iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** XI **Month of publication:** November 2024

DOI: https://doi.org/10.22214/ijraset.2024.65635

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue XI Nov 2024- Available at www.ijraset.com

Implementation of Site to Site IPsec VPN Tunnel using GNS3 Simulation

Ashraf Khalifa M. Hadood
Department of Computer Science, Faculty of Science, University of Gharyan, Libya

Abstract: ***This paper focuses on the implementation of a site-to-site IPsec tunnel to establish a secure connected link over a public network between two sites. To do so, an IP addressing plan was created and a topology was drawn to replicate a local area network between different sites, i.e., LIBYA and TUNIS. After this, an IP tunnel was set up, secure communication was established in the replicating LAN, and all packets were transferred over an encrypted form between the two different sites correctly.***

The area of this study lies in the domains of network security and VPN. When discussing the technicalities, for this research, we will establish an IP tunneling over an encryption layer. For this task, we will implement the Internet Protocol Security (IPsec) suite to authenticate and encrypt the traffic before encapsulating the actual payloads for the connected link on the OSI model Layer 3. After setting the required authentication and encryption methods over the connections, a secure link can be established to share the data neighborly in a public environment. A secure VPN site-to-site link will provide high-quality dedicated bandwidth WAN links to the users, which are considered significant for the network architecture of internetworking. As a result, secure communication features utilizing VPN site-to-site IPsec encryption play a vital role in disaster recovery between the different sites or the replication of services and data for business operations and communications. This paper recommends that it is essential for a growing organization to make their respective communication secure and implement alternative ways to manage, maintain, and control the secure communication environments.

Keywords: IPsec, Site-to-Site VPN, GNS3, IKE, ESP, AH

I. INTRODUCTION

Data is the most vital thing in today's working environment as it lets us easily access information whenever and from wherever needed. It has become essential to share the data between two different sites or networks and thus has led to the creation of a Site-to-Site IPsec tunnel for secure transmission of the data. Businesses are always on board with new and emerging technologies as it is a great solution for safe communication when the physical media is not available, such as satellite links or the internet. They take advantage of private networks which are either implemented using the normal broadband service or private links not accessible to everyone. This paper will cover the various aspects of the Site-to-Site IPsec tunnel connections and how it is configured in real-time practice. Following are the sequential stages for making a successful tunnel connection:

1) Create a virtual firewall to protect the networks located at each site.
2) Design a network connection that will connect two virtual firewall networks.
3) Finally, pass the necessary traffic to create a tunnel between the two sites.

The authentication part can be done by checking a password or by exchanging certificates. These certificates are used for authentication in the Site-to-Site IPsec tunnel. This can ensure the confidentiality of the data file transferred from one network site to the other using the Site-to-Site IPsec tunnel. As IPsec ensures confidentiality data is not accessible to any unauthorized person, integrity data is not changed during transmission, and authentication data is being transferred from the particular device it should. IPsec is designed to work using encryption services such as 3DES, RC5, and AES. IPsec can also use SHA1 for hashing techniques and HMAC for making complex authentications. The same concept is implemented in Site-to-Site IPsec tunnel construction.

II. KEY CONCEPTS AND BENEFITS

Site-to-Site IPsec tunnels are secure connections established between communicating corporate networks or sites. IPsec stands for Internet Protocol Security. It is a protocol suite that is designed to secure data as it is transmitted between hosts. Generally, it provides the following for packets of data: encryption, which provides data confidentiality by making the data unreadable when packets are intercepted by unauthorized users; authentication, which verifies that the sender of the data is who they say they are and not an imposter; integrity,

which ensures that the data was not tampered with in transit and is still in the same state as it was when sent by the originating host. In conclusion, protecting data is essential when there is a need to transmit data between parties over an insecure network. By transmitting data between networked devices in an encrypted manner, an organization can protect the data in transit and prevent breach of contractual obligations or sensitive client information. IPsec can be used to satisfy security policy requirements. Utilizing IPsec with pre-shared keys or digital certificates can ensure non-repudiation by providing data integrity and authenticating network devices. IPsec can effectively be utilized due to the following key reasons: there is a single network engineer responsible, and the skills of the engineer to manage an IPsec deployment are confined to those of the focus of this report.

III. OVERVIEW OF IPSEC

This paper combines theory and practical work in the design and implementation of secure communication using IPsec. First, the key concept of IPsec is discussed, followed by a practical tutorial on how to implement IPsec. The tutorial is a step-by-step procedure that simply accomplishes the end-to-end execution of IPsec and explicitly avoids detailed configuration. The concept of IPsec is introduced with an emphasis on providing cryptographic security to IP datagrams. The security architecture is analyzed, and the possible alternatives to protect communication through IPsec are proposed using emulation tools. Finally, the main limitations and future work are presented.

The Internet Protocol Security (IPsec) is a suite of architectural protocols proposed to add cryptographically based security services to the Internet Protocol Suite. The concept of IPsec is to encrypt at the IP layer, the original network at the origination point of the IP communication, and then to resume it at the endpoint. In other words, the original communication between the communicating points is encrypted by the IPsec gateways. After transiting the untrusted network as encrypted communications at the source, the IPsec packet structure is then decrypted at the destination. The use of cryptographic protection for communication is a more efficient approach as the information passes through a highly trusted network, allowing us to treat the remote nodes as one network. The devices appear as a network to the upper-level protocols, and the network structure is completely hidden from the other nodes. The secure virtual network is known by the term tunnel. When IPsec packets go through a LAN, the packets are typically handled without additional configuration as the LAN devices are trusted.

IV. MOTIVATION OF STUDY SITE-TO-SITE IPSEC TUNNEL

This setup was carried out in order to solve the following issue: by implementing the tunnel over the internet or any public network that is cheaper than dedicated lines, the cost of establishing communication between two offices that are far apart can be reduced. As well as being cheaper, the management of the public network can be transferred outside the responsibility of the operator. The operator only has to worry about forwarding traffic. Through the data plan that we use, it is estimated that it is done to reduce the percentage of the budget that must be issued annually by our agency to the operator in providing communication services to each research institution, government department, or joint project.

The configuration of the Private Address group must be the contact of the IP address that is installed on the two paths that will implement the tunnel. Each group must be made on both sides. Configuration of packets that will travel between the two points to implement the tunnel if it is not installed on the path. However, to provide clarity and to facilitate understanding of the concept, it is expected that the recipient does not have to carry out any additional issues.

V. INTERNET PROTOCOL SECURITY (IPSEC)

IPsec is a protocol suite that authenticates and encrypts the data transmitted between the participating peers. IPsec runs on the hosts and gateways. It uses two protocols, AH (Authentication Header) and ESP (Encapsulating Security Payload). AH provides authentication for the entire packet of IP data and protects it from modification. ESP encrypts and authenticates the payload only and provides an additional mechanism specified in the IPsec protocol suite. The IPsec protocol is used to provide security services at the inbound and outbound processing of the IPsec peers and to ensure that the IPsec peers establish a security association for protecting the communication.

Before setting up this tunnel, we need to understand two concepts. The first is encryption, which is a method developed to convert transmitted data from one form to another, so that unauthorized persons cannot understand the data. The second concept is the secure tunnel, which is an extension of a private network that uses a public network to create a secure site-to-site or site-to-remote connection. In the IPsec channel, after the ESP or AH mechanisms create a security association (SA), they exchange their IPsec attributes and the encryption algorithm used to exchange the symmetric key after the key is obtained. Encrypt/Decrypt creates a secure data packet to be transmitted. The IPsec concept includes a set of Internet Protocol (IP) extensions.

These protocols are required to add security protection to standard IP and are implemented at the Internet Layer. They provide data confidentiality, data integrity, access information security, and source authenticity of the communication path. IPsec is a suite of security protocols and algorithms that are implemented within the IP protocol stack. IPsec is composed of two parts: AH and ESP. AH is a protocol used to provide integrity, data origin authentication, and data retrieval. AH does not provide confidentiality but offers transmission security for the transmitted data. On the other hand, ESP provides integrity, data origin authentication, and data confidentiality. It handles packet payloads, headers, and provides encryption and packet authentication. Within the scope of this text, ESP has been selected for the remote site VPN connection scenario.

VI. IPSEC VPN

Replace the tunnel IP with the Windows VPN Server's LAN adapter IP. Add a static route to the Windows VPN Server's LAN for all post-VPN hosts to find the tunnel hosts in GNS3. Add allow security policies for GNS3 tunnel to the Windows 2008 VPN Server's LAN adapter. Modify the Windows Server's IPsec settings. Configure IPsec for VPN site-to-site connectivity. When setting up a VPN device, you must enter the information from the configuration file.

Example Input: crypto ikev1 policy 1 encryption 3des hash sha group 2 lifetime 86400 crypto ikev1 enable Outside crypto ikev1 key shared ip crypto ipsec ikev1 transform-set esp-3des esp-sha-hmac crypto map 1 ipsec-isakmp set peer set transform-set match address access-list extended permit ip 172.16.0.0 0.0.0.255 255.255.255.255

VII. IPSEC PROTOCOLS

IPsec protocols provide security services at the IP layer, which are implemented by other parameters within the IP packet. Two work modes of IPsec protocols are transport and tunnel mode. Tunnel mode is applied here. ESP is the main protocol and provides most of the security services of IP. It offers data integrity, privacy checking, and authentication for IP packets sent through the network. It also supports traffic flow confidentiality between two hosts. AH only supports IP packet integrity checks and authentication. The simulation environment doesn't simulate real data flow between two or more sites, so there is no high performance requirement for protocol selection. But considering the implementation convenience of ESP, the ESP protocol is selected. Configured ESP provides this site-to-site network secure transmission, but without using any encryption. ESP supports payload flow in encrypted and non-encrypted modes.

VIII. IPSEC AND TCP/IP LAYER

First, the IPsec protocol will be examined due to its structural simplicity, followed by the security association of the IKE protocol. A site-to-site IPsec tunnel is configured, as well as the implementation of the internet tunnel. Finally, data transfer through the secure link will be presented. IPsec operates at both the TCP/IP network level and the firewall level. The IPsec protocol is a set of extensions on the IP network layer, providing semitransparent security and network layer services. The development of IPsec changes the paradigm from secure applications to a secure IP communications channel for the implementation of network layer services.

The various alternative operating modes of IPsec, along with their associated protocols and cryptographic implementations, involve at least four different functions: maintaining security association integrity, ensuring confidentiality of traffic, ensuring message integrity and origin, and managing traffic addresses and protocols. IKE provides a protocol solution for managing security associations and key management functionalities of IPsec. The combination of the operating modes creates an IPsec channel. The IPsec channel extends the basic end-to-end data communication service compatible with the network layer. Data flow security associations can be established between the operating modes and the applied security processing sequence, or between the transport and tunnel mode headers before transmission using either the AH or ESP protocols. IKE and ISAKMP can be used to establish and negotiate security associations, with ISAKMP translating the required IKE security associations and negotiating a shared access key for use by the ISAKMP security association.

IX. IPSEC ROADMAP

The most widely used security standard in virtual private network design and cloud data protection is IPsec, which stands for Internet Protocol Security. IPsec uses a framework of open standards for ensuring private, secure communications over IP networks through the use of cryptographic security services. This paper is aimed at implementing a Site-to-Site IPsec VPN between two remote sites of a telecommunication service provider, ensuring the interconnection of private networks through the use of Virtual Private Network.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue XI Nov 2024- Available at www.ijraset.com

IPsec is a secure mechanism that provides security services for IP datagrams and operates at the network layer. It ensures that packets exchanged over an IP network are protected from forgery, replay, and eavesdropping. IPsec can be used to secure communications between any pair of devices that are both connected to the same IP network, such as host-to-host, gateway-to-host, or gateway-to-gateway. When it is used to secure the communication between computers, it is typically referred to as either host-to-host security or remote-access security. IP Security is an open-standards security framework that enables assured data communications over IP-based networks; it was specifically designed to secure packet-based data flows in the networking layer and therefore support the use of other application protocols that are built on top of IP.

X. SIMULATION TOOLS USED

In this paper practical implementation of IPSec site to site carried out using GNS3 software tool to design and verify the proposed network

Firstly, the scenario of Site-to-Site VPN IPsec tunnelling is explained in detail. We use the inbuilt Firewall/IPS and IPsec features of Cisco C7200 series routers for our implementation. All the inbound traffics to two routers are observed and the trusted interfaces are allowed to connect. In this work, the encryption parameters are configured on router R1 for IPsec tunnel as shown in figure(1) the network diagram create an IPsec VPN tunnel between the two sites. The Cisco routers and Cisco All traffics received by the router's interface are observed to allow only the IPsec secure tunnel data. The other traffic will be dropped

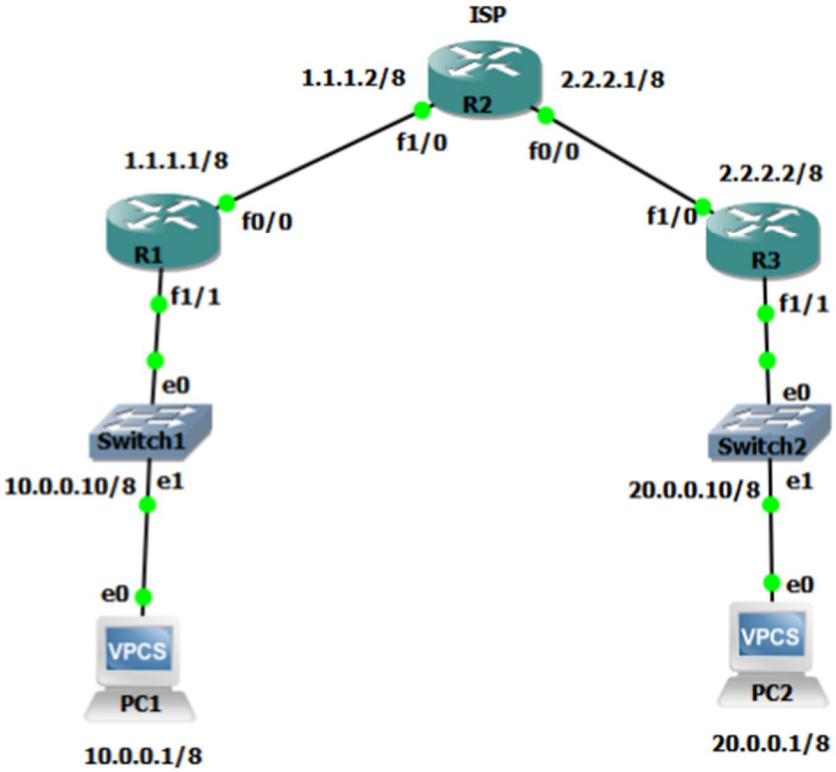


Figure (1) IPsec VPN Topology

A. Implementation and Configure IPsec site-to-site VPN

Configure an IPsec site-to-site between R1 and R3 to make to secure connection between LAN1 of R1(10.0.0.1) and R3 (20.0.0.1)

Process of making an ipsec VPN can simplified by following the sequence of configuration.

1) Define isakmp credentials which are to be used for key exchange
2) Define IPsec credentials, which are used in data exchange.
3) Define interesting traffic using an access-list.
4) Map all the credentials of VPN in a crypto map.
5) Apply the map on interface

B. Wireshark Test

The Wireshark is used to capture the traffic between the routers to analyze the network traffic and ensure the work of the security strategy. Figure (2) shows the capturing of data traffic between router 1 and router 3 that presents the ISAKMP process for negotiation, establishment, key management between the two routers. Figure (3) shows that the data traffic between the routers is encrypted with ESP.

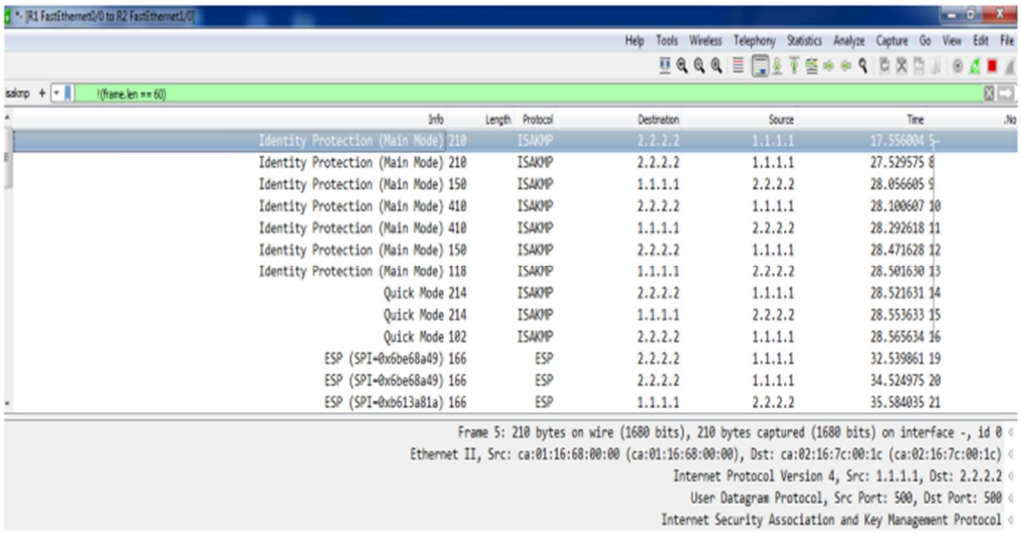


Figure (2) Capturing Data of ISAKMP

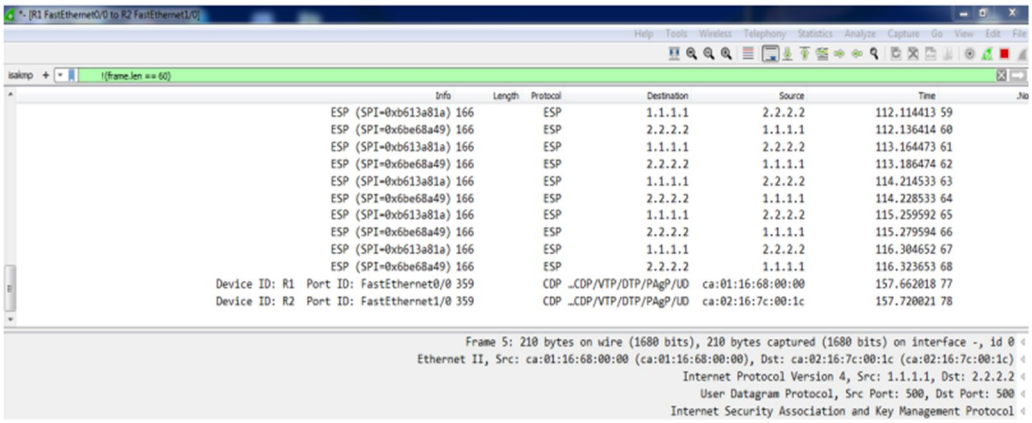


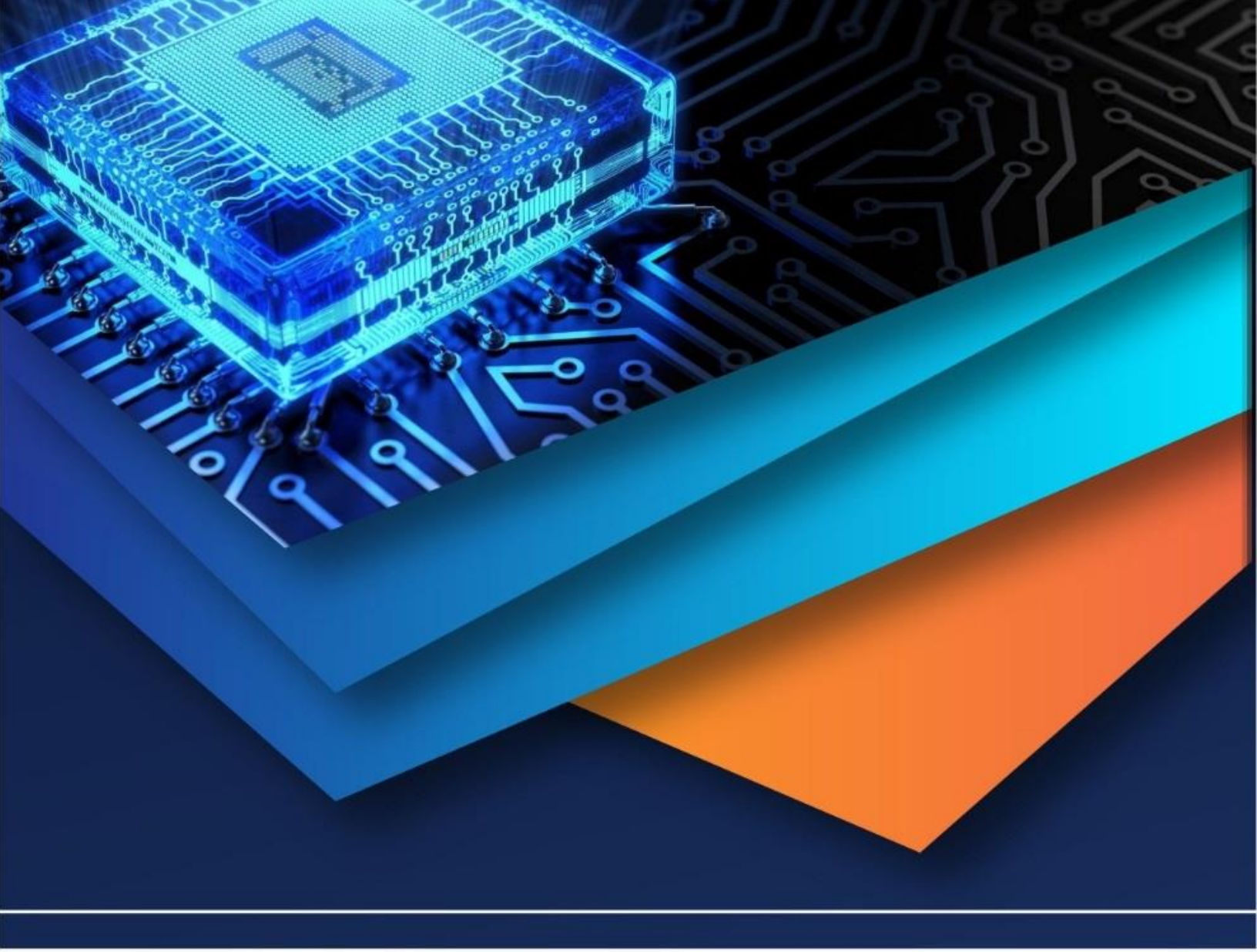
Figure (3) Capturing Data of ESP

XI. CONCLUSION

This paper is an explanation and a discussion of IPsec protocol. It includes the process of the IPsec implementation system. The paper was to demonstrate the VPN service and to consider the IPsec VPN protocol for securing two-site connection in remote areas. Sharing information or connecting branch offices from one place to other places over a public network is always a risk of injecting, altering or modifying the original data. Enterprise networks are the most common targets for hackers in order to abuse the information or to acquire the financial information. In general, an enterprise uses the WAN service, provided by ISP to connect to their branch office. On the other hand, the WAN cost is higher than VPN cost and there is a risk of security threats when the data transfers over a public network. The main goal of this paper it is to implement VPN network using IPsec tunneling mechanism using GNS3, the testing shows the successful verification of the security strategy of IPsec and data packet processing under using security protocols.

REFERENCES

[1] S. C. Forbacha and M. J. A. Agwu, "Design and Implementation of a Secure Virtual Private Network Over an Open Network (Internet)," American Journal of Technology, 2023. gprjournals.org
[2] B. P. Kushwaha, R. K. Singh, and N. Varghese, "Integrating social media and digital media as new elements of integrated marketing communication for creating brand equity," … & Communication, 2020. researchgate.net
[3] U. Modibbo, M. Mohammed, and U. Umaru, "Designing and Implementation of Site-to-Site Ethernet Tunnel Using Internet Protocol Security," Foundation Journal of ..., 2024. sfjesgs.com
[4] A. M. Albayati and F. Zarai, "Protecting Communication Situations Using IPSec and IKE Essentials and Applications," Babylonian Journal of ..., 2024. mesopotamian.press
[5] NQ Tran, KDL Nguyen, and CDT Thai, "Implementation and Evaluation of IPSec in an NFV-Based Network," in *International Conference on …*, 2023. [HTML]
[6] N. K. Shingari and B. Mago, "The Importance of Data Encryption in Ensuring the Confidentiality and Security of Financial Records of Medical Health," in … on Interdisciplinary Approaches in …, 2024. [HTML]
[7] J. Lastinec and L. Hudec, "A study of securing in-vehicle communication using IPSEC protocol," Journal of Electrical Engineering, 2021. sciendo.com
[8] J. C. Mwape, "Performance evaluation of internet protocol security (IPSec) over multiprotocol label switching (MPLS).," 2024. dspace.unza.zm
[9] M. Z. Islam, M. A. R. Khan, M. I. Hossain, and R. Hossain, "Analysis the importance of VPN for creating a safe connection over the world of internet," 2023. academia.edu
[10] S. T. Aung and T. Thein, "Comparative analysis of site-to-site layer 2 virtual private networks," in 2020 IEEE Conference on Computer, 2020. meral.edu.mm
[11] S. H. Alharbi, A. M. Alzahrani, T. A. Syed, and S. S. Alqahtany, "Integrity and privacy assurance framework for remote healthcare monitoring based on IoT," Computers, 2024. mdpi.com
[12] MHA Hamied, "Using an IPsec VPN to Secure The Network Communication in The Smart Grid," in 2023 1st International Conference on Advanced …, 2023. [HTML]
[13] S. Qu, Y. Cheng, and X. Bai, "Research and application of encrypted data transmission based on IPSec," in Proc. 3rd Int. Conf. Data, 2023. [HTML]



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY