IMPLEMENTATION AND ANALYSIS VPN AS VOIP COMMUNICATIONS SECURITY ON CLOUD NETWORK

Bima Sanjaya[1], Dr. Ir. Rendy Munadi, M.T. [2], Leanna Vidya Novita, S.T., M.T.[3]
[1,2,3]Telecommunication Engineering, Faculty of Electrical Engineering, Telkom University.
[1]bimasnjy@gmail.com, [2] rnd@telkomuniversity.ac.id, [3] lvy@telkomuniversity.ac.id

Abstract— Security becomes a very vital part in the development of computer networks, especially in VoIP Communication and Cloud Network. In this final project is implemented Infrastructure As A Service on Cloud Computing system to running a VoIP server and OpenVPN VPN systems, SSTP, and IKEv2 / IPSec as supporting VoIP communications security and Cloud systems. Security aspects will be analyzed VoIP server from DDoS attacks and VoIP communication with sniffing method will then try backing playback RTP packet sent. Included also will be analyzed aspects of performance VoIP communications itself. Scenarios will be done with and without the use of VPN systems.
From the test results it can be concluded that the addition of VPN on the server Asterisk-based Cloud Computing will add aspects of integrity, confidentiality, and authentication on VoIP communications, while the results of measurements of quality of VoIP communications obtained lowest quality of QoS is delayt 44 ms, jitter 0.99 ms, packet loss 0% and MOS 4.01. The performance of various VPN systems almost the same and VPN solutions can not only secure communications of VoIP itself but also useful for securing VoIP servers from DoS attacks.

Keywords—VoIP; Security; DDoS; VPN; QoS

I. INTRODUCTION

Computer network technology today is experiencing very rapid growth, where the security becomes a very vital part, and therefore needed a system that could ensure the security of such technology. Virtual Private Network is a tekologi that build a secure network connections to pass through a public network such as the Internet. Voice communication is also an integral part of the telecommunications world. With the development of Internet technology, the discovery of VoIP services. For ease and release the dependence on physical servers, has grown too Cloud Computing technology, which can allow to build server-based VoIP Cloud Computing.

On the other hand communication using VoIP do not have a guarantee of packet data in each voice communication is done, allowing any party that does not have the authority to conduct interception of communications is being done [1]. In the Cloud Computing system is also highly vulnerable to eavesdropping because the cloud system can be used by many people in the Cloud system. Then in need of security methods that include Cloud based VoIP communications security and also include the security of communications with cloud system itself.

There are several systems that can be used to secure VoIP communications, one of them with a Virtual Private Network techniques. In the VPN systems provide encryption features to keep authentication and message integrity, including security in the signaling process, so if the implementation of Virtual Private Network will provide security in VoIP communications. Therefore, in this final task was made a security implementations VoIP communication based on the cloud using Virtual Private Network based on Open VPN, SSTP, and IKEv2 / IPSec to secure the payload sent and process signaling is done so that VoIP communication becomes more difficult to be tapped.

II. BASIC THEORY

A. Cloud Computing

Cloud Computing is a computing technology where all the resources and computer resources be it memory, application processor, network, operating system, which is used presented virtually with pattern remote access so that we could access the service anytime, anywhere as long as we are connected to the Internet network [3].

B. Voice Over Internet Protocol

Voice Over IP is a technology delivery of voice (it is also possible for multimedia data types other) in real time between two or more users / participants to pass through the network using protocols Internet, and exchange of information needed to control the delivery of voice them. [14]

C. Codec

Codec is a technique of encoding sound into digital code that can be sent in a computer network.

D. Quality of Service

QoS is a parameter that indicates the ability of a network to provide services on a variety of technology platforms [7]. There are several parameters of QoS in VoIP communications, Delay, Jitter, Packet Loss, and MOS

E. Virtual Private Network

Virtual Private Network is a private network that uses public infrastructure (typically the Internet for) for connecting between the user and the website [8]. As the name indicates the VPN connection using "virtual" routed through the Internet from a private network to the destination site and the destination user. VPN can work on wireless and wired networks [14]. A VPN maintain data security using multiple security procedures and tunneling protocols [8].

OpenVPN originally developed by James Yonan and is published under the GNU General Public License (GPL). This technique uses several security protocols including SSL / TLS for key exchange. This technique can also be menggunakna various encryption techniques with the most powerful 256bit AES.

Secure Socket Tunneling Protocol (SSTP) is one of the techniques of communication establishment of the VPN tunnel

which provides a mechanism to send PPP or L2TP traffic passing through the canal SSL 3.0. SSL provides transport-level security with a key negotiation, encryption, and traffic integryti checking. It uses SSL protocol on TCP port 443 that make SSTP can pass through any firewall and proxy.

Internet Key Exchange also called the Internet Security Association and Key Management Protocol (ISAKMP) is the negotiation protocol that lets two hosts agree on how to build an IPsec Security Asossiation security association (SA). IKE creates the cryptographic key used for IPsec authentication, negotiate and distribute the IPsec encryption key, and automatically establish IPsec security associations.

F. Security Aspect

Authentication. This aspect relates to a method for stating that the information truly genuine, people who access or information is really the question, or the server that we contact is really the original server.

Confidentiality. The main core aspects of privacy or confidentiality is an attempt to keep the information from people who are not entitled to access the information. Confidentiality is usually associated with the data that is provided to other parties for specific purposes.

Integrity. This aspect is emphasized that information should not be altered without the permission of the owner of the information

G. Denial Of Service

Denial of Service or commonly called DoS is an attack method in a computer network that aims to create a server, network, and transmission overload which make the system dead. There are a few techniques one Ping Flood DoS.

III. PLANNING AND IMPLEMENTATION

In the process of designing a system, it takes a well-structured scenario. To facilitate the implementation of the required topology design process which helps in understanding the design process to be created.

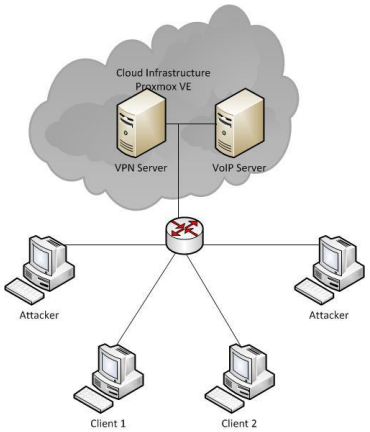

Fig 1. Network Topology

Implementation of the system development and design of VoIP and VPN servers, using cloud servers. Used also two client computers to 2 VoIP client. There are also computer-based Windows and Linux attacker. All of these devices connected to the router.

Testing is done with the following scenario:

1. Without using a VPN solution
2. Using a VPN Solutions

At this stage of system testing will be conducted the same test on each scenario are:

1. Communication Server VoIP Security Test

   This test will be conducted on the ICMP Flood to the server when using VPN or VoIP without using a VPN. Attacks using 2 PCs as DoS Attacker. At maximum condition of each PC attacker will send ICMP packets of 100Mbps to flood the VoIP server and VPN
2. Test the security of VoIP communications

   In the second test will be done tapping on the packets sent by the VoIP technology. Tapping use several tools, wireshark for sniffing VoIP payload, sipcrack and Cain & Abel for a username and password sniffing.
3. Test system performance VPN

   In this test will be tested several aspects of performance VPN protocols that Connection Time, Throughput, and the CPU Usage on each protocol VPN, OpenVPN, IKEv2 / IPSec and SSTP.
4. Test the performance of VoIP

   In the fourth test will be conducted on a VoIP service performance measurement. As for some of the parameters to be tested in this performance testing, which Opinian Mean Score (MOS), Delay, Jitter and Packet Loss.

IV. TESTING AND ANALYSIS

A. Testing Security Server Cloud against DoS attacks

At this attack will be used throughout the ICMP packet 65500 Byte. With all that, the ICMP data ICMP packets will be split into several blocks with a length of Maximum Transmission Unit (MTU) is 1500Byte. With the outbreak of the ICMP packets, the destination server will process return the package to be fragments of ICMP packets are intact. Due to the ICMP Ping process requires computing processing then ping process will take resources from the server, if the ping is done by many computer then in a certain point there will be downtime because the server can't accommodate and process the ICMP packets.

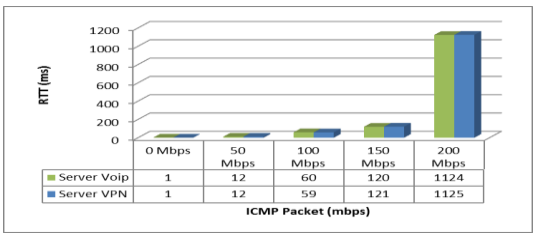

Fig. 2 Without VPN Soulution

Figure 2 looks at the system without using a VPN solution then existing VoIP server in the cloud server will be able to receive all packets from all IP addresses. So the attacker would be easily attacked by DDoS techniques to the VoIP server that is in the cloud.

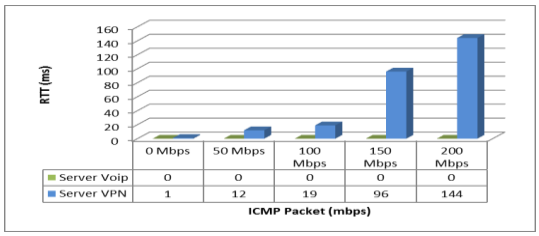

Fig. 3 With VPN Solution

On systems using a VPN solution then existing VoIP server in the Cloud server may not receive all the packets of all IP addresses. By doing so, the attacker can't be attacked with DDoS techniques to the VoIP server that is in the cloud. However, the VPN server as a gateway will still be attacked by DoS techniques. With only one server that can attacked the Cloud Computing system is more resistant than without VPN solutions.

B. Testing Against VoIP Communications Security

At this stage will be tested and analyzed the security of VoIP communication system with and without the system Virtual Private Network. At this stage will be tested some security parameters are Confidentiality, Authentication and Integrity.

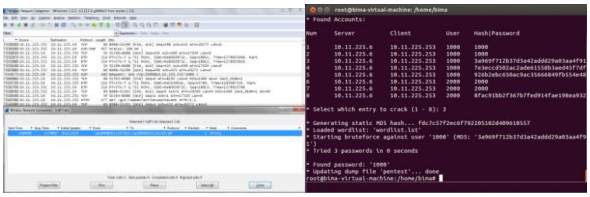

Fig 4. Sniffing VoIP communication without VPN solutions

From Figure 4 it can be concluded that without using the VPN solution, Confindentiality aspect and integrity do not apply because its VoIP communications can be stolen, and also aspects Authentication is not apply because usernames and passwords can be stolen.

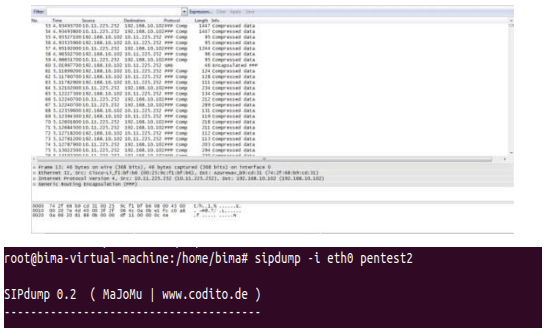

Fig 5. Sniffing VoIP communication without VPN solutions

From Figure 5 it can be concluded that when using a VPN solution as a firewall, Confindentiality aspect and Integrity will prevail because of its VoIP communications can't be detected, and also the aspect Authentication valid because usernames and passwords can't be stolen.

C. VPN Performance Analysis

Testing the connection time

Connection Time is the time for authentication between the VPN client to the VPN server in order to use a VPN connection. This measurement is performed using wireshark software installed on the VPN client. The calculation is done by calculating the difference between the first packet to packet encryption first emerged.

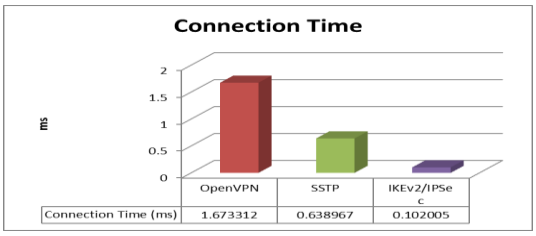

Fig 6. Connection Time

From the measurement results can be seen that the minimum connection time occurs when using connection IKEv2 / IPSec, with a value of 0.102005 ms. Highest when using OpenVPN, with a value of 1.673312 ms. And SSTP are in the middle with a value of 0.638967 ms.

Average packet length measurement

VPN packet length measurement was conducted to determine the packages sent by multiple VPN protocols, OpenVPN, SSTP, and IKEv2 / IPSec.This measurement is performed using wireshark that is installed on the client computer. And will be the average packet sent when using multiple VPN protocols.

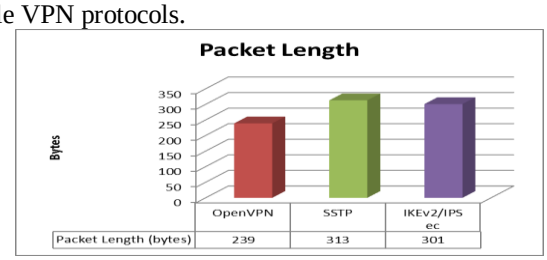

Fig 7. Average Packet Length

From the measurement results can be seen that on average the smallest packet sent occurs while using OpenVPN connection, with a value of 239 bytes. Highest when using SSTP, with a value of 313 bytes. And IKEv2 / IPSec are in the middle with a value of 301 bytes.

CPU Usage Testing

CPU Usage is the percentage of resource usage or use server capabilities at a time. Usage cpu measurement aims to determine the effect of the encryption process or encapsulation with the cpu on the VPN server.

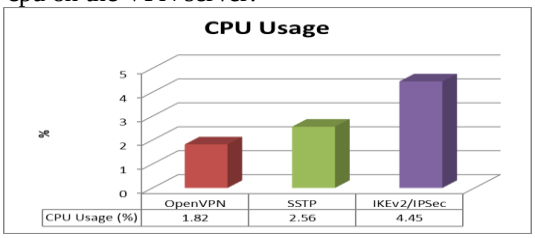

Fig 8. Average CPU Usage

From the measurement results can be seen that most low CPU resource usage occurs while the server is running OpenVPN connection, with a value of 1.82%. Peling high when using the IKEv2 / IPSec, with a value of 4.45%. And SSTP are in the middle with a value of 2.56%.

D. Measurement of Quality of Service

In this research will be used parameter one way delay, jitter, packet loss and MOS. Delay, Jitter and Packet Loss can use Wireshark and MOS can r-factor measurement.

	Without VPN	OpenVPN	SSTP	IKEv2 / IPSec
Delay (ms)	4.7202	13.4553	16.4732	44.6941

Jitter (ms)	0.6327	0.5486	0.5282	0.9911
Packet Loss (%)	0	0	0	0
MOS	4.048	4.0406	4.0381	4.0145

Fig 9. Quality of Service

Seen in Figure 9, the value of Delay when not using VPN protocols obtained at 4.47 ms, while using OpenVPN gained 13.45 ms, while using SSTP obtained at 16.47, and the latter using the IKEv2 / IPSec obtained at 44.59 ms Although both increase the value of delay , the use of a VPN system still meets the standard delay of less than 150 ms.

Seen in Figure 9, it can be concluded the average variation of the lowest Jitter occurs when VoIP communication is done using SSTP connection. And the highest occurred in the use of IKEv2 / IPSec. Jitter values that arise, without VPN solutions obtained 0.6327 ms jitter, jitter obtained using OpenVPN connection 0.5486, using SSTP connections gained 0.5282 ms jitter, and when using connection IKEv2 / IPSec obtained jitter 0.9911. Jitter occurs despite variations in the use of a VPN connection or not, but the resulting jitter values still meet the standards that must have a value below 1 ms.

Seen in Figure 9, it can be concluded packet loss does not occur in all scenarios. This happens because the simulations done on uninterrupted network or a closed network, so that all packets can be sent perfectly. In the absence of packet loss then VoIP memenui personal communication requirements for use.

Seen in Figure 9, it can be concluded relatively the same MOS value of about 4:01 to 4:03. MOS value arising from the system without a VPN at 4.0480, while using OpenVPN MOS obtained by 4.0406, while using SSTP at 4.0381 can, and when using the IKEv2 / IPSec in may 4014. All MOS calculation results can be concluded that the quality of VoIP based MOS calculation is very good. Slight differences occur because there is a difference in the value of delay.

V. CONCLUSION

Based on the results of the process of implementation, testing and analysis, it can be concluded as follows:

Implementation of VoIP-based server in the Cloud Computing Proxmox VE successful. And addition of OpenVPN, SSTP, and IKEv2 / IPSec towards Asterisk server proved safer than the Asterisk servers without using a security protocol when we use tools wireshark, cain and abel, and SIPcrack as attacking tools. Based on the evidence, OpenVPN, SSTP, and IKEv2 / IPSec provide aspects of Confidentiality, Authentication and Integrity for VoIP communications.

VoIP Server on Cloud has a vulnerability to DoS attacks if without using the VPN solution, this vulnerability can be avoided by implementing a VPN solution that VoIP servers can be hidden behind the VPN server.

On Connection Time measurement, the highest result was obtained when using OpenVPN more than 1 ms. The lowest result obtained when using the IKEv2 with 0.002 ms, and when using SSTP obtained value of 0.168 ms. On the measurement of the average packet length, highest result obtained when using SSTP with an average of 313 bytes. The lowest result obtained when using OpenVPN with 239 bytes, and when using the IKEv2 / IPSec obtained value of 301 bytes. On the measurement of CPU Usage, the highest result was obtained when using the IKEv2 / IPSec with 4.45%. The lowest result obtained when using OpenVPN with 1.81%, and the value obtained when using SSTP 2.56%.

From the scenario of measuring the quality of VoIP communication using G.711 codec ulaw, obtained the highest delay occurs when the communication system uses IKEv2 / IPSec in the amount of 44.59 ms. Lowest occurs when not using VPN for 4 ms. When using OpenVPN and SSTP respectively by 14 and 16 ms. All scenarios meets the standard for VoIP communications, below 150ms. And then the largest Jitter occurs when the communication system uses IKEv2 / IPSec is equal to 0.991 ms. Lowest occur when using SSTP at 0:52 ms. When using OpenVPN and without using a VPN system, respectively for 0.63 and 0:54 ms. All scenarios meets the standard for VoIP communications, namely below 1 ms. Packet loss does not occur there all scenarios. The measurement results show that the MOS MOS relatively equal value that is equal to 4.01 to 4.04 due to differences in delay are also very small. Has concluded that VoIP communications quality was very good.

From the above points can be concluded that the addition of security protocols in Cloud-based VoIP communications will slightly increase the value of delay, while also adding security protocols in VoIP communications impact of impairment MOS. A slight decline in the quality of VoIP communications is inversely proportional to the quality of VoIP communications security itself.

REFERENCES

[1] D. Richard Kuhn, Thomas J. Walsh, Steffen Fries, "Security Considerations for Voice Over IP Systems"; NIST Special Publication 800-58. 2011.

[2] Charlie Scott, Paul Wolfe, Mike Erwin, "Virtual Private Networks - Second Edition". 1999.

[3] Peter Mell, Timothy Grance, "The NIST Definition of Cloud Computing"; NIST Special Publication 800-145. 2011.

[4] Zoran Pantić, Muhammad Ali Babar, "Guidelines for Building a Private Cloud Infrastructure"; University of Copenhagen Tech Report TR-2012-153, 2012.

[5] O. W. Purbo, Petunjuk Praktis Cloud Computing Mengunakan OpenSource. 2011.

[6] Ubuntu, "UEC/CDInstall – Ubuntu Documentation." [Online]. Available: https://help.ubuntu.com/community/UEC/CDInstall. [Accessed: 11-November-2014].

[7] Munadi. Rendy, "Teknik Switching", Informatika, Bandung, Mei 2009

[8] Ritika, Kajal, October 2012, "Virtual Private Network". Volume 2, Issue 10, October 2012.

[9] Poonam Arora, Prem R. Vemuganti, Praveen Allani, "Comparison of VPN Protocols – IPSec, OPENVPN, and L2TP". Project Report ECE 646, George Mason University, 2001.

[10] Protocol.com, "SIP Architecture" [Online] Available: http://www.protocols.com/pbook/sip_arch.htm. [Accessed: 11-November-2014].

[11] Gifari, Johan. 2014 "Analisis dan Implementasi Keamanan Layanan Voip based on Cloud Menggunakan Secure Realtime Transport Protocol dan Transport Layer Security".

[12] Youk. Sang-Jo, Yoo. Seung-Sun, Park. Gil-cheol, Tai-hoon Kim. "Design of Internet Phone (VoIP) for Voice Security using the VPN". International Journal of Multimedia and Ubiquitous Engineering Vol. 2, No. 3, October, 2007.

[13] GEREA. Floriana, "Implementation of Cloud Computing into VoIP". Database Systems Journal vol. III, no. 2. 2012.

[14] Y.P Kosta, Upena D. Dalal, Rakesh Kumar Jha. "Security Comparison of Wired and Wireless Network with Firewall and Virtual Private

Network (VPN)" 2013 IEEE International Test Conference (ITC), Mar, 2010.

[15] Protocol.com, "SIP Architecture" [Online] Available: http://techpp.com/2010/07/16/different-types-of-vpn-protocols. [Accessed: 13-Desember-2014].

[16] Protocol.com, "SIP Architecture" [Online] Available: http://technet.microsoft.com/en-us/library/cc780018(v=ws.10).aspx. [Accessed: 13-Desember-2014].

[17] LRI.FR, "AES Encryption" [Online] Available: https://www.lri.fr/~fmartignon/documenti/systemesecurite/5-AES.pdf.

[18] Alan Kaminsky, Michael Kurdziel, Stanisław Radziszowski. "An Overview of Cryptanalysis Research for the Advanced Encryption Standard" 2010 The 2010 Military Communications Conference. 2010.

[19] Juniper, "VPN Security IKEv2 Understanding" [Online] Available: [http://www.juniper.net/documentation/en_US/junos12.1/topics/concept/vpn-security-ikev2-understanding.html].

[20] Aca Apostu, Florina Puican, Geanina Ularu, George Suciu, Gyorgy Todoran. "Study on advantages and disadvantages of Cloud Computing" Applied Computer Science and Digital Services.