International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET218133

Implementation of Site to Site IPsec VPN Tunnel between Routers

Ei Ei Khaing, Khin Than Nyunt, Sandar Moe, Mya Thet Khaing
Faculty of Computer Systems and Technologies, UCS (Hpa-An), FIST, Kayin, Myanmar

Article Info
Volume 8 Issue 1
Page Number: 163-169
Publication Issue :
January-February-2021

Article History
Accepted : 02 Feb 2021
Published : 11 Feb 2021

ABSTRACT

Today, security is very important in the communication system over through the Internet. The Transmission control protocol and Internet protocol (TCP/IP) protocol suite is used in the Internet communication that it includes five layers in which it is construct IPSec VPN Tunnel between two routers at the network layer. IPsec have two protocols that it is authentication header and encapsulation security payload (ESP) in which two protocols is shown simulation and then it is give encryption, authentication and confidentiality in which for packets at the IPSec layer within network layer and adds new IP header at the network layer. IPSec is designed to provide security at the network layer that it protects the entire IP packets. It takes an IP packet and then it includes the header, applies IPSec security methods to the entire packet and adds a new IP header. The system purpose is known use router devices at the network layer and then this layer is built IPSec VPN tunnel between routers that when it is known how does command line. IPsec VPN tunnel is built based on ACL (access list), crypto isakmp (internet security association and key management protocol) policy, transform set and crypto map and then the system is aimed to know it facts configuration and then to know used routers at the network layer and is built IPSec VPN tunnel between two routers. This system is simulated using packets tracer software 7.1.

Keywords - VPN, IPSec, crypto map, isakmp.

I. INTRODUCTION

IPSec is a collection of protocols designed by the internet Engineering Task Force to provide security for a packet at the network level. IPSec provides security services at the IP network layer. IPSec enables to protect message confidentiality, verify message integrity and authenticate message sources. The network layer in the internet is often referred to as the internet protocols or IP layer. IPSec helps create authenticated and confidential packets for the IP layer. IPsec can be useful in several areas. First it can enhance the security of those client/server programs such as electronic mail, that use their own security protocols. Second it can enhance the security of those client/server programs, such as HTTP that use the security services provided at the transport layer. It can provide security for node to node communication programs such as routing protocols.

[1] IPSec have two different mode that it is transport and tunnel mode. In this system is used tunnel mode.

VPNs over the Internet encompass three types of applications [2]. Remote access, intranets and extranets all stem from the growth and diversification of today's enterprise, but each has its own specific set of requirements that can be addressed by a secure VPN. IP is the basis for many large corporate networks, as well as for the Internet.

II. RELATED WORK

Further, the paper focuses on several specific the reliability of the security software. Security is very important in the communication that is voice, data and video communication.

The most popular routing protocols used within enterprises today to see how they differ and where are best used within network infrastructures. Further, using compared to more modern dynamic routing protocols, RIPv2 methods for selecting optimal routes and the substantial convergence time it takes to recalculate paths renders it nearly obsolete. Today the only reason might run across a network running RIPv2 [3] is either that the network is very old and in serious need of an upgrade or the network is running cheaper, consumer-grade routing hardware that can only support RIP. IPSec VPN tunnels can also be configured using GRE (Generic Routing Encapsulation) Tunnels with IPsec. GRE tunnels greatly simply the configuration and administration of VPN tunnels. NAT (Network Address Translation) is most similarly to be configured to provide Internet access to internal hosts.

III. VIRTUAL PRIVATE NETWORK

A VPN means a private network across a public network and enable uses to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. A VPN is a private network that uses a public network to connect remote sites or users together. The VPN uses "virtual" connections routed through the Internet from the business's private network to the remote site.

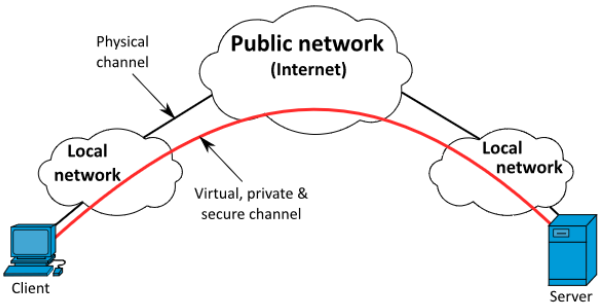

Fig. 1. VPN Connectivity Overview

IV. COMMANDS BASED ON CISCO NETWORK DEVICES

There are mainly different modes cisco routers in the following Table 1.

Table 1. Entering and Exiting in Different Modes

Mode	Command prompt	Description
User execution mode	Router>	
Privilege mode	Router>enable Router#	Entering into privilege mode from user execution mode
	Router#disable Router>	Exiting from privilege mode to user execution mode
global configuration mode	Router#configure terminal Router(config)#	Entering into global configuration mode from

		privilege mode
	Router(config)# exit Router#	Exiting from global configuration mode to privilege mode
Interface mode	Router(config-if)	Use interface command and specify an interface in global configuration mode

V. IPSec VPN REQUIREMENTS

1. ACL
   - Access list permit
2. ISAKMP policy (phase 1)
   - creates the first tunnel, send message to peer router
3. transform set (phase 2)
   - Transform set for one network to another network
   - t protects data.
   - IPSec then cones to encrypt the data using encryption algorithms and then provides authentication, encryption and anti-replay services.
   - Secret key (same key)
4. Crypto map
   - Security association lifetime
5. int g0/0
   - apply the crypto map

VI. DESIGN AND SIMULATION

IPSec VPN Tunnels are used between two cisco routers that to allow the security communication and then transmission packets at the network layer. The tunnel is created over the Internet public network and encrypted using AES algorithm that it is used cryptography is give confidentially and authentication of the data transmitted between two routers (R1 and R3) in the below Fig 2. This system will show how to setup and configure two Cisco routers to create a permanent secure IPSec VPN tunnel between router R1 and R3 over the internet service provider (ISP).

Five steps that are required to get between R1 and R3 IPSec VPN Tunnel to work.

1. ACL
2. ISAKMP policy
3. Transform set
4. Configure ISAKMP
5. Configure IPsec map

In this system, setup is between two network these are 192.168.1.x and 192.168.3.x network. Both the R1 and R3 routers connect to the ISP router and assigned a static IP Address as shown in the following Fig. 3.

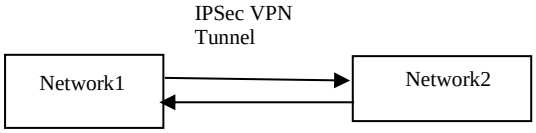

Fig. 2 System flowchart

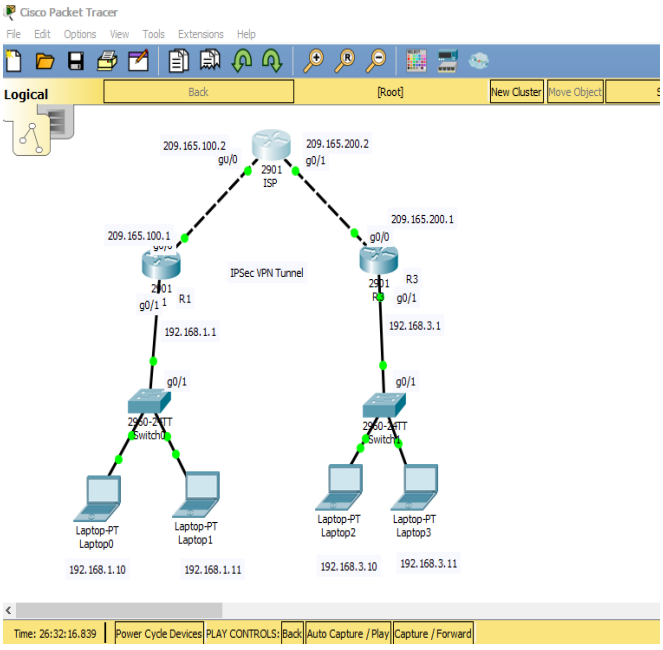

Fig.3. IPSec VPN Tunnel

This system is used three routers and two switch. In the above Fig 3 have two network that it is 192.168.1 and 192.168.3 networks through IPSec VPN tunnel (R1 and R3) and ISP router.

This system is used three cisco routers that it is routers R1, ISP and R3. Router R1 has two interfaces that it G0/0 and G0/1. For router R1 is used command line interface (CLI) that Interface G0/1 is assigend ip address 192.168.1.1 and subnet mask 255.255.255.0 and then interface G0/0 is assigned ip address 209.165.100.1 and subnet mask 255.255.255.0 for router R1 as shown in Fig 4.

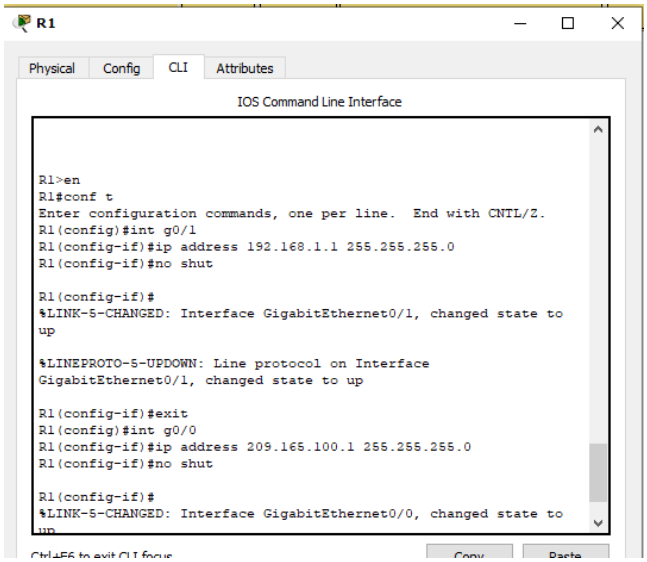

Fig. 4. IP address for Router R1

Router ISP has two interfaces that it G0/0 and G0/1. For router ISP is used command line interface (CLI) that Interface G0/1 is assigend ip address 209.165.200.2 and subnet mask 255.255.255.0 and then interface G0/0 is assigned ip address 209.165.100.2 and subnet mask 255.255.255.0 for router ISP as shown in Fig 5.

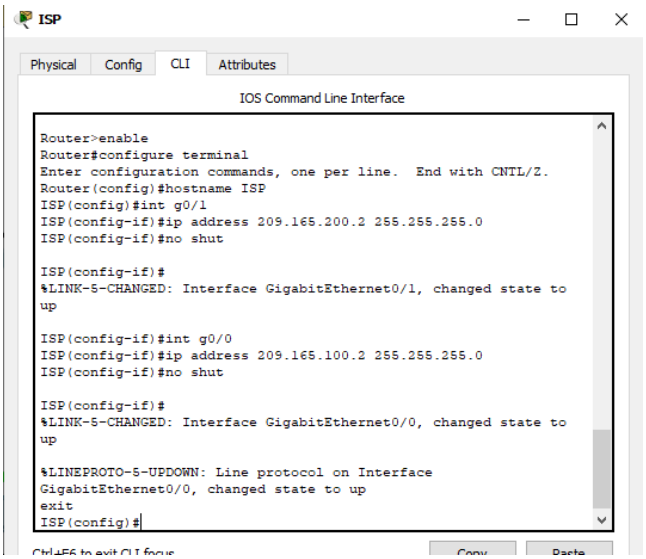

Fig. 5. IP address for Router ISP

Router R3 has two interfaces that it G0/0 and G0/1. For router R3 is used command line interface (CLI) that Interface G0/1 is assigend ip address 192.168.3.1 and subnet mask 255.255.255.0 and then interface G0/0 is assigned ip address 209.165.200.1 and subnet mask 255.255.255.0 for router R3 as shown in Fig 6. Router R1 and R3 is buit IPSec VPN tunnel through ISP, so router R3 is assigned ip route 0.0.0.0 0.0.0.0 209.165.200.2 for ISP.

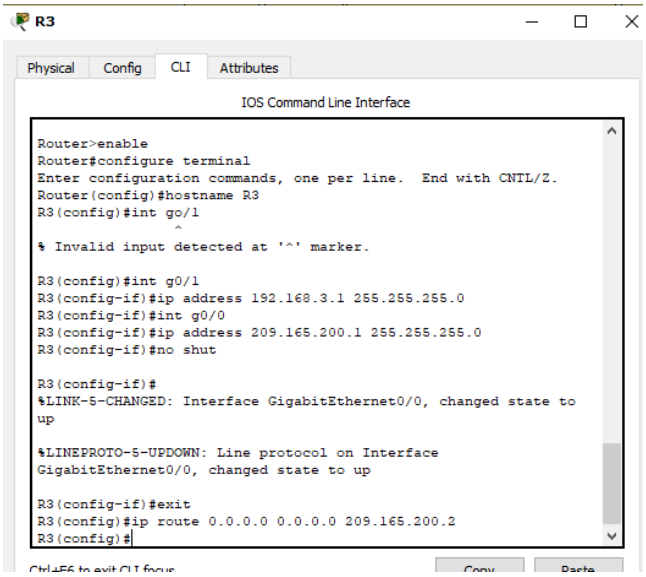

Fig. 6. IP address for Router R3

After routers is assigned ip address, ISP is usedshow ip route commands that it is shown in Fig 7.

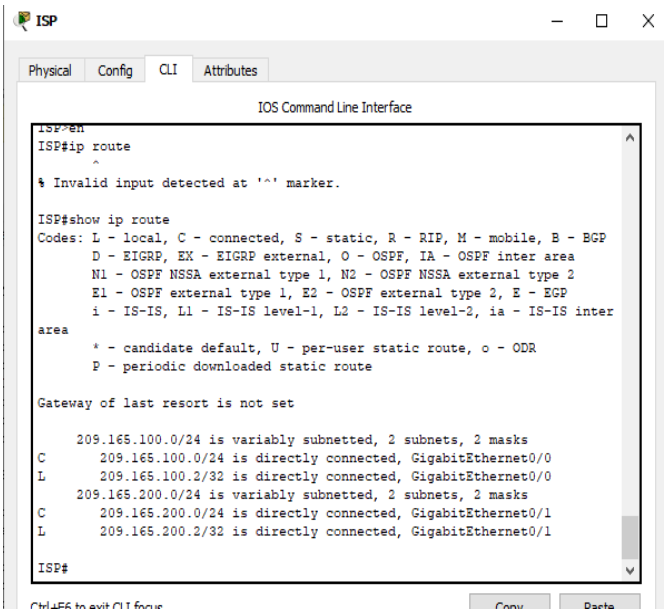

Fig. 7. Connected Network

After router R1is assigned, R1 and R3 is buit Tunnel in which it need to ACL that it is used access list permit how many ip address, isakmp policy that it is used encryption and authentication,transform set (R1->R3) and crypto map as shown in Fig 8 and 9.

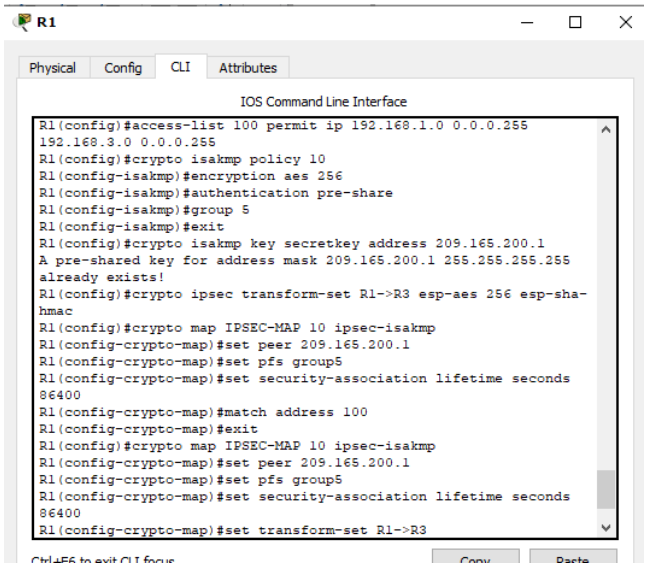

Fig. 8. Built Tunnel for R1

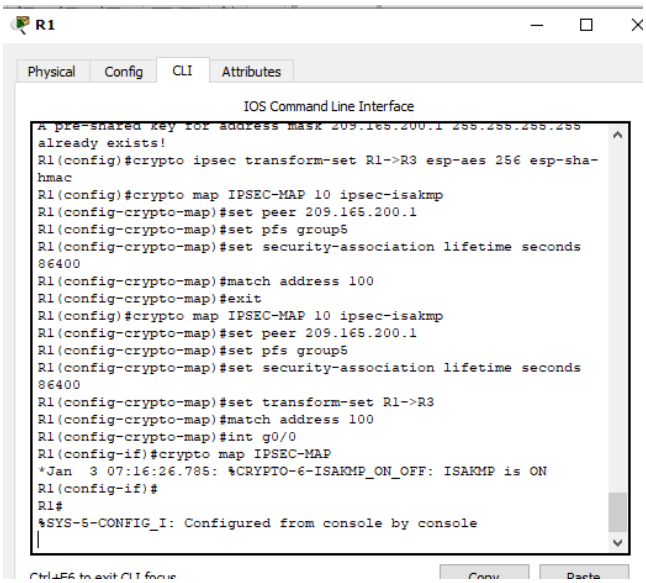

Fig. 9. ISAKMP is ON over router R1

After router R3 is assigned, R3and R1 is buit Tunnel in which it need to ACL that it is used access list permit how many ip address, isakmp policy that it is used encryption and authentication,transform set (R3->R1) and crypto map as shown in Fig 10 and 11.

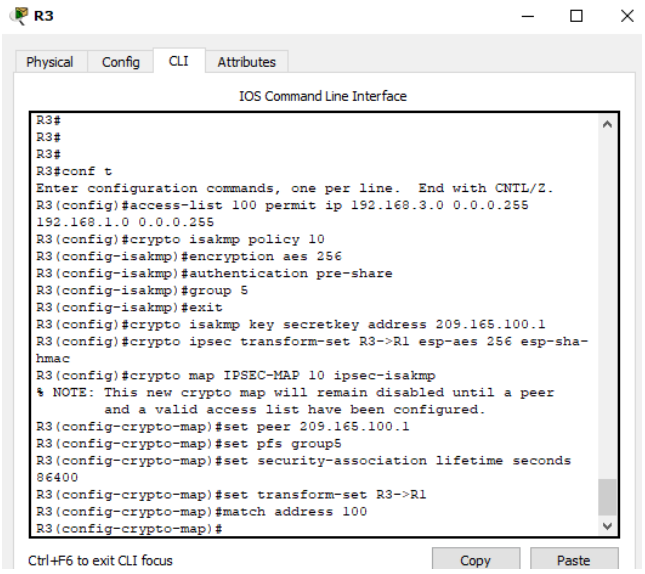

Fig.10. Built Tunnel for R3

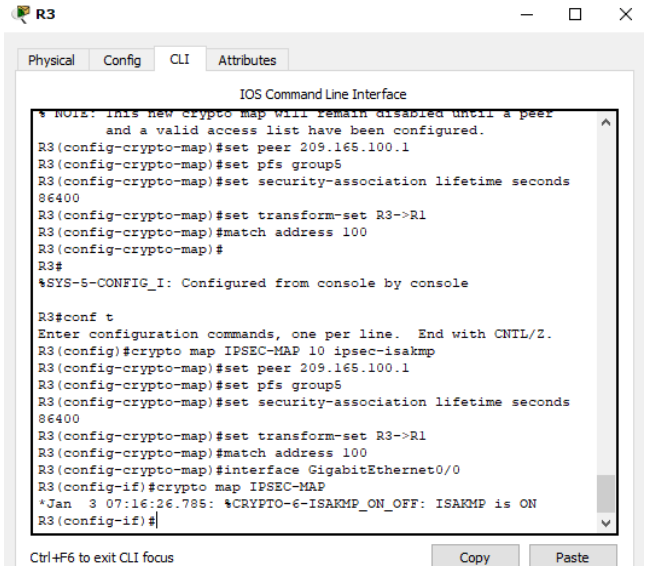

Fig.11. ISAKMP is ON over router R3

Using ping command 192.168.3.10 network through ISP router as shown in Fig 12.

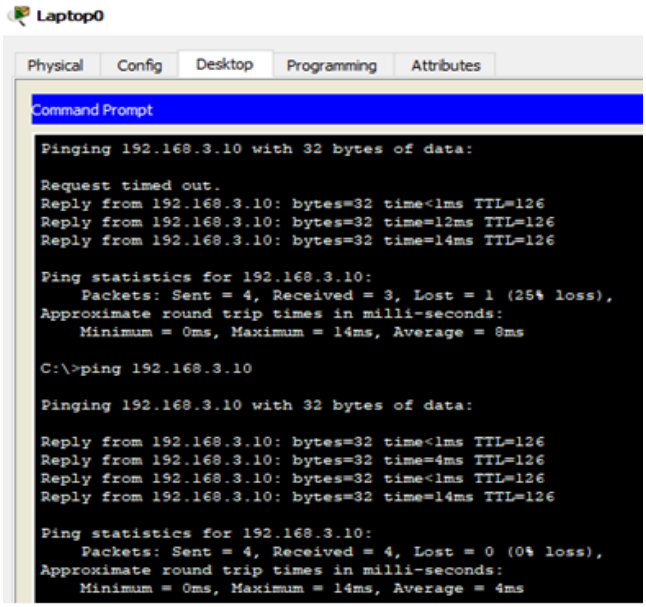

Fig.12. Connection setup through R1

Using ping command 192.168.1.10 network through ISP router as shown in Fig 13.

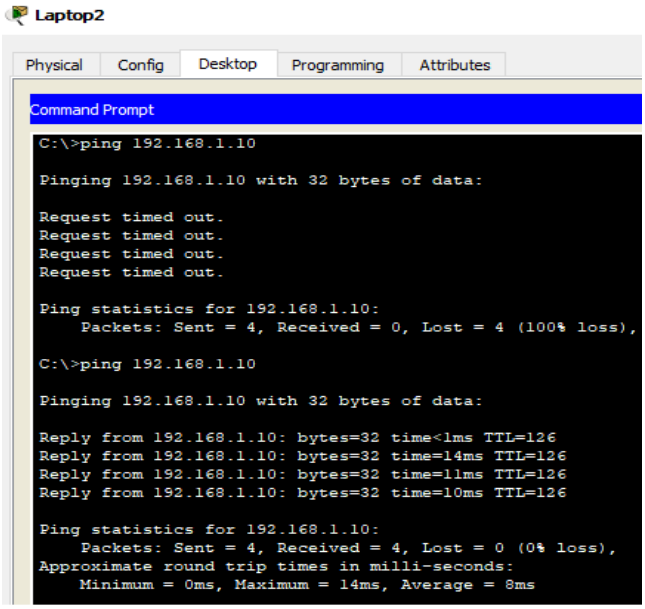

Fig.13. Connection setup through R3

Using ICMP protocol is shown authentication header (AH) and encapsulation security payload (ESP) header to provide authentication and encryption or both for packets at the IP level as shown Fig 14 and 15.

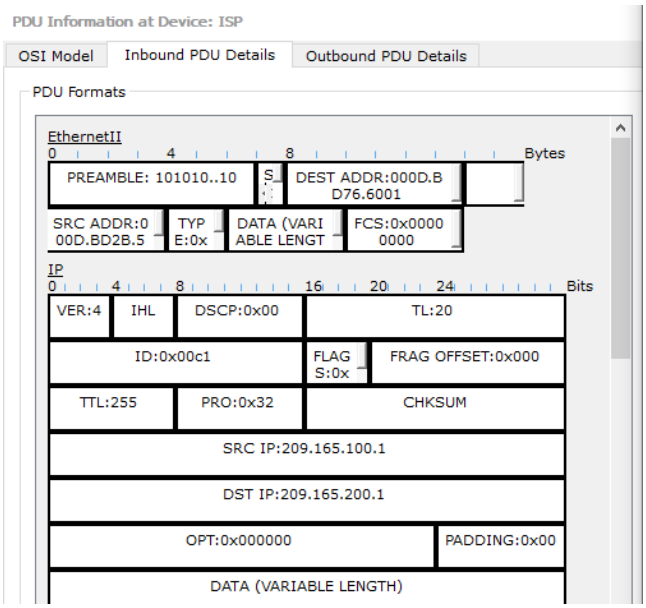

Fig.14. Authentication Header

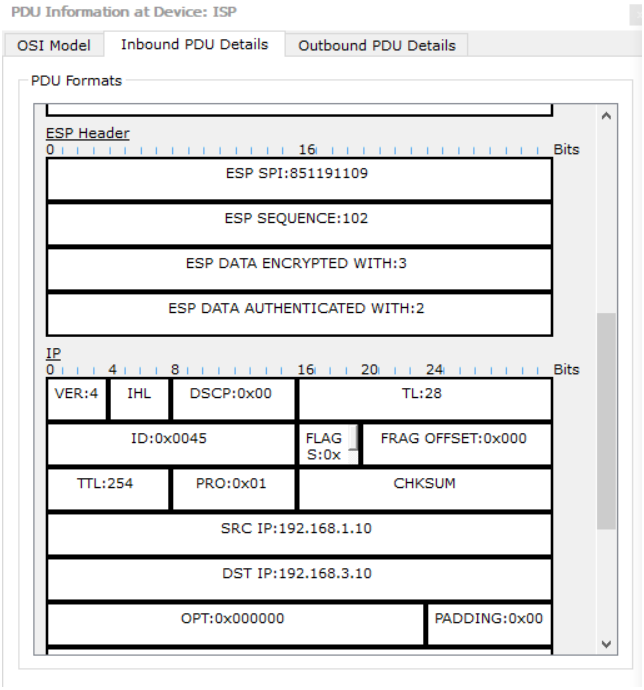

Fig.15. ESP Header

VII. Conclusion

In the paper, Security is very important in the Internet communication on the network infrastructure. The system is used static IP address on the IPSec VPN tunnels within between two routers which implement encryption security that it using cisco router device on the network layer. The IPSec protocol provides many of security in which authentication and confidently. IPSec is used to encrypt the data using encryption algorithms and provides authentication, encryption and anti-replay services. This system is built IPSec VPN tunnel between two routers (R1 and R3) and then IPSec defines two protocols is shown simulation Authentication and ESP header using ICMP (Internet Control Message Protocol) that IP security at the network layer.

VIII. REFERENCES

[1] . Cryptography and network security, MCGRAW – HILL international Editional.

[2] . A Guide to Virtual Private Network-to-network, Martin W Muthammer and others,1998 Virtual Private Networks,Charlie Scott, 2000.

[3] . I. Onut and A. Ghorbani. A Feature Classification Scheme for Network Intrusion Detection. International Journal of Network Security, July 2007.

Cite this article as :

Ei Ei Khaing, Khin Than Nyunt, Sandar Moe, Mya Thet Khaing , "Implementation of Site to Site IPsec VPN Tunnel between Routers", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 8 Issue 1, pp. 163-169, January-February 2021. Available at doi : https://doi.org/10.32628/IJSRSET218133
Journal URL : http://ijsrset.com/IJSRSET218133