УДК 004.9
МРНТИ 81.93.29

COMPREHENSIVE REVIEW OF VIRTUAL PRIVATE NETWORK

A. RAZAQUE, S. AMANZHOLOVA, A. YESSENALINA, D. SOVETOV

International information technology university

Abstract: *A Virtual Private Network (VPN) provides the data encryption and checks security in order to provide privacy authorized users. The VPN restricts the unauthorized person to gain the access to server. This paper presents a detailed information and provides classification on different types of VPN. The detail concept of an encrypted tunnel and data encryption processes are discussed. Furthermore, Internet Protocol Security (IPsec) and layer-based VPN are deliberated. As, the Virtual Network Service (VNS) provides management capabilities and performance properties is also included in this review. Finally, the router's virtualization is obtained by conducting the experiments.*

Keywords*: VPN, VNS, Tunneling, IPsec, Encryption and IKE*

ВИРТУАЛЬДЫ ЖЕКЕ ЖЕЛІНІ ШОЛУ

Аңдатпа: *ВЖЖ (Виртуальды жеке желі) деректерді шифрлау үшін қолданылады, сонымен қатар ақпаратты бөгде адамдардың қолына түспеу үшін, қауіпсіздікпен құпиялықты қамтамасыз етеді. ВЖЖ сервисі рұқсатсыз белгісіз тұлғаларға серверге кіруге мүмкіндік бермейді. Бұл мақалада сіз ВЖЖ жайлы толық ақпаратты қарай аласыз және ВЖЖ-нің әртүрлі типтерге жіктелгені туралы біле аласыз. Деректерді шифрланған туннельден Қауіпсіздік Хаттамасы (IPsec) және ВЖЖ арқылы тасымалдауға болады. Осындай мүмкіндіктерді Виртуальды Желі Қызметі (ВЖҚ) береді. ВЖҚ маршутизаторды деректер және басқару жазықтықтарында виртуальдау үшін қолданылады. Басқару жазықтығында ВЖҚ маршруттау және сигнализацияны, ал деректер жазықтығында пакеттік бағыттау және каналдан өткізу қабілеттілігін қамтамасыз етеді.*

Түйінді сөздер*: ВЖЖ, ВЖҚ, туннельдеу, IPsec, шифрлау және IKE*

ОБШИРНЫЙ ОБЗОР ВИРТУАЛЬНОЙ ЧАСТНОЙ СЕТИ

Аннотация: *Виртуальная частная сеть (ВЧС) обеспечивает шифрование данных и проверяет безопасность для обеспечения конфиденциальности авторизованных пользователей. ВЧС ограничивает доступ постороннего лица к серверу. В этом документе представлена подробная информация и представлена классификация различных типов ВЧС. Обсуждается подробная концепция зашифрованного туннеля и процессов шифрования данных. Кроме того, обсуждаются вопросы безопасности протокола Интернета (IPsec) и ВЧС на основе уровня. Виртуальная сетевая служба (ВСС) предоставляет возможности управления, а свойства производительности также включены в этот обзор. Наконец, виртуализация маршрутизатора получается путем проведения экспериментов.*

Ключевые слова: *ВЧС, ВСС, туннелирование, IPsec, шифрование и IKE*

Introduction

Virtual private network achieves better security in transmission across the all internet users. A VPN service is used to construct a wide area network infrastructure [1-3]. In traditional connectivity, there is no secure communication between client and server and any unauthorized

person can easily connect with internet. So, VPN provide secure communication between client and user. In VPN, we can share common physical network infrastructure among multiple VPNs to provide high security.

VPN technology was developed to allow remote users and branch offices to access corporate applications and resources [4].To ensure security, the private network connection is established using an encrypted layered tunneling protocol and VPN users use authentication methods, including passwords or certificates, to gain access to the VPN [5-6]. In other applications, Internet users may secure their transactions with a VPN, to circumvent geo-restrictions and censorship, or to connect to proxy servers to protect personal identity and location to stay anonymous on the Internet. However, some websites block access to known VPN technology to prevent the circumvention of their geo-restrictions, and many VPN providers have been developing strategies to get around these roadblocks.

To improve security solution, we can provide Effective and Extensive Virtual Private Network called (EEVPN), that is more effective because it is faster and also more secure than other VPNs [7]. We can test the performance of VPN with the help of operating systems. We can check on CPU and memory usage in VPN i) we can reduce usage of CPU and data of memory ii) we can compare in both side of VPN one is hardware and other is software side [8].

In VPN, Layer 2 consists of frame relay and ATM and in layer 3 there is an IPsec & firewall [9]. Frame relay and ATM circuits, it is increasing to use private network other than circuits.

VNS SYSTEM

A Virtual Network Services is defined as value – added network service based on wide area IP network. At firstly, this system is based on leased lines that cost is too much high but then after invented low cost, different virtual circuit services like Frame relay and X.25, where we can possibly find virtual private network. But, it cannot provide two functions like availability and functionality sufficiently. So, we have to ensure that quality of services (QoS) and confidentiality of data (Fig.1).

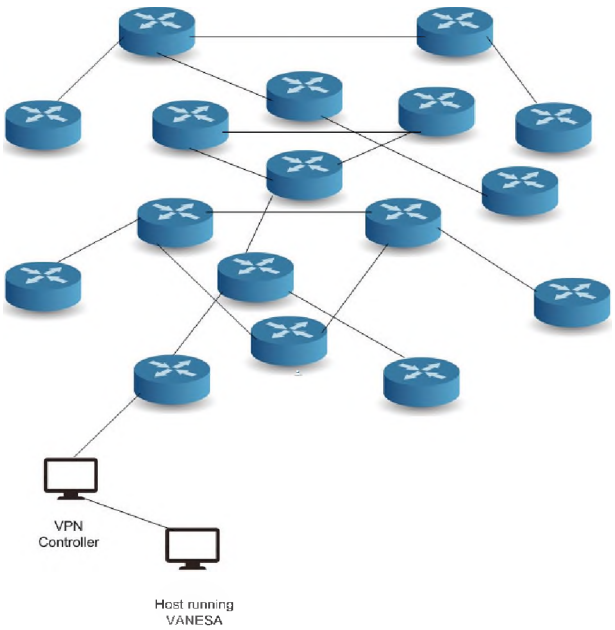


Figure 1 - VPN controller and other VPN connected with virtual link in VNS

A VNS service is mostly used virtual links for better communication. It is used for site to site network connectivity. A virtual link is used for two physical nodes in the VPN [10].

We can say that Darwin based router has single forwarding table and it also has some features like packet scheduling (Fig.2), packet classifier, programmable interface, signaling protocol module.

In the other hand, a virtualized VNS router has two plane names as data plane and control plane, which provide unique needs of each VPN. In data plane, each VPN has own link bandwidth and forwarding table because a virtualized VPN has multiple forwarding table and virtual link, so that each VPN can use own. In control plane, it provides signaling protocols and custom VPN routing protocols.

A. The multiple VPN interfaces

As shown in fig, there is two VPNs are connected by virtual link, we can see that VPN #1 is defined as dotted line and VPN #2 has light shade line. VPN #1 has IP address 10.2.1/24 and VPN #2 has IP address 10.1.1/24.

Difference between VNS router & Virtualized VNS Router

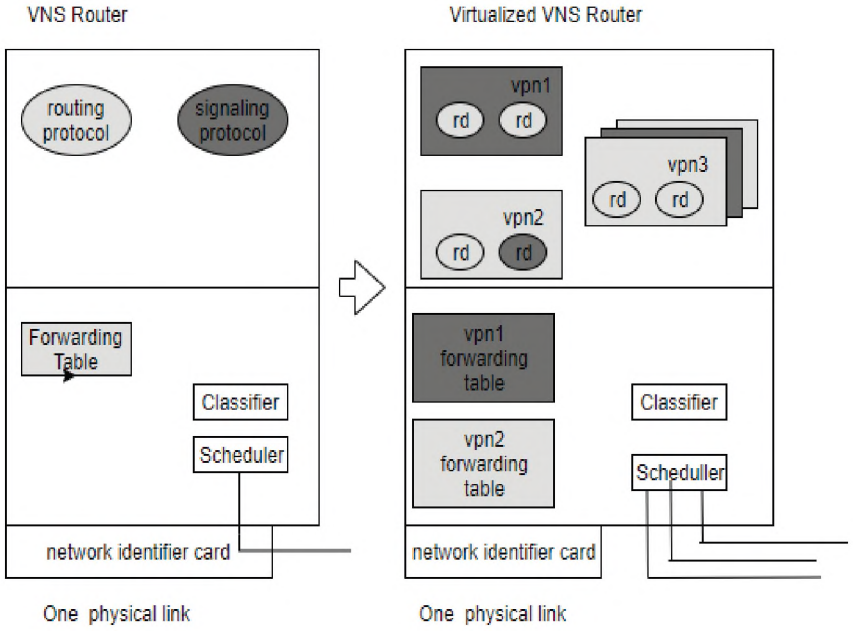


Figure 2 - Virtualized VNS routers

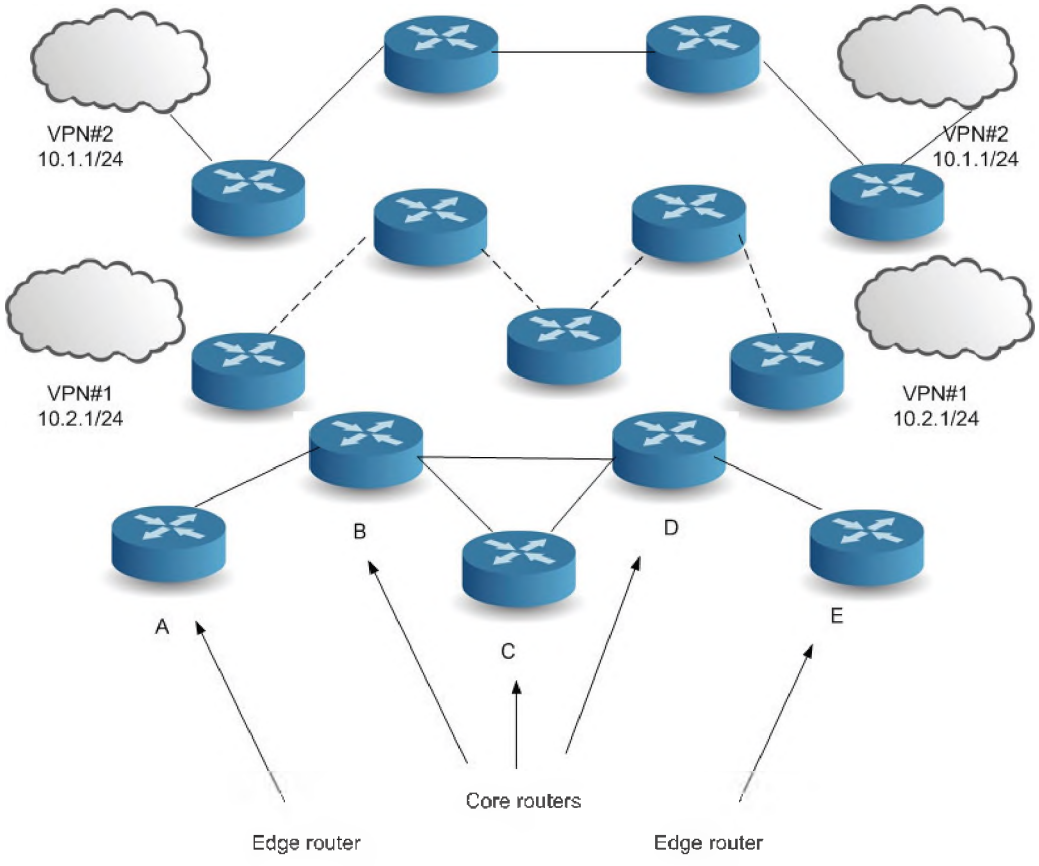
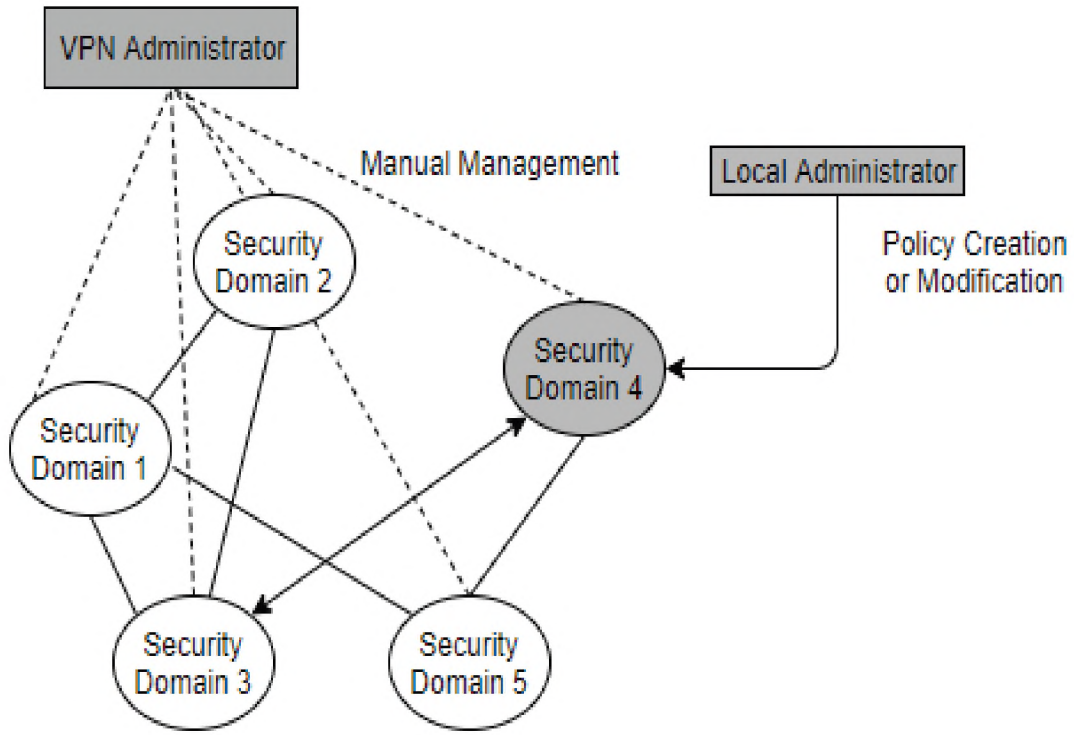


Figure 3 - Basic concept illustrated with 2 VPN



Policy Database in Domain 4

Src	Dest.	Action
H5	H4	Permit
*	*	Deny
H3	H4	Permit

Figure 4 - Illegal policy modification in local policy Server

There is mainly five router used for communication: A, B, C, D, E. Here, A and E are edge routers and they provide Internet protocol security and encapsulating IP headers. Other, B, C, D are core routers that are not directly connected to VPN (Fig.3).

B. Policy Based Hybrid Security Management

In past, any server could use local policy database to any clients. There are many limitations of IETF proposed architecture, for example, lack of consistent. As shown in below fig 4, we can say that global VPN administrator can control global policies on local policy server (PS) and do not have permit to monitor and to control the local policies (Fig.4).

It's possible to control over the VPN if all control and modification is given like access, to only VPN(global) administrator. As shown in fig, local admin of domain create security issues or violating the rules of global policies. This problem can be solved by global policy based management system [8].

C. Design of Hybrid Security Policy System

It's possible to reduce limitations of local based policy system. The hybrid security policy system distributes global policies from VPN administrator and verifies consistency of the policies from local administrator.

Given figure shows all component and structure of the hybrid security management system (Fig.5).

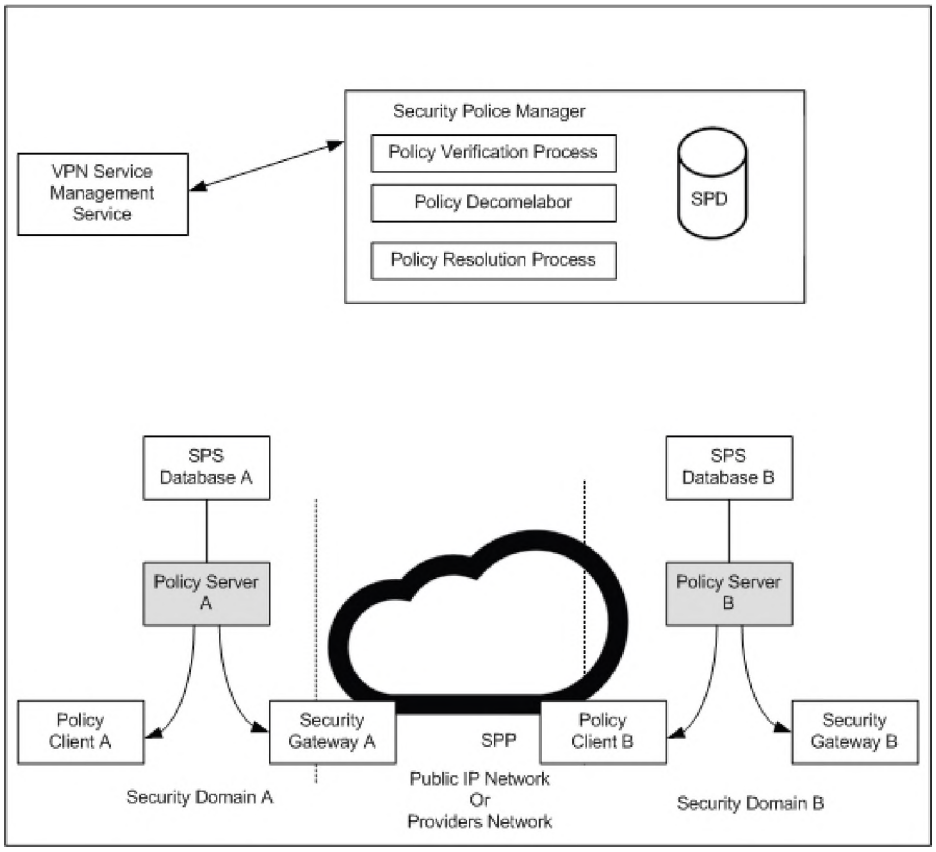


Figure 5 - Interworking between policy server and security policy manager

• ***Security Policy Manager (SPM)*:** It gives response to policy server and transfer policy to security policy server. It has global SPD to exchange policy information. It performs verification, decor relation and policy resolution process and store it into SPD. Also, it checks if the policy is continuous throughout all process of verification [11].

• ***Security Policy Database (SPD)*:** Every security domain must maintain database which is two types of database.

• ***Global Policy Database***: It contains all the policies to the entire provider's network. It is created by the VPN admin by automatically NM tools or manually.

• ***Local Policy Database***: It contains all policies for security domain. New policies are merged with previous SPD by helping policy resolution process.

• ***Security Policy Server (SPS)*:** It plays role of effective local policy into security gateway, policy servers exchange policy information using security policy protocols Policies must be verified by Security policy manager by helping verification process.

• ***Security Policy Protocols*:** It specifies how policies information exchanged and what policies information exchanged and process. It uses six different message types used to exchange policy information.

GRE TUNNELING

GRE is a tunneling protocol and CISCO proprietary for multicast address security. It provides virtual circuit without hiding the information or data while transferring through the network. Currently internet that is provided by any ISP is not secure and does not provide authentication. Due to lack of surety it does not provide good security for users. Through GRE protocol it's possible to create virtual tunnel between source and destination. GRE tunnel interfaces must be configured properly and updated in routing protocols. Here most noticeable point is that destination host must be reachable. On other situation on layer 1 and layer 2 then source cannot connect to destination [11].

A. Security services provided by IPsec

IPsec/VPN tunnel work on two modes, tunnel mode provide virtual connection between two ends whereas transport mode provide authentication and encryption techniques for secure data transmission. It provides good protection against attackers. It used following protocols:

Security protocol: AH, ESP, ESP + AH;
Encryption: DES,3DES, AES;
Authentication: MD5, SHA-1;
Protection: DH1, DH2, DH3.

METHODOLOGY

Given work describe currents problems in tunnel technologies and network performances. It will explain how to solve these issues and prevent our data from malware in the internet.

B. Network equipment

In lab experiments we used three routers: one as HQ(headquarters),on other end Branch and ISP which provide internet connectivity. Some switches are also used at both sides to create LAN and some hosts PCs. Here it's used "Wire shark" to capture the packets and analyze them. Also Jperf 2.0 used to analyze UDP and TCP performance between two systems.

C. Implementation

In above figure, it's shown basic network connectivity. On left hand HQ is connected with its private network and on right hand Branch is connected with its private LAN. Between them internet is provided by ISP. Here we take two scenario, first is creating with GRE tunnel between two end point, and in second scenario we created IPsec/VPN between them. After both scenarios we sent traffic between two end devices. By using "Wire shark" and Jperf we check security information of GRE and IPsec/VPN tunnel and understand TCP and UDP performance.

D. Configurations

- Create OSPF routing process
- Create tunnel interfaces
- Configure tunnel interfaces
- Update OSPF network statements
- Verify OSPF neighbors

Here first of all we configured all IP address on all three routers interfaces, then give tunnel IP address on both end: HQ and Branch routers. We put all routes in OSPF area 0 with in ISP. For our verification we verify ospf neighbors by using OSPF neighbor command. Below figure shows all primary configurations on HQ and Branch [12].

HQ "# sh running-config"

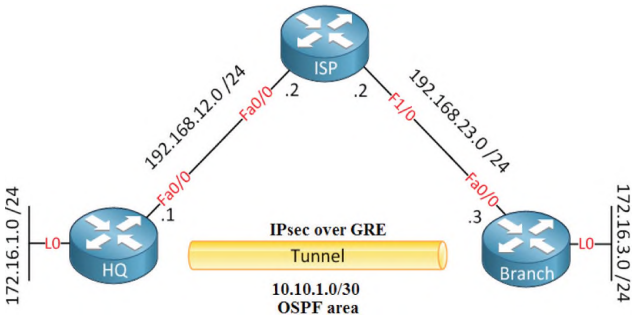


Figure 6 - IPsec over GRE tunnel

In OSPF area 0 all routers must be working properly and have neighbor relationship establish between them. Otherwise, routing will not be successful and traffic from HQ to Branch will not go to other side. We also need to make sure if end devices got their router ID properly or not. In this practical we took loopback interfaces according to ID rule on both sides, so both routers have ID as loopback IP address.

Here, we also updated tunnel interfaces in OSPF routing update. For better security, we can use *keep alive* command by define specific time interval on both sides of tunnel interfaces.

E. Encryption Process

- Define traffic to be encrypted (traffic only goes from HQ to Branch)
- Phase 1: ISAKMP policy
- Define shared secret key
- Phase 2: IPsec transform set
- Create crypto-map
- Apply crypto-map to interfaces
- Verification

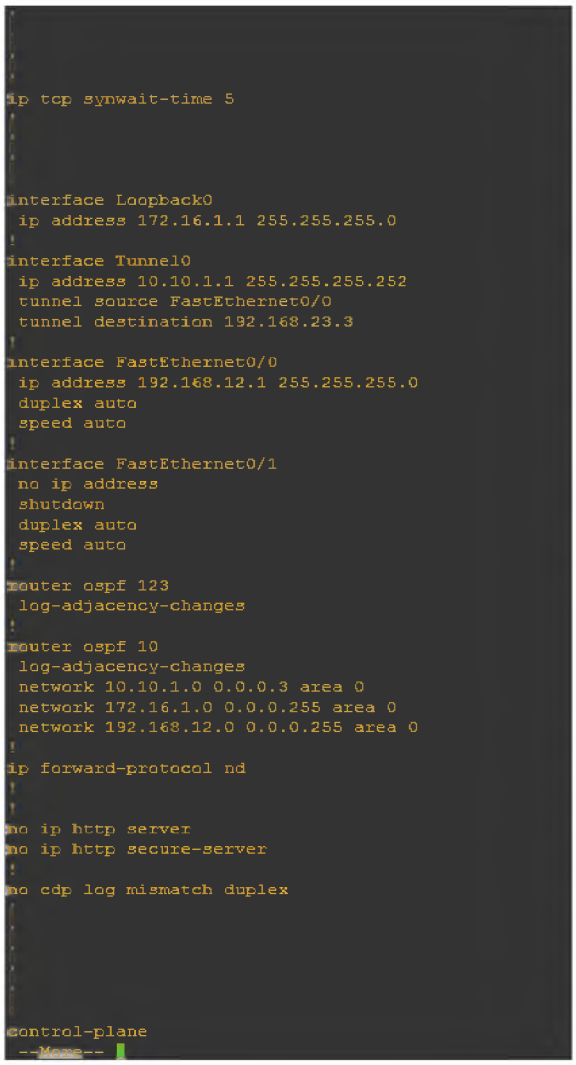


Figure 7 - First Stage configuration

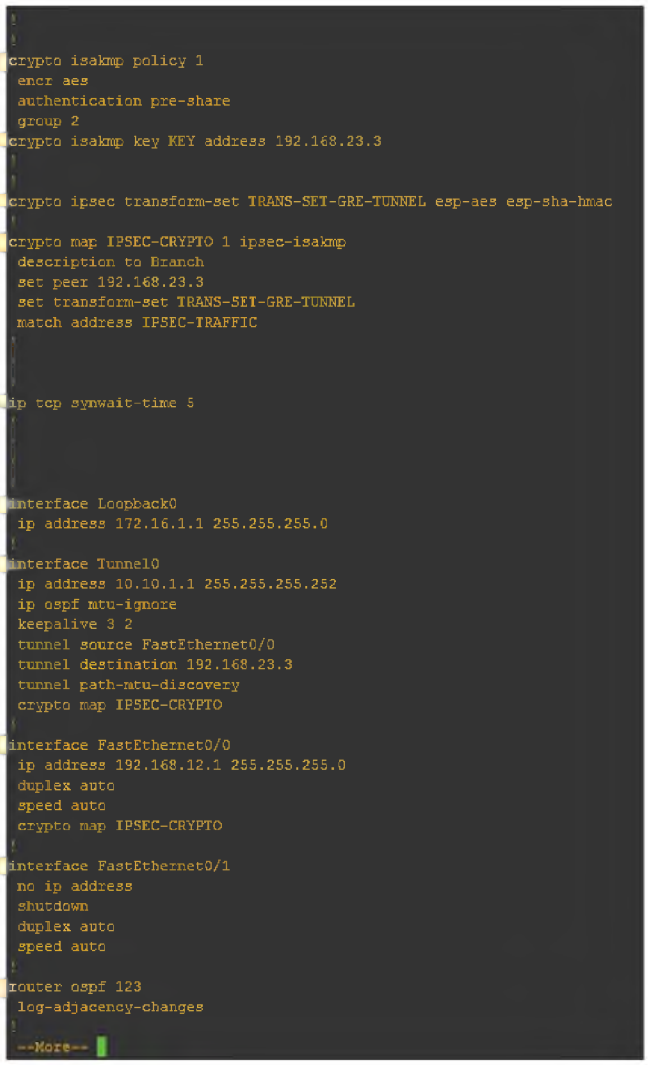


Figure 8 - Applying crypto-map

After all configuration will be done on HQ and Branch router, traffic will goes from HQ to Branch and it will transfer in encrypted form. Here we defined pre-shared secret key "KEY" on both side. Here we defined ISAKMP policy 1 and in this policy we configured authentication as pre-shared key, encryption as AES 128 bit by default, deffi-hellman group 2 key exchanges the algorithms, some description match parameters such as transform-set and destination IP address etc.

It is necessary that crypto-map is given in physical routers interface and virtual tunnel interfaces, otherwise traffic will go in encrypted form. Here is GRE (generic encapsulation) protocol provides multi-cast packet security, because IPsec only provides unicast packet security [13].

In this process we apply crypto-map on both side routers and define some matching parameters such as peer IP address, set transform-set and match access-list address. Here we used path-*mtu-discovery* command for cleanup and *ospf mtu-ignore* to ignore the MTU in DBD packets.

RESULTS

The required commands (*mtu-discovery* and *ospf mtu-ignore*) are used to encrypt data on the both routers depicted in Figure 9.

HQ# SH crypto IPsec SA (security association)

From the picture above, we can say that now our Ipsec/VPN is working perfectly and all traffic is going in encrypted form.

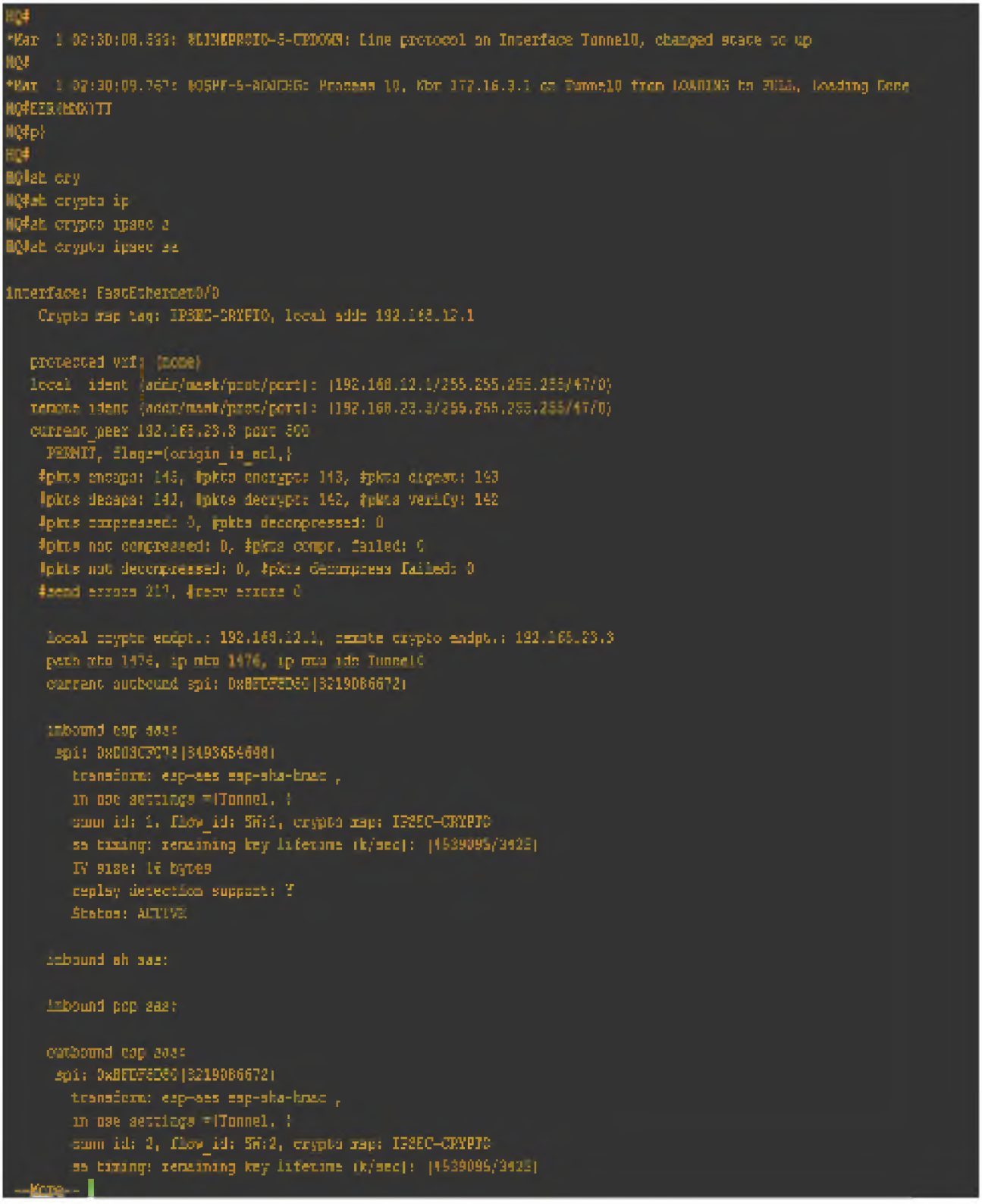


Figure 9 - VPN verification

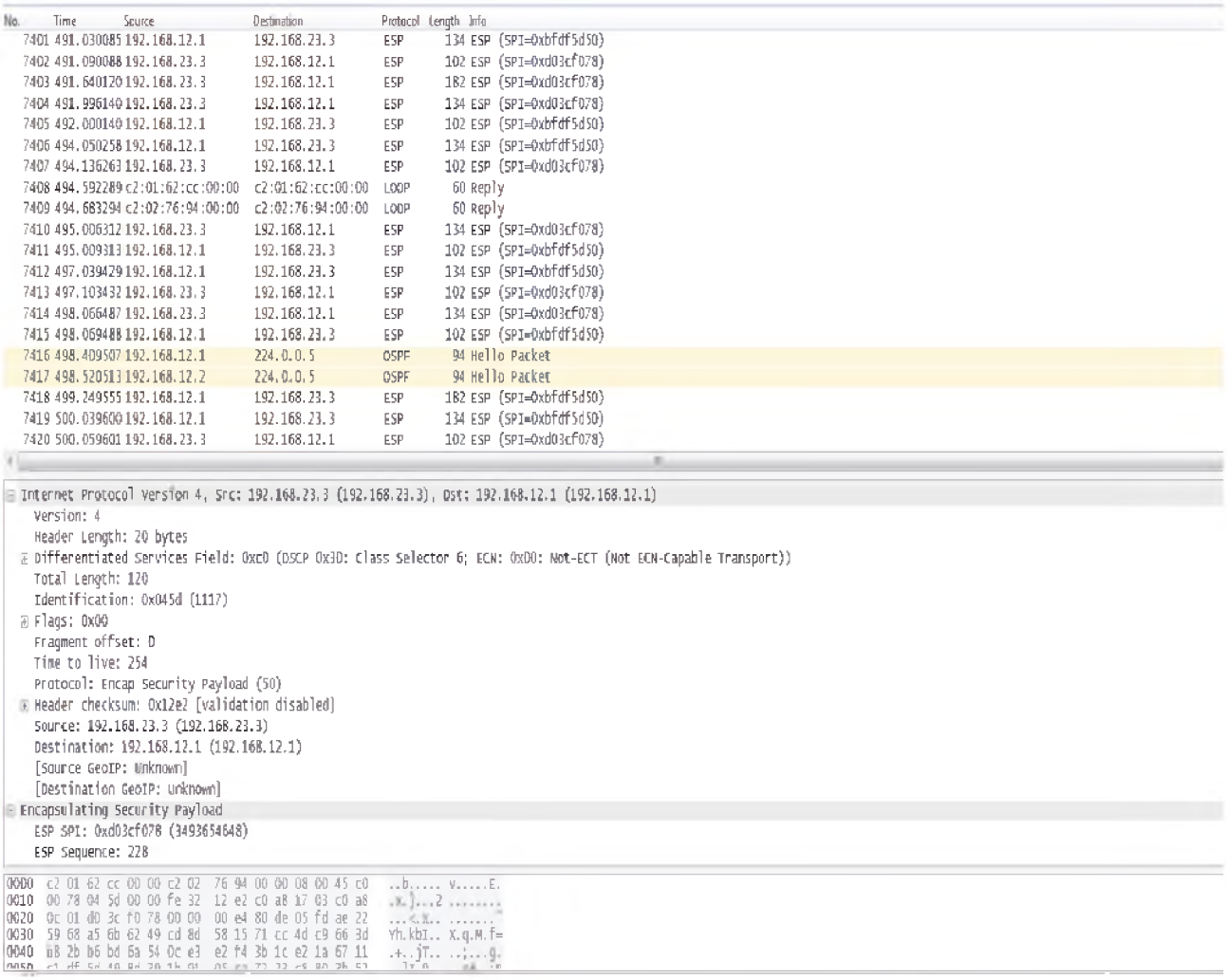


Figure 10 - Capture ESP packets in wire-shark

Packets encrypted here are 143 and packets decrypted are 142. Here is also used wire-shark packet analyzer tool to check traffic packets.

From this result we can figure out what is frame and what is encapsulation type is working. We can also notify frame length from captured packets. Encapsulating security payload is working here [14].

LAYER BASED VPN

A. L1TP: Layer 1 VPN

This is advance of VPN emerged to overcome the need of advance packet switching concept of layer2 and layer3. Nowadays big organizations want to establish their own network infrastructure, but they cannot relocate, and some want to divide their large transport network in to layer 1 virtual network. L1VPN solve this problem by allocating clients resources to their physical network. L1VPN uses GMPLS for interfaces of clients and services provider, whereas GMPLS is mainly used for routing and signaling. L1VPN has 3 main component client edge (CE), provider edge (PE) and provider core nodes (P). The PE is placed near the access point between client and career network. P is connected to either P or PE. CE maintains connectivity between V1VPN.

L1VPN has 2 main services centralize management control and distributed GMPLS control [15-16].

B. L1TP: Layer 2 VPN

Few decades ago the ATM and Frame relay used to be connected through the backbone of service providers layer 2. It is changed now, most of providers following MPLS/IP technology. In L2VPN the service providers follow L2

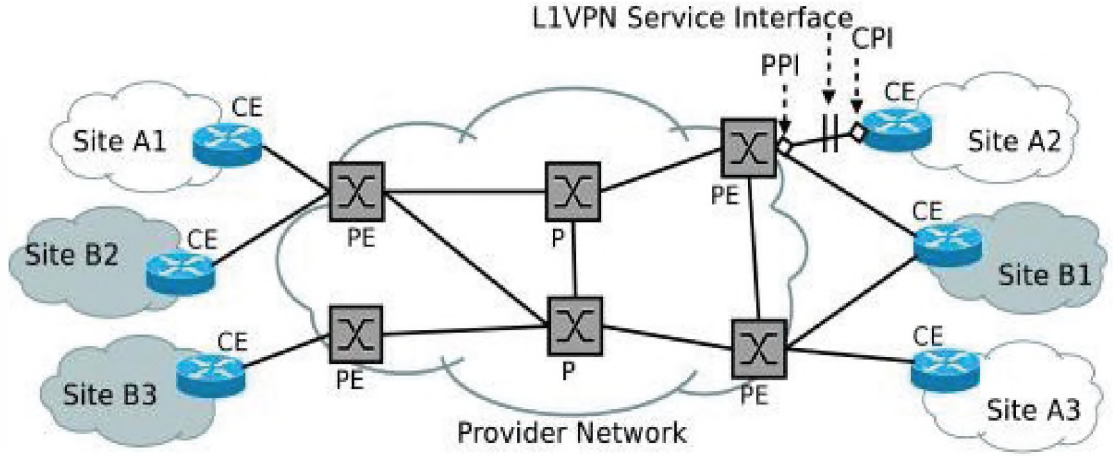


Figure 11 - Layer 1 VPN

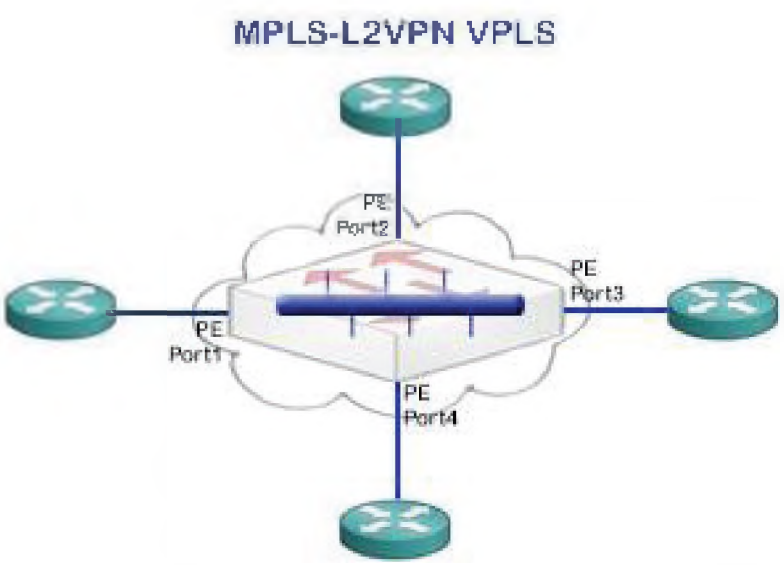


Figure 12 - Layer 2 VPN

connection for client communication by using L3 as backbone.

L2 VPN has 2 service Virtual Private Wire Service and Virtual Private LAN service [17-18].

Virtual Private Wire Service: Based on point to point service this method connects 2 remote customers at remote places by creating illusion so that they appeared to be on same network.

Normally to connect ATM/Frame Relay sites from provider to customers.

Virtual Private LAN Service: Based on single to multi point service, the illusion is created between number customers, so that connection between them appeared on same LAN.

*C. **Layer 3VPN***

The L3VPN are classified as client edge (CE) and provider edge (PE), this VPN creates illusion over its network infrastructure for clients [19].

• Client Edge (CE): Service provider performs all VPN operation such as managing and configuration on customers CE. Tunnel is established between 2 client edges.

• Provider Edge (PE): Service provider performs all VPN operation such as managing and

configuration on customers PE. Tunnel is established between 2 provider edges.

The services of L3VPN

• Network Management: All routing functions of customers are done through this VPN. Clients can save money because they don't need to establish and maintain their own network.

• Private IP addressing: Clients can communicate using private IP address.

• Scalability: Clients can increase their network.

*A. **Implementation of L3VPN***

Mainly 2 types: BGP/MPLS VPN and Virtual Router Based VPN [19].

BGP/MPLS VPN

Using any routing protocol such as OSPF, BGP, and RIP the 2 CE allows to communicate with each other. To establish communication first CE sends the topology requirement of client's side to PE. The duty of PE is to establish and maintain VPN network and route data. PE creates unique routing for every VPN and generates unique VPN forwarding Instance (VFI) for every VPN.

VFI is logical term for PE that has information about routing base and forwarding base for every VPN.

First of all, PE finds active DE which are managing client's VPN. PE broadcasts the routing information with other PE, once it connected to client's side. With this information VFI is generated by PE. Multiprotocol BGP is used to find active PE devices which are managing specific VPN.

To exchange information of VPN, PE mainly uses tunneling method and most of time MPLS tunnels are preferred, but some service providers prefer other tunneling methods like IPsec.

Virtual Router Based VPN

The isolation in traffic is provided by this technology particularly in service provider's network. Because of isolation the influence of one traffic to other is negligible in same network.

The connection process of client to provider in Virtual Based VPN is same as in BGP/MPLS VPN, but instead of VFI this method uses virtual route to establish and maintain VPN's routing process.

VPN TUNNELING

For data transmission VPN uses tunneling, the packet is encapsulated before its transmission and header is added to it. The routing information contains in this header. The logical path taken by encapsulated packet is called tunnel. The de-encapsulation process is happened at the end of tunnel. Same protocol must be applied to both ends of tunnel. The tunneling process can be operated at 3 layers of OSI model, at physical layer or data link layer or at the network layer. Common tunneling protocols used this days are IPsec, L2TP, PPTP and SSL. Data encryption method applied at VPN to improve data security. The data encryption and encapsulation is happened at the entrance of tunnel and reverse process happened at the other end of tunnel [20-21] .

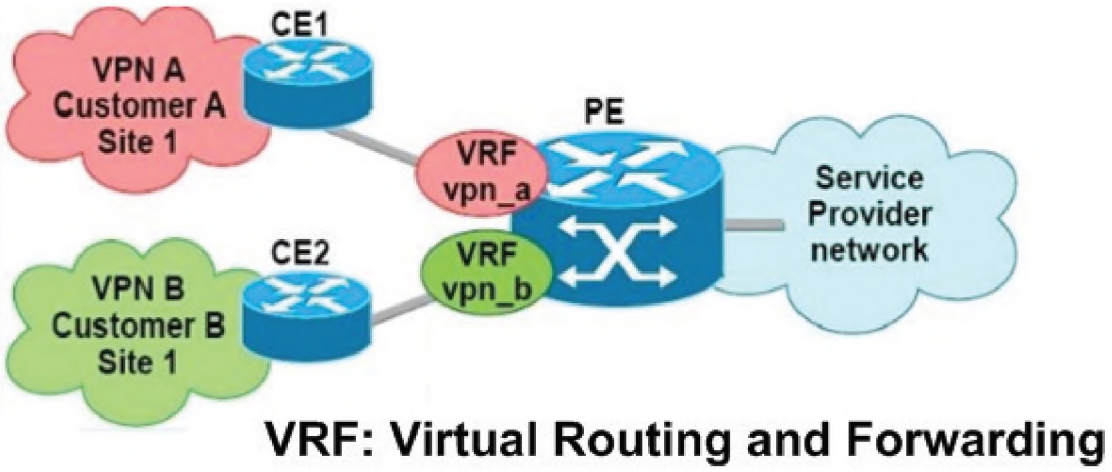


Figure 13 - Layer 3 VPN

A. Point to Point Tunneling Protocol

It is layer 2 protocol built on base of point to point protocol, where for internet access the PPP is used. Using PPTP enables user to access private network, but initially client has to connect with local service provider. PPTP creates virtual network for each of its remote client. It creates session, and tunnel is created without TCP/IP protocol through IP network. In encapsulation process the protocols added to IP packets. Encapsulated packets routed through tunnel over IP network using GRE(Generic Routing Encapsulation), its provider flows as well as congestion control for encapsulated data packets [22].

PPTP is based on PPP so same authentication process supported by PPTP as PPP. For security concerns the PPTP use CHAP(Challenge Handshake Authentication Protocol, Password Authentication protocol) and at last Microsoft Point to Point Encryption.

Password Authentication Protocol: It is simple two-way handshaking method, one the session is established between sender and receiver. Sender continuously transmit ID/Password to receiver, until authentication is provided or connection will be terminated. This is not effective authenticate process.

CHAP(Challenge Handshake Authentication Protocol): It is 3-way Handshaking process once the session is established between sender and receiver, the periodic identity of peer will be verified. Once session established sender sends challenge request message to receiver. Receiver replies it with a value which is calculated by one-way hash function. Then, he checks this value with expected hash value and if it matches, authentication will be accessed, otherwise session will be terminated.

A. L2TP: Layer 2 Tunneling Protocol

The packet to be sending over network in encrypted form before transition occurs through tunnel, over ATM or IP network. L2TP is half of PPTP and half layer 2 of forwarding process. Number of VPN connection can be established in one tunnel[22].

L2TP is based on PPP, so same authentication process supported by PPTP considered as PPP. For security concerns, the L2TP use CHAP, that is Challenge Handshake Authentication Protocol, MS-CHAP, PAP, EAP and SPAP. L2TP and PPP headers stores the PPP data, UDP header, source port number, destination port number address added to data packet. The last packet contains the IP address of source and destination IP of client and server.

To improve security this protocol combined with IPsec.

B. *SSTP: Secure Socket Tunneling Protocol*

It is advancing tunneling Protocol because it has capability to pass through firewall which can block L2TP/IPsec. SSTP can transport PPP or L2TP [23].

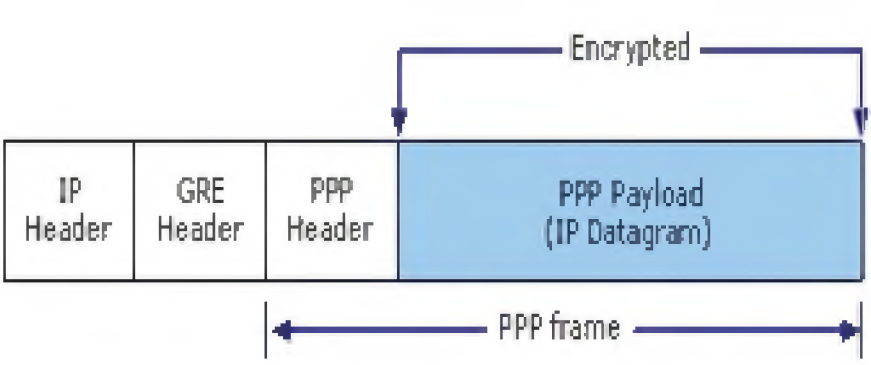


Figure 14 - Point to Point Tunneling Protocol

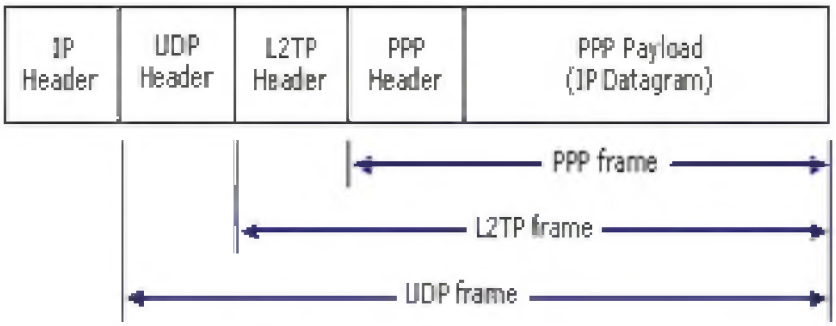


Figure 15 - Layer 2 Tunneling Protocol

Conclusion

The review and classification of VPN is served in this paper. The survey includes the detail concept of an encrypted tunnel and data encryption processes. In this survey, the experimental results have also been included by conducting two different scenarios. Based on the testing, the both scenarios have strength and limitations, the generated scenarios comprise of the security and their network performance in terms of bandwidth and CPU utilization. In Scenario-1, GRE provides better encapsulation process, but it does not have encryption. Thus, the lack of security provides easy access to the attacker to easily deceive the users and get the password and other important information. In Scenario-2, IPsec/VPN provides data encryption, but it reduces the network performance because it takes longer time to transfer the data. These testing results provide the guidelines to users whether to apply scenario-1, if required less security and higher data transfer rate otherwise use scenario-2, if required high security and lesser data transfer rate.

REFERENCES

1. Surantha, Nico. "Secure Portable Virtual Private Network with Rabbit Stream Cipher Algorithm." *Procedia Computer Science*135 (2018): 259-266.
2. Elezi, Muhamed, and Bujar Raufi. "Conception of Virtual Private Networks using IPsec suite of protocols, comparative analysis of distributed database queries using different IPsec modes of encryption." Procedia-Social and Behavioral Sciences 195 (2015): 1938-1948.
3. Elezi, Muhamed, and Bujar Raufi. "Conception of Virtual Private Networks using IPsec suite of protocols, comparative analysis of distributed database queries using different IPsec modes of encryption." Procedia-Social and Behavioral Sciences 195 (2015): 1938-1948.
4. Wesinger, Ralph, and Christopher Coley. "Method for providing a virtual private network connection." U.S. Patent Application 11/250,909, filed March 9, 2006.
5. Chawla, Deepak, and William R. Beckett III. "Methods, systems, and computer program products for providing a virtual private gateway between user devices and various networks." U.S. Patent 9,021,251, issued April 28, 2015.
6. Mayya, Ajit Ramachandra, Parag Pritam THAKORE, Stephen Craig Connors, Steven Michael Woo, Sunil Mukundan, and Thomas Harold Speeter. "Method and system of establishing a virtual private network in a cloud service for branch networking." U.S. Patent Application 16/179,675, filed March 7, 2019.
7. Lospoto, Gabriele, Massimo Rimondini, Benedetto Gabriele Vignoli, and Giuseppe Di Battista. "Rethinking virtual private networks in the software-defined era." In 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM), pp. 379-387. IEEE, 2015.
8. Wang, Wei, and Charles Shen. "Methods and apparatus to improve security of a virtual private mobile network." U.S. Patent 9,172,678, issued October 27, 2015.

9. Ismail, Mohd Nazri. "Study the Best Approach for Virtual Private Network Implementation: CPU and Memory Usage Performance." International Journal of Multidisciplinary Sciences and Engineering (IJMSE) 1, no. 2 (2011): 16-21.
10. Lospoto, Gabriele, Massimo Rimondini, Benedetto Gabriele Vignoli, and Giuseppe Di Battista. "Rethinking virtual private networks in the software-defined era." In 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM), pp. 379-387. IEEE, 2015.
11. Sridevi and Dr. Manjaia D.H, "Network Security Comparision between IPSec and GRE", International Journal of Emerging Trends & Technology. March – April 2014.
12. [Mohd Nazri Ismail, "Study the Best Approach for Virtual Private Network Implementation: CPU and Memory Usage Performance", International Journal of multidisciplinary sciences and engineering. November 2010.
13. Ritik kajal, Deepshikha Saini and Kusum Grewal, "Virtual Private Network" International Journal of Advanced Research in Computer Science and Software Engineering October 2012.
14. Jahan, Sohely, Md Saifur Rahman, and Sajeeb Saha. "Application specific tunneling protocol selection for Virtual Private Networks." In 2017 International Conference on Networking, Systems and Security (NSysS), pp. 39-44. IEEE, 2017.
15. Malheiros, Neumar, Edmundo Madeira, Fabio Verdi, and Mauricio Magalhães. "A management architecture for layer 1 VPN services." In Broadband Communications, Networks and Systems, 2006. BROADNETS 2006. 3rd International Conference on, pp. 1-10. IEEE, 2006.
16. Bensalah, Faycal, Najib El Kamoun, and Ayoub Bahnasse. "Evaluation of tunnel layer impact on VOIP performances (IP-MPLS-MPLS VPN-MPLS VPN IPsec)." International Journal of Computer Science and Network Security (IJCSNS) 17, no. 3 (2017): 87.
17. Barkie, Eric J., Benjamin L. Fletcher, Marco Pistoia, John J. Ponzo, and Andrew P. Wyskida. "Authentication in virtual private networks." U.S. Patent 9,094,400, issued July 28, 2015.
18. Bloch, Noam, Eitan Hirshberg, and Michael Kagan. "Network interface controller supporting network virtualization." U.S. Patent 9,008,097, issued April 14, 2015.
19. Surantha, Nico. "Secure Portable Virtual Private Network with Rabbit Stream Cipher Algorithm." Procedia Computer Science135 (2018): 259-266.
20. Caicedo-Muñoz, Julian Andres, Agapito Ledezma Espino, Juan Carlos Corrales, and Alvaro Rendón. "QoS-Classifier for VPN and Non-VPN traffic based on time-related features." Computer Networks 144 (2018): 271-279.
21. Coonjah, Irfaan, Pierre Clarel Catherine, and K. M. S. Soyjaudah. "Performance evaluation and analysis of layer 3 tunneling between Open SSH and Open VPN in a wide area network environment." In Computing, Communication and Security (ICCCS), 2015 International Conference on, pp. 1-4. IEEE 2015.
22. Garg, Pankaj, and Y. Wang. NVGRE: Network virtualization using generic routing encapsulation. No. RFC 7637. 2015.
23. Lakbabi, Abdelmajid, Ghizlane Orhanou, and Said El Hajji. "VPN IPSEC & SSL technology Security and management point of view." In Next Generation Networks and Services (NGNS), 2012, pp. 202-208. IEEE, 2012.
24. Narayan, Shaneel, Cameron J. Williams, Daniel K. Hart, and Max W. Qualtrough. "Network performance comparison of VPN protocols on wired and wireless networks." In Computer Communication and Informatics (ICCCI), 2015 International Conference on, pp. 1-7. IEEE, 2015.