IMPLEMENTASI OPENVPN MENGGUNAKAN LDAP SEBAGAI MANAJEMEN USER PADA SISTEM OPERASI UBUNTU

Aprilia Ayu Mahardani
D3 Manajemen Informatika, Fakultas Teknik, Universitas Negeri Surabaya, juniaraprilia95@gmail.com

Asmunin
Jurusan Teknik Informatika, Fakultas Teknik, Universitas Negeri Surabaya, asmunin@unesa.ac.id

Abstrak

VPN merupakan singkatan *Virtual Private Network* yang artinya membuat jaringan private secara virtual diatas jaringan *public* (umum) seperti internet.Dalam implementasinya, VPN terbagi menjadi *remote access* VPN dan *site-to-site* VPN.

Penelitian ini bertujuan untuk menghubungkan klien ke PC kantor. Untuk itu penulis menggunakan OpenVPN. OpenVPN ini akan dihubungkan dengan LDAP sehingga klien dapat di identifikasi. Setelah itu melakukan *sharing resource* berupa untuk sesama klien.

Hasil penggujian ini menunjukkan bahwa pada percobaan *autentifikasi* klien dan PC kantor yang terhubung dengan OpenVPN harus login menggunakan LDAP. Pada percobaan *fungsionalitas* menujukkan klien dan PC kantor yang menggunakan OpenVPN dapat terhubung dengan baik . Sedangkan untuk *fungsionalitas* klien dan PC kantor dapat langsung terhubung.

Kata Kunci :*Virtual Private Network, remote access,site-to site, sharing resource*

Abstract

VPN stands for Virtual Private Network which means to create a virtual private network over public network (public) such as internet. In the implementation, VPN is divided into remote access VPN and site-to-site VPN.

This study aims to connect clients to PC office. For that writer use OpenVPN. This OpenVPN will be linked to LDAP so clients can be identified. After that do resource sharing form for fellow clients.

The results of this test show that in the client authentication experiments and the office PC connected to OpenVPN must login using LDAP. In the experiments of functionality showing clients and office PCs using OpenVPN can connect well. As for the functionality of the client and office PC can be directly connected.

Keywords: *Virtual Private Network, remote access, site-to site, resource sharing*

PENDAHULUAN

Pada saat ini layanan internet merupakan suatu kebutuhan bagi semua orang dari berbagai kalangan.Sehingga banyaknya permintaan membuat provider perlu untuk membuat inovasi baru untuk memenuhi kebutuhan tersebut. Dari kurangnya kapasitas internet yang diterima berdampak pada aktivitas di perusahaan, instansi atau lainnya dalam berinteraksi dengan kantor cabang, karyawan di lapangan maupun konsumen melalui jaringan komputer. Untuk itu dirasa perlu menemukan solusi baru dalam hal pertukaran informasi melalui internet secara aman dan cepat.Dalam pengembangannya ditemukan teknologi VPN yaitu dengan melalukan komunikasi melalui internet tetapi tetap melihat sisi keamanannya.

VPN merupakan singkatan *Virtual Private Network* yang artinya membuat jaringan private secara virtual diatas jaringan *public* (umum) seperti internet.Dalam implementasinya, VPN terbagi menjadi *remote access* VPN dan *site-to-site* VPN.Pada penelitian ini ingin mengembangkan konsep *remote access* VPN dengan menggunakan software *open source* OPENVPN pada sistem operasi Ubuntu. Jaringan ini akan di uji coba melalukakn tes fungsionalitas dan konektivitas sehingga sambungan yang telah dibuat berfungsi secara benar. Selain itu dilakukannya uji coba untuk mengetahui jarak yang di lalui paket menggunakan jaringan internet.

Tujuan dari penelitian ini adalah Pembuatan konsep VPN secara *remote site* ke PC kantor dengan menggunakan OpenVPN, serta mengintegrasikan *user autentifikasi* OpenVPN dengan LDAP **dan** mengakses data pada PC kantor dengan menggunakan *file sharing*setelah dilakukannya *tunneling* OpenVPN.

Manfaat yang digunakan dari penelitian ini adalah membangun sebuah server yang berisi OPENVPN

dengan pengaturan *user* menggunakan LDAP pada sistem operasi Ubuntu.

Hasil yang diharapkan pada penelitian ini adalah sebuah metode baru yang dapat digunakan oleh pengguna yang memiliki sistem operasi selain windows.Selain itu penelitian ini dapat digunakan untuk kajian lainnya tentang komunikasi menggunakan jaringan *public.*

KAJIAN PUSTAKA

Tunneling

Tunneling adalag dasar dari vpn untuk membuat suatu jaringan private melalui jaringan internet.Tunneling juga merupakan enkapsulasi atau pembungkusan suatu protokol ke dalam paket protokol.Tunneling menyediakan suatu koneksi point-to-point logis sepanjang jaringan **IP** yang besifat *connectionless*. Proses transfer data dari satu jaringan ke jaringan lain memanfaatkan jaringan internet secara terselubung (*tunneling*). Ketika paket berjalan menuju ke node selanjutnya, paket ini melalui suatu jalur yang disebut tunnel.

Disebut *tunnel* atau saluran karena aplikasi yang memanfaatkannya hanya melihat dua *end point*, sehingga paket yang lewat pada *tunnel* hanya akan melakukan satu kali lompatan atau hop. *Tunneling* pada VPN menggunakan enkripsi untuk melindungi data agar tidak dapat dilihat oleh pihak-pihak yang tidak diberi otorisasi dan membuat suatu enkapsulasi multiprotocol jika dperlukan.

Tunneling merupakan metode untuk transfer data dari satu jaringan ke jaringan lain dengan memanfaatkan jaringan internet secara terselubung. Protokol tunneling tidak mengirimkan frame sebagimana yang dihasilkan oleh node asalnya begitu saja, melainkan membungkusnya men-enkapsulasi dalam header tambahan. Header tambahan tersebut berisi informasi sehingga data frame yang dikirim dapat melewatinya. (Tuxkeren: 2013)

VPN

VPN merupakan jaringan public yang menekankan pada keamanan data dan akses global melalui internet hubungan ini dibangun melalui suatu *tunnel* (terowongan) virtual antara 2 *node.*Dengan menggunakan jaringan public, user dapat bergabung dalam jaringan lokal, untuk mendapatkan hak dan pengaturan yang sama ketika user berada di kantor.

Virtual Private Network (VPN) adalah sebuah koneksi virtual yang bersifat private, disebut demikian karena pada dasarnya jaringan ini tidak ada secara fisik hanya berupa jaringan virtual , dan mengapa disebut private karena jaringan ini merupak jaringan yang bersifat private yang tidak semua orang bisa mengaksesnya. VPN menghubungkan PC dengan jaringan public atau internet namun sifatnya private karena bersifat private maka tidak semua orang bisa terkoneksi ke jaringan ini dan mengaksesnya (Putranto: 2009)

OPENVPN

Merupakan aplikasi open source untuk Virtual Private Networking (VPN), dimana aplikasi tersebut dapat membuat koneksi point-to-point tunnel yang telah terenkripsi. Open*VPN* menggunakan private keys, certificate, atau username/password untuk melakukan authentikasi dalam membangun koneksi. Dimana teknologi yang digunakan untuk enkripsi dalam jaringan Open*VPN* ini menggunakan teknologi SSL dan untuk komunikasinya Open*VPN* bergerak di Layer 2 dan 3 OSI Layer. Karena Open*VPN* berbasis protocol SSL maka Open*VPN* ini dapat digunakan di berbagai sistem operasi tanpa perbedaan yang signifikan. (Putra, Nugraha: 2011)

UBUNTU

Rilis pertama Ubuntu adalah pada tanggal 20 Oktober 2004. Sejak itu, Canonical telah merilis versi baru dari Ubuntu setiap enam bulan dengan komitmen untuk mendukung setiap rilis selama delapan belas bulan dengan menyediakan perbaikan keamanan, patch untuk bug kritis dan update minor untuk program. Diputuskan bahwa setiap rilis keempat, yang dikeluarkan atas dasar dua tahun, akan menerima dukungan jangka panjang (LTS). LTS rilis secara tradisional didukung selama tiga tahun pada desktop dan lima tahun pada server. Namun dengan rilis Ubuntu 12.04 LTS, dukungan desktop untuk LTS rilis diperpanjang hingga lima tahun (misalnya, Ubuntu 12.04 LTS dijadwalkan akan didukung sampai April 2017). Dukungan diperpanjang untuk lebih mengakomodasi bisnis dan perusahaan TI pengguna Ubuntu yang beroperasi pada siklus rilis lebih lama dan lebih sadar biaya yang berkaitan dengan upgrade software sering. LTS rilis mendapatkan rilis titik untuk memastikan bahwa versi LTS bekerja pada lebih baru hardware . The rilis LTS bisa mendapatkan upgrade LTS rilis dengan versi poin pertama. The 10.04 LTS rilis misalnya mendapat upgrade rilis dengan rilis titik 12.04. (Sukmaaji, Anjik: 2008)

LDAP

LDAP adalah sebuah protokol yang mengatur mekanisme pengaksesan layanan direktori (Directory Service) yang dapat digunakan untuk mendeskripsikan banyak informasi seperti informasi tentang people, organizations, roles, services dan banyak entitas lainnya.

LDAP menggunakan model client-server, dimana client mengirimkan identifier data kepada server menggunakan protokol TCP/IP dan server mencoba mencarinya pada DIT (Directory Information Tree) yang tersimpan di server. Bila di temukan maka hasilnya akan dikirimkan ke client tersebut namun bila tidak maka hasilnya berupa pointer ke server lain yang menyimpan data yang di cari.

LDAP tersebut memiliki bentuk struktur yang berhirarki, bukannya berformat kolom dan baris, seperti halnya database normal, sehingga memudahkan untuk memasukkan sejumlah besar detail yang mirip dalam bentuk yang terorganisir. Awalnya, server LDAP merupakan sesuatu yang terdapat diantara LDAP client dan sebuah server DAP (X 500), jadi untuk mengurangi resource yang dibutuhkan menjalankan client. (Prasetyo, Agus: 2015)

METODE

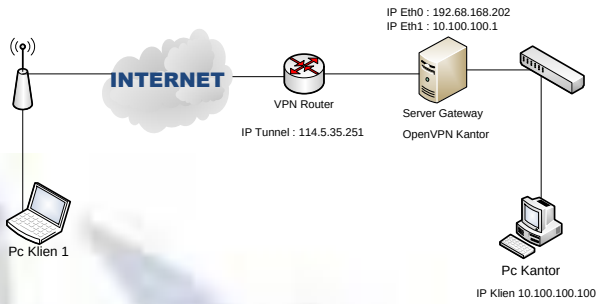
Analisis Sistem

Analisa merupakan suatu tindakan untuk mengetahui lebih jauh tentang objek yang akan diteliti. Bab ini akan menguraikan proses analisis pembangunan sistem *remote access* VPN dan perancangan manajemen user menggunakan OpenLDAP. Sebelum dilakukan pengembangan dan perancangan sistem, terlebih dahulu dilaksanakan analisis kebutuhan-kebutuhan pokok sistem *remote access* VPN yang akan di bangun.

Kebutuhan pokok yang diperlukan pada penelitian ini menggunakan OpenVPN sebagai aplikasi utama yang dibangun pada sistem operasi Ubuntu. Setelah dilakukan proses instalasi OpenVPN maka akan menghasilkan berupa CA, Key Server, dan Key Client. Beberapa file tersebut diperlukan oleh *client* agar dapat terhubung dengan *server*. Setelah itu OpenVPN akan di intergrasi dengan OpenLDAP sebagai *manajemen user*. OpenLDAP disini akan berperan guna menyimpan dan mengatur *id* dariklien. *Id* dan *password* dari *client* ini akan di atur oleh admin dan akan otomatis tersimpan pada database dari OpenLDAP itu sendiri.

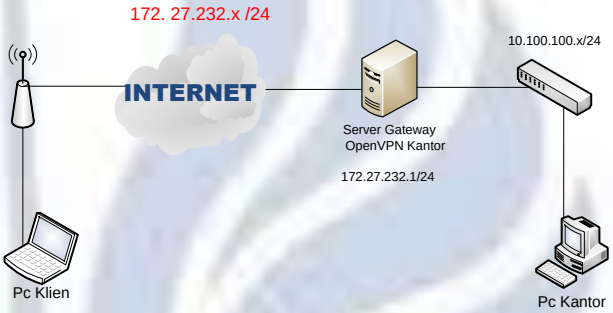
Dalam penerapannya klien yang menggunakan jaringan yang berasal dari modem maupun Lan dapat langsung terhubung dengan *server* dan *client* .

Tahap 1 : Tunneling ke Router JTIF



Gambar 1.Tahap 1 tunneling Router Jtif

Tahap 2 : Tunneling ke Server Gateway (OpenVPN kantor)



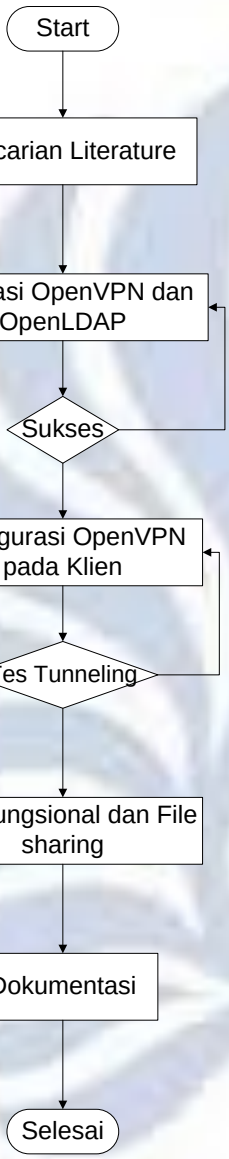
Gambar 2.Tahap 2 Tunneling OpenVPN server

Pada rancangan ini penulis tidak melakukan proses pembangunan topologi baru, melainkan mengembangkan dari jaringan yang telah ada. Terdapat 2 tahapan, dimana pada tahap 1 melakukan tunneling ke *VPN Router*.Sedangkan pada tahap 2 yaitu melakukan tunneling pada server gateway (OpenVPN kantor).

Pada tahap 1 klien membangun***tunneling***pada *router* JTIF, dimana *router* ini juga berfungsi sebagai *router tunnel* yang akan digunakan klien agar dapat terhubung dengan *server gateway* maupun PC kantor. Tahap ini klien yang memiliki ip yang berasal dari jaringan public hanya dapat terhubung dengan VPN *router* dan belum dapat terhubung dengan *server gateway* atau PC kantor.

P Ada tahap 2, tahapan ini dapat dijalankan ketika server gateway sudah memiliki OpenVPN dan terhubung dengan LDAP. Setelah itu klien harus terhubung terlebih dahulu dengan OpenVPN serve, setelah terhubung klien akan memiliki IP publik dimana IP tersebut dapat digunakan untuk mengakses PC kantor. IP publik ini tidak hanya di miliki oleh klien saja tetapi server gateway dan PC kantor juga memiliki IP publik ini. Sehingga ketika klien akan terhubung dengan PC kantor dapat

melalui IP publik ini. Ketika klien dan PC kantor akan terhubung dengan OpenVPN maka akan melalui autentifikasi yang berasal dari LDAP sehingga dapat dilakukan pembatasan hingga penolakan akses yang dilakukan oleh admin.

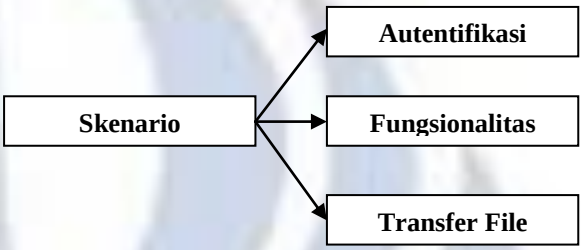


Gambar 3. Flowchart Perancangan Sistem

Kebutuhan Perangkat

1. Perangkat Keras
   Menggunakan 1 buah komputer yang digunakan untuk meremote server sekaligus client 1 virtual dan juga di gunakan sebagai client 2.
2. Perangkat Lunak
   Pemilihan sistem operasi untuk OPENVPN menggunakan sistem operasi Ubuntu 14.04 LTS dan untuk klien menggunakan sistem operasi Windows XP dan Windows 10.
3. Aplikasi
   Untuk aplikasi yang digunakan pada penelitian ini menggunakan OPENVPN, OpenLDAP, Putty, BitViseSSH.

Skenario pengujian



Gambar 4. Skenario Pengujian

Berikut penjelasan Flowchart scenario pengujian openvpn pada penelitian ini sebagai berikut.

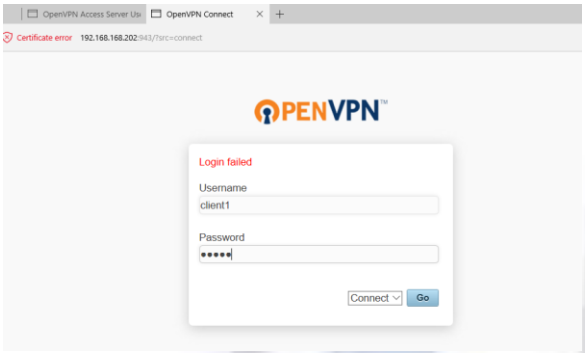
1. Pengujian Autentifikasi, pengujian ini dilakukan untuk menguji user dan password t=yang telah di buat di LDAP untuk dipakai sebagai user pada OpenVPN.
2. Pengujian Fungsionalitas, pengujian ini digunakan agar mengetahui apakah antar PC klien dan PC kantor dapat terhubung. Pengujian ini juga digunakan untuk membandingkan hasil dari konektifitas dan rute yang dilewati oleh paket sebelum maupun sesudah terhubung dengan OpenVPN.
3. Pengujian Transfer File, pengujian ini dilakukan untuk menguji akses data yang dilakukan oleh PC klien pada PC kantor sebelum dan sesudah OpenVPN.
4.

HASIL DAN PEMBAHASAN

Pengujian Autentifikasi,

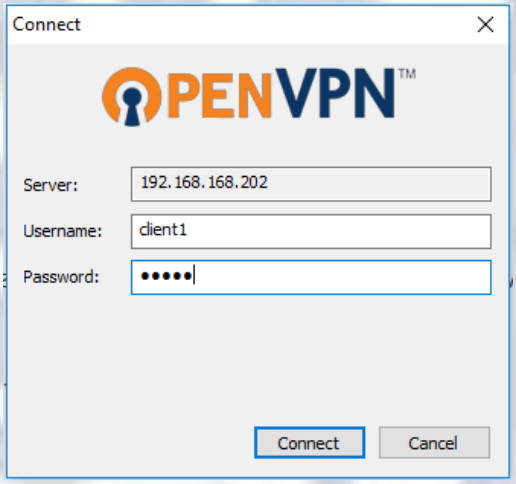
Pengujian ini bertujuan untuk menguji autentifikasi dari openvpn yang menggunakan openldap.

Tahapan yang dilakukan adalah klien harus terhubung dengan openvpn terlebih dahulu, software ini dapat di unduh pada https://192.168.168.202:943/ seperti pada gambar 5 Setelah itu login menggunakan username dan password yang telah dibuat sebelumnya. Seperti pada gambar 6



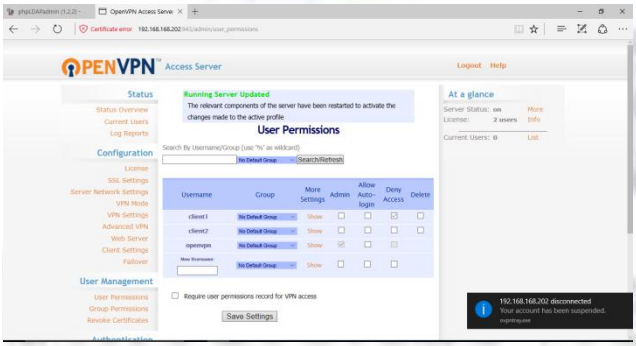
Gambar 5. Login OpenVPN

Setelah berhasil login silahkan untuk menjalankan software tersebut dan selanjutnya akan keluar autentifikasi dan login seperti pada gambar 6



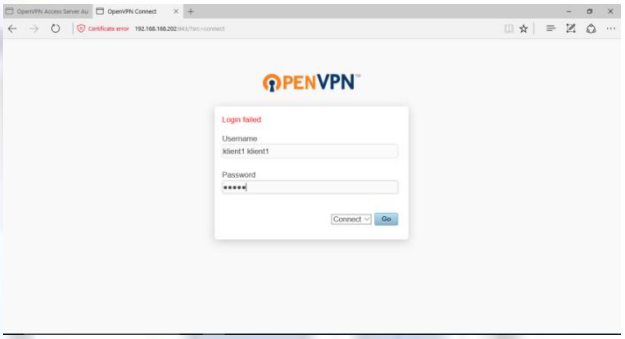
Gambar 6. Koneksi pada OpenVPN server

Untuk membatasi koneksi dari klien, maka harus login pada https://192.168.168.202:942/admin masuk pada user permission dan deny access pada klien yang akan dibatasi sepeti pada gambar 7



Gambar 7. Membatasi akses klien

Pada percobaan tersebut yang akan dibatasi adalah klien 1, karena klien 1 adalah laptop yang digunakan uji coba maka ketika akses ditolak keluar sebuah notifikasi seperti pada gambar 7



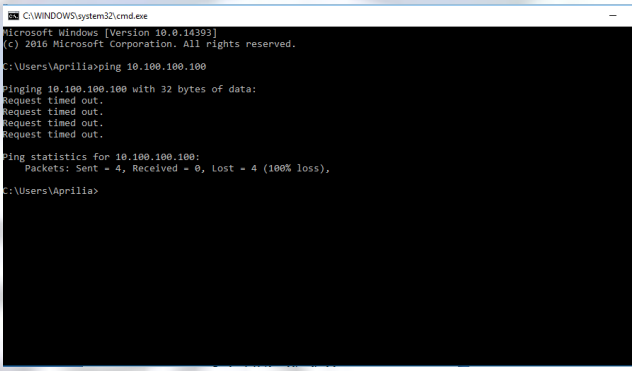
Gambar 8. Akses klien di tolak

Ketika akses telah ditolak oleh admin maka pada gambar 8 klient tidak dapat terhubung dengan OpenVPN.

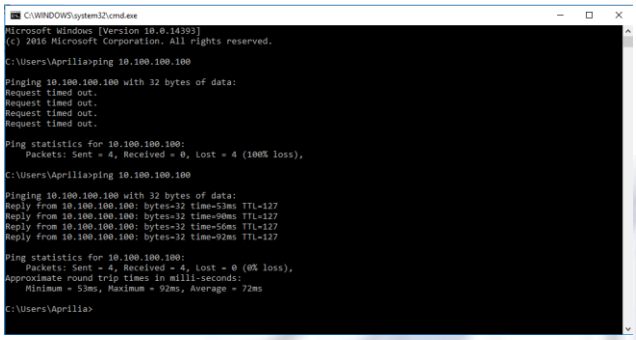
Pengujian Konektifitas,

Pengujian ini dilakukan dengan cara tes PING dari klien menuju PC kantor dan pengujian traceroute guna mengetahui jalur yang dilewati oleh klien.

1. Pengujian ping pada gambar 9 dan 10 merupakan pengujian yang dilakukan antara klien dengan kantor, pada percobaan ini juga membandingkan klien yang terhubung dengan kantor yang menggunakan OpenVPN lebih cepat daripada klien yang terhubung tanpa OpenVPN.

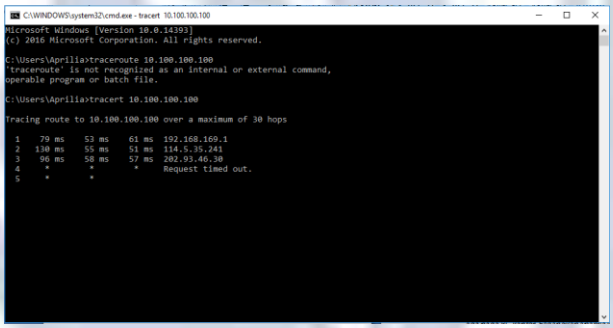


Gambar 9. Hasil PING kantor tanpa OpenVPN

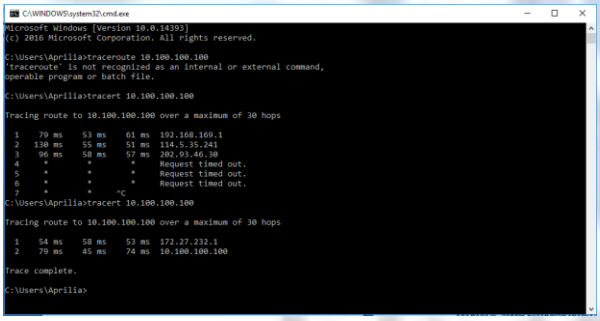


Gambar 10. Hasil Ping kantor menggunakan OpenVPN

2. Pengujian Traceroute, perngujian ini dilakukan antara klien dengan kantor. Pada pengujian ini juga dilakukan perbandingan untuk mengetahui jalur yang di lalui paket dari klien menuju kantor.



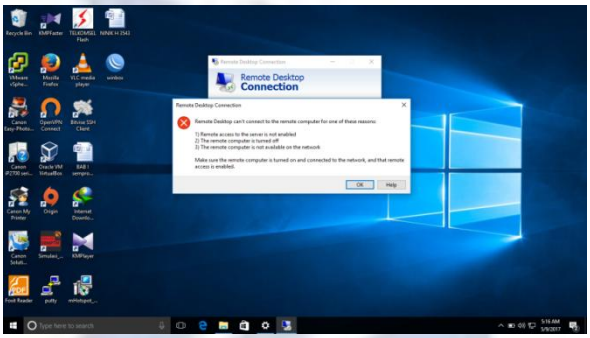
Gambar 11. Hasil traceroute tanpa OpenVPN



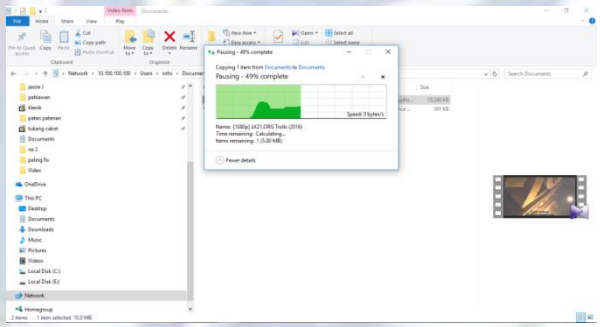
Gambar 12. Hasil Traceroute menggunakan OpenVPN

Dari hasil yang dilakukan pada gambar 12 menujukkan bahwa pada node ke 4 klien tidak dapat menjangkau PC kantor di karenakan jalur yang dilalui sangat panjang. Sedangkan pada bagian atas dapat disimpulkan bahwa klien yang akan terhubung dengan PC kantor hanya melalui 2 node sehinga tidak memerlukan waktu yang lama untuk dapat terhubung dengan PC kantor.

1. ***Pengujian File Transfer***
   Pengujian ini dilakukan ketika masing-masing klien terhubung dengan OpenVPN. Selanjutnya adalah dengan melakukan perbandingan kecepatan dari transfer file antara file yang menggunakan OpenVPN dengan tidak menggunakan.



Gambar 13. Hasil Remote desktop tanpa Openvpn



Gambar 14. Pengambilan file pada PC kantor

Dapat disimpulkan melalui gambar 12 dan 13 bahwa klien dan PC kantor yang terhubung dengan OpenVPN dapat langsung melakukan sharing file, dalam percobaan tersebut klien mengambil file yang ada pada PC kantor. Sedangkan apabila klien dan PC kantor tidak terhubung dengan OpenVPN maka baik klien maupun PC kantor tidak dapat melakukan sharing file karena terhalang oleh kapasitas akses data.

PENUTUP

Simpulan

Dari hasil penggujian dan pembahasan pada percobaan diperoleh kesimpulan sebagai berikut :

1. Hasil Autentifikasi, menunjukkan bahwa masing-masing user yang akan terhubung dengan OpenVPN harus melalui LDAP sebagai system autentifikasi.
2. Hasil Fungsionalitas didapatkan hasil dimana ketika klien dan PC kantor terhubung maka

menggunakan OpenVPN maka terhubung dengan baik, tetapi bila tidak menggunakan OpenVPN maka klien tidak dapat menjangkau PC kantor.

3. Hasil File sharing menunjukkan bahwa klien dan PC kantor yang menggunakan OpenVPN dapat langsung bertukar informasi.

Saran

1. Openvpn yang digunakan dapat dikonfigurasi lagi untuk keperluan lebih lanjut dan bila akan digunakan untuk skala yang besar maka memerlukan license untuk keperluan user.
2. Openldap dapat di konfigurasi dengan menambahan skema guna mengembangkan autentifikasi yang lebih lanjut.

DAFTAR PUSTAKA

Afriani A, Ainul. 2015. *Implementasi Routing Ospf melalui OpenVPN Tunnel Menggunakan VPS sebagai Server Openvpn.* Surabaya: Unesa.

Cartealy, Imam. 2013. *Linux Networking(Ubuntu, Kubuntu, Debian).* Jakarta:Jasakom

Hadndayana, Wilfridus, Bambang Triadi, Bernard Renaldy Suteja, Ahmad Ashari. 2010. *Linux System Administrator.*Bandung : Informatika.

Musajid, Akrom. 2016. *CENTOS , Paduan Singkat Membangun Server.* Jakarta : Jasakom. .

Openvpn Access Server Guide. https://openvpn.net/index.php/access-server/docs/admin-guides-sp-859543150.html. Terakhir diakses 17 Maret 2017.

Openldap. https:// www.youtube.com/ watch?v= p857CNi60LM&list =WL&index=5&t=23s. Terakhir diakses 31 Maret 2017.

Prasetyo, Agus. 2015. *Membangun Server dengan Debian 7.*Jakarta : Jasakom.

Putra, Nugraha, Erlangga Nanda. 2011. *Membangun Virtual Private Network (VPN) Server menggunakan Teknologi Open Source pada PT. Muara Dua Palembang.* Palembang : STMIK PalComTech.

Sukmaaji, Anjik. 2008. *Konsep Dasar Pengembangan Jaringan dan Keamanan Jaringan.*Penerbit Andi: Yogyakarta.

Samba.https://www.liberiangeek.net/2015/01/install-configure-samba-ubuntu-14-10/. Terakhir diakses 20 April 2017

Server Guide Ubuntu 14.04. https:// help.ubuntu.com/ 14.04/serverguide/index.html.Terakhir diakses 5 april 2017

Tuxkeren. 2013. *Ubuntu Server Paduan Singkat dan Cepat.* Jakarta : Jasakom.

Tim, Penulis. 2004. *Buku Pedoman Penulisan danUjian Skripsi Unesa.*Surabaya:Unesa.