BAB IV

IMPLEMENTASI DAN PENGUJIAN SISTEM

Pada bab ini akan dilakukan implementasi dan pengujian terhadap jaringan VPN yang dibangun. Implementasi dilakukan berdasarkan analisis dan perancangan yang telah dibuat. Setelah implementasi selesai, maka selanjutnya akan dilakukan pengujian pada kinerja dari jaringan VPN yang telah dibangun.

4.1 Implementasi Sistem

Tahapan implementasi sistem merupakan tahap penerjemahan perancangan berdasarkan hasil analisis serta penerapan kebutuhan pada keadaan yang sebenarnya. Pengunaan VPN untuk Client personal adalah menghubungkan suatu client dengan network VPN Server melalui jalur internet dan pengguna seolah-olah berada dalam satu jaringan lokal. Dalam mengkoneksikan client dengan VPN server dibutuhkan beberapa tahapan settingan pada komputer client. Berdasarkan pada analisis sistem operasi yang digunakan oleh para pegawai, maka VPN ini akan diimplementasikan pada sistem operasi Windows.

4.1.1 Implementasi Perangkat Keras

Perangkat keras yang dibutuhkan untuk mengimplementasikan remote access VPN di Balai Besar Keramik ini dapat dilihat pada tabel berikut.

Tabel 4.1 Perangkat Keras Client

Perangkat Keras	Keterangan
Processor	Intel Pentium Dual Core CPU t3200
RAM	3 Gb
Harddisk	160 Gb

Monitor	1024x768
Modem	USB Modem
Monitor	LCD 14 Inch, resolusi 1024 x 768 pixel

4.1.2 Implementasi Perangkat Lunak

Perangkat lunak yang dibutuhkan untuk mengimplementasikan remote access VPN di Balai Besar Keramik ini dapat dilihat pada tabel.

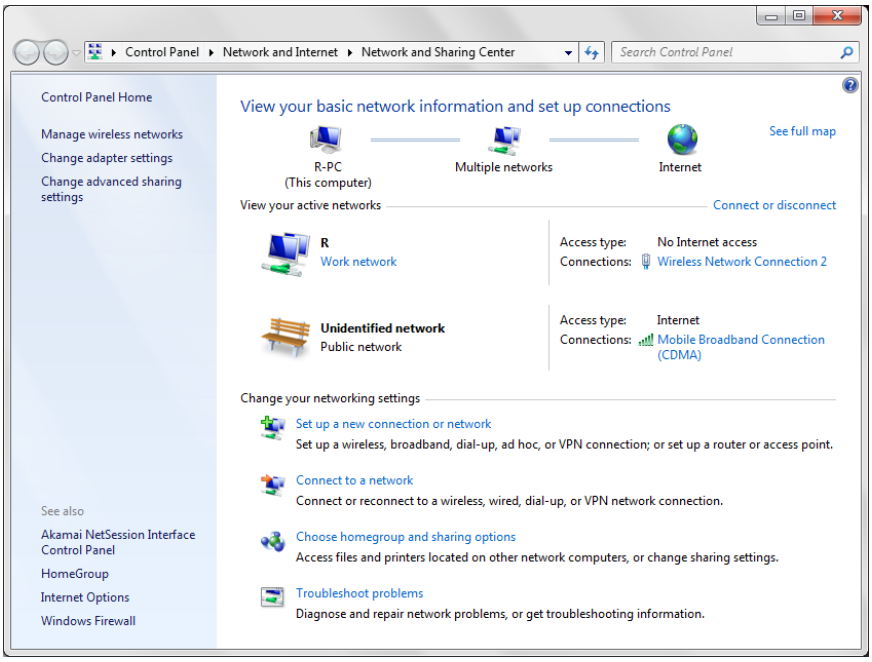
Tabel 4.2 Perangkat Lunak Client

Perangkat Lunak	Keterangan
Sistem Operasi	Ms. Windows 7
Web Browser	Google Chrome, Mozilla Firefox
FTP Client	WinSCP

4.1.3 Konfigurasi Client

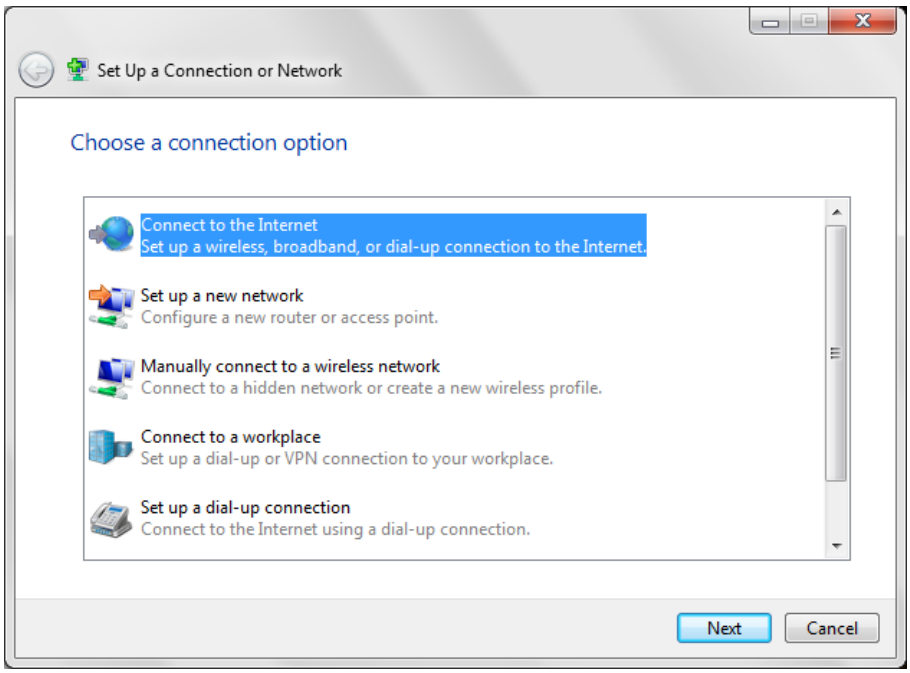
Penggunaan VPN untuk Client personal adalah menghubungkan suatu client dengan network VPN Server melalui jalur internet dan pengguna seolah-olah berada dalam satu jaringan lokal. Dalam mengkoneksikan client dengan VPN server dibutuhkan beberapa tahapan settingan pada komputer client. Berikut adalah tahapan client/user untuk koneksi ke VPN menggunakan sistem operasi windows

1. Masuk ke “ Network and Sharing Center”:, lalu pilih “Set up a new connection or network”



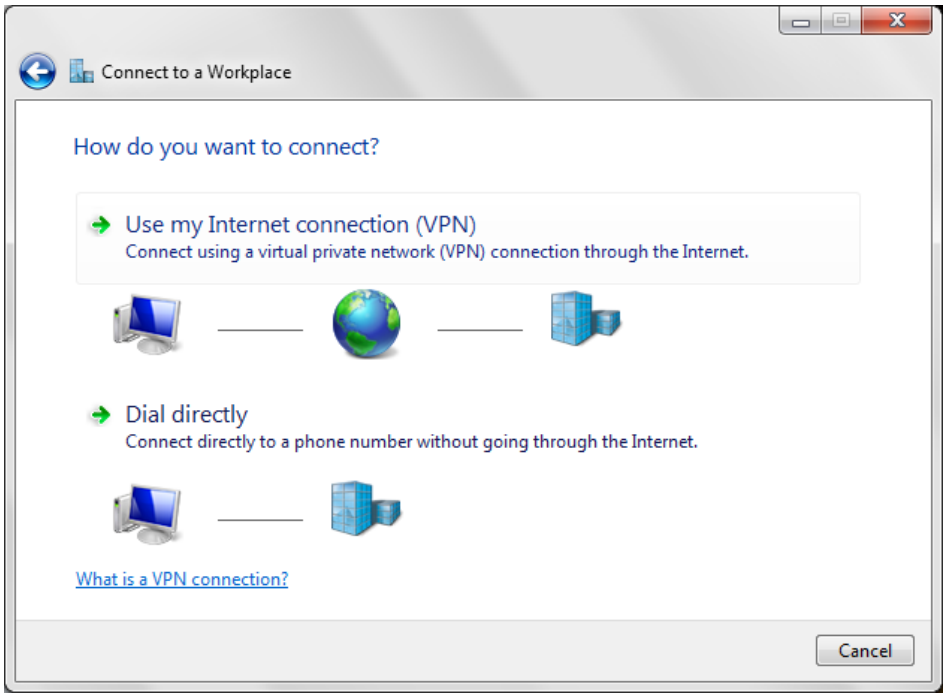
Gambar 4.1 Network and Sharing Center

2. Pilih ‘Connect to a workplace’ dari daftar dan klik next.



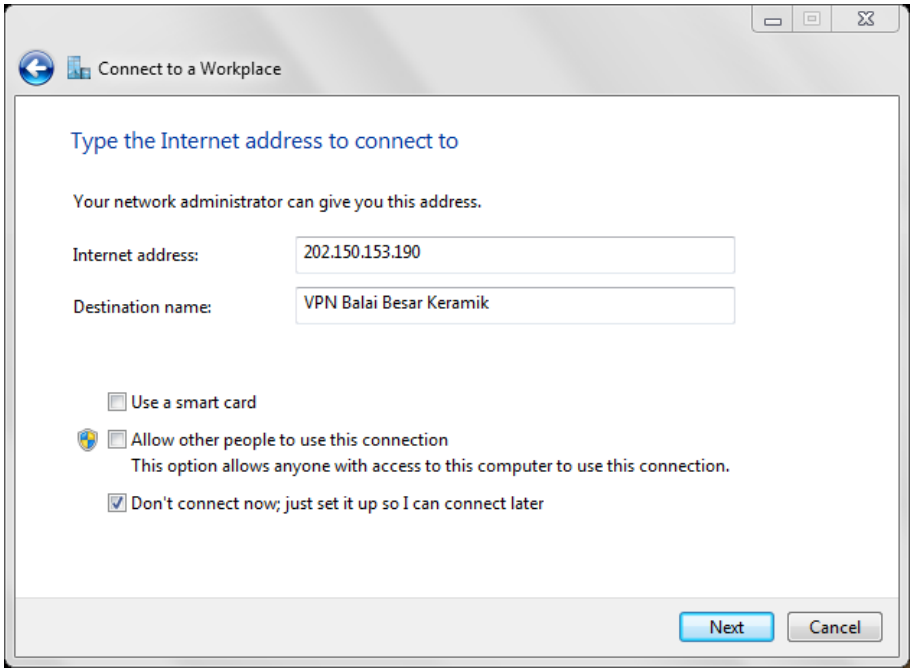
Gambar 4.2 Setup a Connection

3. Setelah itu lalu pilih “Use my internet connection VPN”



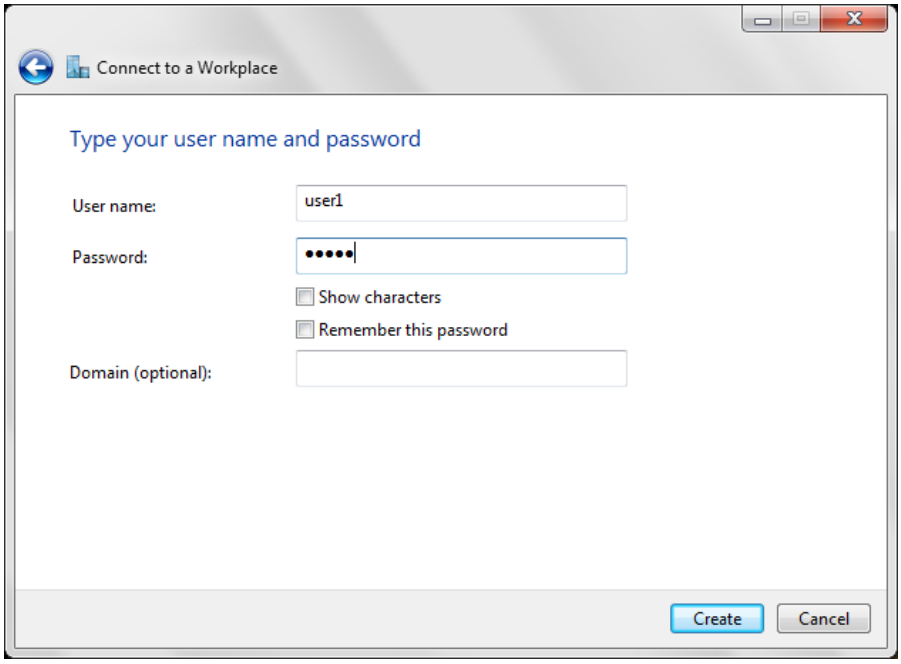
Gambar 4.3 Use My Internet Connection

4. Masukan IP Publik Balai Besar Keramik dan nama untuk VPN, lalu ceklis “Don’t connect now.”



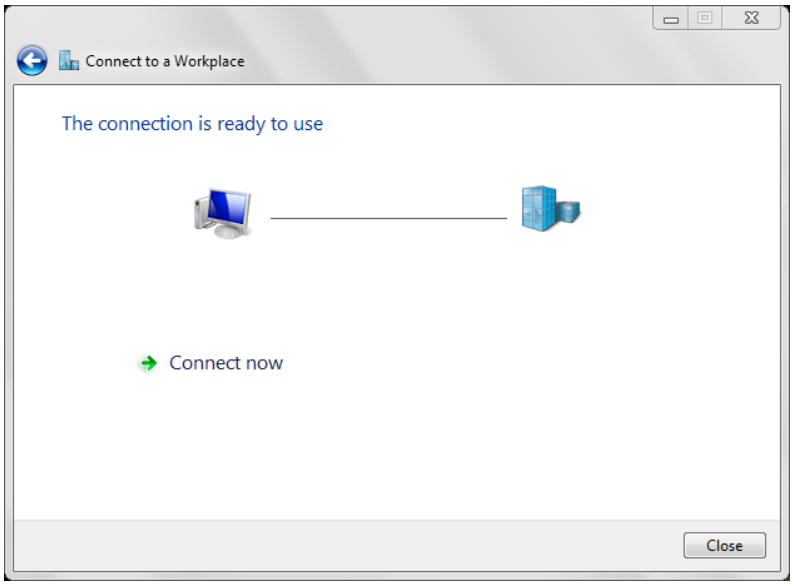
Gambar 4.4 Penamaan Koneksi Jaringan VPN

5. Masukan username dan password yang telah disetting di VPN server sebagai secret PPP atau user di User Manager.



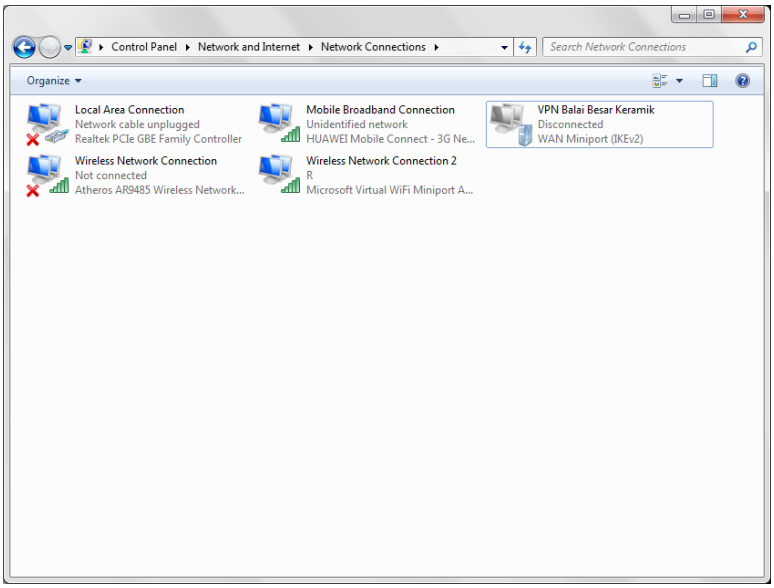
Gambar 4.5 Masukkan Username dan Passoword

6. Selanjutnya close pada bagian connect to a workplace.



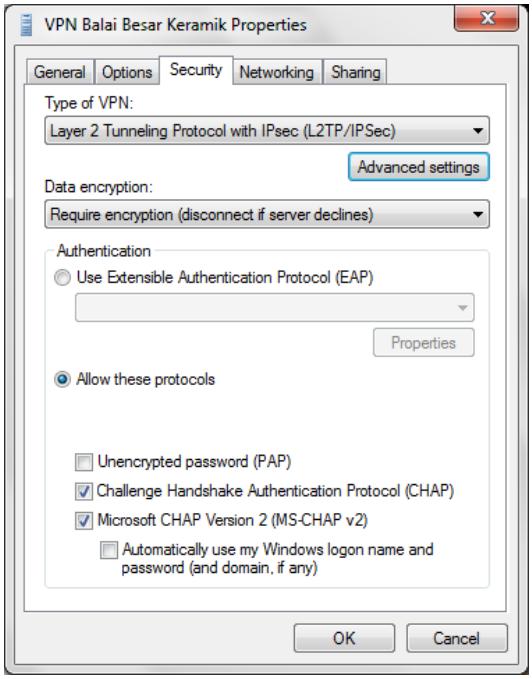
Gambar 4.6 Connect To VPN

7. Lalu pada VPN Balai Besar Keramik yang tadi dibuat, klik kanan pilih properties.



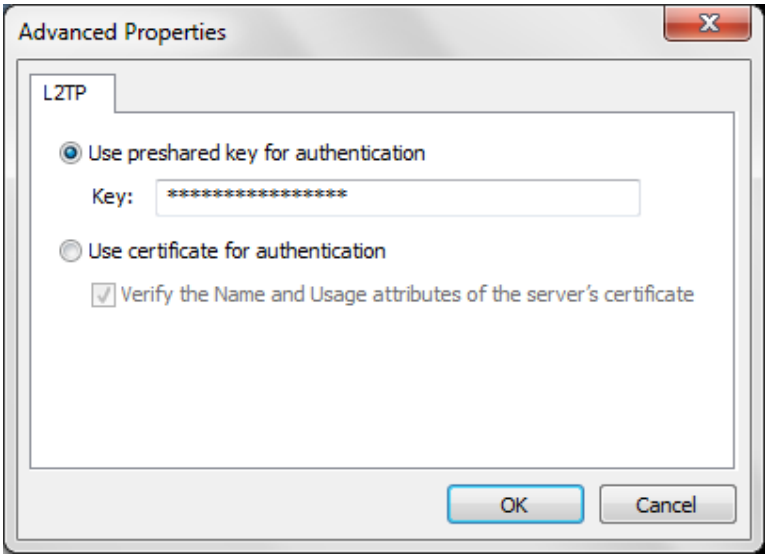
Gambar 4.7 Nework Connection

8. Pilih tab Security, lalu pilih type of VPN menjadi L2TP/IPSEC



Gambar 4.8 Setting Security

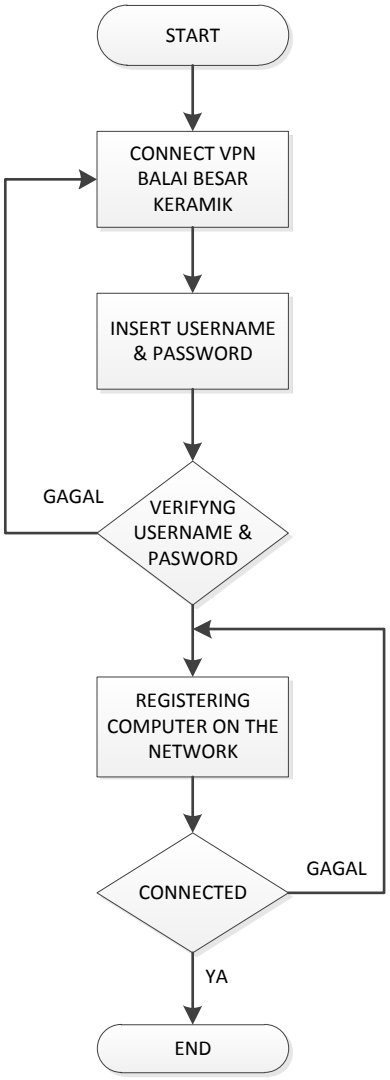
9. Lalu pada advanced setting masukkan preshared key yang sudah dibuat di IPsec Peers di VPN server.



Gambar 4.9 Masukkan Pre-shared Key

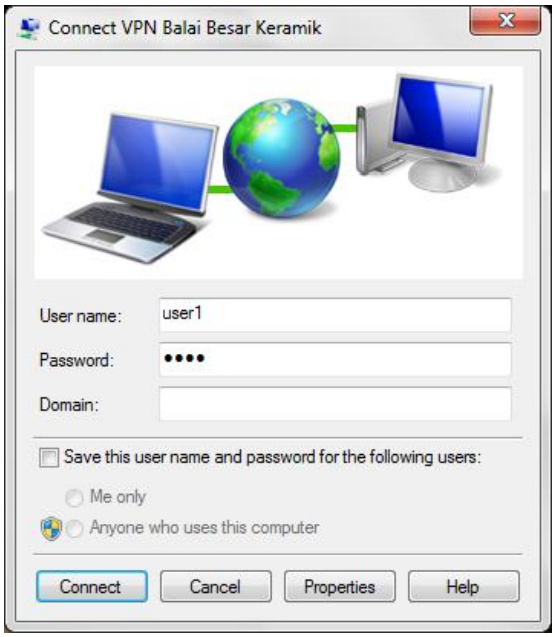
4.1.4 Tahap Dialing VPN

Langkah selanjutnya adalah koneksi ke akses remote atau server VPN yang sudah dibangun di Balai Besar Keramik. Tahapan dialing VPN ini dijelaskan dengan flowchart sebagai berikut :



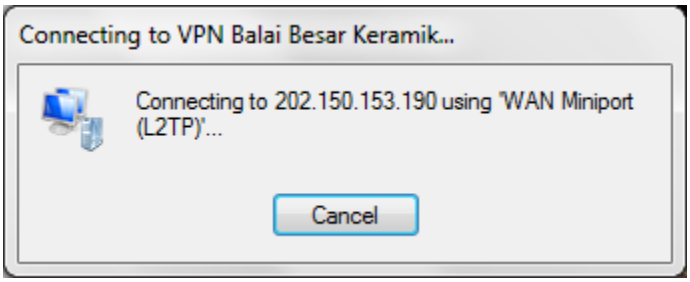
Gambar 4.10 Flowchart Dialing VPN

Masuk ke network connection lalu pilih connection yang sudah dibuat yaitu VPN Balai Besar Keramik. Lalu masukkan nama dan password yang telah dibuat berdasarkan secret PPP atau user di user manager.



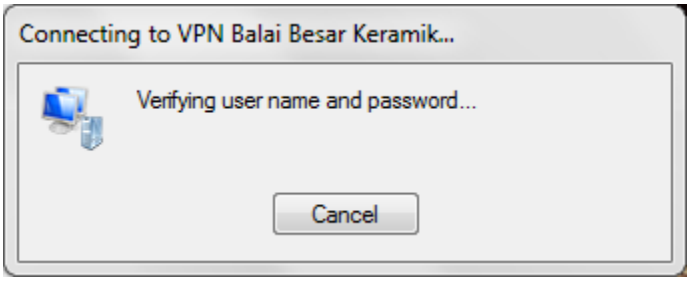
Gambar 4.11 Connect VPN Balai Besar Keramik

1. Setelah itu proses koneksi ke VPN akan dimulai.



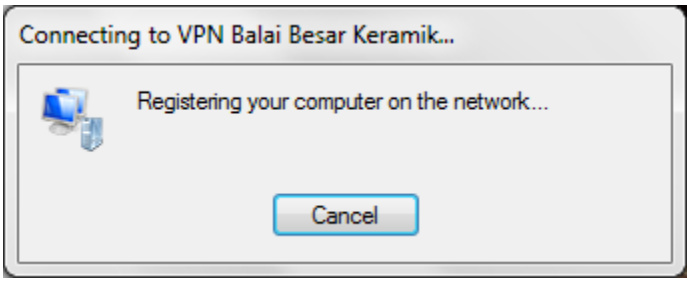
Gambar 4.12 Proses Connecting

2. Proses verifying user name dan password.



Gambar 4.13 Proses Verifying

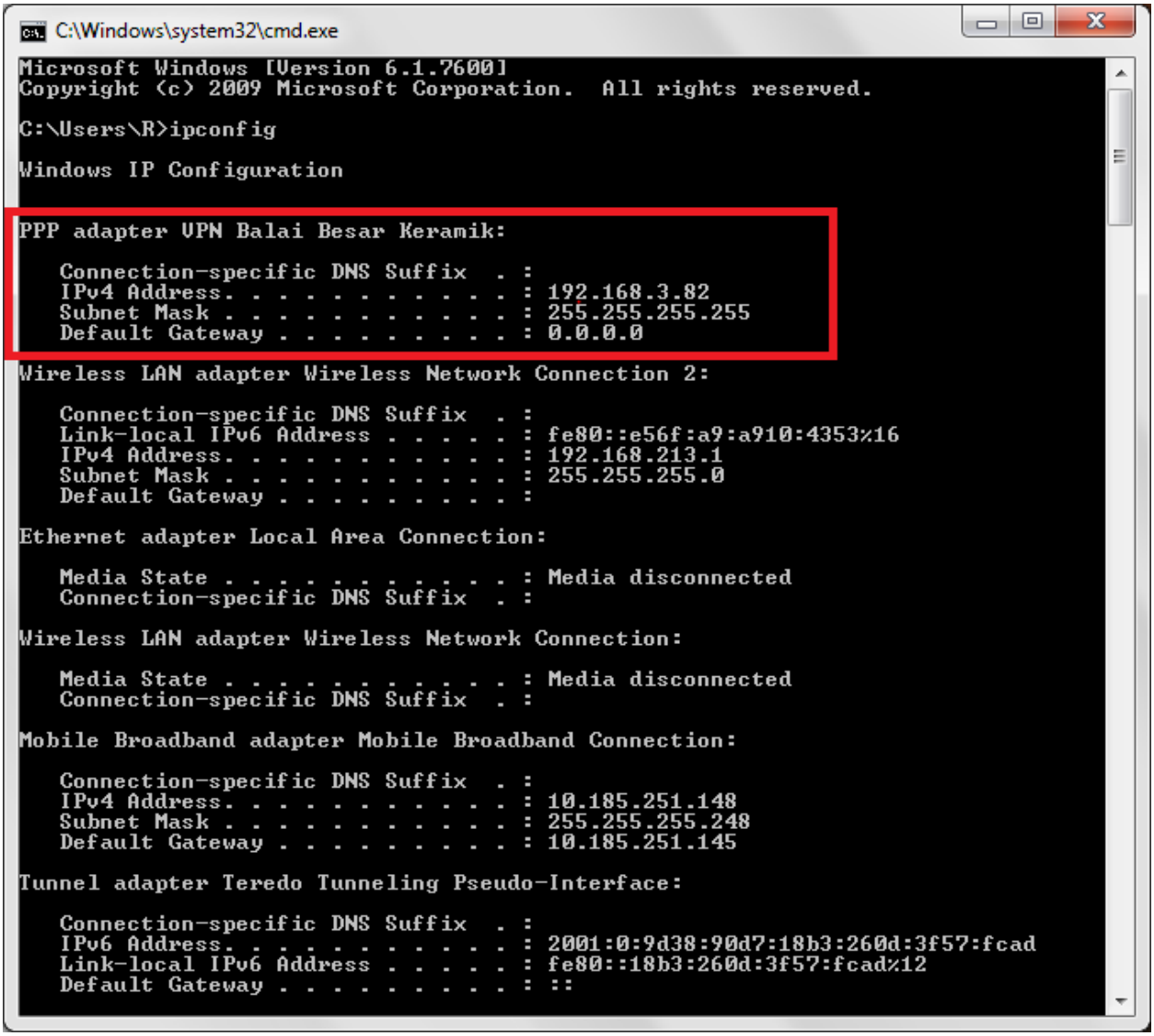
3. Dan yang terakhir proses registering komputer ke network.



Gambar 4.14 Registering Komputer ke Network

4.1.5 Tes Ping

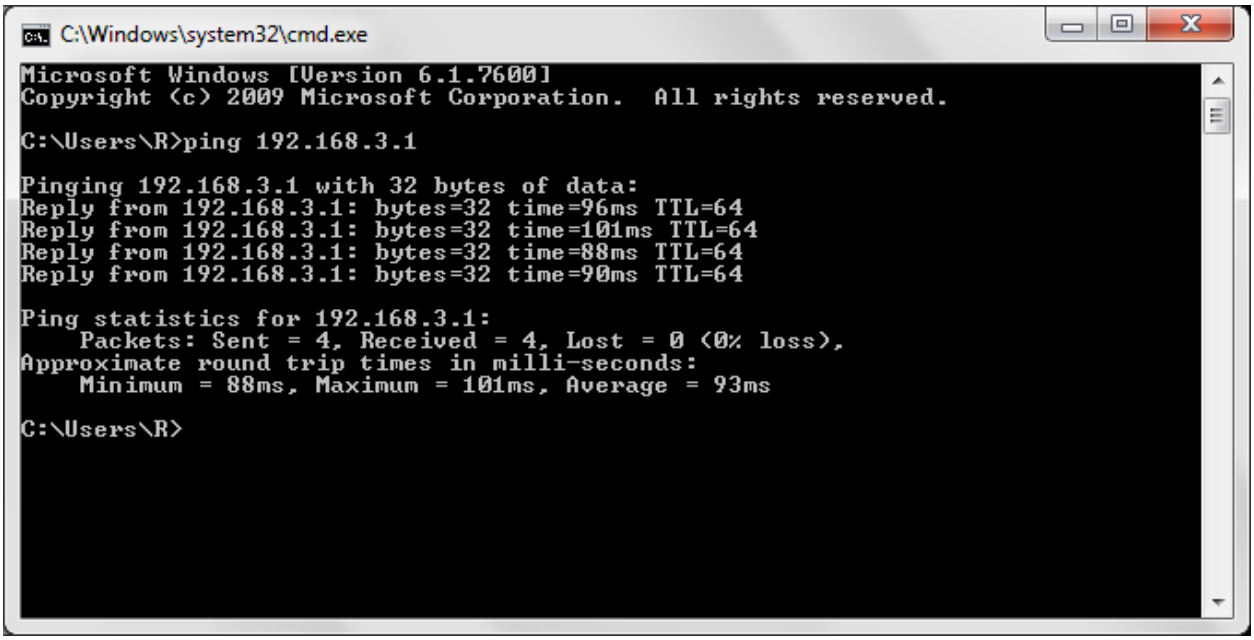
Pengujian ini bertujuan untuk mengetahui perbedaan kondisi ipconfig pada command prompt. Pada pengujian startup client ini memggunakan sistem operasi berbasis Windows. Berikut ini adalah kondisi ipconfig setelah connect ke VPN :



Gambar 4.15 CMD IPconfig Setelah Connect VPN

Setelah melakukan perintah ipconfig, dapat diketahui bahwa ip address yang didapat adalah 192.168.3.82 untuk koneksi saat ini, ip address yang didapat bisa berubah – ubah karena VPN server mempunyai DHCP server yang dinamis. Range IP address untuk VPN client adalah 192.168.3.2-192.168.3.100 yang telah di-setting di IP Pool mikrotik.

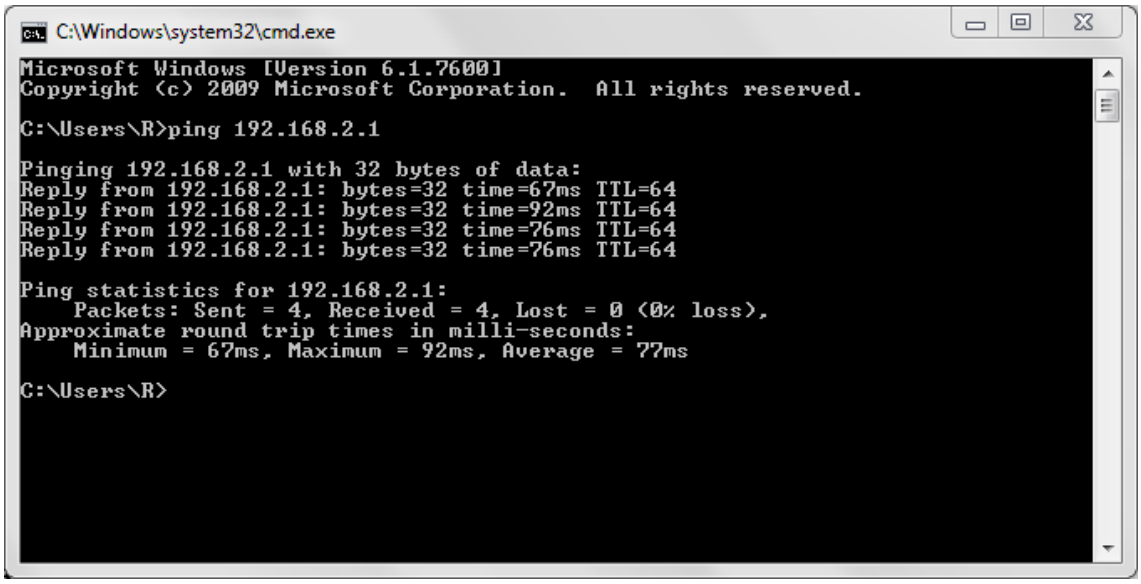
Tahap selanjutnya pengujian koneksi dengan tes ping ke IP adress server VPN yang mempunyai IP address 192.168.3.1 seperti gambar di bawah..



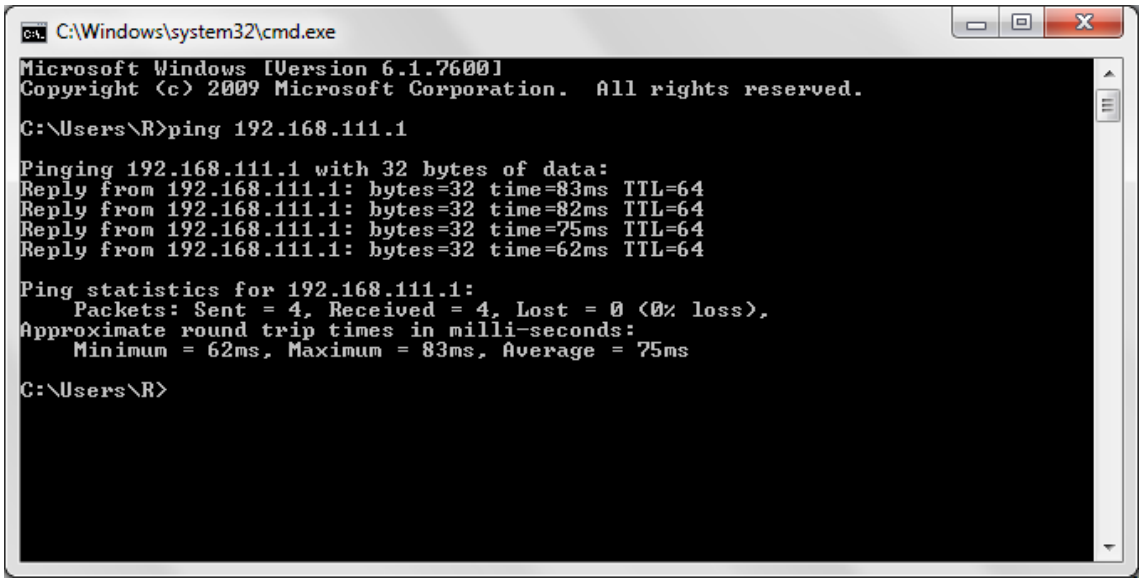
Gambar 4.16 Ping Server VPN

Setelah dilakukan proses ping ke IP address VPN server, langkah selanjutnya adalah pengujian ke IP address lokal VPN yang masuk ke jaringan LAN Balai Besar Keramik. Proses tes ping diatas menandakan user VPN sudah terkoneksi ke jaringan lokal Balai Besar Keramik melalui VPN server.

Untuk memastikan lebih lanjut koneksi VPN ke jaringan lokal maka akan dilakukan tes ping ke IP address server yang ada di Balai Besar Keramik.



Gambar 4.17 Ping Loka



Gambar 4.18 Ping File Server

4.2 Pengujian

Pada penelitian ini, dilakukan pengujian terhadap performansi remote access VPN yang yang telah dibuat dengan beberapa skenario pengujian. Pada penelitian ini dilakukan pengujian terhadap remote access VPN dengan beberapa skenario.

4.2.1 Skenario Pengujian Alpha

Pada pengujian alpha akan dilakukan skenario pengujian yang terdiri atas dua pengujian diantaranya.

1. Pengujian login sebagai Admin

   Pengujian ini dilakukan pada winbox dan user manager sebagai admin, dengan mencoba memasukkan user name dan password.

Tabel 4.3 Login Admin

Kasus dan hasil Uji (Data Normal)	
Data Masukan	User ID : admin dan Password : admin
Yang Diharapkan	User ID dan password yang dimasukkan benar sehingga dapat masuk ke winbox
Pengamatan	User ID dan password yang dimasukkan diterima dan masuk ke winbox
Kesimpulan	Diterima
Kasus dan hasil Uji (Data Salah)	
Data Masukan	Username: a atau kosong dan Password: b atau kosong
Yang Diharapkan	Setelah klik tombol login maka muncul pesan accsess was denide login invalid

Pengamatan	Muncul pesan bahwa Login Invalid
Kesimpulan	Ditolak

2. Login User VPN

Pengujian ini dilakukan dengan mencoba connect ke VPN sebagai user, dengan memasukkan username dan password.

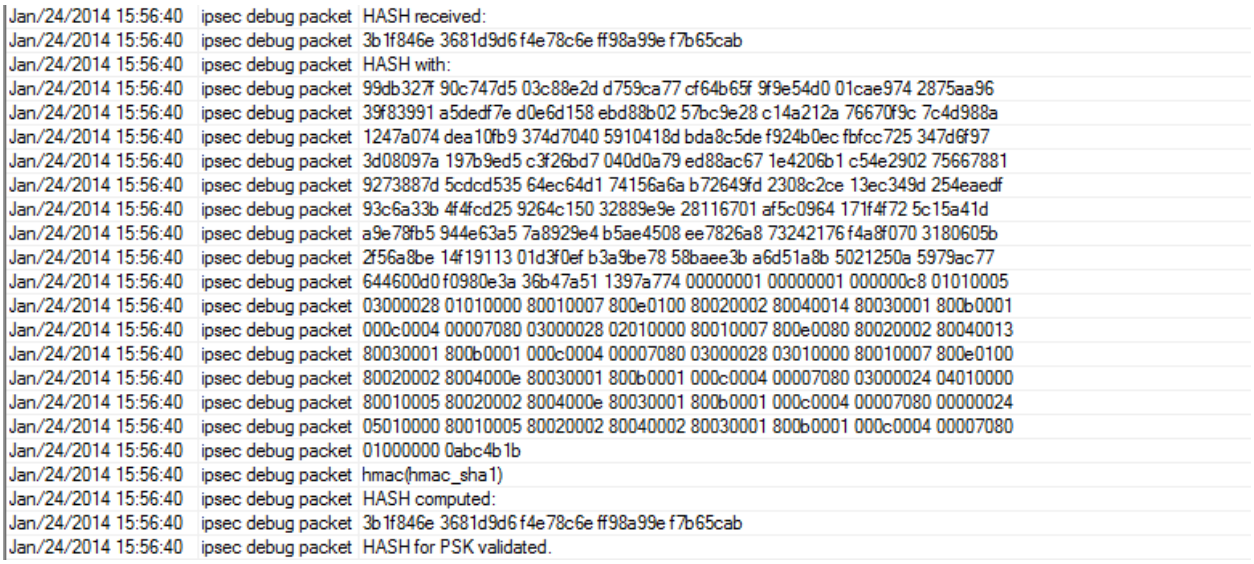
Tabel 4.4 Login User

Kasus dan hasil Uji (Data Normal)	
Data Masukan	User ID : admin dan Password : admin
Yang Diharapkan	User ID dan password yang dimasukkan benar sehingga dapat masuk ke jaringan loka
Pengamatan	User ID dan password yang dimasukkan diterima dan masuk ke jaringan lokal
Kesimpulan	Diterima
Kasus dan hasil Uji (Data Salah)	
Data Masukan	Username: a atau kosong dan Password: b atau kosong
Yang Diharapkan	Setelah klik tombol login maka muncul pesan accsess was denide login invalid
Pengamatan	Muncul pesan bahwa Login Invalid
Kesimpulan	Ditolak

4.2.2 Pengujian IPSec

Dalam pengujian ini akan dilihat bagaimana cara kerja IPSec saat koneksi VPN terhubung. Pengujian ini dilakukan dengan melihat log di mikrotik, untuk melihat packet apa saja yang melintas ketika client melakkan dial ke VPN server.

1. Berikut ini adalah proses kinerja dari fungsi hash untuk memvalidasi preshared key



Gambar 4.19 Validasi Preshared Key

2. Berikut ini adalah proses kinerja dari algoritma enkripsi 3DES.

Jan/24/2014 15:56:40	ipsec debug packet	begin encryption.
Jan/24/2014 15:56:40	ipsec debug packet	encryption(3des)
Jan/24/2014 15:56:40	ipsec debug packet	pad length = 4
Jan/24/2014 15:56:40	ipsec debug packet	0800000c 011101f4 ca9699be 00000018 bf90ca55 73fe7a50 99920816 98526a03
Jan/24/2014 15:56:40	ipsec debug packet	2e173145 4c2e2e03
Jan/24/2014 15:56:40	ipsec debug packet	encryption(3des)
Jan/24/2014 15:56:40	ipsec debug packet	with key:
Jan/24/2014 15:56:40	ipsec debug packet	b5a96663 ceeaac1c e80f1f74 dd5166ac 27705baa 884a3afe
Jan/24/2014 15:56:40	ipsec debug packet	encrypted payload by IV:
Jan/24/2014 15:56:40	ipsec debug packet	ce1cdc59 448c79ab
Jan/24/2014 15:56:40	ipsec debug packet	save IV for next:
Jan/24/2014 15:56:40	ipsec debug packet	c175a00e d2298b01
Jan/24/2014 15:56:40	ipsec debug packet	encrypted.

Gambar 4.20 Kinerja 3DES

Dari gambar di atas bisa disimpulkan bahwa autentikasi dan enkripsi pada tunneling L2TP/IPsec berjalan dengan baik.

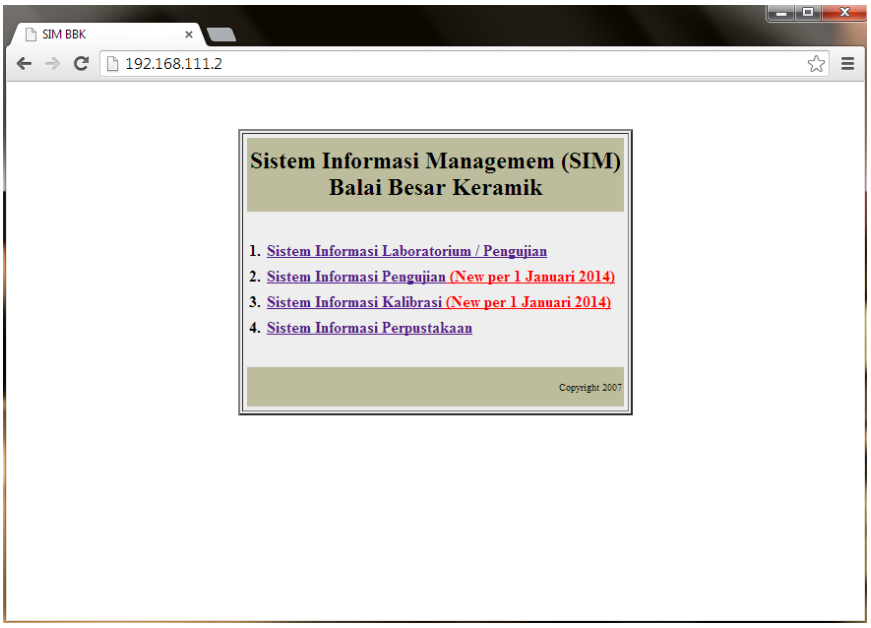
4.2.3 Pengujian akses server

Pengujian akses server ini akan dilakukan pada dua server yang sudah terhubung dengan VPN server sebelumnya, yaitu :

1. Webserver Lokal
2. FTP server
3. IP Camera
4. Aplikasi Intranet BBK

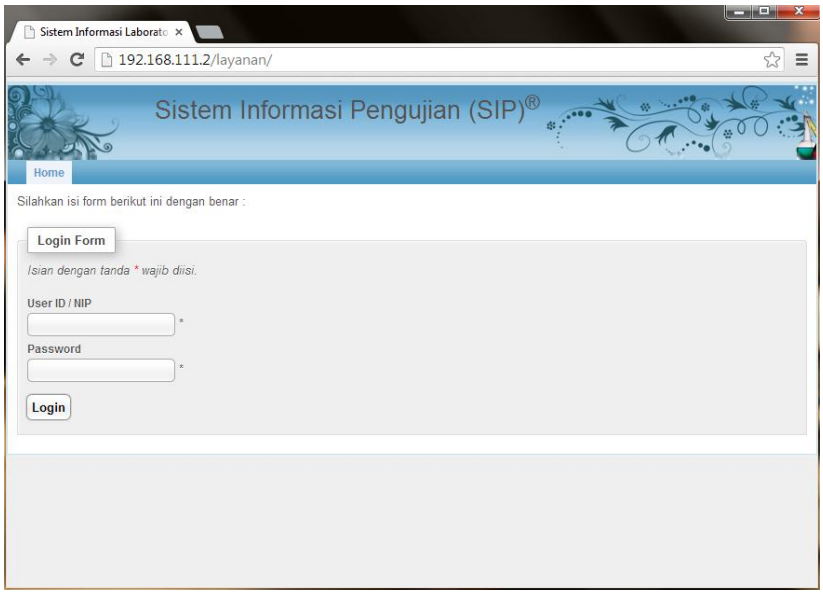
1. Berikut ini adalah pengujian akses server pada webserver lokal :

a. Akses terhadap Sistem Informasi Managemen (SIM)



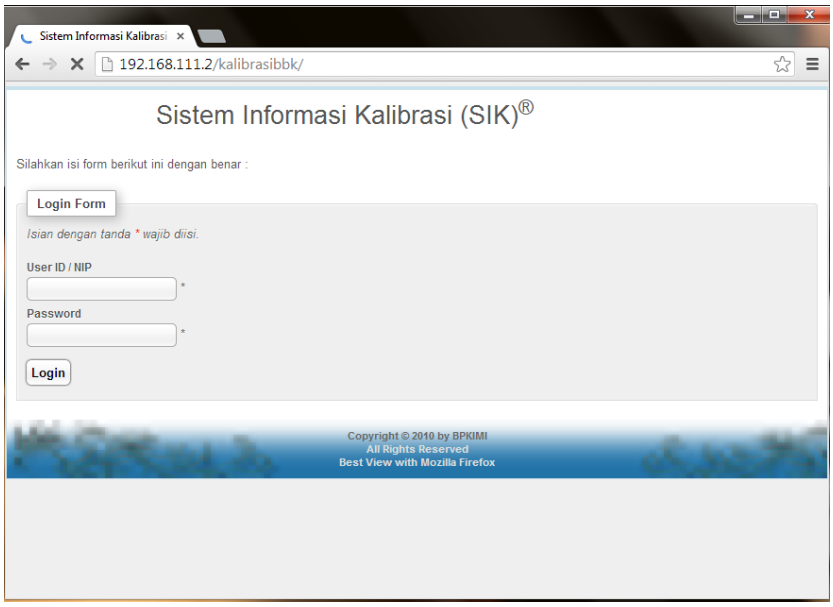
Gambar 4.21 Sistem Informasi Managemen

b. Akses terhadap Sistem Informasi Pengujian (SIP)



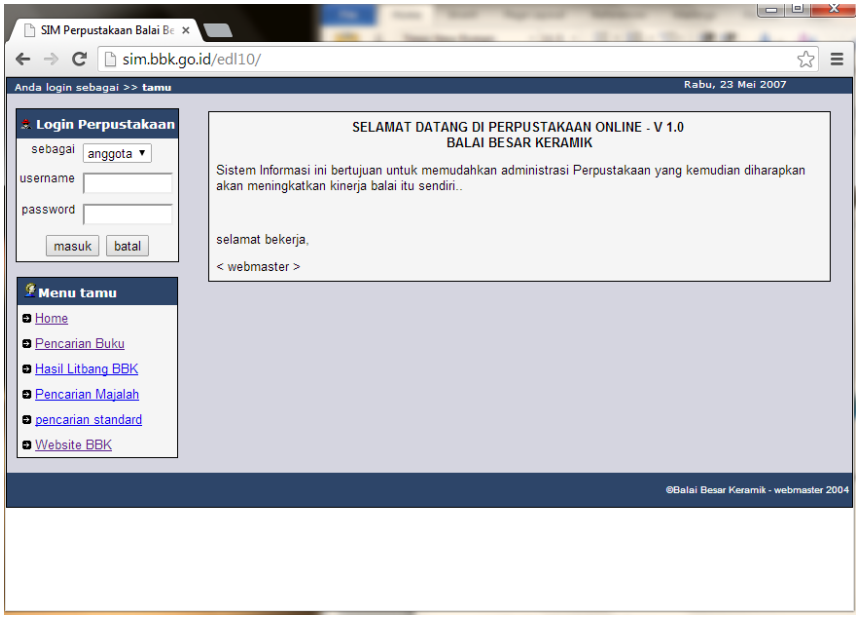
Gambar 4.22 Sistem Informasi Pengujian (SIP)

c. Akses terhadap Sistem Informasi Kalibrasi (SIK)



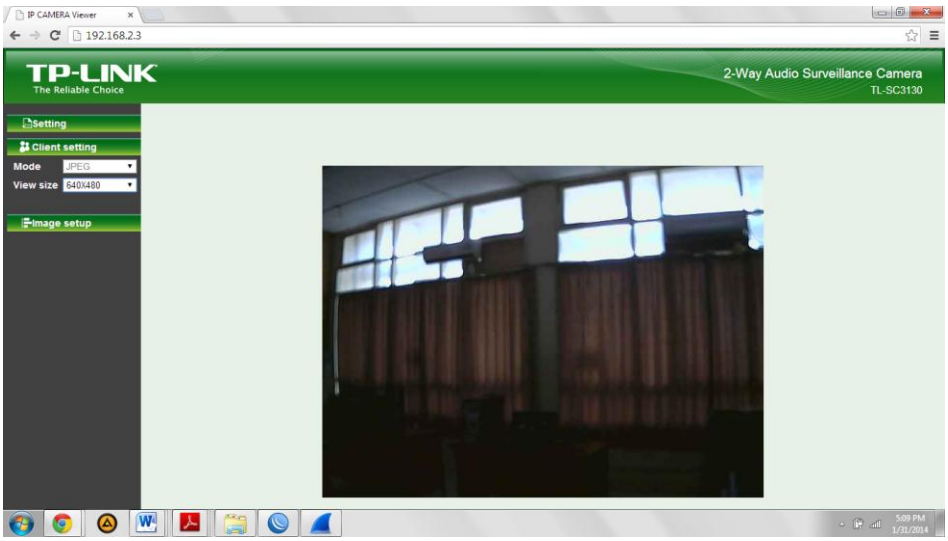
Gambar 4.23 Sistem Informasi Kalibrasi

d. Akses terhadap Sistem Informasi Perpustakaan



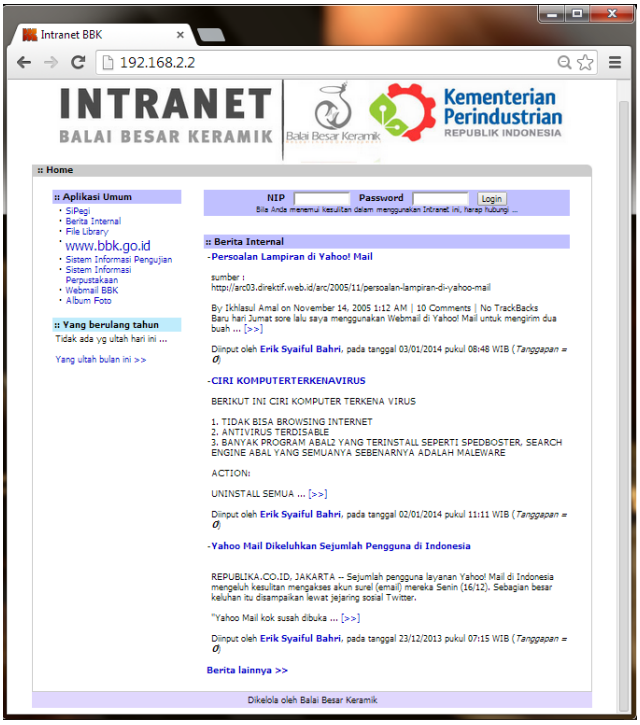
Gambar 4.24 Sistem Informasi Perpustakaan

2. Pengujian Akses IP Camera



Gambar 4.25 IP Camera

3. Pengujian akses pada aplikasi intranet BBK

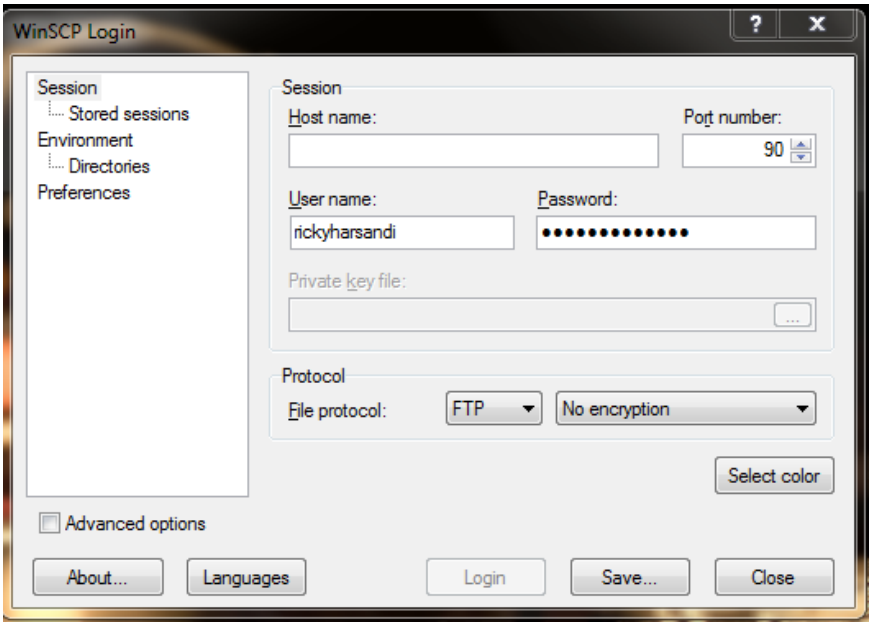


Gambar 4.26 Aplikasi Intranet BBK

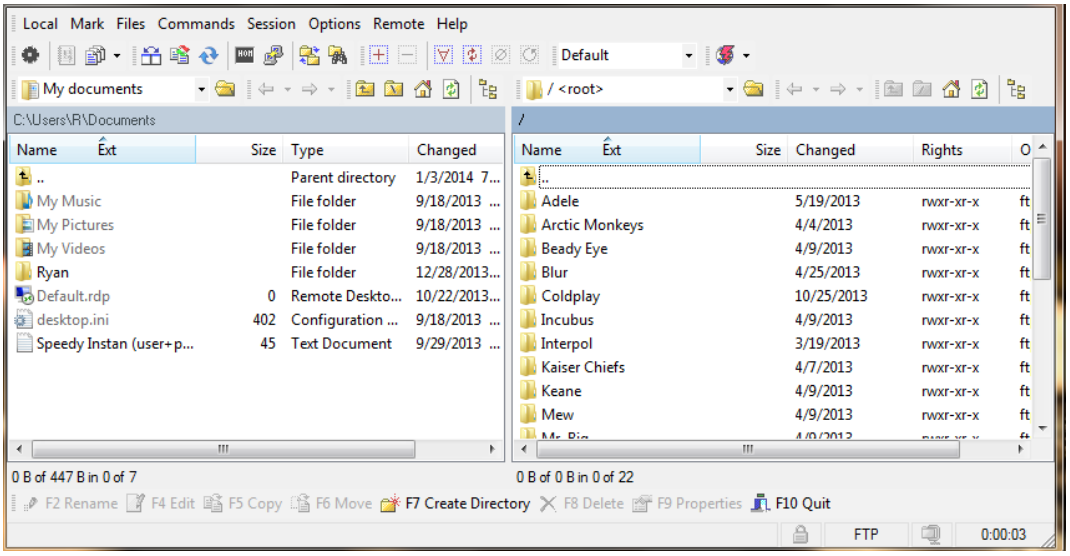
Dari pengujian akses ke server di atas maka dibuktikan bahwa remote access VPN berhasil masuk ke jaringan lokal dan mengakses sumber daya informasi yang ada di lokal.

4.2.4 Pengujian Transfer File

Pengujian dilakukan dengan percobaan transfer file, client akan mengambil file dari FTP server menggunakan WinSCP. Berikut adalah percobaan yang dilakukan :



Gambar 4.27 Pengujian Transfer File Dengan WinSCP



Gambar 4.28 Transfer file

Dari pengujian yang telah dilakukan di atas maka dapat dibuktikan bahwa transfer file dengan WinSCP berhasil dilakukan, tanpa mengubah bentuk atau keutuhan data.

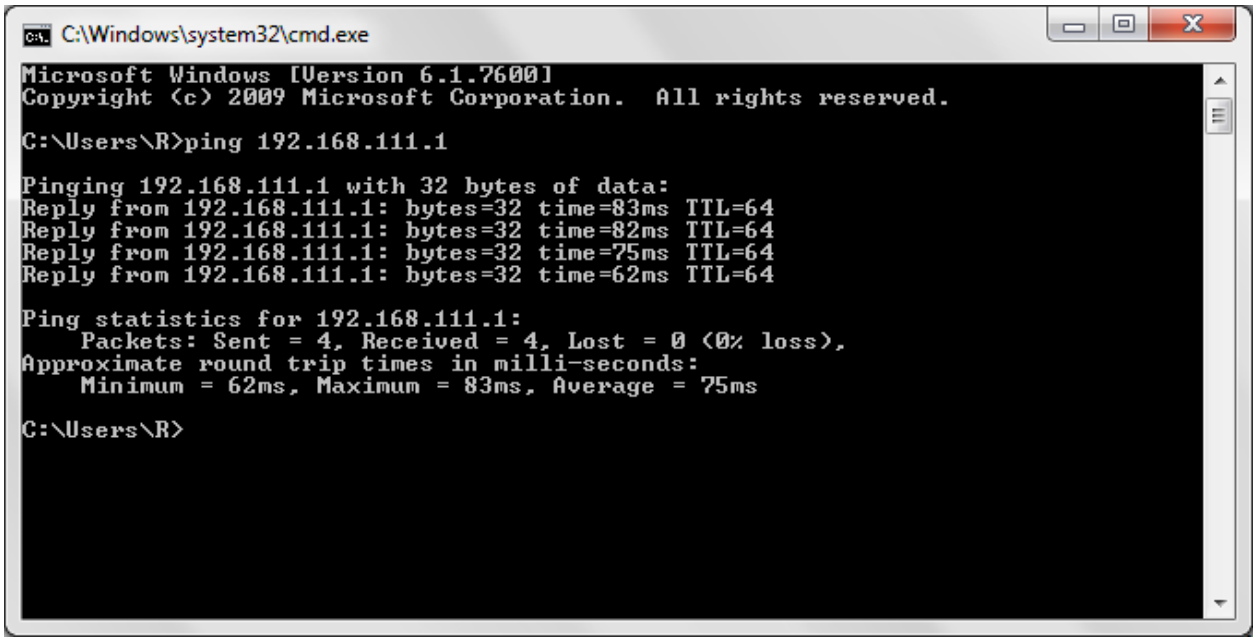
4.2.2 Pengujian Performansi

Ada beberapa hal yang akan duji terhadap jaringan remote access VPN yang telah diimplementasikan. Hal ini dilakukan untuk mengukur kinerja dari jaringan remote access VPN di Balai Besar Keramik. Pengujian dilakukan dengan beberapa faktor yaitu :

1. Pengujian Respond Time

Respond time adalah waktu yang dibutuhkan oleh peralatan jaringan dalam hal ini adalah VPN server untuk mengolah setiap paket data yang ditrima. Hal ini dapat menjadi tolak ukur untuk melakukan perbandingan kinerja dari koneksi VPN yang telah diimplementasikan. Waktu respon yang cepat dari sebuah jaringan amat penting untuk memenuhi kebutuhan user dengan waktu terbatas.

Pengujian respond time koneksi VPN dilakkan dengan command ping yang terdapat pada command prompt Windows. Pengujian dilakukan sebanyak 20 kali koneksi webserver.



Gambar 4.29 Ping Ke Server Dengan VPN

Berikut ini adalah hasil pengujian dari respond time terhadap VPN server :

Tabel 4.5 Pengujian Respond Time Lokal

Besar Paket	Waktu Respond Time (Minimum)
32 bytes	38.05 ms
100 bytes	62.95 ms
200 bytes	88.85 ms

Tabel 4.6 Pengujian Respond Time VPN

Besar Paket	Waktu Respond Time (Maksimum)
32 bytes	39 ms
100 bytes	63.15 ms
200 bytes	90.20 ms

Dari data tersebut dapat disimpulkan bahwa terjadi penambahan waktu respon untuk setiap paket data yang dikrimkan dengan koneksi VPN. Hal ini terjadi karena proses enkripsi dan dekripsi yang harus dilakukan untuk setiap paket yang akan dikirimkan dengan menggnakan koneksi VPN. Adapun rata-rata waktu respon (delay time) untuk setiap paket melalui koneksi VPN rata-rata 18 ms.

2. Pengujian Transfer Rate

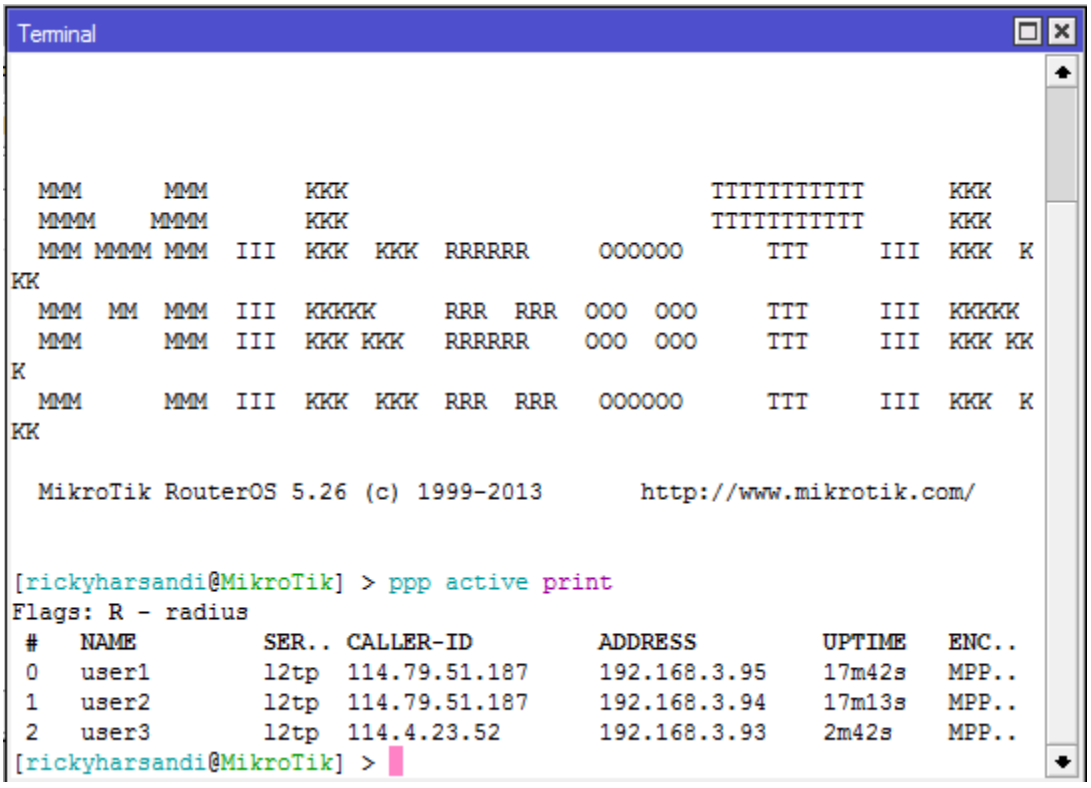
Pengujian ini dilakukan untuk mengetahui bahwa remote access VPN yang telah dibuat bisa diakses oleh banyak user dalam satu waktu. Pengujian ini dilakukan oleh 3 client yang mencoba masuk ke VPN dalam waktu yang bersamaan.

Tabel 4.7 Pengujian Banyak User

No	User	Caller ID	IP Address
1	User1	114.79.51.187	192.168.3.95
2	User2	114.79.51.187	192.168.3.94
3	User3	114.4.23.52	192.168.3.93

Pengujian ini dilakukan untuk mengetahui bahwa remote access VPN yang telah dibuat bisa diakses oleh banyak user dalam satu waktu. Pengujian ini

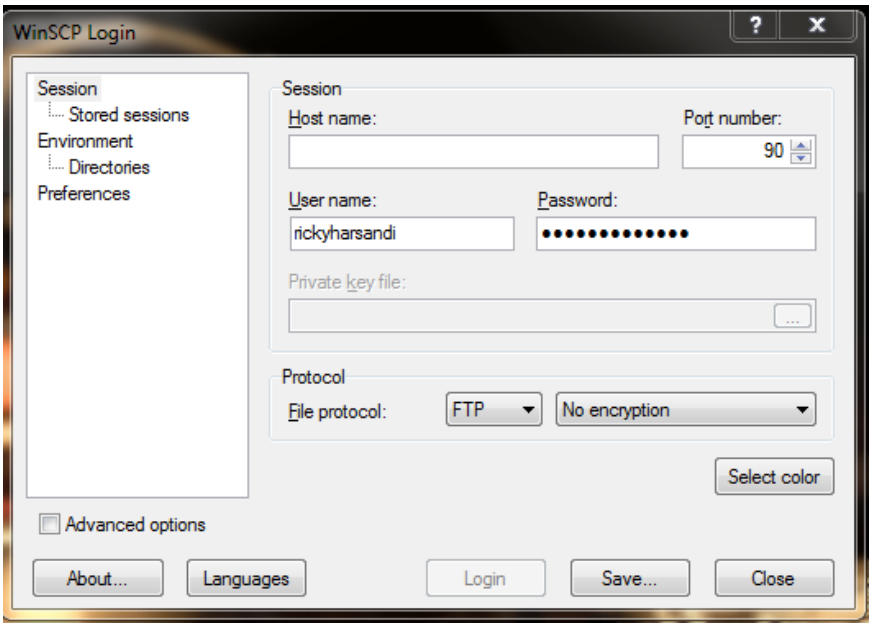
dilakukan oleh 3 client yang mencoba masuk ke VPN dalam waktu yang bersamaan. Berikut adalah tampilan dari terminal untuk melihat user yang active dalam satu waktu bersamaaan:



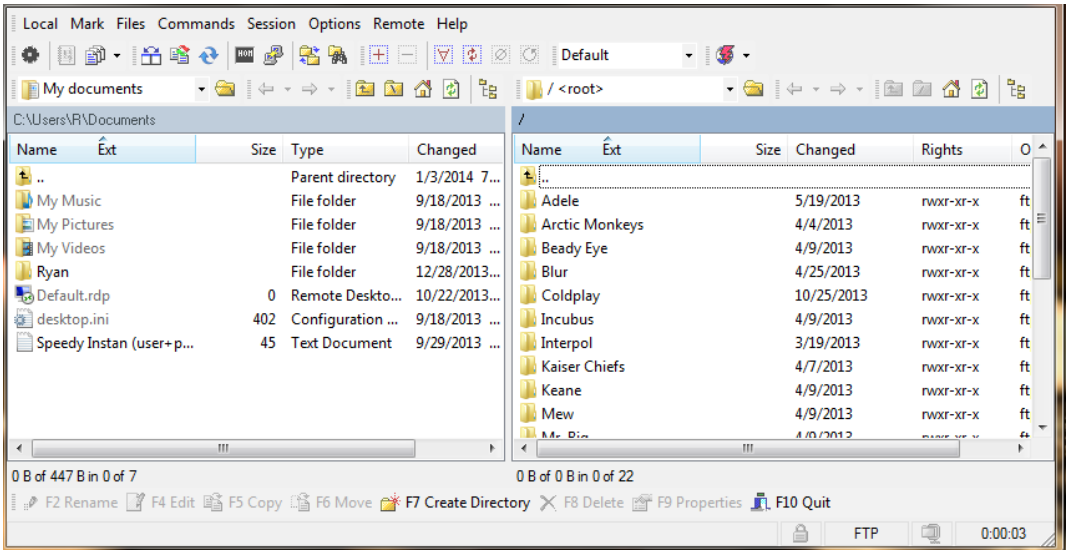
Gambar 4.30 PPP Active

Setelah user di atas masuk ke jaringan lokal maka selanjutnya dilakukan pengujian transfer rate. Transfer rate adalah kemampuan dari sebuah koneksi untuk mengirimkan data dalam selang waktu tertentu. Pengujian ini dilakukan dengan mendownload file dari ftp server melalui koneksi VPN. Pengujian ini melibatkan 3 user dengan bvesar file adalah 1 MB.

Pengujian dilakukan dengan percobaan transfer file, client akan mengambil file dari FTP server menggunakan WinSCP. Berikut adalah percobaan yang dilakukan :



Gambar 4.31 Pengujian Transfer File Dengan WinSCP



Gambar 4.32 Transfer file

Dari pengujian yang telah dilakukan di atas maka dapat dibuktikan bahwa transfer file dengan WinSCP berhasil dilakukan, tanpa mengubah bentuk atau keutuhan data. Dari pengujian yang telah dilakukan didapat data sebagai berikut :

Tabel 4.8 Pengujian Download

Jumlah User	Download 9kbps)	Upload (kbps)
1	30.98	3.48
2	17.04	1.84
3	8.36	1.12

Dari pengujian yang dilakukan terlihat bahwa lebih dari satu user bisa mengakses dan mendownload file dari server yang sama dalam waktu yang bersamaan. Peningkatan jumlah user yang melakukan koneksi VPN menyebabkan semakin kecilnya transfer rate masing-masing user. Hal ini disebabkan bandwith yang tersedia untuk upload di Balai Besar Keramik terbagi sesuai jumlah user yang terkoneksi.

4.2.6 Pengujian Trafik

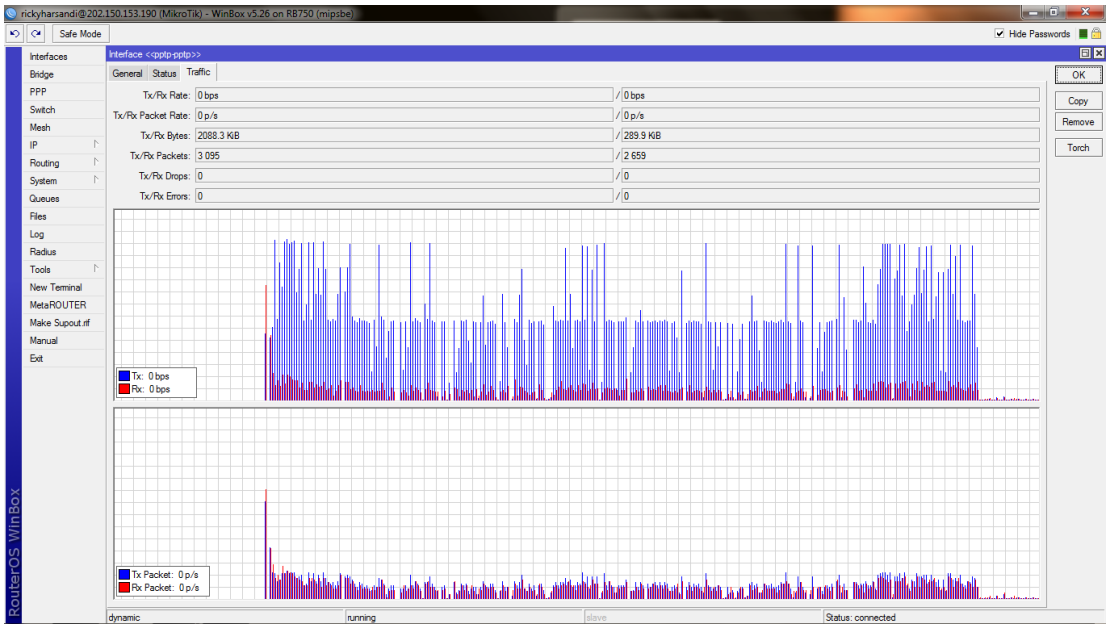
Pengujian ini dilakukan untuk mengetahui perbandingan trafik saat koneksi ke IP camera, dan membuktikan bahwa L2TP lebih baik diimplementasikan untuk komunikasi data berbasis streaming seperti IP camera.

1. Pengujian menggunakan PPTP

a) Pengujian dari sisi server VPN

Pada pengujian ini akan dilakukan koneksi ke IP camera yang dengan menggunakan protokol PPTP. Pengujian ini dilakukan dari sisi server VPN dengan menggunakan fitur torch pada mikrotik dengan lama waktu 5

menit. Berikut adalah gambar trafik saat melakukan koneksi ke IP camera menggunakan PPTP :

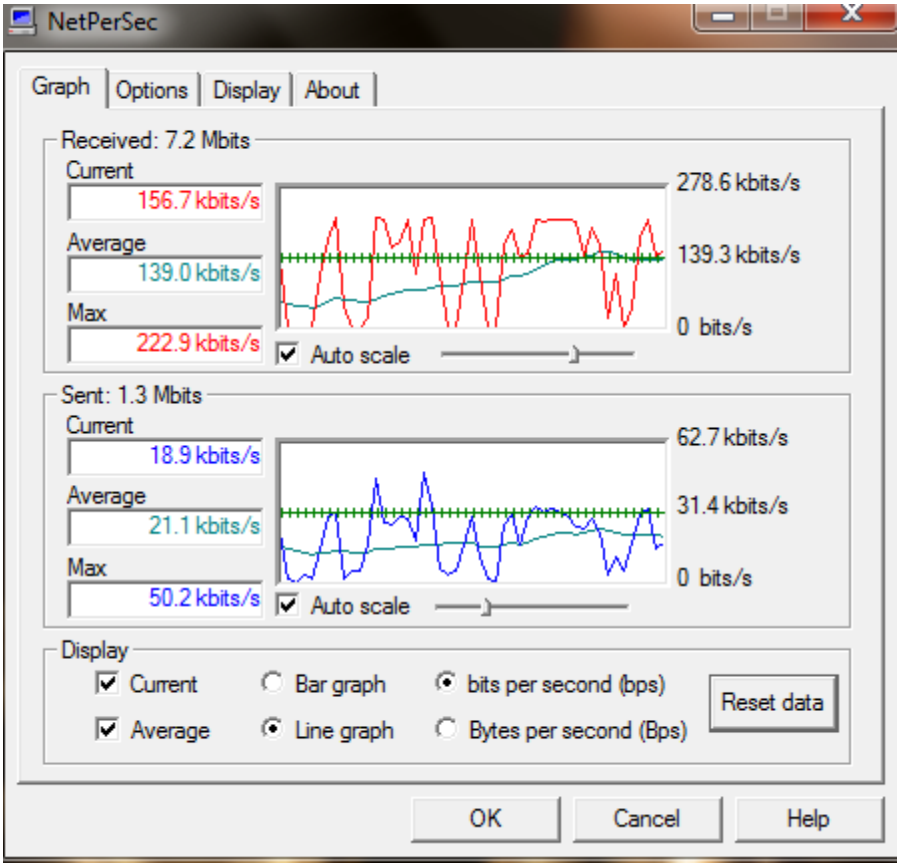


Gambar 4.33 Grafik PPTP

Dari gambar di atas bisa dilihat bahwa transfer rate rata-rata sebesar 2088.3 KiB dan transfer packet rata-rata sebesar 3.095 p/s.

b) Pengujian dari sisi client VPN

Pada pengujian ini akan dilakukan koneksi ke IP camera yang dengan menggunakan protokol PPTP. Pengujian ini dilakukan dari sisi client VPN dengan melakukan aplikasi NetPerSec dengan lama waktu 60 detik. Berikut adalah gambar trafik saat melakukan koneksi ke IP camera menggunakan PPTP :



Gambar 4.34 NetPerSec PPTP

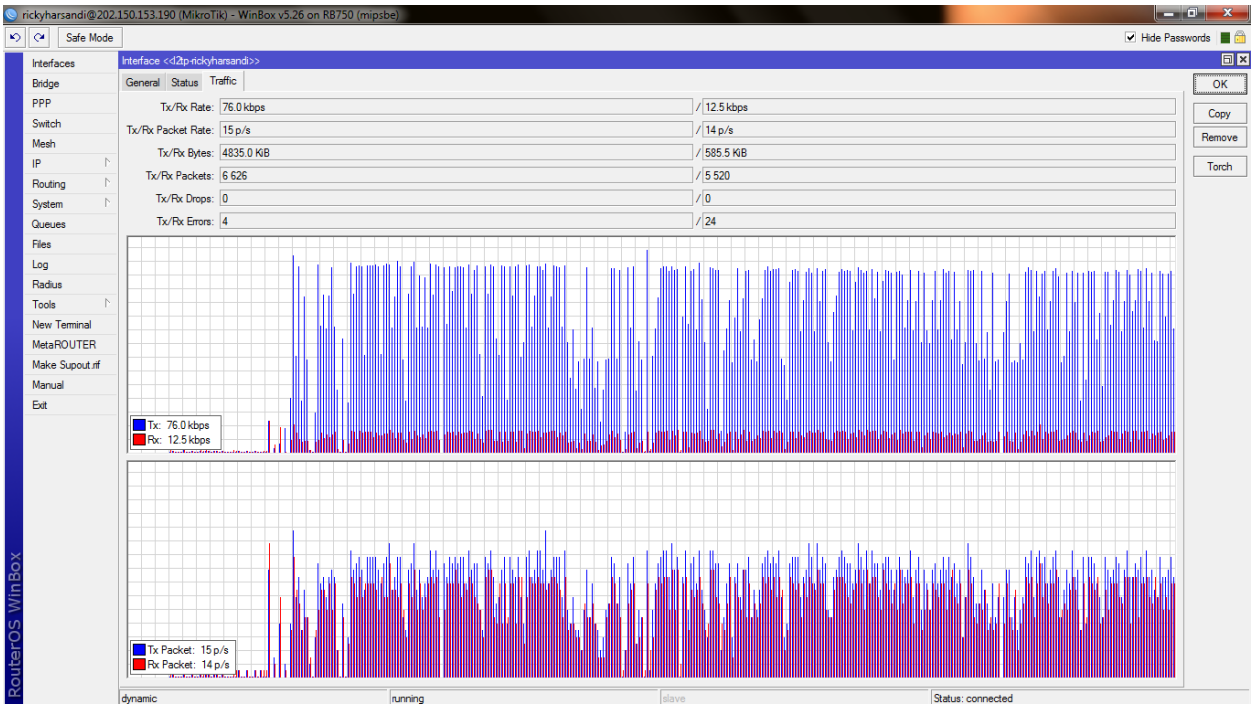
Dari gambar di atas bisa dilihat bahwa jumlah paket yang diterima (received) sebesar 7.2 Mbits dan received rate rata-rata sebesar 139.3 kbits/s.

2. Pengujian menggunakan L2TP

a) Pengujian trafik dari sisi server

Pada pengujian ini akan dilakukan koneksi ke IP camera dengan menggunakan protokol L2TP. Pengujian ini dilakukan dari sisi server VPN dengan menggunakan fitur torch pada mikrotik dengan lama waktu 5 menit.

Berikut adalah gambar trafik saat melakukan koneksi ke IP camera menggunakan L2TP :

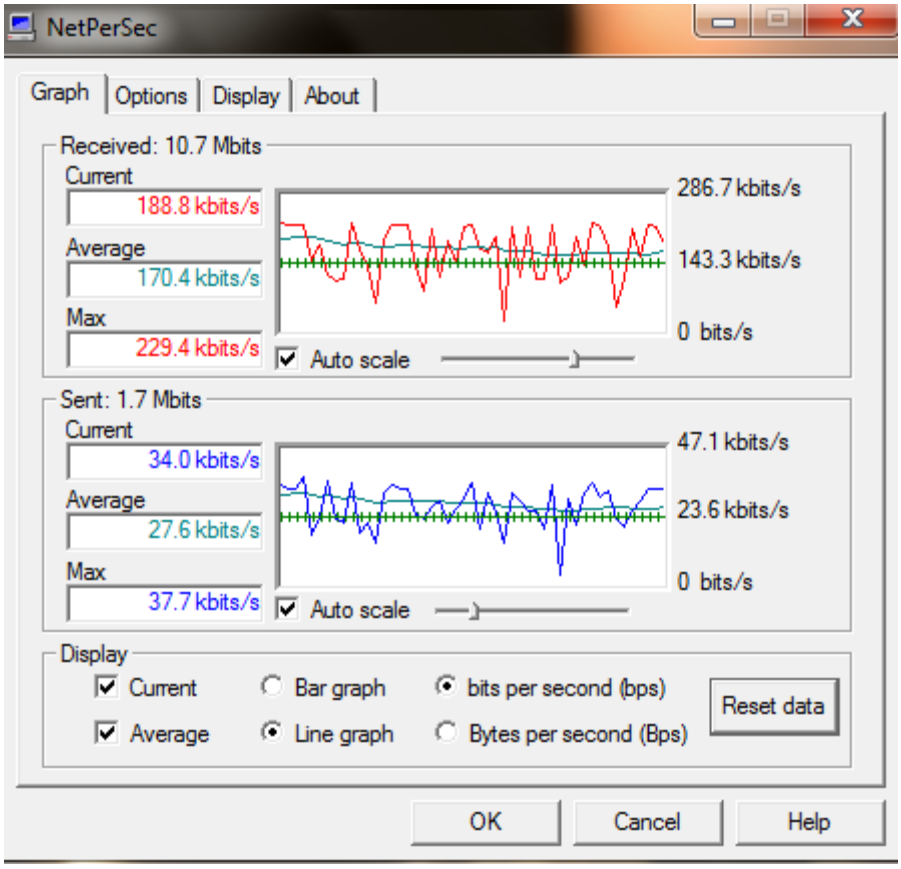


Gambar 4.35 Torch L2TP

Dari gambar di atas bisa dilihat bahwa transfer rate rata-rata sebesar 4835.0 kbps dan transfer rate packet rata-rata sebesar 6.626 p/s.

b) Pengujian trafik dari sisi client

Pada analisis ini akan dilakukan koneksi ke IP camera yang berbasis UDP dengan menggunakan protokol PPTP. Pengujian ini dilakukan dari sisi client VPN dengan melakukan aplikasi NetPerSec dengan lama waktu 60 detik. Berikut adalah gambar trafik saat melakukan koneksi ke IP camera menggunakan L2TP :



Gambar 4.36 NetPerSec L2TP

Dari gambar di atas bisa dilihat bahwa jumlah paket yang diterima (received) sebesar 10.2 Mbits dan received rate rata-rata sebesar 143.3 kbits/s.

Kesimpulan hasil pengujian trafik terhadap koneksi ke IP Camera:

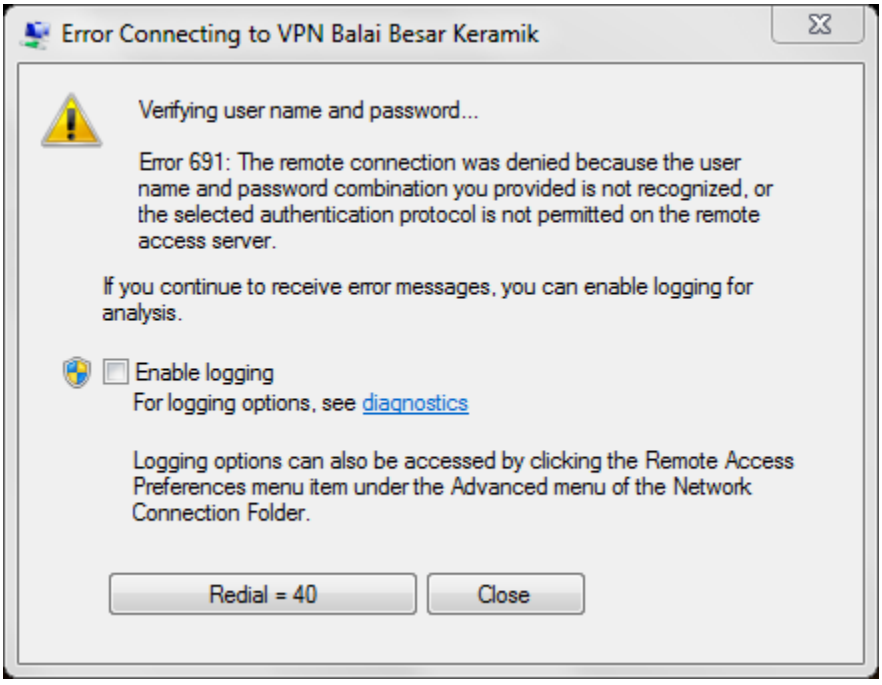
1. L2TP lebih baik untuk komunikasi streaming seperti IP Camera karena jika dibandingkan dengan PPTP, transfer rate L2TP lebih besar.
2. Jumlah paket yang diterima client untuk koneksi L2TP lebih besar dibandingkan dengan PPTP saat melakukan koneksi ke IP camera.

4.2.7 Pengujian Keamanan

Pengujian keamanan ini dilakukan untuk membuktikan keamanan remote access VPN yang telah dibangun. Pengujian keamanan ini dilakukan terhadap 2 cara yaitu pengujian keamanan dari sisi server dan pengujian keamanan dari sisi tunneling.

1. Pengujian keamanan dari sisi client

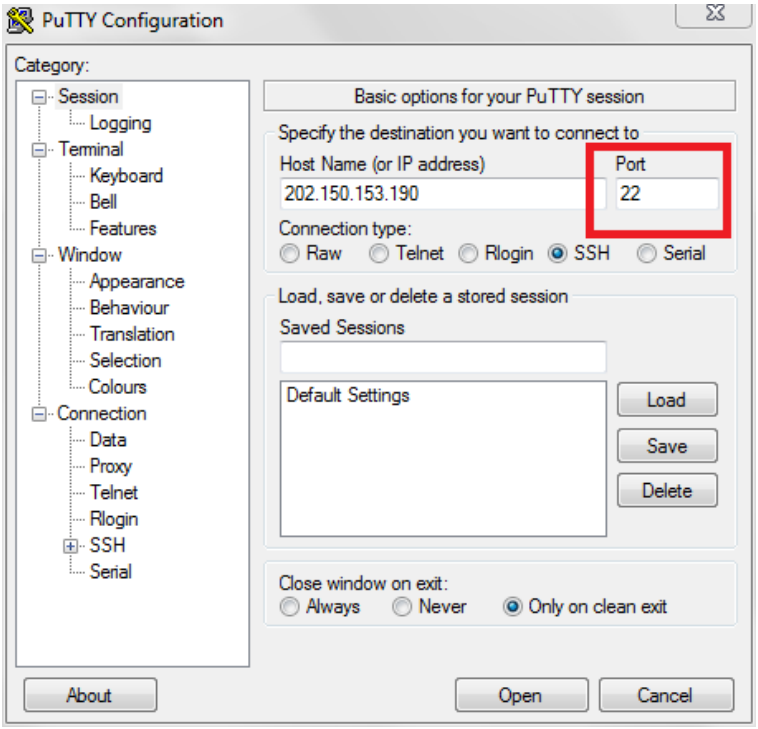
Pengujian ini dilakukan dengan memasukkan user name dan password yang salah ketika akan connec ke VPN. Ketika user salah memasukan username atau password, maka akan muncul kotak pesan bahwa kombinasi user name atau password salah.



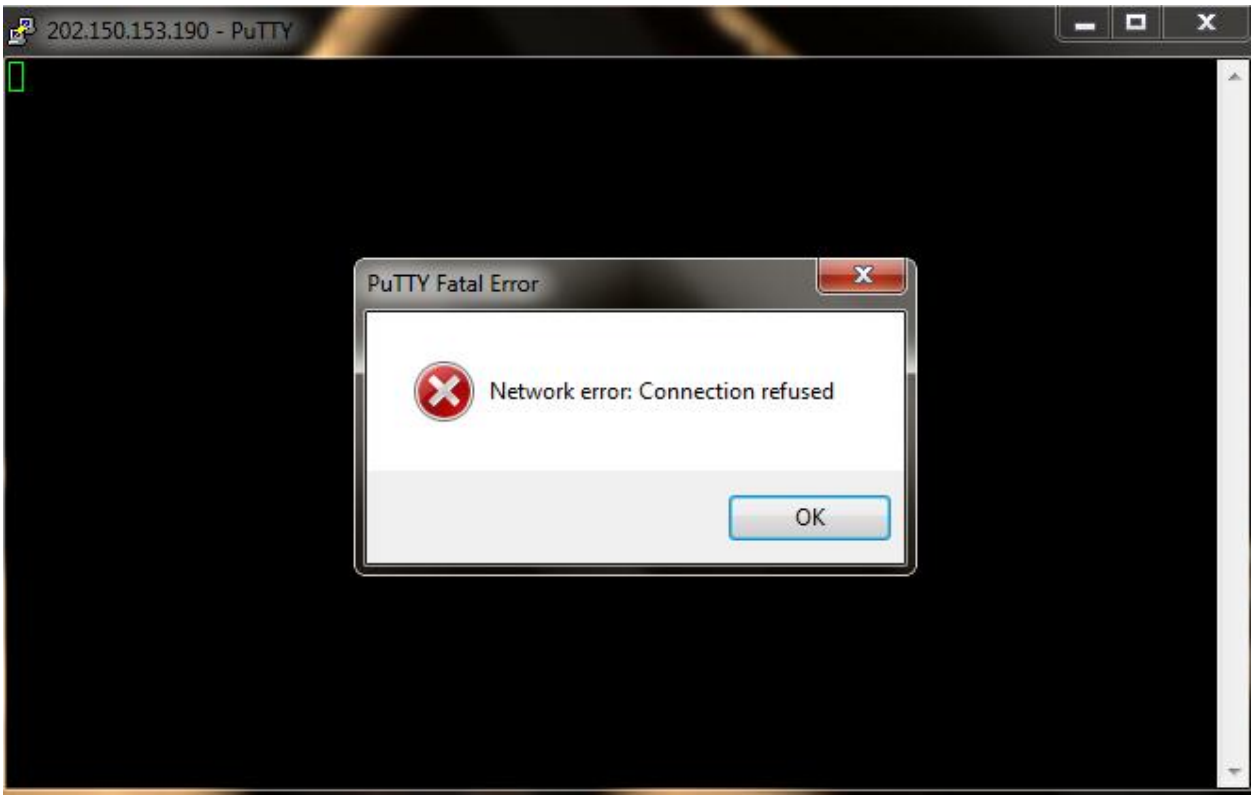
Gambar 4.37 Error Connecting VPN

2. Pengujian keamanan dari sisi server

Pengujian ini dilakukan untuk mengetahui bahwa port SSH yang sudah diblock berhasil atau tidak. Pada pengujian ini dilakukan percobaan masuk ke router menggunakan aplikasi PuTTY dengan masih menggunakan default port untuk SSH yaitu port 22.



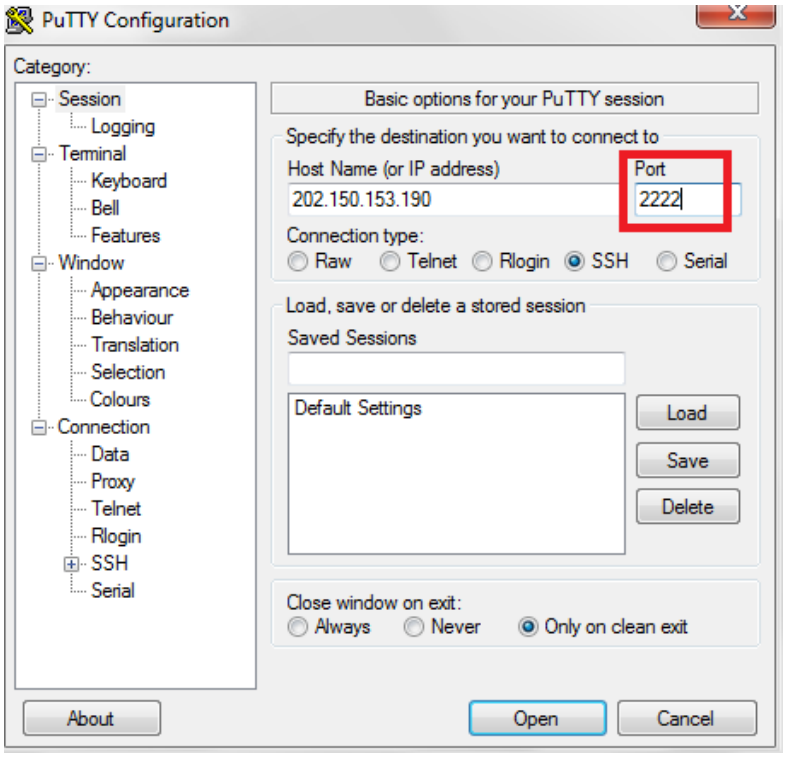
Gambar 4.38 SSH Port 22



Gambar 4.39 Network Error

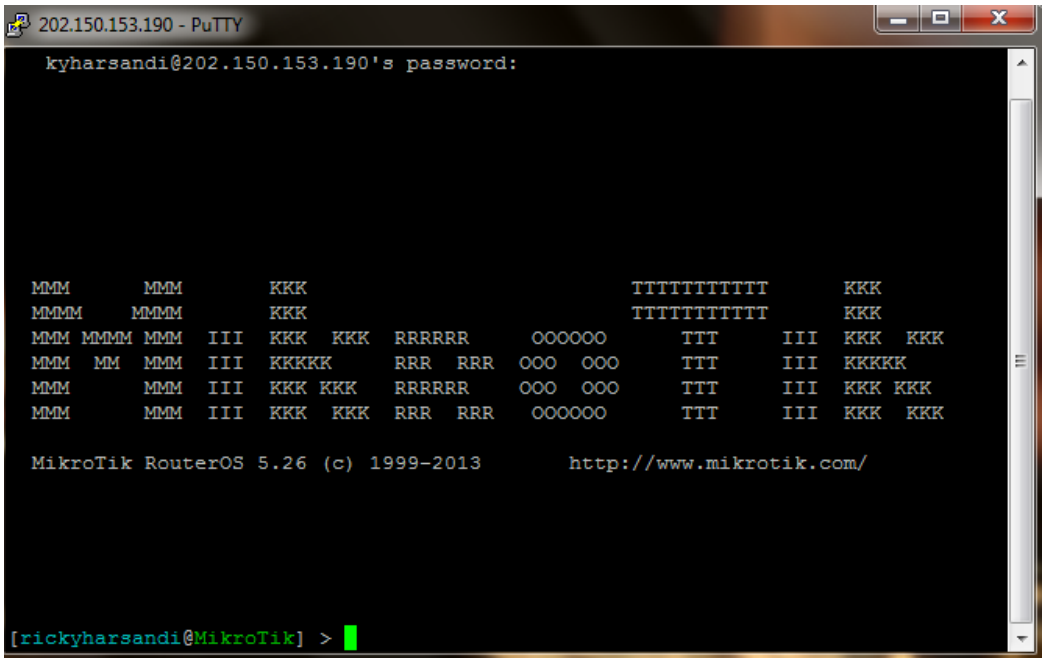
Dari hasil pengujian di atas maka dapat dilihat bahwa ketika port diganti, maka para penyerang tidak mudah menyerang karena port sudah diganti. Karena port SSH ini sangat rentan terhadap serangan brute force attack.

Pengujian masuk dengan SSH dengan port yang sudah diganti sebelumnya yaitu port 2222.



Gambar 4.40 SSH Port 2222

Setelah port diganti, maka selanjutnya akan mencoba masuk menggunakan PuTTy dengan port yang telah diganti menjadi 2222.



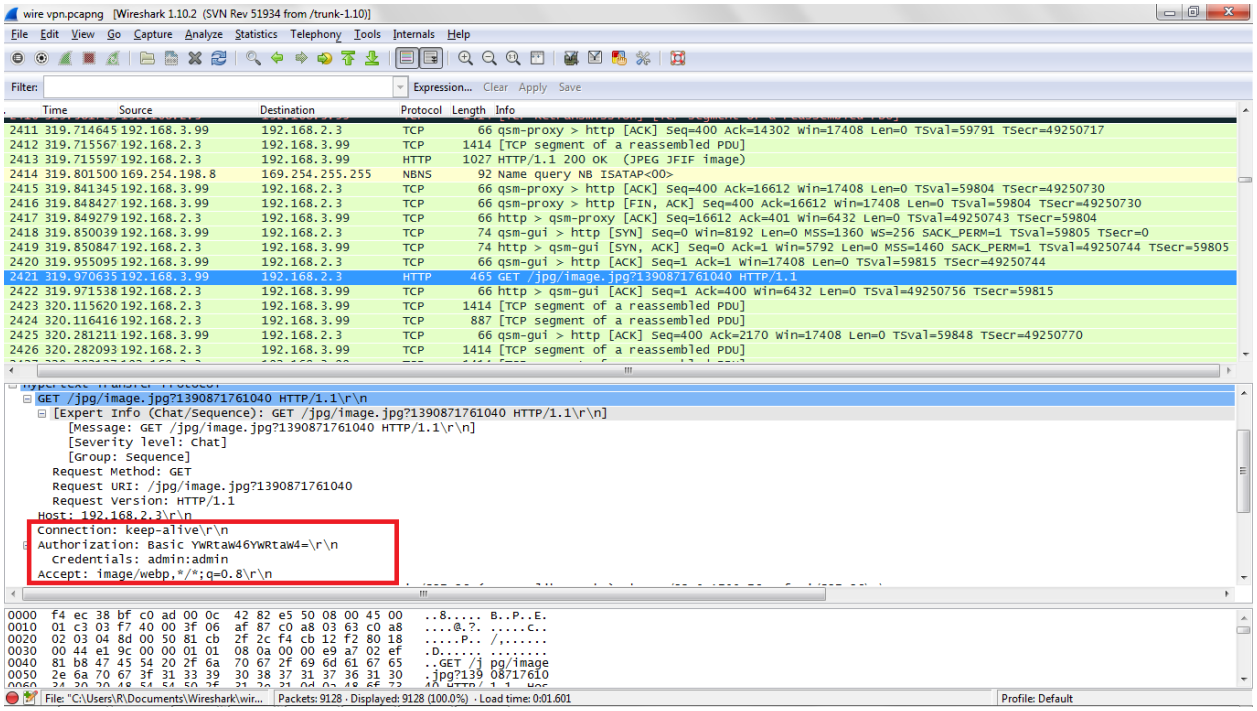
Gambar 4.41 SSH Berhasil

Dari pengujian di atas bisa dilihat bahwa admin bisa masuk ke SSH dengan menggunakan port yang sudah diganti sebelumnya menjadi port 2222.

3. Pengujian keamanan saat transmisi data

Pengujian ini dilakukan untuk melihat paket yang melintas tanpa menggunakan VPN dan dengan menggunakan VPN. Pengujian ini dilakukan di jaringan lokal dengan menggunakan fitur port mirroring pada mikrotik router RB750.

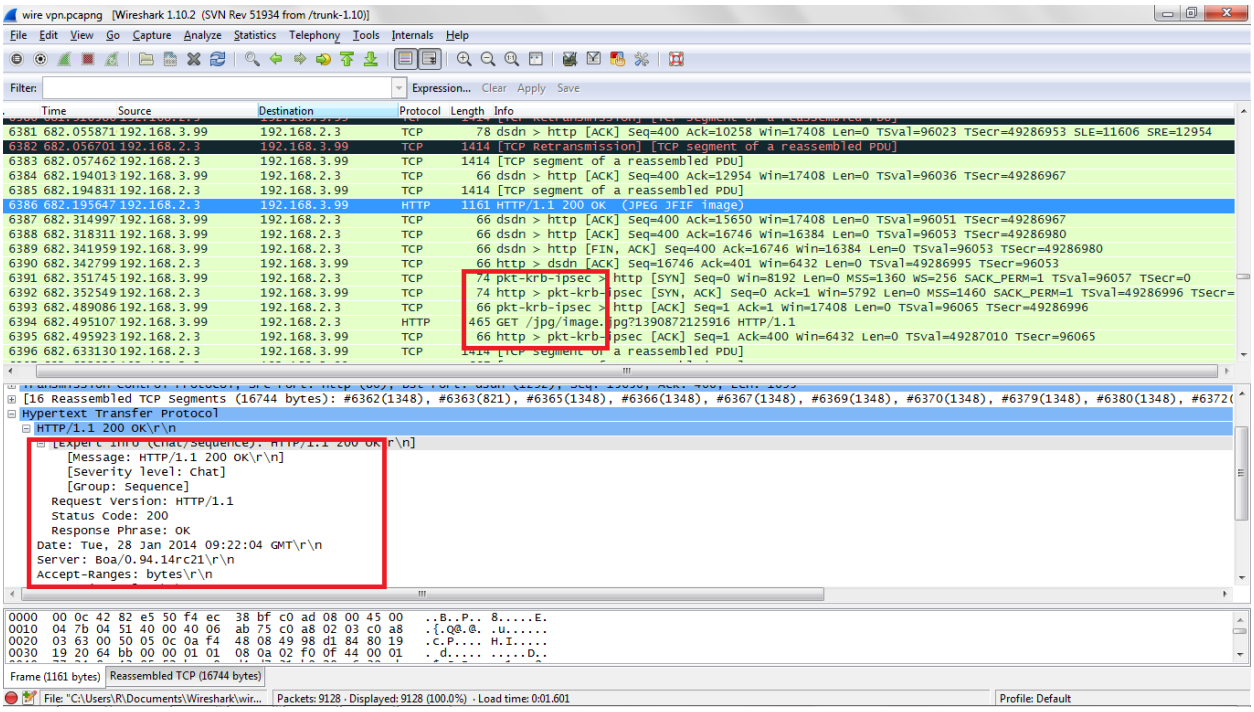
a. Sniffing paket terhadap jaringan tanpa menggunakan VPN



Gambar 4.42 Sniffing Tanpa VPN

Dari capture di atas bisa dilihat saat melakukan koneksi ke HTTP, credential user dan password client dapat diketahui.

b. Sniffing paket terhadap jaringan VPN

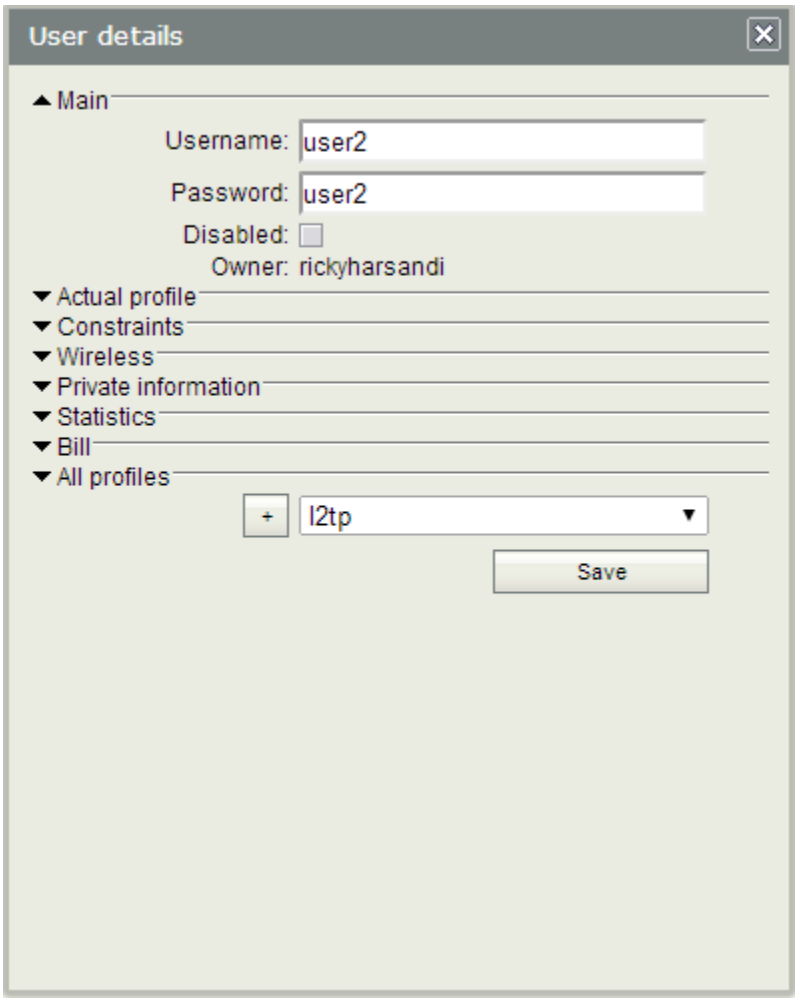


Gambar 4.43 Sniffing VPN

Dari capture di atas bisa dilihat bahwa paket yang melintas telah dienkripsi oleh IPSec sehingga data maupun user name atau password tidak terdeteksi.

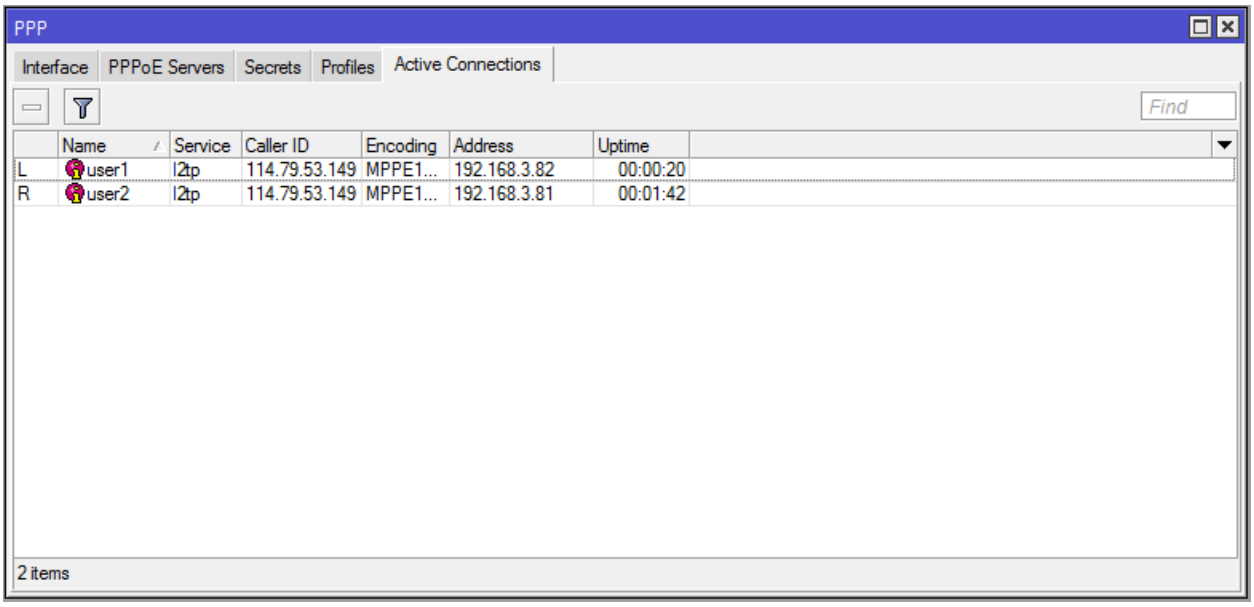
4.2.8 Pengujian User Manager

Pengujian ini bertujuan untuk melihat kinerja dari user manager dalam pembuatan user. Pengujian ini dilakukan dengan membuat user di user manager.



Gambar 4.44 Buat User di User Manager

Berikut ini merupakan tabel informasi session client VPN yang sedang aktif dan terhubung ke VPN server.



Gambar 4.45 PPP Active Connections

Keterangan :

Flag L : client terautentikasi dari database local secret

Flag R : client terautentikasi dari database RADIUS

4.2.9 Pengujian Beta

Pengujian Beta merupakan pengujian yang dilakukan secara objektif dimana diuji secara langsung ke lapangan yaitu instansi yang bersangkutan mengenai kepuasan pengguna dengan kandungan poin yaitu pemenuhan kebutuhan dari tujuan awal pembangunan remote access VPN. Pengujian beta dilakukan melalui sebuah teknik pengambilan data, yaitu melalui wawancara pada admin. Berikut ini adalah hasil wawancara pada tanggal 22 Januari 2014 kepada Bapak Erik selaku administration IT mengenai remote access VPN yang telah dibangun.

Tabel 4.9 Hasil Wawancara

1. Apakah anda kesulitan dalam mengelola jaringan VPN yang telah dibangun?	
Jawaban Narasumber	Saya cukup mengerti dalam pengelolaan jaringan, dan tidak begitu kesulitan.
2. Apakah Radius yang dibangun untuk VPN mudah untuk menambah dan menghapus user ?	
Jawaban Narasumber	Radius yang telah dibangun cukup membantu dalam pembuatan user.
3. Apakah performansi jaringan VPN yang dibangun sangat baik ?	
Jawaban Narasumber	Sistem informasi, aplikasi intranet dan file server sudah bisa diakses dan berjalan dengan baik.
4. Apakah anda setuju bahwa remote access VPN telah membantu pekerjaan kantor, terutama saat anda membutuhkan data di luar kantor?	
Jawaban Narasumber	Setuju, VPN ini telah membantu pekerjaan kantor, sehingga pekerjaan tidak hanya bisa dikerjakan di dalam kantor, tapi juga di luar kantor.
5. Berdasarkan hasil penelitian di Balai Besar Keramik , bahwa data yang	

berada di jaringan lokal cukup penting dan rahasia, apakah anda setuju bahwa remote access VPN digunakan untuk keamanan transmsisi data?	
Jawaban Narasumber	Berdasarkan keamanan enkripsi dan autentiaksi yang disajikan VPN, saya rasa cukup aman.

Berikut ini merupakan hasil pengolahan data kuesioner berdasarkan pertanyaan yang telah diajukan kepada 30 client dari Balai Besar Keramik.

Tabel 4.10 Tabel Pengolahan Data Kuesioner

Pertanyaan Ke -	Sangat Setuju/Sangat Tahu	Setuju/Tahu	Ragu-ragu/Cukup Tahu	Tidak Setuju/Kurang Tahu	Sangat Tidak Setuju/Tidak Tahu	Jumlah
1	-	5	25	-	-	30
2	10	15	5	-		30
3	17	10	3	-	-	30
4	15	15	-	-	-	30
5	15	5	10	-	-	30

Berdasarkan tabel 4.7, maka dapat dihasilkan nilai rata-rata berdasarkan setiap pertanyaan yang diajukan. Berikut pertanyaan dan nilai rata-ratanya.

1. **Apakah anda telah mengetahui informasi tentang remote access VPN?**
   Tahu : 5/30 = 0,17
   Cukup Tahu : 25/30 = 0,83

2. **Apakah anda setuju bahwa remote access VPN digunakan untuk akses jaringan lokal di kantor?**
   Sangat Setuju : 10/30 = 0,33

Setuju : 15/30 = 0,5

Ragu-ragu : 5/30 = 0,17

3. **Apakah anda setuju bahwa konfigurasi VPN di sisi client mudah?**

   Sangat Setuju : 17/30 = 0,56

   Setuju : 10/30 = 0,33

   Ragu-ragu : 3/30 = 0,1

4. **Apakah anda setuju bahwa penggunaan remote access VPN ini memberikan kemudahan dalam mengakses jaringan lokal?**

   Sangat Setuju : 15/30 = 0,5

   Setuju : 15/30 = 0,5

5. **Apakah anda setuju bahwa remote access VPN telah membantu pekerjaan anda, terutama saat anda membutuhkan data di luar kantor?**

   Sangat Setuju : 15/30 = 0,5

   Setuju : 5/30 = 0,16

   Ragu-ragu :10/30 = 0,33

4.2.9.1 Kesimpulan Hasil Pengujian

Berdasarkan kuesioner yang diajukan kepada client Balai Besar Keramik mulai dari pertanyaan 1 sampai 5, maka diperoleh hasil berikut :

1. Para pegawai sudah banyak yang mengetahui tentang remote access VPN.
2. Para pegawai Balai Besar Keramik setuju dengan implementasi remote access VPN untuk akses jaringan lokal dari jarak jauh..
3. Para pegawai Balai Besar Keramik setuju dengan remote access VPN untuk mengakses data yang dibutuhkan saat berada di luar kantor.

4. Para pegawai Balai Besar Keramik setuju bahwa remote access VPN sangat membantu dalam pekerjaannya saat berada di luar kantor.
5. Berdasarkan kerahasiaan data, para pegawai Balai Besar Keramik setuju jika remote access VPN digunakan untuk keamanan saat transmisi data berlangsung.