PROTOTYPE OF REMOTE ACCESS VIRTUAL PRIVATE NETWORK USING SECURE SOCKET LAYER METHOD

HERWAN HERWANSYAH

JURUSAN TEKNIK INFORMATIKA
FAKULTAS ILMU DAN KOMPUTER
UNIVERSITAS KOMPUTER INDONESIA
Jl. Dipati Ukur No. 112-114 Bandung
Email: h2s_cyber@yahoo.com

ABSTRACT

VPN (Virtual Private Network) is a communications technology that enables users to be connected to a public network and use it to join the local network. This private network as if it is accessing the local network but use the public network. VPN allows formed a private data network that can be accessed through public networks like the Internet, and can only be accessed by parties who have authority. Remote Access VPN is one that serves the implementation of the VPN to access remotely to a private service that is accessed via a public network. Secure Socket Layer (SSL) VPN is a data communication protocol mechanisms that can be used in remote access VPN using the concept of asymmetric encryption for key and certificate-based mechanism. Remote Access VPN to process data communications using SSL protocol, will perform encryption on the key and the encryption of data transfer process from the server to the client or vice versa by using encryption algorithms, so that the host is connected to a VPN network can make a secure connection.

Keywords: VPN, Remote Access, SSL, Encryption

---

1. INTRODUCTION

1.1 Background Problem

An ideal network may be any link between the point to any. In the past, companies wishing to connect branch offices in a network will use the rental channel point to point (point to point) whose cost is very expensive.

In a computer network, security in transmission and reception of data is very important to ensure that the data sent does not fall into any third party, especially if the data is confidential. It is necessary for the implementation of methods to secure data on the network. Many methods can be implemented, such as the use of digital signatures, encryption or firewall installation.

Along with the proliferation of Internet use, many companies who then switch to using the internet as part of their networks to save costs. However, security problems remain the main factors in reliability in a network. Virtual Private Network (VPN) is one way to make any connections to any on the public network like the Internet, without a single client with another client to know each other which is a way to make a network is "private" and secure with the use of network public.

Today there are several techniques that are known to develop a VPN over the Internet network that is Point to Point Tunnelling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), Secure Socket Layer / Transport Layer Security (SSL / TLS) and

Internet Protocol Security (IPSec). IPSec working group (under the security area), concentrated on the protection by designing the network layer security mechanisms randomization (cryptographic). The mechanism can flexibly support combinations of authentication, integrity, access control, and confidentiality..

In the SSL-based VPNs, SSL VPNs use cryptographic algorithms to encrypt data so that only computers that are communicating that can read and understand the message being sent. SSL supports various encryption algorithms so that modifications to the application are not required and users do not need to create a security system for every application or every computer. SSL is one good solution for remote access VPN user or mobile. So with the construction of an SSL-based VPN service is an effective alternative for network security solutions.

1.2 Identification Problem

1. *How to configure Remote Access VPN with SSL method.*
2. *How to build a Remote Access VPN service using SSL.*
3. *How does the comparison service that uses the Remote Access VPN using SSL with services that do not use VPN.*

1.3 Aims and Objectives

The purpose of this paper is to build a prototype service from Remote Access VPN with SSL method.

Objectives to be achieved in this research is:

1. *Untuk menganalisis arsitektur dari VPN, terutama Remote Access VPN dengan metode SSL.*
2. *To implement a service-based Remote Access VPN using SSL.*
3. *To compare the services that use the Remote Access VPN using SSL method with a network that does not use VPN.*

1.4 Problem Definition

1. *Configuring Remote Access VPN with SSL method of configuration in the operating system.*
2. *The operating system used on the VPN server is Linux.*
3. *Configuration Implementation Remote Access VPN with SSL method of network simulation (real network) by using 2-4 computers.*
4. *Remote Access VPN connection when across the Internet at a maximum bandwidth of 256 Kbps.*
5. *VPN (Virtual Private Network) is implemented using the IP version 4 (IPv4).*

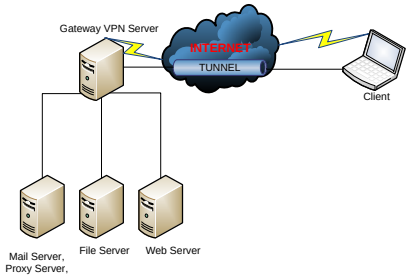
2. MODEL, ANALYSIS, DESIGN, IMPLEMENTATION

Remote Access Virtual Private Network is usually used to connect mobile users from various remote locations. Usually this type of VPN used by employees of companies that want to connect to a particular company's network from various remote locations from the company.

2.1 Analysis

Remote Access is the ability to access the resource in a service or computer network from any location. Application of remote access vpn will provide a capability to access the resources in a service or a private computer network through a safer route.

Network topology model Remote Access Virtual Private Network that is commonly used usually consist of a computer as a VPN server, the other server supporters such as web servers, file servers, and other servers and client computers to form a topology as shown below:



Pigure 1. Remote Access VPN Topology

Secure Socket Layer (SSL) is the protocol used to communicate securely over the internet. Technology SSL uses public key cryptography technology concepts in order

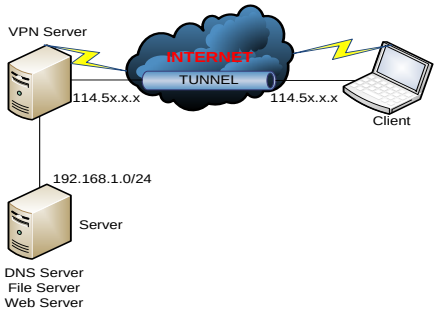
to achieve a secure communication between server and client.

In the process works, SSL consists of several phases, namely:

1. *Negotiation between the peer of algorithms supported by each peer / these endpoints.*
2. *The exchange of Public Key (PKI) for encryption and authentication mechanism-based certificates.*
3. *Symmetric encryption and asymmetric encryption.*

2.2 Design

Designing Network that will be used in this research consists of a computer as a VPN server, the server and client computers with the shape topology as shown in figure 2:



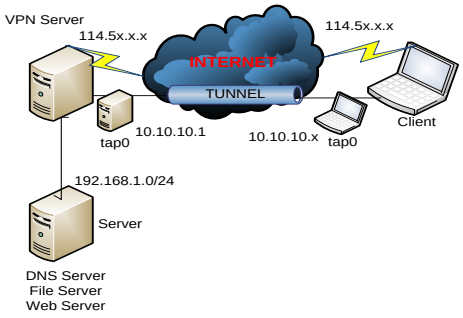
Pigure 2. Remote Access VPN Network Simulation

Table 1. IP Address Alocation

Device	***IP Address***	***Publik/ Private***	***Interface***
VPN Server	*114.5x.x.x.*	*IP Publik*	*Modem HSDPA*
	192.168.1.1	*IP Private*	*Eth0*
	10.10.10.1	*IP VPN*	*Tap0*
Server	*192.168.1.100*	*IP Private*	*Eth0*
Client	*114.5x.x.x*	*IP Publik*	*Modem HSDPA*
	10.10.10.x	*IP VPN*	*Tap0*

2.3 Implementation

In the implementation of network vpn, vpn server IP address will be given 10.10.10.1 with a subnet 255.255.255.0 and the IP address of the client will be in the range 10.10.10.2-10.10.10.254 with a subnet 255.255.255.0. So the logical topology will be formed as shown in Figure 3 below



Pigure 3. Logical Toppology of Remote Access VPN-based SSL

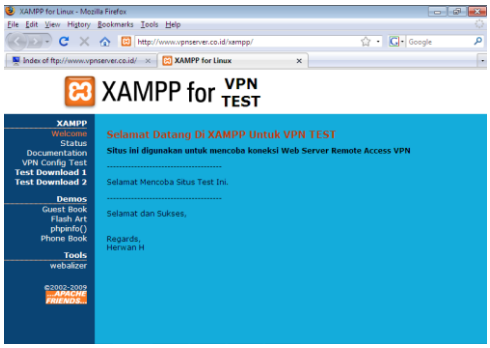
With the following IP address allocation:

Table 2. IP Address Alocation

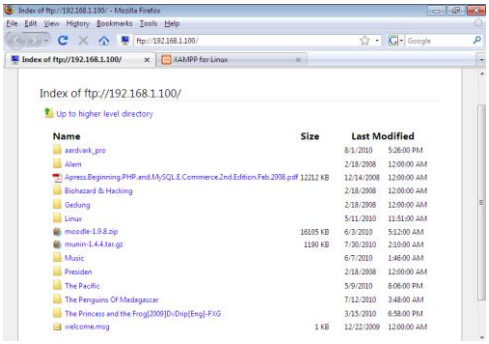
Device	***IP Address***	***Publik/ Private***	***Interface***
VPN Server	*114.5x.x.x.*	*IP Publik*	*Modem HSDPA*
	192.168.1.1	*IP Private*	*Eth0*
	10.10.10.1	*IP VPN*	*Tap0*
Server	*192.168.1.100*	*IP Private*	*Eth0*
Client	*114.5x.x.x*	*IP Publik*	*Modem HSDPA*
	10.10.10.x	*IP VPN*	*Tap0*

3. RESULTS AND DISCUSSION

Tests conducted on web access and ftp server with server located on the server computer.

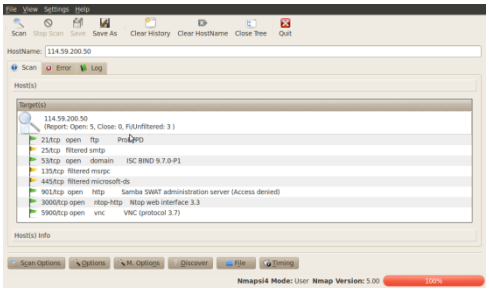


Pigure 4. Web Server Access



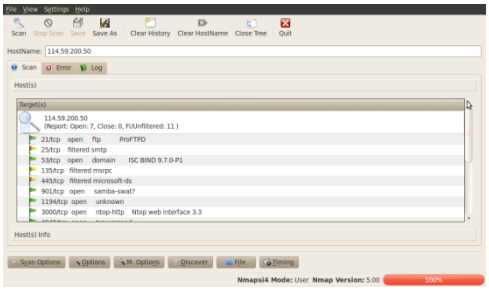
Pigure 5. FTP Server Access

In normal mode port scanning results showed that there were five open ports, and VPN port that has been made before, ie not port 1194 is not detected by Nmap.



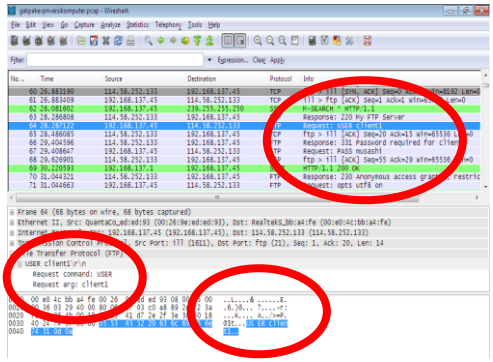
Pigure 6. Scanning Port Normal Mode

However, if the port scanning to vpn server using all modes, it will be detected seven ports are open, and the vpn server port (1194) detected by Nmap applications, however, the application can not know information Nmap port 1194 by determining the type of port- it is an unknown port.



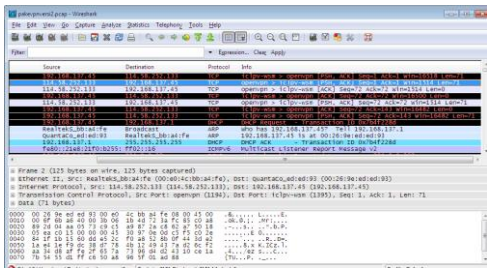
Pigure 7. Scanning Port All Mode

Results of monitoring data on the network that does not connect vpn, client access the ftp server, can know username, password and files that are used for access to ftp server.



Pigure 8. Monitoring Without Through-Based Remote Access SSL VPN

In the process of monitoring data through remote access vpn-based SSL, username and password used by the client to access the ftp server is not known, and data on-request by the client can not be monitored by wireshark.



Pigure 9. Monitoring Data Through VPN

4. CONCLUSIONS AND SUGGESTION

4.1 Conclusions

1. *Configuring Virtual Private Network Remote Access SSL method can be done using OpenVPN who have supported to build SSL-based VPN network.*
2. *Service-services such as Web Server, FTP Server, DNS Server, and other servers, can work well in an environment-based remote access SSL VPNs.*
3. *Remote Access SSL-based VPN will encrypt the key and the process of data transfer from server to client and vice versa.*

4. *SSL is a protocol that is used in remote access VPNs provide security mechanisms with one proof that the data is passed through the VPN route proved to be safe with no detection of user information and data on-request by the user.*
5. *Results of scanning ports on the VPN Server show that no detection of the in-assign ports for remote access VPN in normal mode and can not be known which type of service used at the VPN server port. So that it can be said that the remote access VPN provides security mechanisms to the system.*

4.2 Suggestion

For further development, detailed analysis is eeded on the mechanisms of security testing remote access virtual private network, with a ratio of security protocol used in VPN environments.

5. REFERENCES

[1] Bauer, Michael, 2003, Building Secure Servers With Linux, O'Reilly.

[2] Feilner, Markus, 2009, Beginning OpenVPN 2.0.9: Build and Integrate Virtual Private Networks Using OpenVPN, PACKT.

[3] Feilner, Markus, 2006, OpenVPN:Building and Integrating Virtual Private Networks, PACKT

[4] Negus, Cristoper, 2007, Ubuntu Linux Toolbox, WILEY.

[5] Sander, Van Vugt, 2006, Beginning Ubuntu Server Administration: From Novice to Professional, Apress

[6] Scott, Charlie, 1999, Virtual Private Network 2nd Edition, O'Reilly

[7] Scroder, Carla, 2007, Linux Networking Cookbook, O'Reilly.

[8] Steinberg, Joseph, 2005, SSL VPN: Understanding, Evaluating, and Planning Secure, Web-Based Remote Access, PACKT.

[9] Tanembaum,A.S., 2003, Computer Networks, Prentice Hall, NewJersey

[10] Irawan, Budhi., 2005, Jaringan Komputer. Graha Ilmu. Yogyakarta.

[11] ____ _, Ubuntu Server Guide, Canonical Ltd.

[12] _____, Langkah Mudah Administrasi Jaringan Menggunakan Linux Ubuntu 9, ANDI.