IMPLEMENTATION SINGLE ACCOUNT PDC VPN BASED ON LDAP

Gregorius Hendita Artha Kusuma

Teknik Informatika, Fakultas Teknik

Universitas Pancasila
gregorius@univpancasila.ac.id

Abstrak

Data is an important for the company. Centralized data storage to facilitate users for accessing data in the company. Data will be stored centrally with PDC (Primary Domain Controller). Build communicate between head office and branch office requires high cost for each connection is not enough to ensure safety and security of data. Exchange data between head office and branch office should be kept confidential. VPN (Virtual Private Network) makes communication more efficient, not only the cost affordable that connection, security and safety will be the primary facility of VPN (Virtual Private Network). Service were established in the system will be integrated using LDAP (Lightweight Directory Access Protocol) to create a single account in each services such as PDC (Primary Domain Controller) and VPN (Virtual Private Network). The purposes of this final project to design and implementation a system centralized data storage and build communicate between head office and branch office are integrated with LDAP (Lighweight Active Directory Protocol). Hopefully this system can give more advantage to each network users.

Keyword: PDC, VPN, LDAP, Single Account.

I. Introduction

Centralized data storage makes it easy for users to access data. many companies need a centralized storage system, because the data is often a problem when there is a mutation of employees in the company. Users can not work on new workstations with the same data as in previous workstations. To support the performance of the employees of the company of course has a variety of network services are formed in it such as ftp, mail server, file sharing etc. These services of course have their respective accounts. IT support services often serve about account complaints because every network

service has an account that is made differently or made unequal by the users, can often occur wrong password or username.

Currently the exchange of data that occurs between companies become an important part that should be kept secret, in order to avoid theft and tapping / data destruction. With data or information, people easily know about what happened at the time.

Therefore it is necessary to manufacture a PDC (Primary Domain Controller) as a centralized data storage system and has security authentication and VPN (Virtual Private Network) is used to connect the communication between companies that ensure the safety and preservation of data or information exchanged between companies for working in virtual network on an Internet network and the LDAP base (Lightweight Directory Access Protocol) is used as a directory service with a single account that is integrated with network services is a very appropriate solution to handle the above problems.

II. Overview

PDC (Primary Domain Controller)

Primary domain controller (PDC) and backup domain controller (BDC) are roles that can be assigned to a server in a network of computers that use the Windows NT operating system. Windows NT uses the idea of a domain to manage access to a set of network resources (applications, printers, and so forth) for a group of users. The user need only to log in to the domain to gain access to the resources, which may be located on a number of different servers in the network. One server, known as the primary domain controller, manages the master user database for the domain. One or more other servers are designated as backup domain controllers. The primary domain controller periodically sends copies of the database to the backup domain controllers. A backup domain controller can step in as primary domain controller if the PDC server fails and can also help balance the workload if the network is busy enough.

In Windows NT, a domain combines some of the advantages of a workgroup (a group of users who exchange access to each others' resources on different computers) and a directory (a group of users who are managed centrally by an administrator). The domain concept not only allows a user to have access to resources that may be on different servers, but it also allows one domain to be given access to another domain in a trust relationship. In this arrangement, the user need only log in to the first domain to also have access to the second domain's resources as well.

Samba

Samba is able to run as an Active Directory (AD) domain controller (DC). If you are installing Samba in a production environment, it is recommended to run two or more DCs for failover reasons.

Since 1992, Samba has provided secure, stable and fast file and print services for all clients using the SMB/CIFS protocol, such as all versions of DOS and Windows, OS/2, Linux and many others. Samba is an important component to seamlessly integrate Linux/Unix Servers and Desktops into Active Directory environments. It can function both as a domain controller or as a regular domain member. Samba is a software package that gives network administrators flexibility and freedom in terms of setup, configuration, and choice of systems and equipment. Because of all that it offers, Samba has grown in popularity, and continues to do so, every year since its release in 1992.

VPN

A virtual private network (VPN) extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Applications running across a VPN may therefore benefit from the functionality, security, and management of the private network.

VPN technology was developed to allow remote users and branch offices to securely access corporate applications and other resources. To ensure security, data would travel through secure tunnels and VPN users would use authentication methods – including passwords, tokens and other unique identification methods – to gain access to the VPN. In addition, Internet users may secure their transactions with a VPN, to circumvent geo-restrictions and censorship, or to connect to proxy servers to protect personal identity and location to stay anonymous on the Internet. However, some Internet sites block access to known VPN technology to prevent the circumvention of their geo-restrictions, and many VPN providers have been developing strategies to get around these roadblocks.

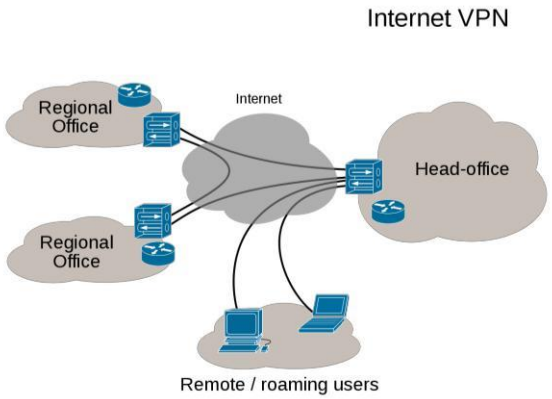

Figure 1 VPN Connectivity Overview

A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryption. A VPN available from the public Internet can provide some of the benefits of a wide area network (WAN). From a user perspective, the resources available within the private network can be accessed remotely.

Traditional VPNs are characterized by a point-to-point topology, and they do not tend to support or connect broadcast domains, so services such as Microsoft Windows NetBIOS may not be fully supported or work as they would on a local area network (LAN). Designers have developed VPN variants, such as Virtual Private LAN Service

(VPLS), and Layer 2 Tunneling Protocols (L2TP), to overcome this limitation.

Security mechanism

VPNs cannot make online connections completely anonymous, but they can usually increase privacy and security. To prevent disclosure of private information, VPNs typically allow only authenticated remote access using tunneling protocols and encryption techniques.

The VPN security model provides:

- Confidentiality such that even if the network traffic is sniffed at the packet level (see network sniffer and deep packet inspection), an attacker would see only encrypted data
- Sender authentication to prevent unauthorized users from accessing the VPN
- Message integrity to detect any instances of tampering with transmitted messages.

Secure VPN protocols include the following:

- Internet Protocol Security (IPsec) was initially developed by the Internet Engineering Task Force (IETF) for IPv6, which was required in all standards-compliant implementations of IPv6 before RFC 6434 made it only a recommendation. This standards-based security protocol is also widely used with IPv4 and the Layer 2 Tunneling Protocol. Its design meets most security goals: authentication, integrity, and confidentiality. IPsec uses encryption, encapsulating an IP packet inside an IPsec packet. De-encapsulation happens at the end of the tunnel, where the original IP packet is decrypted and forwarded to its intended destination
- Transport Layer Security (SSL/TLS) can tunnel an entire network's traffic (as it does in the OpenVPN project and SoftEther VPN project or secure an individual connection. A number of vendors provide remote-access VPN capabilities through SSL. An SSL VPN can connect from locations where IPsec runs into trouble with Network Address Translation and firewall rules.
- Datagram Transport Layer Security (DTLS) – used in Cisco AnyConnect VPN and in OpenConnect VPN to solve the issues SSL/TLS has with tunneling over UDP.

OpenVPN

OpenVPN is a full-featured SSL VPN which implements OSI layer 2 or 3 secure network extension using the industry standard SSL/TLS protocol, supports flexible client authentication methods based on certificates, smart cards, and/or username/password credentials, and allows user or group-specific access control policies using firewall rules applied to the VPN virtual interface. OpenVPN is not a web application

proxy and does not operate through a web browser.

OpenVPN 2.0 expands on the capabilities of OpenVPN 1.x by offering a scalable client/server mode, allowing multiple clients to connect to a single OpenVPN server process over a single TCP or UDP port. OpenVPN 2.3 includes a large number of improvements, including full IPv6 support and PolarSSL support.

LDAP

LDAP, the Lightweight Directory Access Protocol, is a mature, flexible, and well supported standards-based mechanism for interacting with directory servers. It's often used for authentication and storing information about users, groups, and applications, but an LDAP directory server is a fairly general-purpose data store and can be used in a wide variety of applications.

The Lightweight Directory Access Protocol (LDAP) is an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network. Directory services play an important role in developing intranet and Internet applications by allowing the sharing of information about users, systems, networks, services, and applications throughout the network. As examples, directory services may provide any organized set of records, often with a hierarchical structure, such as a corporate email directory. Similarly, a telephone directory is a list of subscribers with an address and a phone number.

LDAP is specified in a series of Internet Engineering Task Force (IETF) Standard Track publications called Request for Comments (RFCs), using the description language ASN.1. The latest specification is Version 3, published as RFC 4511 (a road map to the technical specifications is provided by RFC4510).

A common use of LDAP is to provide a central place to store usernames and passwords. This allows many different applications and services to connect to the LDAP server to validate users.

LDAP is based on a simpler subset of the standards contained within the X.500 standard. Because of this relationship, LDAP is sometimes called X.500-lite.

OpenLDAP

OpenLDAP is a free, open source implementation of the Lightweight Directory Access Protocol (LDAP) developed by the OpenLDAP Project. It is released under its own BSD-style license called the OpenLDAP Public License.

LDAP is a platform-independent protocol. Several common Linux distributions include OpenLDAP Software for LDAP support. The software also runs on BSD-variants, as well as AIX, Android, HP-UX, macOS, Solaris, Microsoft Windows (NT and derivatives, e.g. 2000, XP, Vista, Windows 7, etc.), and z/OS.

Historically the OpenLDAP server (slapd, the Standalone LDAP Daemon) architecture was split between a frontend which handles network access and protocol processing, and a backend which deals strictly with data storage. This split design was a feature of the original University of Michigan code written in 1996[9] and carried on in all subsequent OpenLDAP releases. The original code included one main database backend and two experimental/demo backends. The architecture is modular and many different backends are now available for interfacing to other technologies, not just traditional databases.

Ordinarily an LDAP request is received by the frontend, decoded, and then passed to a backend for processing. When the backend completes a request, it returns a result to the frontend, which then sends the result to the LDAP client. An overlay is a piece of code that can be inserted between the frontend and the backend. It is thus able to intercept requests and trigger other actions on them before the backend receives them, and it can also likewise act on the backend's results before they reach the frontend. Overlays have complete access to the slapd internal APIs, and so can invoke anything the frontend or other backends could perform. Multiple overlays can be used at once, forming a stack of modules between the frontend and the backend.

Overlays provide a simple means to augment the functionality of a database without requiring that an entirely new backend be written, and allow new functionalities to be added in compact, easily debuggable and maintainable modules. Since the introduction of the overlay feature in OpenLDAP 2.2 many new overlays have been contributed from the OpenLDAP community.

III. Structure

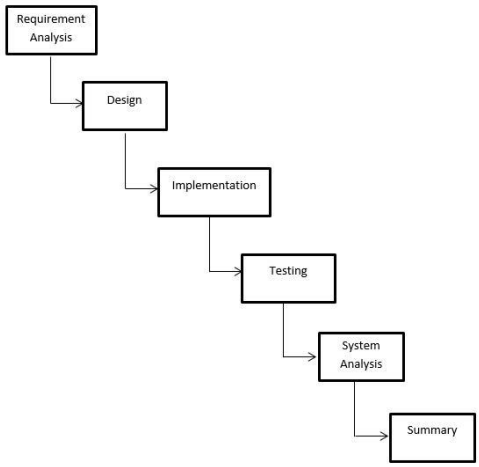

Figure 1 Method system

1. **Requieremet Analysis**

   Analyze what it takes build the system in terms of software and hardware. This information can be obtained through interviews or discussions.

2. **Design System**

   Designing a network topology that will be used by the system that aims to provide an overview of what should be done and petrified specify the needs in terms of hardware and define the overall system architecture.

3. **Implementation System**

   This phase undertakes a thorough system development whereby the application of analysis and design.

4. **Testing system**

   Testing the system on the server is already running in accordance with the problems that arise.

5. **Analysis System**

   Analyze the system in terms of hardware that has been created and cover the shortcomings to be more perfect. This information can be obtained through testing.

6. **Summary**

   This phase summarizes the overall results of whether the system is working perfectly or not.

IV. DESIGN AND ANALYSIS

The network system to be created consists of two servers that act as PDC (Primary Domain Controller) and VPN (Virtual Private Network) with different device specifications. PDC (Primary Domain Control) is used as data storage and centralized login using single account while VPN (Virtual Private Network) is built to connect reliable inter-company communication. The topology below with the addition of 2 new servers namely LDAP + PDC and VPN (Virtual Private Network).

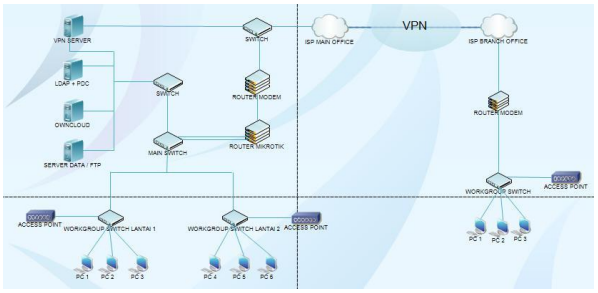

Figure 2 System Topology

Based on the topology system above, as for the advantages of the topology to be built are:

- The enterprise storage system becomes centralized with the presence of a domain controller.
- A single account can be used to access all available network services.
- Communication between companies can be established reliably and confidentially
- Save costs, because there is no need to build infrastructure to connect between companies.

V. IMPLEMENTATION

In the implementation phase of the server using Ubuntu as the operating system. Implementation is the application of the system design that has been designed in the previous chapter.

Testing

In testing method of system function which have been implemented in the form of domain controller, active directory, single account and VPN as connection built between office. to test the VPN is capable of encrypting data on the network.

Join PDC Testing

The creation of the user is done with the purpose of creating a user PDC (Primary Domain Controller) as well as create a user VPN (Virtual Private Server) used to login to the domain and VPN.

The user creation is done on the terminal server with command-line with the following command:

```
#smbldap-useradd -a -m 'fadly'

#smbldap-passwd fadly
```

Testing on the client is done as follows:

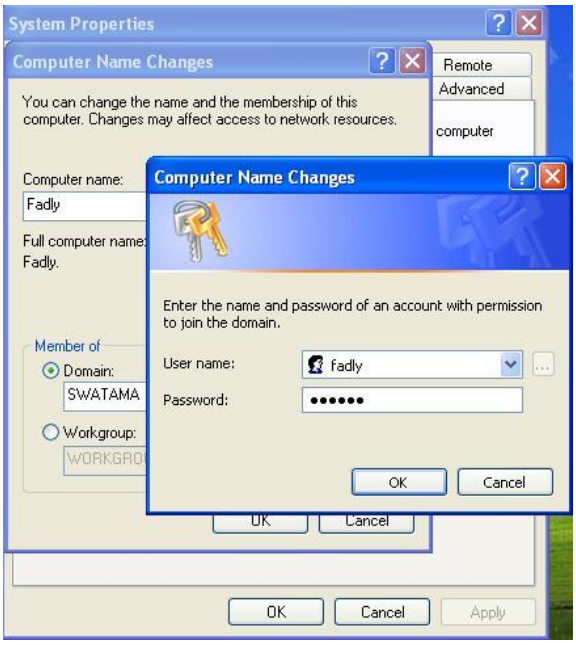

Figure 3 Join Domain

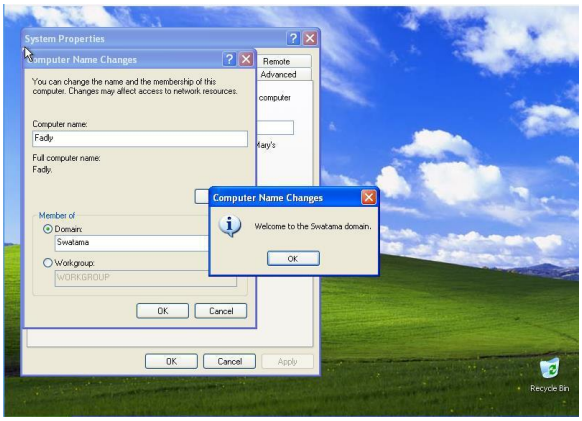

Figure 4 Success Join

based on the image above, the client successfully logged on the domain will succeed with authentication from LDAP.

Restart the client PC and boot as usual, it will display the login page username and password before heading to the operating system of the client.

Figure 5 Login Page Windows

If the username and password entered are listed on the LDAP server, then login on windows will work and the configuration has been done correctly.

VPN Tunneling Testing

Tunneling is a connection made by a VPN when connected to its VPN client, it will automatically create a new tunnel path for data exchange between the server and the client.

Testing the VPN client is done by using windows XP operating system that has been installed a windows based openVPN GUI application. Copy the ca.crt and client.ovpn certificates from the server to the client and save them in the / Openvpn / config folder on the client computer.

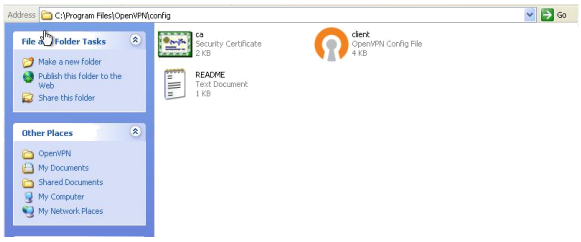

Figure 6 OpenVPN Certifacate

As in the picture above, the ca.crt and client.ovpn certificate files are only stored on client computers and not distributed, as they are confidential for authentication on the VPN Server.

Run the OpenVPN app on the client computer

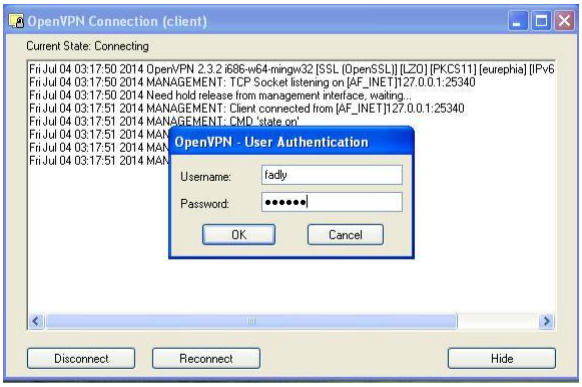

Figure 7 OpenVPN Authentication

as in the picture above, enter the password and username OpenVPN

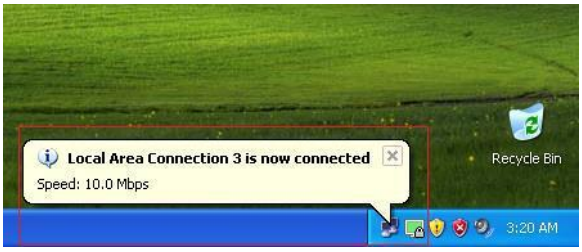

Figure 8 OpenVPN Client Connected

If the VPN client is successfully connected to the VPN server then the OpenVPN icon will change its color to green.

Sniffing Testing With OpenVPN

This test uses a system that has been built previously with VPN (Virtual Private Server) and FTP and wireshark applications used to view packets that pass on the network.

Running OpenVPN, Wireshark application and login to VPN Server as usually. Access FTP server via browser using IP Tunneling that has been formed and enter Username and Password from FTP.

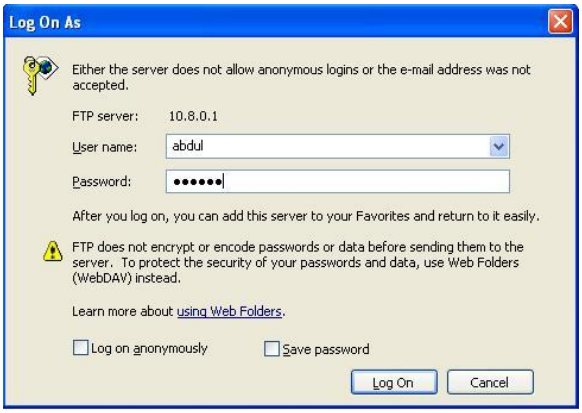

Figure 9 FTP Server access through VPN

View wireshark apps that run before.

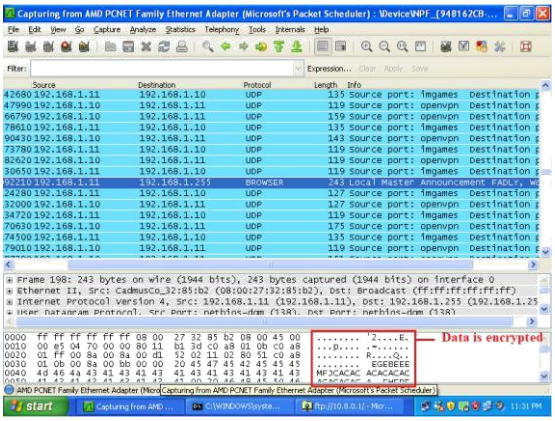

Figure 10 Sniffing page from wireshark

VI. CONCLUSION

1. The implementation of PDC (Primary Domain Controller) as a centralized storage system has been successfully done with Samba system that is integrated with LDAP using samba-samba-samba-samba samba tool.

2. The VPN (Virtual Private Network) is implemented as a reliable communications link between headquarters and branches. This is evidenced by testing sniffing using wireshark applications on the system.

3. Implementation of a single account on the system is to create an account used for both services that is PDC (Primary Domain Controller) and VPN (Virtual Private Network) using LDAP as Management users and Directory service.

VII. REFERENCES

[1] PDC, Domain Controller [Online] Available https://en.wikipedia.org/wiki/Domain_controller July 2018

[2] Margaret Rouse, Domain Controller [Online]. Available: https://searchwindowsserver.techtarget.com/definition/domain-controller .

[3] Samba, What is Samba [Online] Available: https://www.samba.org/samba/what_is_samba.html March 2018.

[4] Wikipedia, Virtual Private Network [Online]Available: https://en.wikipedia.org/wiki/Virtual_private_network. July 2018

[5] OpenVPN Technologies, Open VPN[online] available: https://openvpn.net/index.php/open-source/documentation/howto.html September 2013

[6] Neil Wilson, LDAP [Online] Available: https://ldap.com/ July 2018.

[7] Wikipedia, Lightweight Directory Access Protocol [Online] Available: https://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol July 2018.

[8] Wikipedia, OpenLDAP [Online] Available: https://en.wikipedia.org/wiki/OpenLDAP June 2018.