

IMPLEMENTASI NETWORK STORAGE DAN INTERNET GATEWAY MENGUNAKAN AUTENTIKASI OPENLDAP

Ari Sujarwo, S.Kom.¹

¹Jurusan Teknik Informatika, Fakultas Teknik Industri, Universitas Islam Indonesia

Jl. Kaliurang Km. 14,5 Yogyakarta 55584

E-mail: ari.sujarwo@staff.uui.ac.id

ABSTRAK

Perubahan pola hidup manusia turut serta berpengaruh pada penerapan teknologi informasi. Semakin banyak layanan yang dibutuhkan oleh pengguna sebagai pendukung aktivitasnya, semakin banyak pula proses autentikasi yang harus dilakukan oleh pengguna untuk dapat menggunakan layanan tersebut. Beberapa contoh layanan yang diperlukan oleh pengguna jaringan komputer, yaitu layanan sumber daya penyimpanan jaringan atau *network storage resources* dan layanan koneksi internet. Agar masing-masing pengguna memiliki privasi dan terpisah dari pengguna yang lain, maka diperlukan proses autentikasi untuk validasi pengguna.

Network storage dibangun di atas platform OpenFiler yang memiliki berbagai keunggulan, yaitu dapat menyatukan konsep media penyimpanan NAS dan SAN dalam sebuah mesin, manajemen data menggunakan *quota*, serta kompatibilitasnya jika digunakan sebagai media penyimpanan dengan berbagai sistem autentikasi. *Network storage* dapat secara otomatis termapping sebagai sebuah drive pada komputer client dengan bergabung ke dalam domain yang ditangani oleh sebuah domain controller menggunakan Samba. Proses autentikasi pengguna sistem dibangun di atas platform OpenLDAP sehingga selanjutnya dapat dipergunakan untuk validasi pengguna pada berbagai sistem yang mendukung interkoneksi dengan OpenLDAP seperti FreeRadius yang akan digunakan untuk mendukung validasi pengguna layanan koneksi internet pada internet gateway.

Kata Kunci: validasi, akun pengguna tunggal, network storage, domain controller

1. PENDAHULUAN

1.1 Latar Belakang Masalah

Perubahan pola hidup manusia dewasa ini turut serta berpengaruh pada penerapan teknologi informasi. Saat ini manusia dalam hal ini adalah pengguna jaringan komputer semakin membutuhkan sebuah kemudahan untuk mengakses bermacam sumber daya dalam jaringan. Semakin banyak layanan yang dibutuhkan oleh pengguna sebagai pendukung aktivitasnya, antara lain seperti mengakses sumber daya internet, melakukan penyimpanan file pada media penyimpanan jaringan, serta berbagi data dengan sesama pengguna.

Semakin banyaknya layanan yang dimiliki oleh pengguna semakin banyak pula proses autentikasi yang harus dilakukan oleh pengguna untuk dapat menggunakan layanan tersebut.

Beberapa layanan yang diperlukan oleh pengguna jaringan komputer, yaitu layanan sumber daya penyimpanan jaringan atau *network storage resources* dan layanan koneksi internet. Agar masing-masing pengguna memiliki *privacy* dan terpisah dari pengguna yang lain, maka diperlukan proses autentikasi untuk validasi pengguna.

Pada layanan *network storage* terdapat berbagai contoh sistem yang telah banyak digunakan, salah satunya yaitu Novell Netware, sebuah sistem yang menawarkan sebuah *network storage* yang dikeluarkan oleh Novell, Inc.. Netware dibangun

hingga versi terakhirnya yaitu versi 6.5 yang mulai mensupport berbagai layanan seperti *CIFS* dan *SAN*. (Novel, 2008)

Netware kemudian digantikan oleh Novell Open Enterprise Server yang dirilis pada tahun 2005. OES merupakan sebuah sistem berbayar yang menggunakan lisensi '*per-user seat*' yaitu lisensi yang tidak memperhitungkan berapa jumlah server yang menggunakan produk tersebut, sehingga memungkinkan seorang pengguna membangun sebuah clustering system menggunakan sebuah lisensi. (Novel, 2008)

OES yang dibangun sebagai sebuah *enterprise system*, menawarkan berbagai fitur seperti NCP, eDirectory, NSS, dan iPrint. Versi inilah yang akhirnya menawarkan sebuah solusi lengkap bagi sebuah *network storage* berbayar yang *powerfull*. (Novel, 2008)

Pesaing Novell OES saat ini adalah *Windows Active Directory* yang disupport oleh Windows Server 2003. Microsoft menawarkan manajemen pengguna sekaligus media penyimpanan yang sangat lengkap dan kompleks dalam sebuah mesin. Seperti yang diaplikasikan pada Nanyang Technological University (NTU) Singapore, dan Universiti Teknologi PETRONAS Malaysia. Mahasiswa diberikan fasilitas tambahan berupa media penyimpanan jaringan sehingga bagi mahasiswa yang menggunakan perangkat akses yang minimal semacam NetBook yang memiliki spesifikasi media

penyimpanan yang kecil, atau pengguna fasilitas komputer anjungan dapat menitipkan data temporer pada server.

Sistem ketiga yang menawarkan sebuah solusi *network storage* adalah OpenFiler, yaitu sebuah sistem operasi berbasis Linux yang dikembangkan sebagai sebuah perangkat lunak bebas dan tidak berbayar. OpenFiler berkembang sebagai sebuah *Storage Management System* dengan kemampuan interkoneksi ke berbagai sistem autentikasi dan berbagai macam protokol penyajian data.

Berdasarkan data dari situs resmi OpenFiler, *Network storage* telah banyak digunakan oleh perusahaan-perusahaan besar seperti MLP (<http://www.mlp.de>), Synovus (<http://www.synovus.com>), NHS (<http://www.nhs.uk>), ATMOSi (<http://www.atmosi.com>), dan Rader Solutions (<http://www.radersolutions.com>), disamping pengguna-pengguna lain yang tidak terdaftar yang tidak terhitung jumlahnya. (OpenFiler, 2008)

Sistem autentikasi yang didukung oleh OpenFiler salah satunya adalah *Lightweight Directory Access Protocol (LDAP)* yang varian gratisnya dapat kita kenali dengan nama OpenLDAP. Sebuah teknologi yang mampu berkomunikasi dengan banyak *platform* perangkat lunak seperti FreeRadius, yang apabila dikoneksikan dapat digunakan sebagai sistem autentikasi *hotspot* internet. Dapat pula berkomunikasi dengan OpenFiler yang dapat dipergunakan sebagai *storage management system*.

Keuntungan yang dapat diperoleh dengan penerapan sistem ini adalah kemudahan bagi pengguna untuk mengeksplorasi layanan-layanan pada jaringan komputer dengan hanya menggunakan sebuah *account* pengguna yang terdaftar pada sistem.

Akhirnya, terdapat sebuah pembandingan bagi seorang pengembang sistem *network storage* dan *internet gateway* untuk memilih sebuah sistem murah yang memiliki kualitas sekelas *enterprise*. Oleh karena itu maka dalam implementasi kali ini digunakan OpenFiler sebagai sistem yang menangani manajemen *network storage* dengan OpenLDAP sebagai *backend* autentikasi.

1.2 Tujuan Penelitian

Memanfaatkan jalur internet yang tersedia di FTI UII tidak hanya sebagai media transfer data teks atau gambar tetapi juga menyediakan *network storage* bagi pengguna jaringan internet FTI. Dengan dibangunnya *Network Storage* dan *Internet Gateway* menggunakan autentikasi OpenLDAP maka pengguna jaringan internet di FTI dapat menggunakan *single user account* untuk mengakses sumber daya jaringan di FTI.

1.3 Manfaat Penelitian

Memberikan solusi kemudahan pengaksesan sumber daya jaringan di kampus FTI dengan menggunakan sebuah *single user account*, serta

memberikan layanan tambahan kepada pengguna berupa *network storage resources*. Tren semakin banyaknya pemberian layanan tambahan kepada pengguna jaringan, akan sangat mudah jika dapat ditangani dengan sebuah *account* bagi masing-masing pengguna.

Hasil *polling* kuesioner yang dilakukan penulis, seluruh responden yang berasal dari berbagai bidang kerja menyatakan bahwa adanya *network storage* bagi pengguna jaringan internet sudah harus ada dengan ukuran yang disesuaikan dengan bidang kerja. Seorang pekerja dengan dokumen-dokumen dan jurnal tentu memerlukan media penyimpanan yang jauh lebih sedikit jika dibandingkan dengan kebutuhan media penyimpanan bagi seorang *graphic designer*. Rata-rata responden mengungkapkan ukuran minimal *network storage* bagi masing-masing pengguna pada kisaran 250 MB hingga 2048 MB. (Sujarwo, 2008)

Animo pengguna yang seperti ini telah menunjukkan kepada kita semua bahwa adanya *network storage* pada jaringan sangat diperlukan untuk mendukung kebutuhan pengguna dalam mengarsipkan dan menyimpan file-filenya dalam jaringan.

2. LANDASAN TEORI

2.1 Autentikasi

Autentikasi adalah proses usaha pengecekan identitas seorang pengguna sistem komunikasi pada proses *login* ke dalam sebuah sistem. pengguna yang telah lolos pengecekan identitas adalah pengguna resmi pada sistem, orang yang memiliki otoritas atas sistem, atau mungkin aplikasi yang berjalan pada sistem.

Penggunaan sistem autentikasi diharapkan dapat membentuk sebuah sistem khusus, yang hanya dapat dipergunakan oleh orang-orang yang memiliki hak guna. (Patrick, 2007)

Autentikasi seringkali diasumsikan identik dengan otorisasi, banyak protokol keamanan dan peraturan yang berdasarkan asumsi ini. Akan tetapi, penggunaan istilah autentikasi yang lebih tepat adalah pembuktian sebagai proses pengecekan identitas seorang pengguna, sedangkan otorisasi adalah proses pengecekan bahwa pengguna yang dikenal memiliki kekuasaan untuk melakukan tindakan tertentu.

2.2 LDAP

Lightweight Directory Access Protocol, atau LDAP adalah protokol aplikasi yang digunakan untuk melakukan pengontrolan pada layanan direktori yang berjalan pada protokol TCP/IP. (Foundation, 2008)

Direktori adalah sebuah layanan terstruktur yang disusun secara logis dan hierarkis. pada LDAP terdapat struktur yang mirip dengan struktur *database* sehingga dapat dipergunakan sebagai pengganti *database*. Karena kemiripan inilah, LDAP

sering digunakan sebagai alat autentikasi pada beragam sistem sesuai dengan struktur yang digunakan. pada perkembangannya, LDAP memanfaatkan penggunaan *Domain Name System* untuk mendukung penamaan pada struktur direktori. lebih jauh, LDAP dapat menggambarkan pengguna, organisasi atau hal lain sesuai dengan struktur yang diberikan pada LDAP.

2.3 Struktur Direktori LDAP

Protokol pengaksesan direktori LDAP, sesuai dengan model standar *X.500*, standar jaringan komputer yang mencakup layanan direktori, edisi tahun 1993, yaitu direktori adalah struktur isian direktori. Isian terdiri atas rangkaian atribut yang memiliki nama berupa tipe dan penjelasan atau data yang sesuai dengan skema. (Harrison, 2008)

Setiap isian memiliki penanda khusus yang berupa *Distinguish Name (DN)* yang berisi *Relative Distinguish Name (RDN)* yang disusun atas beberapa atribut isian, yang diikuti oleh induk isian DN.

DN adalah nama lengkap sedangkan RDN adalah nama file dalam folder. DN dapat berubah seiring perubahan isian dalam struktur. sebuah isian dalam LDAP diwujudkan dalam LDIF seperti contoh berikut,

```
dn: cn=jarwo,dc=fti-iii,dc=org
cn: jarwo
givenName: jarwo
sn: jarwo
mail: jarwo@fti-iii.org
manager: cn=admin,dc=fti-iii,dc=org
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
```

2.4 Samba Domain Controller

Samba adalah himpunan aplikasi yang bertujuan agar komputer dengan sistem operasi Linux, BSD (atau UNIX lainnya) dapat bertindak sebagai file dan print server yang berbasis protokol SMB (*server message block*). Jaringan yang semacam ini biasa dijumpai pada *Windows Workgroup* atau *Windows NT Domain*. Samba juga dilengkapi dengan beberapa program bantu sehingga sistem operasi Linux (dan UNIX lainnya) bisa mengakses sumber daya yang ada pada jaringan Windows yang telah ada. Samba berfungsi sebagai jembatan penghubung antara Windows dan UNIX. (Sisjarkom, 2007)

Samba PDC (*Primary Domain Controller*) adalah samba yang difungsikan untuk melakukan validasi pengguna kepada setiap *client* yang akan bergabung dalam satu *domain* tertentu. (Matthews, 2007)

Dengan kata lain hanya pengguna yang terdaftar yang diijinkan masuk ke *domain* tersebut dan mengakses semua fasilitas *domain* yang disediakan.

2.5 Network Attached Storage

Network Attached Storage (NAS) adalah sebuah media penyimpanan jaringan yang dapat berupa sebuah *dedicated hardware* atau dapat pula berupa

media penyimpanan yang dibangun dari sebuah komputer. (Mitchell, 2008)

Tujuan adanya *network attached storage* adalah sebagai penyedia layanan penyimpanan data berupa file yang dapat dipergunakan oleh perangkat lain dalam jaringan. Sistem operasi dan perangkat lunak pada NAS membangun sebuah fungsi penyimpanan data, sistem file, dan bagian manajemen fungsi-fungsi media penyimpanan jaringan.

NAS bekerja menggunakan protokol berbasis file seperti *Network File Server (NFS)* yang populer pada sistem operasi Linux atau *Server Message Block (SMB)* yang digunakan pada sistem operasi Windows. Namun pada saat memberikan layanan kepada pengguna, NAS mengarahkan pengguna untuk menggunakan salah satu dari beberapa protokol yang didukung tersebut.

2.6 Network Storage Management dengan OpenFiler

OpenFiler merupakan sistem penyimpanan yang mengakomodasi konsep NAS dan SAN yang sangat fleksibel dan ideal untuk digunakan pada bermacam *platform* sistem jaringan dan sistem operasi yang bermacam seperti Windows, Linux, dan Macintosh. sehingga memungkinkan bagi sebuah sistem penyimpanan yang terdiri atas bermacam platform untuk dapat dikelola dalam sebuah sistem tunggal. (OpenFiler, 2008)

3. PERANCANGAN

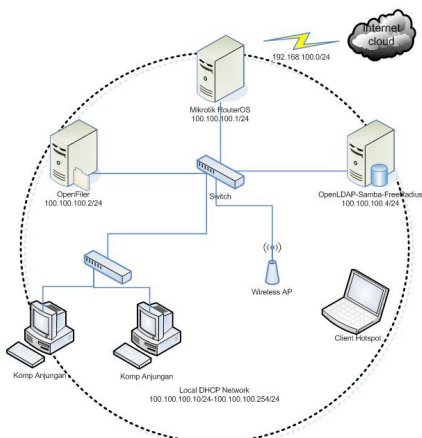
3.1 Gambaran Umum Sistem

Implementasi *Network Storage* dan *Internet Gateway* menggunakan autentikasi OpenLDAP yang dibangun ini akan memiliki kinerja sebagai sebuah *server* yang dapat mengatur autentikasi *client* pada beberapa layanan.

Pengaturan tersebut dibagi atas beberapa hal, yaitu:

1. Autentikasi pengguna ketika melakukan pengaksesan sumber daya jaringan.
2. Autentikasi pengguna ketika melakukan pengaksesan media penyimpanan jaringan.
3. Autentikasi pengguna ketika akan bergabung ke dalam *domain*.

3.2 Arsitektur Sistem



Gambar 1. Desain Arsitektur Jaringan

Pada perancangan arsitektur jaringan seperti tercantum di gambar 2 yang digunakan dalam sistem autentikasi ini, diperlukan minimal dua buah alamat jaringan atau Network Address.

1. Local Area Network
 - Network Address : 100.100.100.0/24
 - Internet Gateway RouterOS: 100.100.100.1/24
 - OpenFiler : 100.100.100.2/24
 - OpenLDAP, FreeRadius, Samba: 100.100.100.4/24
 - Client : menggunakan IP Address pada lingkup *Local Area Network* dari range 100.100.100.10 hingga 100.100.100.254
2. Internet Network
 - Network Address 192.168.100.0/24
 - RouterOS IP address 192.168.100.2/24

3.3 Alokasi Akun Pengguna

Agar pengguna dapat melakukan aktifitas di dalam jaringan dengan memanfaatkan berbagai macam layanan jaringan, maka diperlukan pengalokasian akun yang berfungsi sebagai kunci autentikasi pengguna pada *server*. Sehingga bila terjadi koneksi baru dari pengguna untuk mengakses sumber daya jaringan, maka dapat direspon oleh *server*. Aplikasi *LDAP Account Manager* mensyaratkan sebuah nama pengguna tidak diawali dengan angka, sehingga dalam pembuatan *user account* diawali dengan huruf 'm' yang diasosiasikan sebagai 'mahasiswa'.

Dibuat sejumlah enam buah *user account* yang masing-masing dapat dipergunakan dengan *password* yang sama dengan nama pengguna, dalam implementasinya, seorang pengguna dapat mengganti *password* menggunakan prosedur penggantian *password* pada sistem operasi.

Tabel 1. Daftar Pengguna

Username	Password
m09523001	m09523001
m09523002	m09523002
m09523003	m09523003

m09523004	m09523004
m09523005	m09523005
m09523006	m09523006

4. IMPLEMENTASI

4.1 Implementasi Secara Umum

Implementasi sistem merupakan tahap dimana sistem mampu diaplikasikan dalam keadaan yang sesungguhnya. Dari implementasi ini akan diketahui apakah sistem yang dibuat dapat berjalan dengan baik atau tidak. Serta apakah sistem menghasilkan *output* yang sesuai dengan perancangan yang ada.

4.2 Tahapan Implementasi

Dalam pengaplikasian perangkat lunak, terdapat beberapa tahap yang terdiri atas:

1. Tahap Instalasi dan konfigurasi OpenLDAP

Pada tahap ini dilakukan pemasangan OpenLDAP pada *server* dan pengkonfigurasi tahap awal yang diperlukan untuk mendukung kinerja sistem autentikasi agar dapat berjalan sesuai dengan perancangan.
2. Tahap Instalasi dan konfigurasi Samba Domain Controller

Pada tahap ini dilakukan instalasi dan konfigurasi *domain controller* menggunakan Samba dan mengkonfigurasi file-file yang diperlukan agar dapat terkoneksi dengan OpenLDAP. *Domain Controller* dikatakan bekerja dengan baik jika dapat terkoneksi ke OpenLDAP dan terbaca sebagai *primary domain controller* pada *client*.
3. Tahap Instalasi dan konfigurasi OpenFiler

Pada tahap ini dilakukan instalasi *OpenFiler Operating System* pada *server* yang telah disiapkan. OpenFiler dikonfigurasi melalui antarmuka *web* disesuaikan dengan perancangan yang telah ada.
4. Tahap Instalasi FreeRadius

Pada tahap ini dilakukan instalasi dan konfigurasi FreeRadius sebagai autentikator *hotspot*. file konfigurasi diset sehingga dapat terkoneksi ke dalam OpenLDAP.
5. Tahap Instalasi Mikrotik RouterOS

Pada tahap ini dilakukan instalasi Mikrotik RouterOS pada *server* yang telah disediakan, RouterOS akan bekerja berdampingan secara langsung dengan FreeRadius yang telah dikonfigurasi sebelumnya untuk menangani autentikasi *hotspot*.
6. Tahap Konfigurasi LDAP Account Manager (LAM)

Pada tahap ini dilakukan konfigurasi *LDAP Account Manager* yang digunakan untuk mengorganisir pengguna yang terdaftar pada sistem. Pengguna dapat menggunakan semua

layanan yang disediakan oleh sistem setelah terdaftar melalui LAM.

7. Tahap Konfigurasi Client

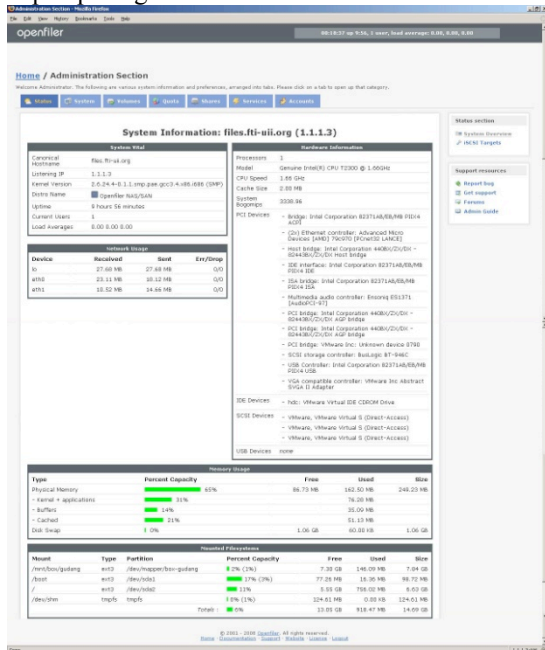
Pada tahap ini dilakukan konfigurasi pada client agar dapat terkoneksi ke jaringan. Pengalokasian IP dilakukan secara otomatis, sehingga penggunaannya perlu mengkonfigurasi komputer agar dapat terkoneksi ke dalam domain controller.

4.3 Instalasi Openfiler

Instalasi Openfiler dilakukan langsung pada komputer yang akan didedikasikan khusus untuk Openfiler. Openfiler bukan berupa paket aplikasi tunggal saja, namun sebuah sistem operasi kompleks yang memiliki kemampuan sebagai *network storage server*, lengkap dengan antarmuka *web* untuk manajemennya. [OPE08b]

4.4 Konfigurasi Openfiler

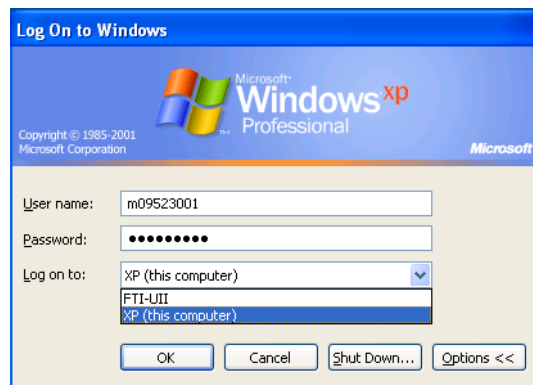
Setelah instalasi selesai, Openfiler siap dikonfigurasi melalui *web browser*. Akses alamat IP melalui salah satu komputer yang terkoneksi dengan mesin server Openfiler. Pada implementasi ini, halaman konfigurasi Openfiler dapat diakses melalui alamat <https://100.100.100.2:446> seperti tampak pada gambar 3.



Gambar 2. Konfigurasi Openfiler

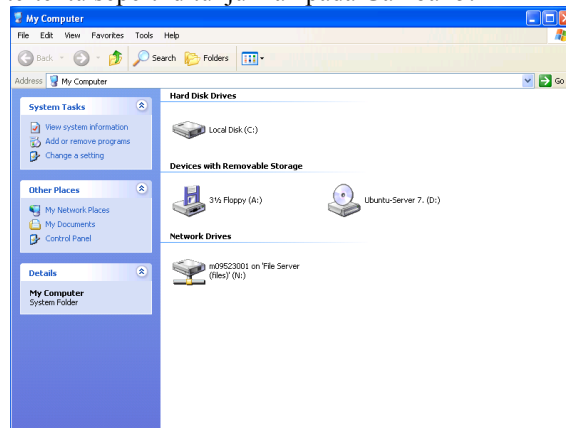
4.5 Pengujian Sistem

Implementasi sistem autentikasi akan melibatkan *client* sebagai mesin yang digunakan untuk melakukan pengujian. *Client* akan menggunakan sistem operasi Windows XP Professional yang terhubung langsung ke dalam jaringan lokal. Komputer yang telah terkoneksi ke Domain akan memunculkan nama domain ketika proses login seperti tampak pada gambar 4.



Gambar 3. Proses login pengguna ke sistem

Pengguna yang telah berhasil masuk ke dalam komputer menggunakan data *account* sistem akan memperoleh fasilitas *network drive* yang dapat dipergunakan sesuai dengan *quota* yang diberikan oleh sistem. *Network drive* dapat langsung digunakan tanpa harus melakukan konfigurasi tertentu seperti ditunjukkan pada Gambar 5.



Gambar 4. Network Drive pada komputer client

Agar dapat terkoneksi ke jaringan dan menggunakan sumber daya jaringan termasuk di dalamnya koneksi ke internet, seorang pengguna diwajibkan untuk melakukan *sign in* ke dalam sistem. Pengguna harus memasukkan *Username* dan *Password* melalui browser seperti tampak pada Gambar 6.

Please log on to use the mikrotik hotspot service



Powered by mikrotik routers © 2005 mikrotik

Gambar 5. Proses login akses Internet

4.6 Analisa Hasil Pengujian

Pengujian hasil implementasi *Network Storage* dan *Internet Gateway* menggunakan autentikasi OpenLDAP telah membuahkan beberapa analisa yaitu :

1. *Client* yang terdaftar telah berhasil melakukan *sign in* ke dalam sistem hotspot dengan sebuah *account* yang terdaftar dalam sistem.
2. Seluruh *client* telah berhasil memiliki satu buah *network drive* ketika *log in* ke dalam *domain controller* dengan menggunakan *account* yang sama.
3. Sistem *quota* pada Openfiler dapat digunakan untuk membatasi penggunaan *network drive* sesuai dengan kebijakan sistem.
4. Openfiler dapat beroperasi dengan baik dalam pengelolaan *network storage* bagi pengguna dan sangat fleksibel ketika ada penambahan atau pengurangan *perangkat keras*.
5. Sistem *Network Storage* secara umum memberikan manfaat bagi pengguna untuk menyimpan dan mengarsipkan file dalam jaringan.
6. Pada perkembangannya apabila ukuran *quota* bagi masing-masing cukup besar dan kecepatan akses data pada *network storage* mendekati kecepatan akses sumberdaya lokal, maka akan dapat menghemat sumberdaya lokal karena penyimpanan file yang berkaitan dengan pekerjaan dapat disimpan pada media tersebut. Seperti pada beberapa perusahaan pengguna OpenFiler yang disampaikan pada bagian pendahuluan, adanya *network storage* akan memberikan sebuah nilai tambah bagi aktivitas kerja pada sebuah institusi.

5. KESIMPULAN

Implementasi *Network Storage* dan *Internet Gateway* menggunakan autentikasi OpenLDAP telah selesai dibangun dan telah diupayakan sesuai dengan perencanaan dan perancangan pada tahap analisis kebutuhan jaringan, perangkat keras, perangkat lunak, serta konfigurasinya. Setelah dilakukan tahap pengujian, maka dapat diambil kesimpulan bahwa :

1. OpenLDAP sangat mungkin untuk diintegrasikan dengan sistem yang lain.
2. OpenFiler sebagai sebuah Sistem Operasi yang digunakan untuk pengelolaan media penyimpanan jaringan sangat mampu menangani tugasnya dengan baik dan fasilitas-fasilitas yang ada didalamnya sangat mendukung dalam penyimpanan dan pengaksesan file.
3. Pembatasan media penyimpanan menggunakan *quota* dapat berjalan dengan baik.

4. Pengguna dapat menggunakan *network storage* dan koneksi internet dengan menggunakan *user account* tunggal.

PUSTAKA

- Novell, Inc., 2008. Novell NetWare® 6:File Protocol Support Section, diakses 7 Oktober 2008 dari <http://www.novell.com/info/collateral/docs/4621202.01/4621202.html>
- Novell, Inc., 2008. Novell Licensing Programs:Novell Open Enterprise Server 2 Licensing, diakses pada 2 Oktober 2008 dari http://www.novell.com/licensing/oes_licensing.html
- Novell, Inc., 2008. File & Storage Services: Novell Open Enterprise Server 2, diakses pada 4 Oktober 2008 dari http://www.novell.com/products/openenterpriseserver/file_and_storage_services.html
- Openfiler, 2008. Openfiler – Openfiler Homepage, diakses pada 10 Juni 2008 dari <http://www.openfiler.com>
- Sujarwo, Ari, 2008. Kuesioner Pengumpulan Data Pendukung Dalam Rangka Penyusunan Tugas Akhir, diakses pada 31 Oktober 2008 dari <http://likwarjo.web.id/blog/wp-content/ukara/2008/11/kuesioner-ta.rar>
- Patrick, Andrew, 2007. Authentication Technology and Identity Theft, diakses pada 4 Oktober 2008 dari <http://www.andrewpatrick.ca/essays/authentication-technology-and-identity-theft>
- Foundation, OpenLDAP , 2008. OpenLDAP Software 2.4 Administrator's Guide, diakses pada 3 Oktober 2008 dari <http://www.openldap.org/doc/admin24/>
- Harrison, Peter, 2008. Quick HOWTO : Ch31 : Centralized Logins Using LDAP and RADIUS, diakses pada 3 Agustus 2008 dari http://www.linuxhomenetworking.com/wiki/index.php/Quick_HOWTO:_Ch31:_Centralized_Logins_Using_LDAP_and_RADIUS
- Sisjarkom, et all, 2007. Modul Praktikum Jaringan Komputer 2007, Yogyakarta:Teknik Informatika
- Matthews, Paul, 2007. OpenLDAP LAM SAMBA as PDC, diakses pada 1 Juni 2008 dari <http://www.opensourcehowto.org/howto/samba/openldap-lam-samba-as-pdc.html>
- Mitchell, Bradley, 2008. Network Attached Storage – NAS – Introduction to NAS, diakses pada 3 Oktober 2008 dari <http://compnetworking.about.com/od/itinformatics/technology/l/aa070101a.htm>
- Openfiler, 2008. Openfiler Administration Guide, diakses pada 6 Agustus 2008 dari <http://www.old.openfiler.com/docs/openfiler-guide-1.1/#d0e1614>