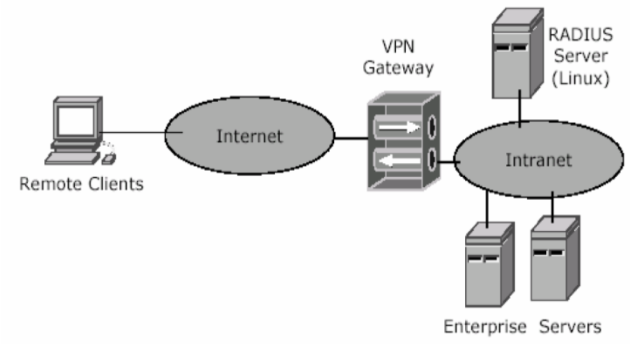

Figure 1. Client-to-Gateway VPN Configuration

IPSec provides two encryption schemes:

- Authentication Header (AH, RFC2402)
- Encapsulating Security Payload (ESP, RFC2406)

Most IPSec implementations are based on ESP as it is considered more secure than AH. The experimental data presented in this paper is based on ESP. There are two VPN configurations for the enterprise environment

- Client-to-Gateway VPN
- Gateway-to-Gateway VPN.

In a client-to gateway VPN, mobile workers and telecommuters can access secure information on the company's intranet over the public Internet as illustrated in Figure 1. The RADIUS server provides the AAA (authentication, authorization, and accounting) function to support remote clients.

The gateway-to-gateway VPN configuration is used between headquarters and remote branch offices or between branch offices. This connection is traditionally provisioned via leased lines, frame relay, ATM, ISDN, or dial-up where they are either too expense or too slow to be effective. If the connection is across multiple countries, it will not only be very expensive but also requires a long waiting time. For example, an office in Chicago needing to communicate proprietary information with a branch office in Brazil would not be able to easily communicate via a completely independent and private network. Establishing a tunnel VPN is an ideal solution to this problem as illustrated in Figure 2.

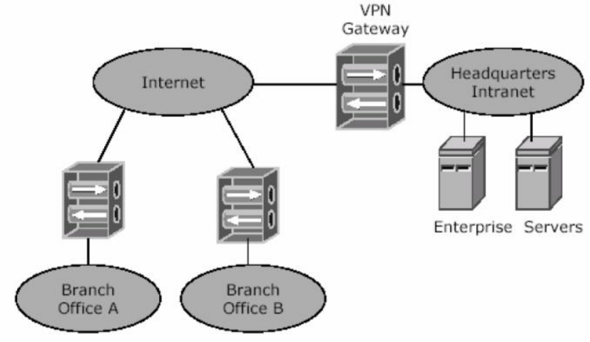

Figure 2. Gateway-to-Gateway VPN Configuration

The VPN tunnel is transparent to clients on private IP subnets, and there is no need for user authentication by the VPN gateways. The VPN gateways share a secret among themselves as the mechanism for authentication and data encryption. As previously mentioned, this type of VPN is commonly used to send private, encrypted information over a public internet telecommunications line.

II. LITERATURE REVIEW

In 2000 John P. McGregor[et.al] presented a paper for VPN(Virtual Private Network) which connect two or more than two different clients to communicate securely over the network. For the securely communication cryptographic method is using so that VPN can provide the secure connection over the network. In this paper, They characterize the extent to which data compression can alleviate this performance degradation. More specifically, They study the performance obtained when combining the IP Payload Compression Protocol (IPComp) with the IP Security Protocol (IPsec). They evaluate performance using 3 system models; each of these models consists of some or all of the computation and transmission operations required to support VPN transactions. Using speedup equations that describe the performance impact of compression in the system models, They derive inequalities that specify the conditions required for data compression to improve performance. They also gather and analyze empirical performance results by simulating packet transmission over several network types and by timing the execution of IPComp and IPsec procedures on a 367 MHz HP PA-8500 processor. The results indicate that the performance depends on the compressibility of the payload data, on the throughput of the cryptographic and compression algorithms, and on the network speed. They find that compression usually improves performance when using 10 Mbps or slower networks, but compression only improves performance in systems with 100 Mbps or 1 Gbps networks when encryption is being used.

In 2007 Peter Dulany[et.al] presented a paper for the IPsec-based Virtual Private Network(VPN) of the gateway to gateway configuration. Due to high requirement of the internet , customer required the secure and fast internet connection and cost effective also. So these type of connection is reviewed by frame relay trunk and expensive leased lines .In this paper, they present a software-based secured VPN for providing the fast internet connection. These type of VPN are built on Linux operating system and provide secure and high traffic secure network connection. They conducted many experiments to emulate different traffic and presented the results of ICMP traffic over Gigabit Ethernet. Our study demonstrated the feasibility of the proposed solution and the performance results show significant overhead of a software-based VPN solution. Directions of further research to expand the work scope and to improve the performance are also presented in this paper.

The experiment shows that VPN traffic requires a significant amount of processing overhead. There is a need to study methods of reducing the overhead of an encrypted VPN tunnel. Future work could include comparing these results to a Cisco-based VPN solution (with a VPN accelerated card), to see if performance is improved in a proprietary, hardware-based implementation. A recent study [2] measured packet loss, jitter, and latency of the VPN but did not measure total throughput. In addition, that study utilized several different types of data (ICMP, FTP, HTTP, voice and video traffic) while ours only used one – ICMP traffic.

In 2016 R.Manikandan[et.al] presented a paper for wireless communication, which creates the interaction in between machine and human. In the 4G LTE and for all type of mobile communication, they all are based on IPV6 compatibility. It provides the reliable connection with high security. In this paper, they confirm that mobile VPN (Virtual Private Network) can be used for secure interconnection. Mobile VPN is using for transmitting the voice securely over the LTE network. The performance of the VPN over 4G LTE network is improved when compared with the 3G network. The metrics to be measured are Throughput, delay, packet delivery ratio. Throughput of the VPN over 4G LTE network is increased by 67% , The delay is reduced by 36% and also packet delivery ratio is improved by 54%.

In 2006 Ravi S.Ravindran[et.al] presented a paper for VPN so that it can provide the most demanding and revenue generating service. In this paper, they are providing the solution for problem of the bandwidth service providing on demand of IP/MPLS network. They propose a managed VPN architecture for such a service highlighting the novelty in our architecture. They concentrate on an important aspect of service definition called the topology abstraction service and define a new problem called the VPN core capacity sharing problem that arises in this context. They propose three schemes to solve this problem borrowing from results from graph theory. As part of our simulation study, They evaluate each of these strategies with different call arrival scenarios and present the results.

In this paper, they proposed a dynamic managed VPN service and noted its differences from the traditional VPN definitions. An architecture as an extension to the existing IP-VPN solution was proposed. They then defined the core capacity sharing problem in a dynamic managed VPN service context. As a way to solve this problem They proposed three heuristics. The maximum capacity abstraction, which is an aggressive way to sharing resource, has satisfying Success ratio, but its Crankback ratio is almost twice those of the other two schemes. Mixed Bound approach tries to address the drawbacks of the maximum capacity scheme by defining a virtual upper bound and lower bound for the bandwidth that can be requested from the VSP. This scheme was the most conservative of the three schemes with poor Success Ratio and high algorithm complexity. The third scheme They proposed uses Tree Graphs, using Steiner trees as a way to virtualized capacity applying a method to minimize overlap of the trees that were later used to generate abstract topologies. This scheme also faired better in all the four performance metrics in comparison to the other proposed schemes.

In 2010 Ravishankar Ravindran[et.al] presented a paper for sharing the VPN services provider and link stak information along with VPN. It will use as a principal of topology abbreviation . In this paper, they deal for generating topology abstraction in a centralized manner. In this context we define a problem called the VPN core capacity sharing problem. We study this problem using algorithms based on multi-commodity flow theory. We observe from simulation analysis over several topologies that applying the maximum multi-commodity flow based partitioning scheme improves the call performance and network utilization statistics compared to a previously proposed topology abstraction scheme based on maximum concurrent flow theory.

In 2005 Ravi S. Ravindran[et.al] presented a paper for VPN which is managing g the service and provided the more requirable and demanding service for the customer. Some common managed VPN services are auto-discovery, security and potential ability for performing demanding signal. This paper focus on a major problem of VPN customer that is topology dissemination for Dynamic Bandwidth services. Topology dissemination can easily be translated into a VPN service. In this regard we define this service and its associated SLA. Further we elaborate on four basic QoS enabled topology abstraction services: fully meshed, source rooted star, star, and simple node. The paper also describes a generic framework to generate these abstractions and presents simulation results comparing performance of each of these schemes.

In 2010 He Yan[et.al] presented a paper for network IP. Network IP is very wide and large field for the internet based applications like internet games, streaming videos, e-commerce and online banking. The transformation is required in network management in which they cover the detection of the faulty network elements and manage the service of quality. In this paper, they proposed a Generic Root Cause Analysis Platform(G-RCA) for service quality management in a big IP network. GRCA contains a comprehensive service dependency model that includes network topological and cross-layer relationships, protocol interactions, and control plane dependencies. G-RCA abstracts the RCA process into signature identification for symptom and diagnostic events, temporal and spatial event correlation, and reasoning and inference logic. GRCA provides a flexible rule specification language that allows operators to quickly customize G-RCA into different RCA tools as new problems need to be investigated. G-RCA is also integrated with the data trending, manual data exploration, and statistical correlation mining capabilities. GRCA has proven to be a highly effective SQM platform in several different applications and we present results regarding BGP flaps, PIM flaps in Multicast VPN service, and end to end throughput drop in CDN service.

In 2002 Arnaud Gonguet[et.al] presented a paper for present policy information model for IP-VPN. Policy-based management is based on policy information model. They show the collection of the specific services policy condition or policy actions. These are used for formulating the policy rules. In this article, the principles of Policy-based Management are reminded, and the role and usage of Policy Information Models is introduced. Then this article provides a description of the way an RFC2547-like IP VPN is provisioned in a network. Finally the authors propose a Policy Information Model for managing RFC2547-like IP VPNs in the context of network Policy-based Management.

ISSN No: - 2456- 2165

III. CONCLUSION

A Virtual Private Network (VPN) is a type of private network for the public. It allows to the user for send or receives the data from the public network, but for this service, we have to connect computing device directly to the private network. Applications running across the VPN may therefore benefit from the functionality, security, and management of the private network. In this paper, we give the review of various papers for VPN (Virtual Private Network).

References

[1]. John P. Mcgregor And Ruby B. Lee," Performance Impact Of Data Compression On Virtual Private Network Transactions". In 2000.

[2]. Peter Dulany, Chang Soo Kim, And James T. Yu," A Performance Analysis Of Gateway-To-Gateway Vpn On The Linux Platform" In 2007.

[3]. R.Manikandan, N.N. Pragash," A Broad Band Mobile VPN For Realtime Reliable Multi-Media Communication For Lte Networks", In *International Conference On Explorations And Innovations In Engineering & Technology Iceiet - 2016.*

[4]. Ravi S.Ravindran, Changcheng Huang, K.Thulasiraman," A Dynamic Managed Vpn Service: Architecture And Algorithms", In 2006.

[5]. Ravishankar Ravindran, Changcheng Huang," Vpn Topology Abstraction Service Using Centralized Core Capacity Sharing Scheme", In 2010.

[6]. Ravi S. Ravindran, Changcheng Huang, K.Thulasiraman," Topology Abstraction As VPN Service", in IEEE 2005.

[7]. He Yan, Lee Breslau, Zihui Ge, Dan Massey1 Dan Pei, Jennifer Yates," G-RCA: A Generic Root Cause Analysis Platform for Service Quality Management in Large IP Networks", in 2010.

[8]. Arnaud GONGUET, Olivier POUPEL ALCATEL," A Policy Information Model for RFC2547-like IP VPNs", in 2002.

[9].