Advances in Social Science, Education and Humanities Research, volume 410
1st International Multidisciplinary Conference on Education, Technology, and Engineering (IMCETE 2019)

Network Integration and Security Using IDS and Tunneling Methods

1st Edy Nasri
Departemen Ilmu Komputer, Program Studi Teknik Informatika, Sekolah Sarjana
Universitas Banten Jaya
Banten. Indonesia

2nd R. Kania
Departemen Ilmu Komputer, Program Studi Komputer Akuntansi, Sekolah Sarjana
Universitas Banten Jaya
Banten, Indonesia

3rd S Tsauri
Departemen Ilmu Komputer
Sekolah Sarjana
Universitas Banten Jaya
Banten, Indonesia.
sufyan.tsauri45@gmail.com

***Abstract*—Security on computer networks is very important to be monitored so that network traffic runs well because a good network architecture can support existing business processes to carry out their duties and responsibilities In a network system a good security is needed so that it can support the company's business processes. The research location is in PT ABC where there are often difficulties in accessing information due to network disruption, the implementation of network security is still weak and risky to attacks, there is no network monitoring system to monitor traffic based on these problems, it is necessary to design a network integration system with using EoIP and IPsec tunneling methods, implementing IDS (Intrusion Detection System) in network security with snort and establishing a network monitoring system with The Dude. Methods of data collection using literature studies, field analysis and conducting interviews with relevant parties. The development method system uses NDLC (Network Development Life Cycle). The results of the study it was concluded that the application of IDS and Tunneling network security integration systems can overcome the problems that occur so that business processes can run well.**

Keywords: computer network, IDS, tunneling

I. INTRODUCTION

The development of internet science and technology in people's lives is very rapid and to deal with new concepts in the development of world technology that can be known as society 5.0 in which there is a rapid development of the Internet of Things, including the development of global information where all life requires an internet network so that the threat to the security of the international network is increasing in the internet network there are several threats to steal, destroy, force to obtain unauthorized data.

From the above explanation we have a problem to integrate between one company with another or also between the head office and branch offices, because of this integration through the internet network, network security problems arise, so we approach the tunneling method of a concept offering that can be implemented into the integration system, in this method offered easy and fast data and information access through Ethernet Over IP (EoIP) and IP Security (IPSec) approaches. For the method of monitoring network activity using the Intrusion Detection System (IDS) approach with this method IDS will provide information to monitoring officers who have been given a rule.

II. METHODS

The problems that we are exploring cannot yet be integrated between the head office and branch offices and to minimize the risks to network security and data traffic monitoring, we conduct the following research:

A. Networking

A form of telecommunications that allows computers to exchange data. Purpose: so that every part of the computer network can request and provide services.

B. Intrusion Detection System

A system that monitors network traffic and monitors suspicious activities in a network system. If suspicious activities are found related to network traffic, IDS will alert the system or network administrator

C. Server

A place filled with various kinds of information, where the server has the main task of providing a service for clients connected to it.

D. Snort

IDS Snort works by analyzing protocols, searching and matching content, and is actively used to detect an attack.

E. Tunneling

The technique of encapsulating all data packets into other protocol formats to interconnect can share files, Voice Over Internet Protocol (VOIP), and exchange information.

III. RESULT AND DISCUSSION

To apply this research we use and configure we provide the following conditions:

- Mikrotik
- The Dude
- Snort
- WinPCap

To illustrate the results of this study:

A. Deployment Diagram IDS and Tunneling

Deployment diagram for mapping where each hardware and software component is installed or placed in a node, to show the communication relationships between device

components and to show the structure of the existing system [1].

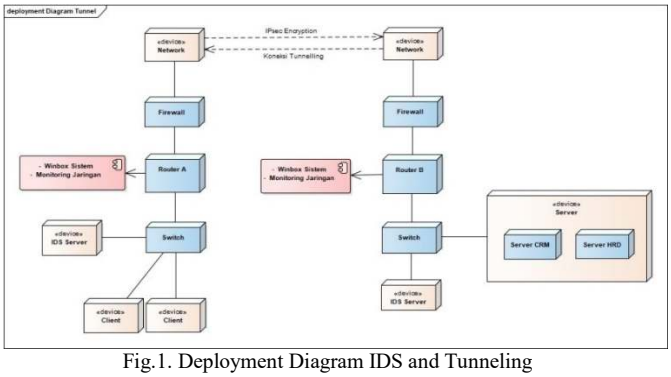

Fig.1. Deployment Diagram IDS and Tunneling

B. Prototype Design

Explain prototyping for system integration consisting of clients, switches, router boards, internet, tunneling, officedom, IDS Systems.

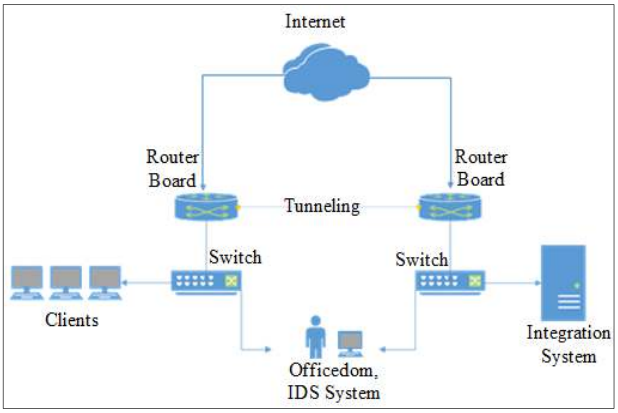

Fig.2. Prototyping Design

C. Network EoIP Tunneling + IPSec

Network EoIP (Ethernet over IP) Is a protocol of the proxy routers that has the function of developing a Router network tunneling router, to build routers in the Head Office and routers in the branch office [2]. IPSec (Internet Protocol Security) is a set of protocols defined by the Internet Engineering Task Force (IETF) to secure packet exchanges over IP / IPv6 networks that are not protected like the Internet [3].

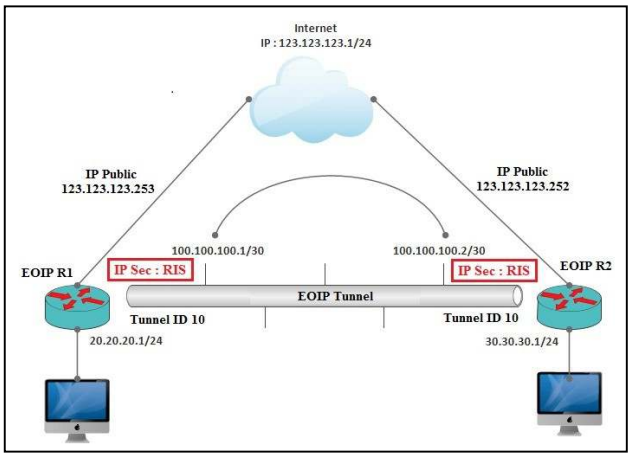

Fig.3. Topology Network EoIP Tunneling + IPSec

To develop a communication network between branch offices and the central office must be connected to the internet, tunneling is one of the ways to develop a router for TCP / IP connections, tunneling methods can exchange information and exchange files.

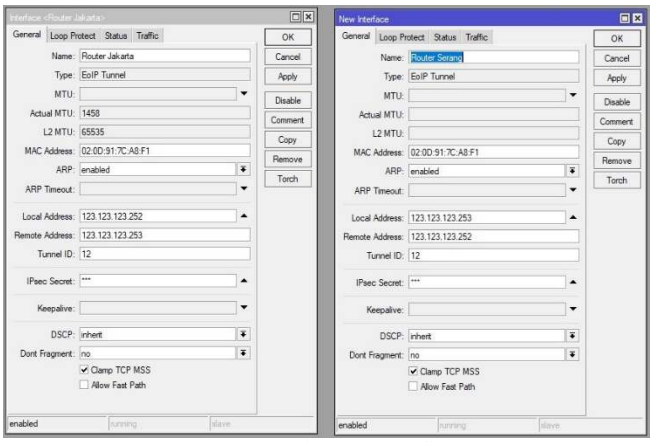

Fig.4 . Menu Network EoIP Tunneling + IPSec

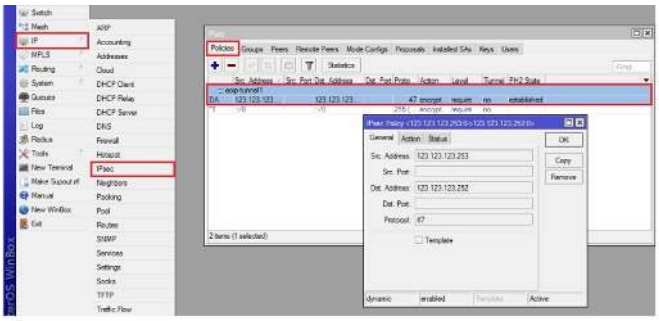

Fig.5 .List IPSec

Successfully implemented traffic Tunneling head office and branch office

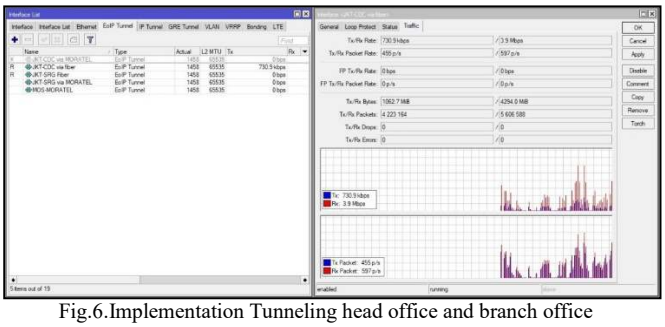

Fig.6.Implementation Tunneling head office and branch office

D. Snort Operating

Ada 3 mode snort operating:

1) Sniffer mode, to see packets that are passing through the network

Type on cmd : cd:\snort\bin

snort -v

snort -vd

snort -vde

snort -v -d –e

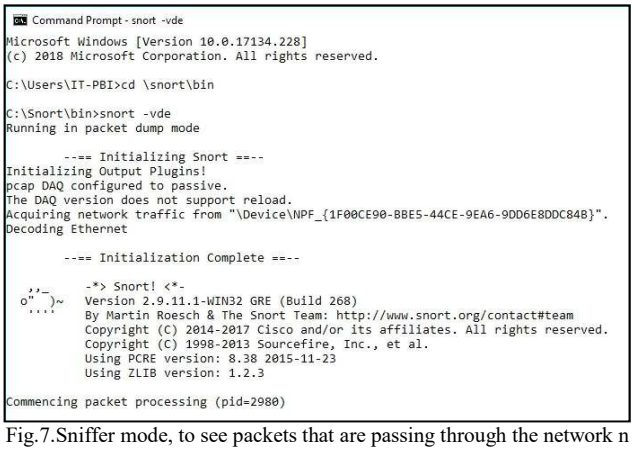

Fig.7.Sniffer mode, to see packets that are passing through the network n

2) Packed Logger Mode, to record all packets that pass *through the network for analysis.*

Type on cmd : cd:\snort\bin

snort -v

snort -vd

snort -vde

snort -v -d -e

Fig.8.*Packed Logger Mode,* to record all packets that pass through the network for analysis.

3) Intrusion Detection Mode, to detect attacks carried out through computer networks

Typing On cmd : cd:\snort\bin

snort -dev -1 c:\ snort\log –h 192.168.100.1/24 - c c:\snort\etc\snort.conf

Fig.10. *Intrusion Detection Mode,* to detect attacks carried out through computer networks

E. Mikrotik-The Dude

Performing management monitoring the network, detecting devices connected to one segment management, to compile network topology and to provide information if there are problems with devices connected to the network. Besides discovery systems can be done as well as brand layouts, remote systems.

1) Monitoring

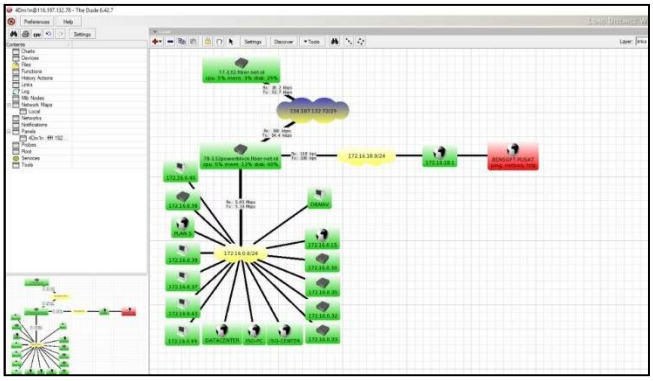

Fig.11.Management Monitoring Network

2) Discovery: to add devices that will be monitored, within the parameters performed are network scans to scan devices that are on the network.

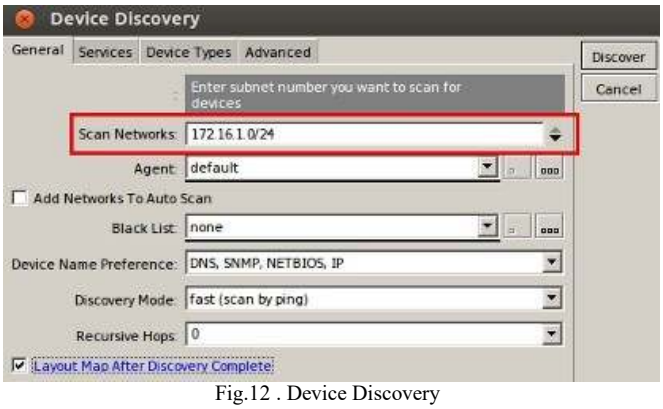

Fig.12 . Device Discovery

Network Map

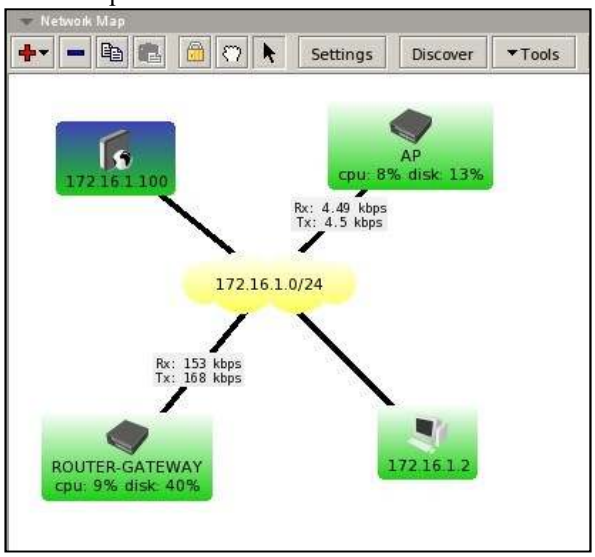

Fig.13.Result Scanning

Monitoring Device, can see the current service status whether the device is active or down.

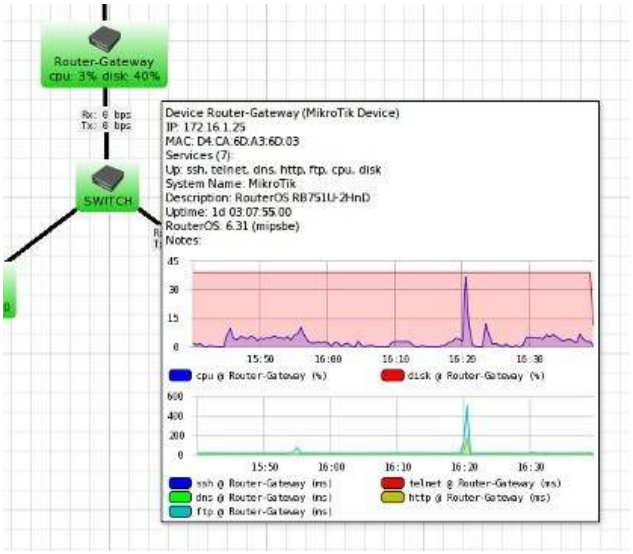

Fig.14.Monitoring Devices

IV. CONCLUSION

In the above research conclusions can be concluded in the Intrusion Detection System (IDS) method can provide information for prevention in network security, as well as making it easier to monitor the network so as to speed up if a trouble or attack occurs, the IDS method can also add the intrusion prevention system (IPS) method. In the snort model can be divided into 3 models, namely sniffer mode to monitor packets that pass through the network, packet logger mode to record the traffic that passes through the network and intrusion detection mode to detect attacks that pass through the network. In the Tunneling method it can facilitate the integration and access of data more effectively and efficiently, in the concept of tunneling it can also use VPN, IPIP, IPsec and others as such. Adding the Mikrotik-the dude method for network monitoring and making it easier to get information about network conditions.

ACKNOWLEDGMENTS

In this study the researcher realized that during the process many encountered difficulties, obstacles. In these difficulties and obstacles will not be resolved and realized by researchers without the help and encouragement of various parties.

REFERENCES

[1] OReilly.Learning.UML.2.0.Apr.2006
[2] http://mikrotik.co.id/artikel_lihat.php?id=91
[3] https://wiki.mikrotik.com/wiki/Manual:Interface/EoIP