

RANCANG BANGUN JARINGAN ENTERPRISE DENGAN VIRTUAL PRIVATE NETWORK DAN CENTRAL AUTHENTICATION SYSTEM PADA PABRIK GULA PT. PERKEBUNAN NUSANTARA X (PERSERO)

Ahmad Aziz, A.Md¹, Idris Winarno, SST, M.Kom.²
Mahasiswa Jurusan Teknik Informatika¹, Dosen Jurusan Teknik Informatika
Jurusan Teknik Informatika
Politeknik Elektronika Negeri Surabaya
Institut Teknologi Sepuluh Nopember
Kampus ITS Sukolilo, Surabaya 60111, Indonesia
Tel: +62 (31) 594 7280; Fax: +62 (31) 594 6114
e-mail : aziz@student.eepis-its.edu¹ , idris@eepis-its.edu²

Abstract—Dalam proses produksi gula, perangkat lunak sistem informasi cukup berpengaruh besar dalam peningkatan hasil produksi. Perangkat lunak yang digunakan sangat mempengaruhi keputusan dari setiap proses produksi dan mengontrol perhitungan serta laporan sehingga sesuai dengan keadaan riil di lapangan serta mengurangi kemungkinan kecurangan dan human error. PT. Perkebunan Nusantara X (Persero) selaku pemimpin produksi dari 11 pabrik gula di seluruh Jawa Timur tentunya harus selalu memantau secara langsung proses dan hasil produksi dari setiap pabrik gula. Dan jika hal tersebut dilakukan secara manual, tentunya akan menghabiskan dana yang jelas tidak sedikit. Selain itu juga, ancaman keamanan terhadap data-data vital perusahaan cukup riskan. Terutama dalam manipulasi data yang bisa merugikan perusahaan.

Dilatarbelakangi masalah-masalah tersebut diatas, dalam penelitian ini dibangun sebuah solusi berupa Enterprise Network Application System yang berfungsi untuk mengintegrasikan seluruh Aplikasi Produksi Pabrik Gula PT Perkebunan Nusantara X (Persero) melalui Jaringan Private dan mengoptimalkan proses monitoring dan reporting produksi gula untuk pengambilan keputusan secara cepat dan akurat, serta mampu menghemat anggaran perusahaan dalam peningkatan proses produksi gula nusantara.

Semua komunikasi pada infrastruktur ini adalah melalui jaringan private dengan menggunakan openVPN yang terenkripsi dengan menggunakan SSL sehingga mengurangi celah keamanan dari aktivitas sniffing dan setiap aplikasi juga terintegrasi dengan CAS Server untuk membentuk lingkungan Single Sign On yang mana memberikan kemudahan untuk pengguna dalam mengakses aplikasi-aplikasi tersebut dalam proses peningkatan produksi gula nusantara.

Index Terms—: Jaringan Private, Central Authentication, Monitoring

I. LATAR BELAKANG

SEBAGAI salah satu produsen Gula Nusantara, PT. Perkebunan Nusantara X (Persero) mempunyai 11 unit pabrik gula yang tersebar berbagai wilayah di Jawa Timur. Selain itu pula juga mempunyai beberapa unit usaha seperti Rumah Sakit, Perkebunan Tembakau dan lain-lain.

Dalam proses produksi gula, banyak faktor-faktor yang mempengaruhi hasil dari produksi gula tersebut mulai dari bahan baku, otomasi pabrik, sampai dengan perangkat lunak

yang digunakan untuk mempercepat proses produksi gula. Perangkat lunak yang digunakan sangat mempengaruhi keputusan dari setiap proses produksi dan mengontrol perhitungan serta laporan sehingga sesuai dengan keadaan riil di lapangan serta mengurangi kemungkinan kecurangan dan human error.

PT. Perkebunan Nusantara X (Persero) selaku pemimpin produksi dari 11 pabrik gula di seluruh Jawa Timur tentunya harus selalu memantau secara langsung proses dan hasil produksi dari setiap pabrik gula. Dan jika hal tersebut dilakukan secara manual, tentunya akan menghabiskan dana yang jelas tidak sedikit. Apalagi untuk monitoring secara langsung setiap proses pada tiap bagian, misal adalah timbangan, kemudian Gilingan, akan membutuhkan akomodasi yang besar dan waktu yang cukup lama.

Dilatarbelakangi masalah-masalah tersebut diatas, kami ingin membangun sebuah solusi berupa Enterprise Network Application System yang berfungsi untuk mengintegrasikan seluruh Aplikasi Produksi Pabrik Gula PT Perkebunan Nusantara X (Persero) melalui Jaringan Private dan mengoptimalkan proses monitoring dan reporting produksi gula untuk pengambilan keputusan secara cepat dan akurat, serta mampu menghemat anggaran perusahaan dalam peningkatan proses produksi gula nusantara.

II. PERUMUSAN MASALAH

Beberapa lingkup permasalahan yang akan dibahas dalam penelitian proyek akhir ini diantaranya :

- 1) Membangun Infrastruktur Virtual Private Network, yang berfungsi sebagai environment lalu lintas data dalam proses integrasi aplikasi produksi Pabrik Gula PT. Perkebunan Nusantara X (Persero)
- 2) Membangun Central Authentication System, untuk meningkatkan keamanan akses data pada Central Application PT. Perkebunan Nusantara X (Persero) dan aplikasi-aplikasi middleware lain seperti Web-mail, Fileserver, dan lain-lain
- 3) Membangun Monitoring Streaming Server untuk monitor proses produksi di setiap pabrik gula yang terpusat di PT. Perkebunan Nusantara X (Persero)

III. BATASAN MASALAH

- 1) Sistem operasi yang akan digunakan adalah Linux Debian Lenny
- 2) Aplikasi Virtual Private Network Yang digunakan adalah OpenVPN dengan Enhancement Security
- 3) Protokol yang digunakan untuk komunikasi data adalah protocol HTTPS (HTTP Over SSL) dengan port 443 sehingga melindungi data dari proses sniffing (pengintaian) dan serangan-serangan lain.
- 4) Aplikasi yang digunakan untuk Central Authentication System menggunakan CAS
- 5) Untuk Monitoring Server Streaming dan video on demand menggunakan Aplikasi Red5 dan Flash Media Server 6. Bahasa pemrograman yang digunakan adalah Java, PHP, dan Shell Script
- 6) Pilot Project untuk tugas akhir ini sesuai dengan Arahan dan Perijinan dari PT. Perkebunan Nusantara X (Persero) adalah pada :
 - Kantor Direksi PT. Perkebunan Nusantara X (Persero) Surabaya
 - Unit Pabrik Gula Pesantren Baru, Kediri
 - Unit Pabrik Gula Tjoekir, Jombang
 - Unit Pabrik Gula Modjopangoong, Tulungagung.

IV. PERANCANGAN DAN PEMBUATAN SISTEM

Pada perencanaan dan pembuatan perangkat lunak ini akan dibahas tentang proses instalasi dan penyesuaian perangkat lunak agar dapat berjalan sesuai dengan infrastruktur pada PT. Perkebunan Nusantara X (Persero). Semua komunikasi antara node pusat server di Kantor Pusat Surabaya dan node pada Unit Pabrik di daerah-daerah adalah melalui jaringan Private secara virtual. Dengan menggunakan Central Authentication Service Pengguna yang belum terautentikasi akan diarahkan ke halaman autentikasi yang berada pada server autentikasi, seperti pada figure 1 dibawah ini :

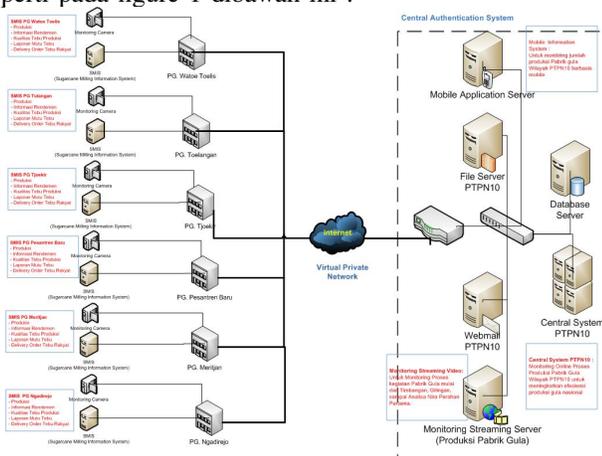


Figure 1. Gambar Desain Sistem Enterprise Network Application

Halaman autentikasi ini hanya berjalan pada mode https untuk memastikan semua proses autentikasi aman. Pada Figure 2 dan 3 diilustrasikan proses otentikasi antara web browser di sisi klien dan server CAS sebagai server otentikasi. Pengguna akan diautentikasikan berdasarkan database user ldap, setelah

pengguna terautentikasi maka aplikasi CAS akan mengirimkan tiket ke aplikasi yang membutuhkan otentikasi.

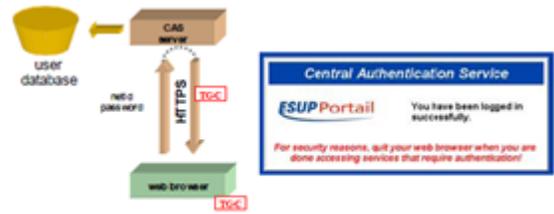


Figure 2. Proses Autentikasi pada Browser

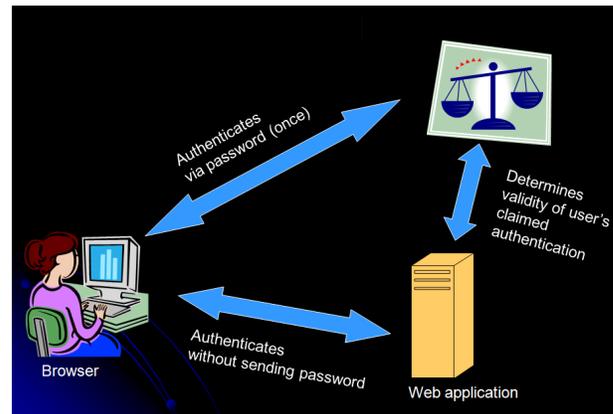


Figure 3. Proses Autentikasi dengan Ticket (single sign on)

Seluruh aplikasi yang digunakan dalam Infrastruktur dan aplikasi dalam proyek akhir ini, berjalan pada sistem operasi Linux untuk Server dan Sistem Operasi Windows untuk Client Yang terhubung dengan spesifikasi :

- Sistem Operasi : Debian Linux Kernel 2.6.26-2-686 i686
- Web Server : Apache2 versi 2.2.9-10+lenny8
- Tomcat Web Server : Tomcat6 versi 6.0.28-9
- Bahasa Pemrograman : PHP5 Versi 5.3.3-6
 - php5
 - php5-cli
 - php5-common
 - php5-curl
 - php5-imap
 - php5-ldap
 - php5-mysql
 - php5-suhosin
- Java Environment : Sun-java6 Versi 6-22-0lenny
- PEAR : php PEAR versi 5.3.3-6
- OpenVPN Server : OpenVPN 2.1.3-2 1
- CAS Server : CAS Server 3.4.4 Jasig
- phpCAS : phpCAS 1.2.0
- PEAR : php PEAR
- pam_cas : Cas-Client 2.0.11
- Flash Media Server : FMS 3.0.1 r
- Flash Media Live Encoder : FMLE 3.2

V. PENGUJIAN

A. Pengujian Tiap Modul Aplikasi

1) *Pengujian LDAP:* Pada pengujian dan analisa server LDAP ini akan di cek apakah server LDAP telah berjalan sesuai dengan yang diinginkan. Proses pengecekan dilakukan dengan metode yang telah dijelaskan pada bab 2. Akan tetapi pada proses pengujian ini hanya akan digunakan sebagian proses dari operasi-operasi yang ada pada LDAP.

Operasi yang digunakan pada pengujian ini adalah search and query yang tidak memerlukan proses bind. Proses search and query dapat dilakukan dengan mengetikkan perintah :

```
$ldapsearch -x -b dc=torrent,cn=admin,dc=enterprise-ptpn10,dc=com
```

Keluaran dari perintah diatas adalah seperti Figure 4 dibawah :

```
root@enterprise-ptpn10:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:00:e2:a2:c0:71
          inet addr:10.252.2.150  Bcast:10.252.2.255  Mask:255.255.255.0
          inet6 addr: 2001:470:8049:2:200:e2ff:fea2:c071/64 Scope:Global
          inet6 addr: fe80::200:e2ff:fea2:c071/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:166711208  errors:0  dropped:0  overruns:3581  frame:3581
          TX packets:161180875  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0  txqueuelen:1000
          RX bytes:2883860092 (2.6 GiB)  TX bytes:3864722767 (3.5 GiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:15818  errors:0  dropped:0  overruns:0  frame:0
          TX packets:15818  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0  txqueuelen:0
          RX bytes:38646776 (36.8 MiB)  TX bytes:38646776 (36.8 MiB)

tun0     Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:10.8.0.1  P-t-P:10.8.0.2  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:52  errors:0  dropped:0  overruns:0  frame:0
          TX packets:56  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0  txqueuelen:100
          RX bytes:7392 (7.2 KiB)  TX bytes:28371 (27.7 KiB)

root@enterprise-ptpn10:~#
```

```
root@enterprise-ptpn10:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:00:e2:a2:c0:71
          inet addr:10.252.2.150  Bcast:10.252.2.255  Mask:255.255.255.0
          inet6 addr: 2001:470:8049:2:200:e2ff:fea2:c071/64 Scope:Global
          inet6 addr: fe80::200:e2ff:fea2:c071/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:166711208  errors:0  dropped:0  overruns:3581  frame:3581
          TX packets:161180875  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0  txqueuelen:1000
          RX bytes:2883860092 (2.6 GiB)  TX bytes:3864722767 (3.5 GiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:15818  errors:0  dropped:0  overruns:0  frame:0
          TX packets:15818  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0  txqueuelen:0
          RX bytes:38646776 (36.8 MiB)  TX bytes:38646776 (36.8 MiB)

tun0     Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:10.8.0.1  P-t-P:10.8.0.2  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:52  errors:0  dropped:0  overruns:0  frame:0
          TX packets:56  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0  txqueuelen:100
          RX bytes:7392 (7.2 KiB)  TX bytes:28371 (27.7 KiB)

root@enterprise-ptpn10:~#
```

Figure 5. Output openVPN Server gateway

B. Prosedur Pengujian Normal

Pada pengujian dengan prosedur normal ini, yaitu dimana pengguna menjalankan sesuai dengan alur sistem yang telah dibangun.

1) *Proses Pengujian Webmail:* Untuk proses pengujian kali ini, akan diuji integrasi antara Roundcube webmail dan Login CAS Server. Selanjutnya, ketika user memilih menu Webmail Enterprise-PTPN10, maka browser akan langsung membuka tab baru, berupa halaman login CAS dengan service nya berupa Webmail. Terlihat seperti Figure 5 dibawah :

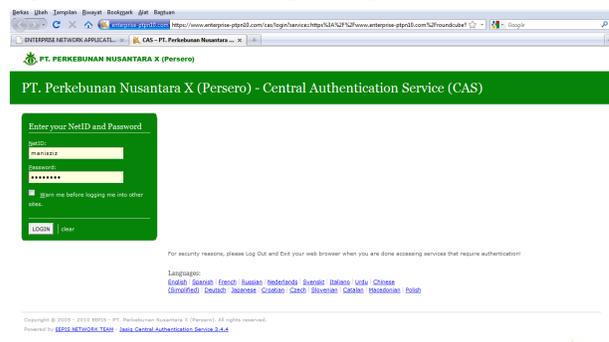


Figure 6. Halaman Login Webmail yang diintegrasikan dengan CAS

Figure 4. Output LDAPSearch pada server enterprise-ptpn10.com

Jika keluaran diatas result – success, berarti proses binding pada LDAP telah sukses dan bias digunakan untuk autentikasi oleh CAS server.

2) *Pengujian pada OpenVPN Server Gateway:* Selanjutnya adalah pengujian pada aplikasi OpenVPN server. Untuk pengujian openVPN, diperlukan koneksi langsung pada client, untuk melihat, apakah openVPN berjalan dan berhasil membuat TUN/TAP network adapter yang akan digunakan untuk berkomunikasi dengan server gateway dan client.

Pengujian pada server adalah dengan perintah :

```
#!/etc/init.d/openvpn restart
```

```
#!/etc/init.d/openvpn restart
```

Output dari perintah diatas seperti Figure 5 dibawah ini :

Terlihat dari figure 6 diatas, URL dari roundcube telah diredirect menuju halaman login CAS, karena terdeteksi user belum login pada aplikasi sebelumnya.

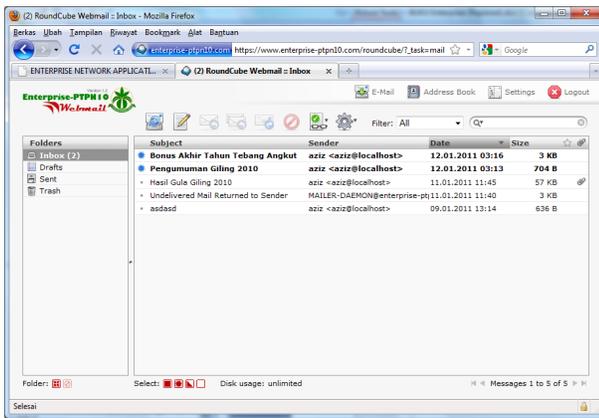


Figure 7. Halaman Webmail User yang berhasil Authentikasi

Dari output figure 7 diatas, integrasi antara Roundcube Webmail dan CAS Server telah berhasil dan user bisa masuk ke dalam webmail, usai login dengan menggunakan CAS. Kemudian untuk proses logout, sudah tergabung dalam interface roundcube, sehingga proses `session_destroy()` benar-benar telah bersih dari browser seperti pada figure 8 dibawah ini :

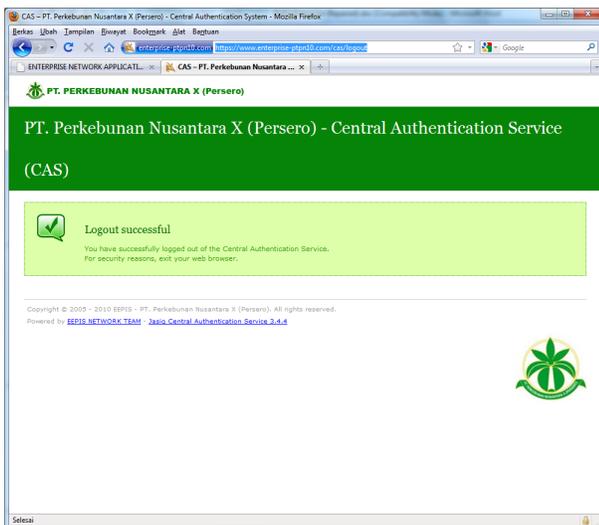


Figure 8. Proses Logout Webmail

2) *Pengujian Dengan Central Application System:* Central Application System adalah sebuah Sistem Informasi Pelaporan Bidang Produksi yang berbasis Web dan Mobile. Pada pengujian kali ini, akan dibagi menjadi 2 bagian, yaitu pengujian aplikasi berbasis Web dan aplikasi berbasis Mobile. Pada halaman utama, user akan memilih menu Central Application yang mana akan langsung menuju pada halaman Central Application di Tab baru dan jika berhasil login maka akan langsung diredirect menuju central application system, seperti Figure 9 dibawah :



Figure 9. Central Application System yang terintegrasi dengan CAS

Berikut Figure 9 diatas adalah halaman utama, setelah berhasil login pada CAS Server dan setelah user terautentikasi pada Sistem, maka CAS akan melempar service pada Central Application.

3) *Pengujian Dengan WAP Mobile Application:* Untuk melakukan uji coba pada aplikasi WAP, terlebih dahulu adalah menyiapkan environment browser yang mendukung format WAP. Dalam hal ini pada browser Mozilla Firefox telah menyediakan plugin untuk bias mengakses halaman WAP pada browser Firefox. Setelah dipasang plugin tersebut, maka aplikasi WAP bisa langsung dijalankan di Firefox. Untuk pengujian aplikasi WAP Mobile ini, sama dengan aplikasi-aplikasi sebelumnya, yaitu pengguna memilih menu "WAP Mobile Application" pada halaman utama. Setelah pengguna login pada CAS, maka aplikasi akan diredirect pada halaman WAP yang sebenarnya. Seperti pada Figure 10 dibawah :

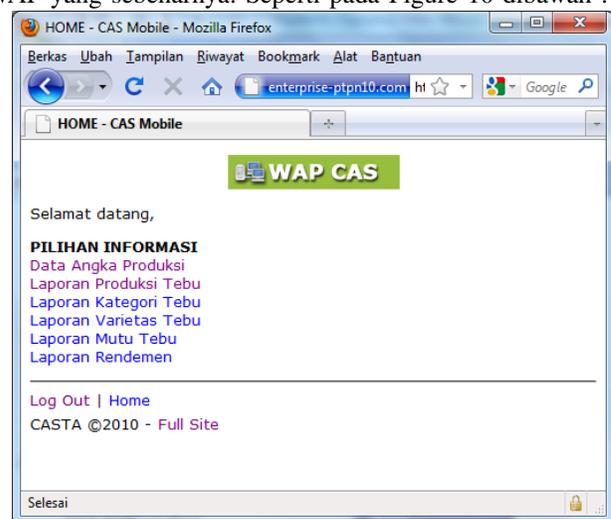


Figure 10. Halaman Utama aplikasi WAP Mobile

Pada gambar diatas aplikasi WAP Mobile berhasil login dengan menggunakan login CAS.

4) *Pengujian Monitoring Streaming Server*: Untuk pengujian aplikasi Monitoring Streaming Server ini, dilakukan pada server Streaming RTMP dan client yang mengirimkan input encoder. Langkah pertama untuk pengujian ini adalah menjalankan aplikasi Flash Media Live Encoder (FMLE) pada client untuk memberikan input pada server streaming. Sehingga proses pengujian bisa dilakukan untuk Monitoring Streaming Server seperti terlihat pada Figure 11.

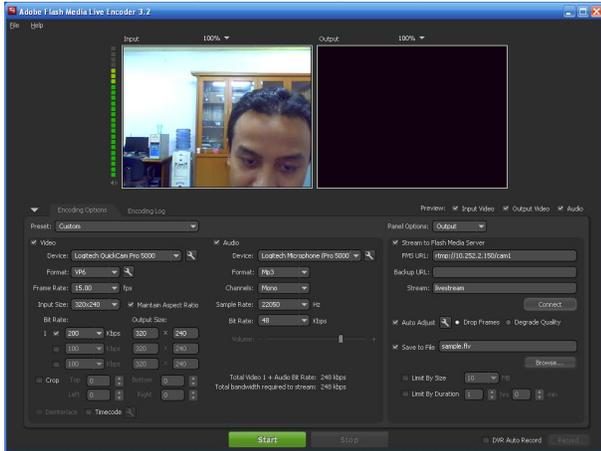


Figure 11. Aplikasi FMLE

Kemudian pada aplikasi Monitoring Streaming Server pada browser, juga akan menampilkan video live streaming dari Webcam client yang melakukan encoding dan dikirimkan pada server RTMP. Pada gambar dibawah ini terlihat pada browser, aplikasi Monitoring Streaming Server berhasil menampilkan video Streaming dari client seperti Figure 12.

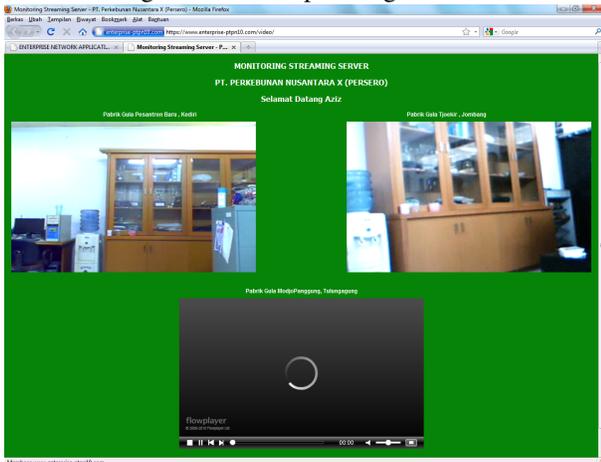


Figure 12. Aplikasi Monitoring Streaming Server

C. Prosedur Tidak Normal

Terdapat beberapa penanganan kesalahan input oleh user yang sudah diterapkan dalam aplikasi ini dan prosedur yang tidak tepat yang mengakibatkan aplikasi tidak berjalan dengan sesuai :

1) *Error dengan Sertifikat SSL tidak Terpercaya*: Komunikasi antara server dan client pada Proyek Akhir ini semua menggunakan SSL dan termasuk pada CAS Server juga menggunakan SSL. Tetapi ada perlakuan khusus pada CAS Server, yaitu membutuhkan SSL yang Terpercaya dari Vendor penyedia Sertifikat Digital.

Jika sertifikat tersebut adalah berupa self signed certificate maka autentikasi akan gagal dan proxy ticket tidak bisa divalidasi untuk dapat meneruskan service yang akan dituju oleh CAS setelah user melakukan login. Berikut adalah Figure 13 yang menunjukkan autentikasi yang gagal ketika sertifikat yang digunakan adalah berupa self signed certificate.



Figure 13. Autentikasi gagal karena sertifikat SSL tidak valid pada CAS

VI. ANALISA

Hasil dari uji coba aplikasi diagnosis telah memenuhi tujuan dari pembuatan perangkat lunak yang telah dipaparkan pada Bab I. Berdasarkan analisa dari beberapa pengujian pada bab sebelumnya, kesimpulan yang didapatkan adalah :

- 1) OpenVPN dapat membangun infrastruktur jaringan virtual secara private antara Server node (VPN gateway) dan 3 node lain yang direpresentasikan berada dalam lokasi geografis berbeda dan mampu berjalan seperti jaringan lokal yang terenkripsi.
- 2) CAS Server dapat diintegrasikan pada aplikasi-aplikasi seperti Roundcube Webmail, Sistem Informasi Central Application System, WAP Mobile Application, dan Monitoring Streaming Server untuk proses autentikasi sehingga tercipta lingkungan aplikasi berbasis Single Sign On
- 3) Monitoring Streaming Server dapat berjalan lancar dan mampu melakukan streaming tiap node yang tercentral pada Server enterprise-ptpn10. Aplikasi ini merepresentasikan yaitu mampu memberikan informasi keadaan dari tiap Unit pabrik gula untuk melihat secara live proses produksi di tiap Unit melalui Monitoring Streaming Server pada kantor pusat PTPN10.

VII. KESIMPULAN

Berdasarkan hasil pengujian dan analisa yang telah di bahas pada bab sebelumnya maka dapat diberikan beberapa kesimpulan sebagai berikut :

- 1) Aplikasi ini dijalankan pada komputer bersistem operasi Debian Linux 2.6.26-i686 sebagai server dan Microsoft

Windows XP SP2, SP3, Vista dan Windows 7 sebagai Client.

- 2) Semua Aplikasi yang terintegrasi dengan CAS, berjalan pada HTTPS sehingga memberikan keamanan yang cukup tinggi pada setiap aplikasi dan terintegrasi menjadi environment Single Sign On.
- 3) Semua Komunikasi pada Infrastruktur ini, melalui jaringan Private dengan menggunakan openVPN dan terenkripsi oleh SSL, sehingga mengurangi celah keamanan dari aktivitas Sniffing.

REFERENCES

- [1] VPN - Virtual Private Network and Open-VPN. From : http://www.openvpn.org/VPN_-_Virtual_Private_Network_and_OpenVPN, (Diakses 23 Juli 2010)
- [2] Sufian, Indra (2010). Pengertian Virtual Private Network. From : <http://www.indrasufian.web.id/2007/09/19/pengertian-virtual-private-network-vpn/>, (diakses 20 Juni 2010)
- [3] Santoso, Budi (2009). Enkripsi Komunikasi Data dengan OpenVPN. From : <http://ardelindo.livejournal.com/1768.html>, (diakses 16 february 2009)
- [4] Aubry Pascal, Julien Marchal, Vincent Matheieu, ESUP-Portail: open source Single Sign-On with CAS (Central Authentication Service) Paper On EUNIS2004, 2004
- [5] Wikan A., Gatra, Winarno, SST, M. Kom, Idris (2009). Implementasi Central Authentication Service Pada Eepis-Network, Teknik Informatika PENS ITS, Surabaya
- [6] Tutorial Genting Started With Red5 Server. From : http://www.red5tutorials.net/index.php/Tutorials:Getting_Started_With_Red5_Server, (diakses 1 Oktober 2010)
- [7] Adobe System Inc. 2010. Adobe® Flash® Media Server 3.0.1 Developer Guide.
- [8] Adobe System Inc. 2010. Adobe® Flash® Media Live Encoder 3.2 Developer Guide.
- [9] Mazurek, Drew, uPortal And Yale Central Authentication Service, ITS Technology & Planning, Yale University, JA-SIG Summer Conference '04, Denver
- [10] Roundcube - Ajax Modern Webmail. From : <http://www.wiki.roundcube.org/>, (Diakses 27 Desember 2010)