BAB 4
IMPLEMENTASI DAN HASIL PENGUJIAN SISTEM

4.1 Implementasi Sistem

Implemenasi sistem merupakan tahapan penerapan hasil analisis dan perancangan berdasarkan kebutuhan pada keadaan sebenarnya. Penerapan EoIP sebagai penghubung antara dua jaringan lokal PT. Blesslink Rema akan mempercepat proses transfer data baik dari kantor cabang ke kantor pusat ataupun sebaliknya. Dan penggunaan IP Security akan menjamin proses transfer data secara aman dan terpercaya meski menggunakan internet.

4.2.1 Implementasi Perangkat Keras

Perangkat keras yang dibutuhkan dalam penerapan EoIP dan IP Security ini adalah sebagai berikut :

Tabel 4.1. Perangkat Keras

No	Nama	Spesifikasi	Keterangan
1	Komputer *Built up*	- 2 Ghz Dual Core - 2 Gb RAM - 128 Mb VRAM - 500 Gb HDD - Windows XP	*Server* (LAN)
2	Komputer *Built up*	- 1,8 Ghz Dual Core - 1 Gb RAM - 128 Mb VRAM - 500 Gb HDD - Windows 7	*Client* (LAN)
3	Komputer	- 2 Ghz Single Core - 512 RAM	*Client* (LAN)

		- 64 Mb VRAM - 250 Gb HDD - Windows XP	
4	*All in One Computer*	- 2 Ghz Dual Core - 2 Gb RAM - 128 Mb VRAM - 500 Gb HDD - Windows XP	*Client* (LAN)
5.	Printer	*Inkjet Printer*	
6.	*Route*rBoard RB 951-2n	- 5 Port UTP - Single Core 400 Mhz - RAM 32 Mb - *Route*rOS Level 4	*Route*r yang akan diimplementasikan EoIP dan IP Security
7	Switch	- 16 Port UTP - 10/100mbps	

4.2.2 Implementasi Perangkat Lunak

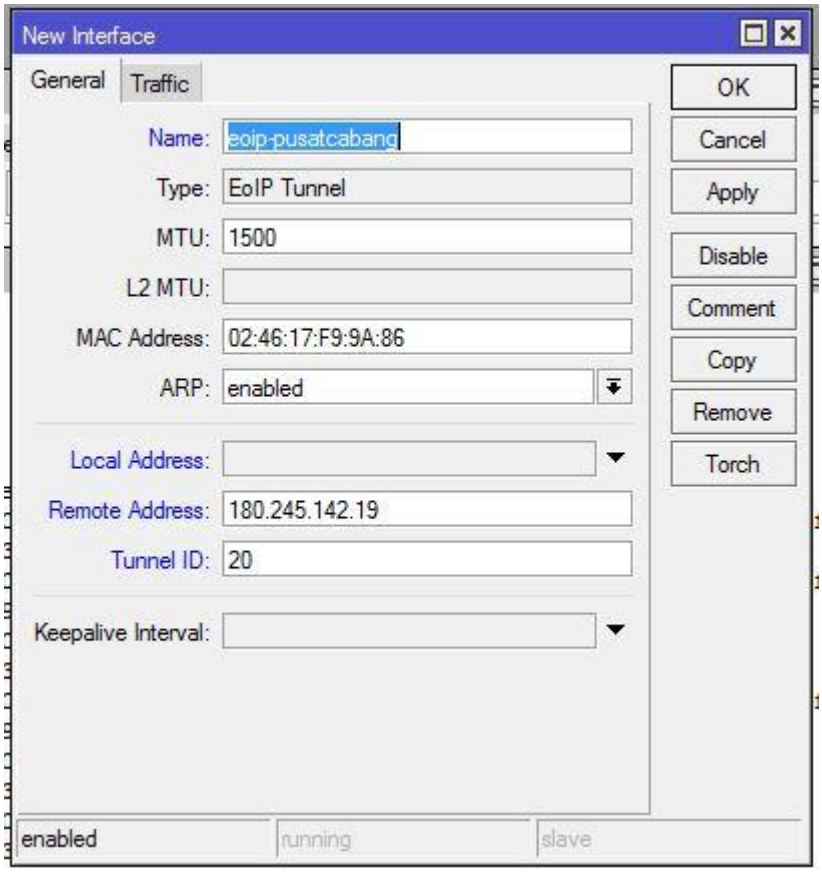
Implementasi perangkat lunak mencakup konfigurasi EoIP dan IPSec pada kedua kantor PT. Blesslink Rema. Kantor Pusat di Bandung dan kantor cabang di Jakarta. Konfigurasi ini menggunakan terminal untuk memasukan script konfiguasi pada *route*r board.

4.1.2.1 Konfigurasi di Pusat

Konfigurasi di kantor pusat mencakup konfigurasi EOIP dan IPSec. Yang perlu diperhatikan adalah EOIP digunakan sebagai *Tunnel* sementara IPSec hanya digunakan sebagai keamanan komunikasi data.

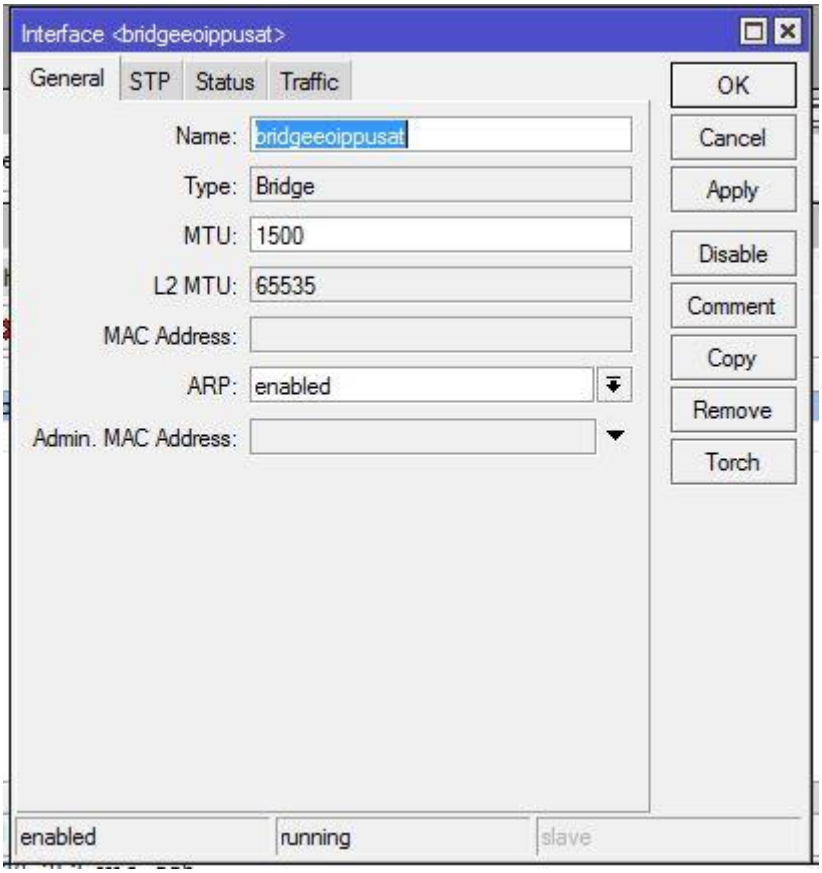
4.1.2.2.1 Konfigurasi EOIP di Kantor Pusat

Konfigurasi yang dilakukan adalah mengkonfigurasi EOIP dengan membuat *interface* baru bernama eoip-pusatcabang. Pada gambar 4.1 merupakan konfigurasi EOIP di kantor pusat. Kolom *remote addres* diisi dengan IP *public* kantor cabang dan kolom tunel ID harus sama dengan Tunnel ID di cabang.



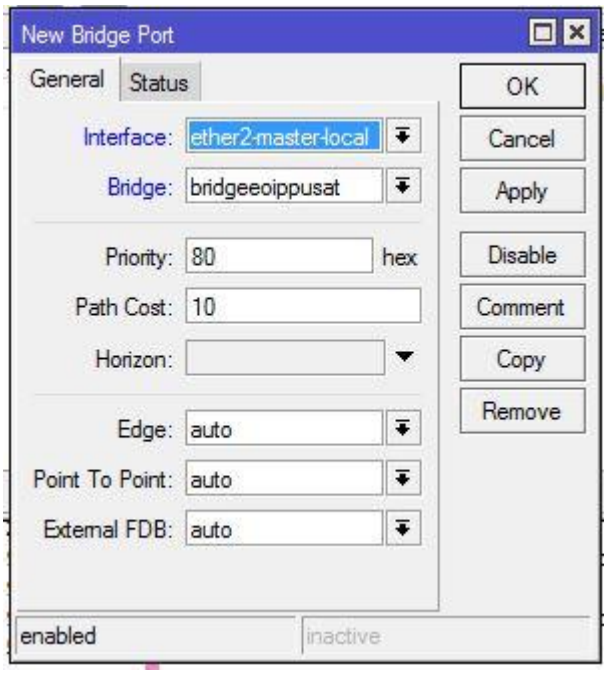
Gambar 4.1. Interface EOIP Pusat

Setelah membuat *interface* eoip, maka tahapan selanjutnya adalah membuat *bridge* antara *interface* LAN lokal dengan *Interface* EOIP yang baru dibuat.

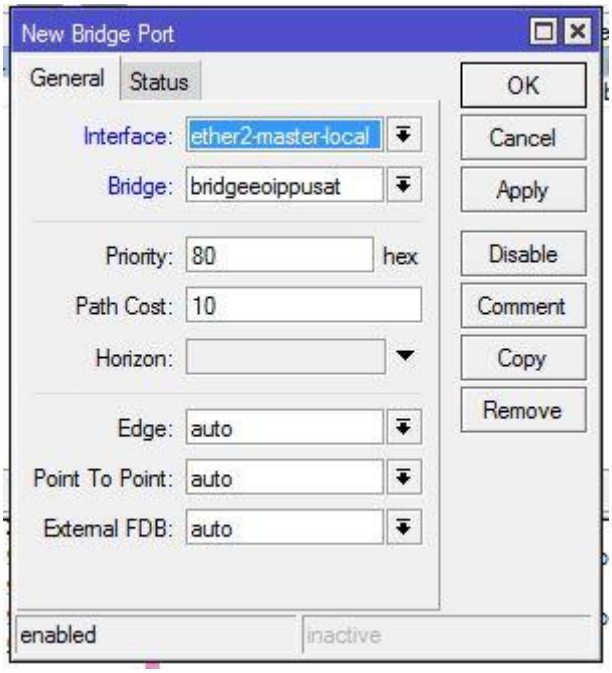


Gambar 4.2. *Bridge* EOIP Pusat

Setelah membuat *Bridge* selanjutnya adalah menghubungkan *interface* LAN Lokal dengan EOIP

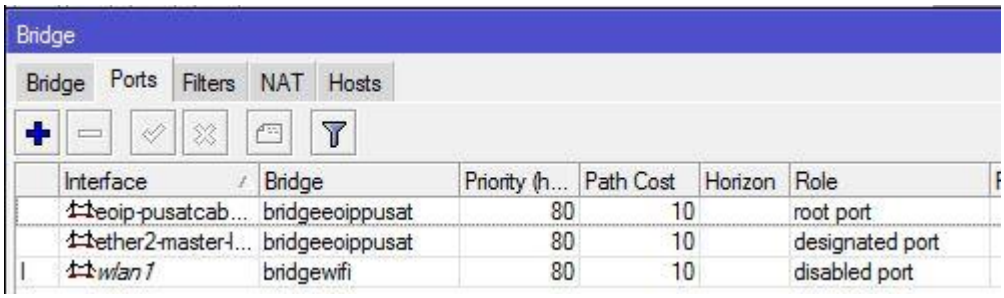


Gambar 4.3. Bridge Port LAN Lokal



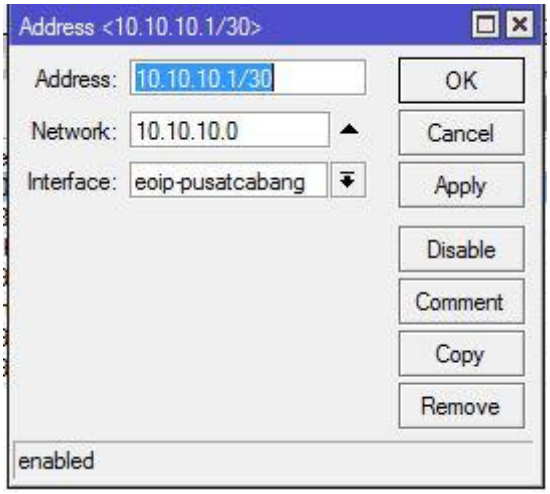
Gambar 4.4. *Bridge* Port EOIP

Setelah *Bridge* selesai, maka port yang terhubung akan seperti pada gambar 4.5 dibawah ini.



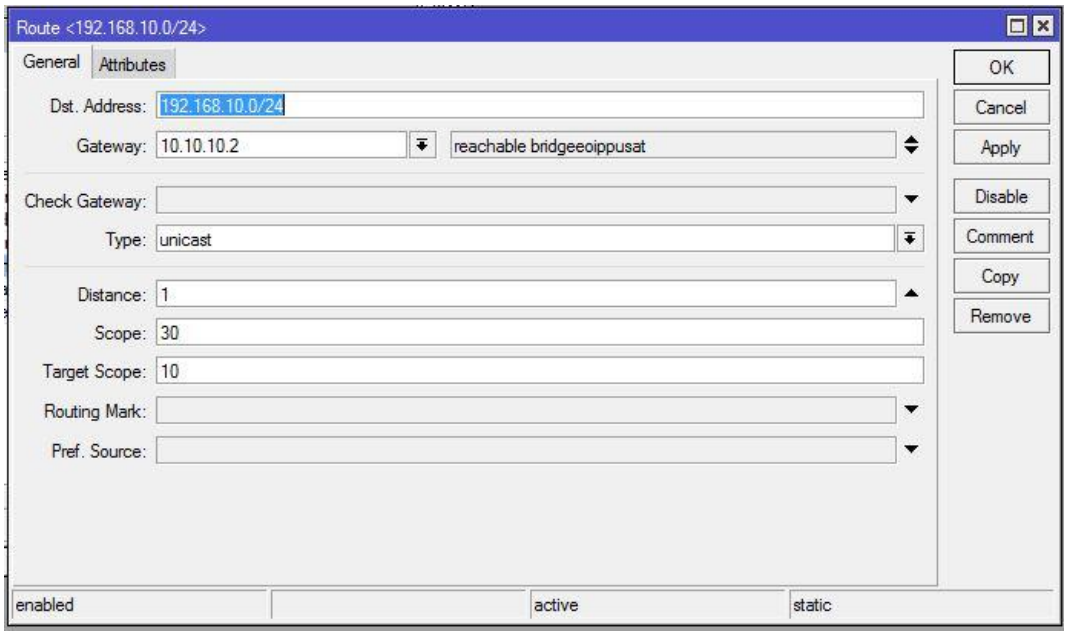
Gambar 4.5. *Bridge* Pusat

Setelah menkonfigurasi EOIP dan *Bridge* selanjutnya adalah menetapkan *route* dari LAN di kantor cabang ke LAN di kantor pusat melalui gateway EOIP yang sudah dibuat. Tahap pertama adalah dengan memberikan IP pada interface EOIP Cabang. IP yang digunakan pada EOIP Cabang harus dalam satu segmen dengan IP EOIP Pusat.



Gambar 4.6 IP Address EOIP Pusat

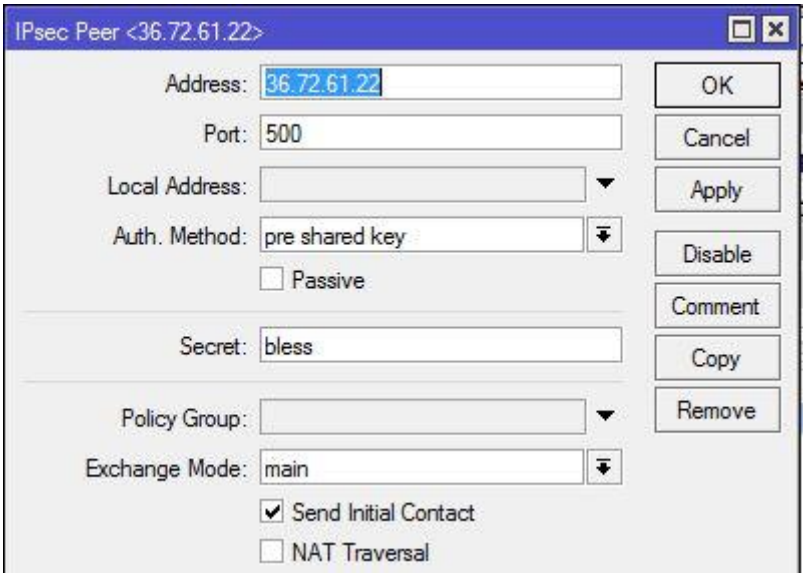
Setelah memberikan IP pada EOIP pusat, selanjutnya adalah menentukan *route* agar LAN lokal cabang dapat berkomunikasi dengan LAN lokal pusat. Konfigurasi dengan memasukan IP Segmen LAN Lokal di kantor pusat dengan gateway EOIP pusat.



Gambar 4.7. *Route* Pusat ke Cabang

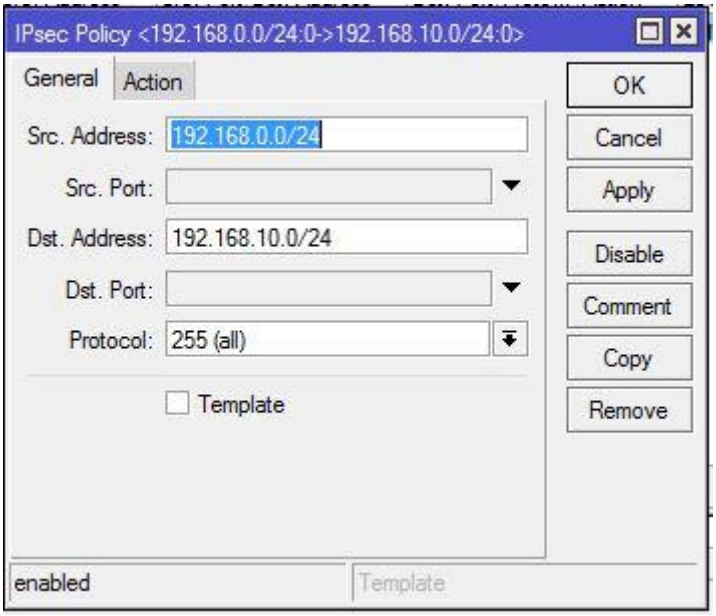
4.1.2.2.2 Konfigurasi IPSec di Kantor Pusat

Setelah konfigurasi setelah selanjutnya adalah mengkonfigurasi IPSec di kantor pusat yang terhubung ke kantor cabang. Tahapan pertama dalam mengkonfigurasi IPSec adalah menentukan *Peer* yang berarti kemana IPSec ini terhubung. Selain itu yang perlu diperhatikan disini adalah mengisi *secret*



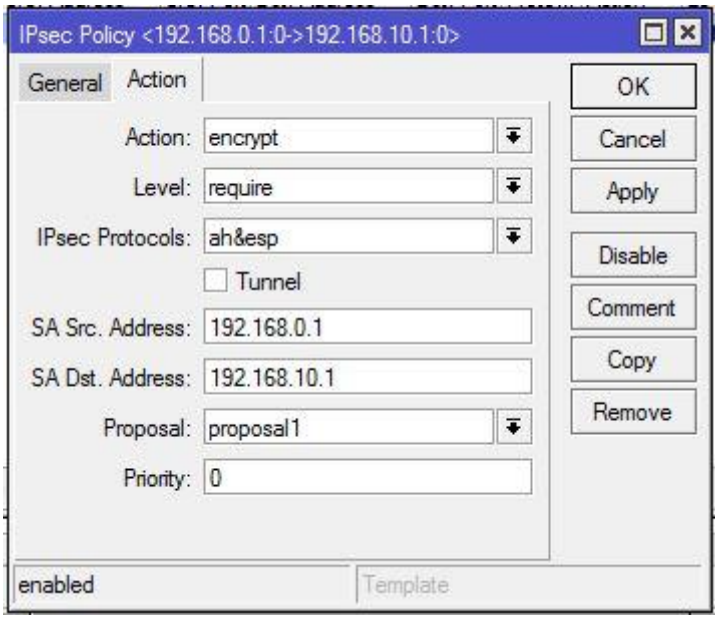
Gambar 4.8. IPSec *Peer* Pusat

Selanjutnya adalah menkonfigkurasi IPSec *Policy.* Pada bagian ini yang perlu diperhatikan adalah *src-address* yang diisi dengan IP LAN kantor pusat, *dst-address* yang diisi dengan IP LAN kantor cabang.



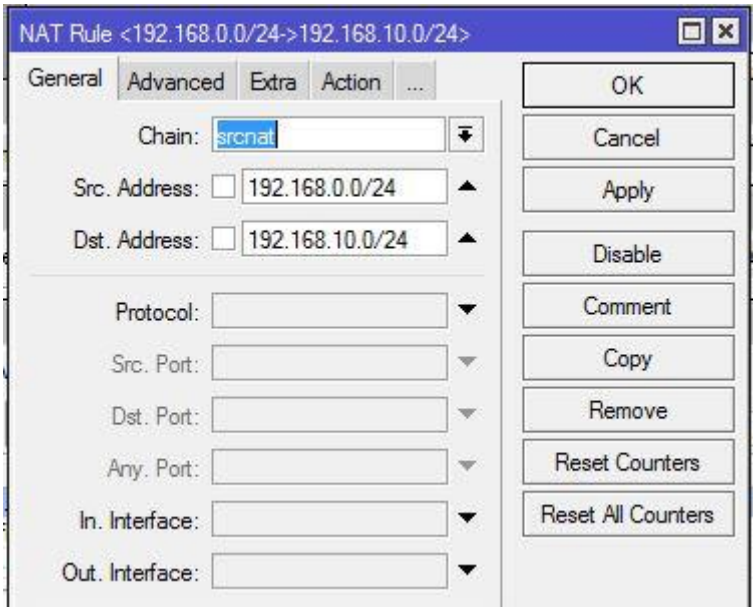
Gambar 4.9. IPSec *Policy General*

Kemudian konfigurasi IPSec *Policy* di tab *Action* dengan memperhatikan *SA Src-Address* yang diisi dengan IP Lokal di kantor pusat dan *SA Dst-Address* yang diisi dengan IP Lokal di kantor cabang. *Uncheck Tunnel* karena menggunakan *tunnel* dari EOIP dan menggunakan IPSec *Transport Mode*

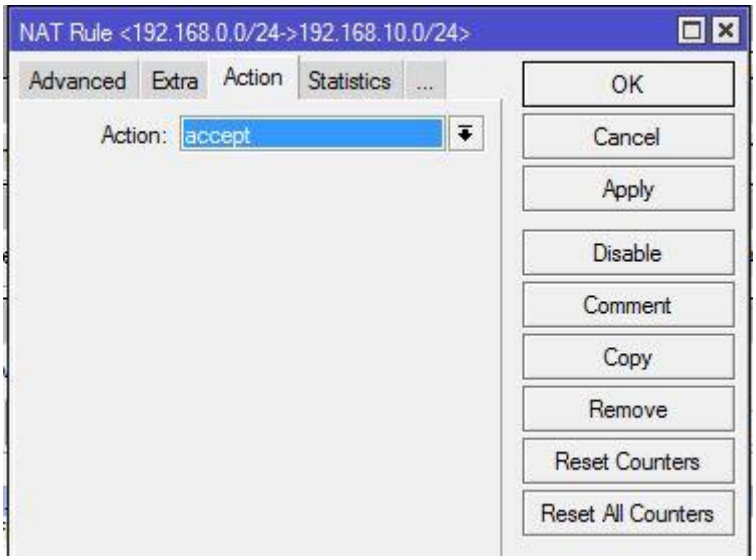


Gambar 4.10. IPSec *Policy Action*

Setelah menkonfigurasi IPSec, dikarenakan IPSec tidak dapat menembus NAT maka harus membuat rule dengan *chain* srcnat dengan *action Accept*



Gambar 4.11. NAT IPSec *General*



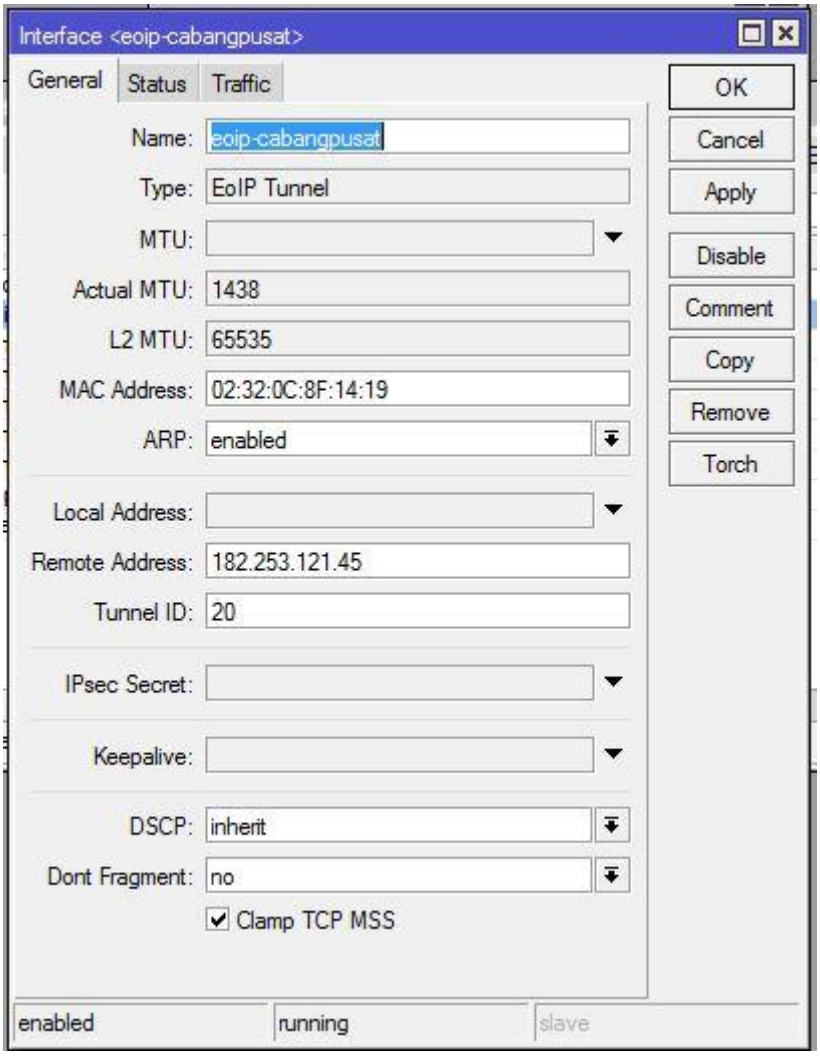
Gambar 4.12. NAT IPSec *Action*

4.1.2.2 Konfigurasi di Cabang

Konfigurasi di kantor cabang mencakup konfigurasi EOIP dan IPSec. Yang perlu diperhatikan adalah EOIP digunakan sebagai *Tunnel* sementara IPSec hanya digunakan sebagai keamanan komunikasi data.

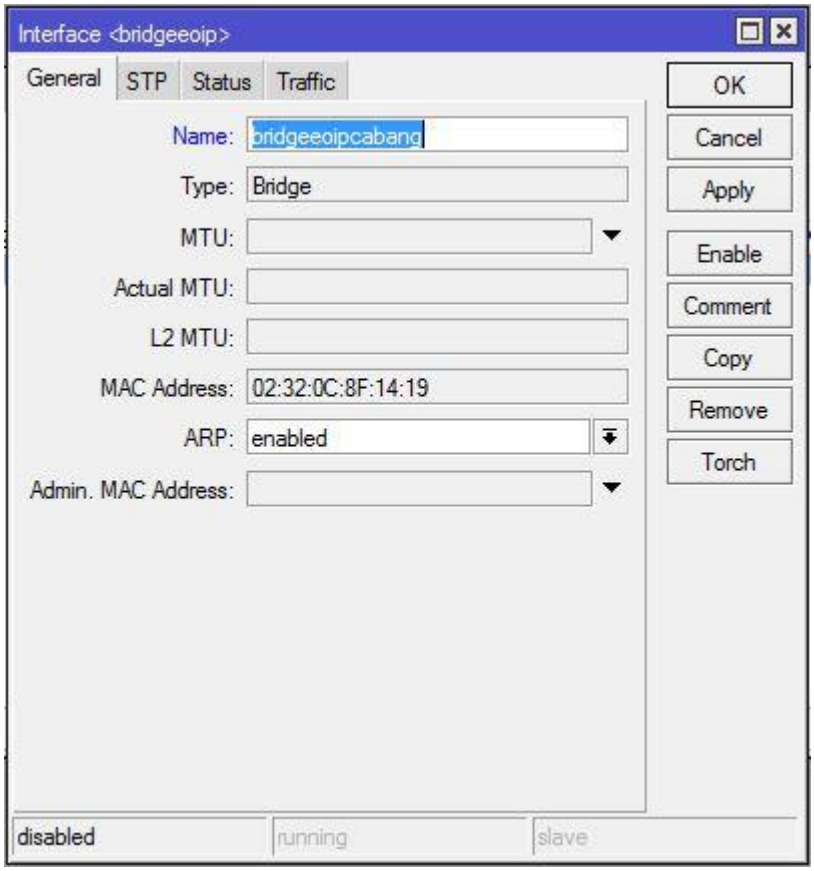
4.1.2.2.1 Konfigurasi EOIP di Kantor Cabang

Konfigurasi yang dilakukan adalah mengkonfigurasi EOIP dengan membuat *interface* baru bernama eoip-cabangpusat. Pada gambar 4.13 merupakan konfigurasi *interface* EOIP di kantor pusat. Kolom *remote addres* diisi dengan IP kantor pusat dan kolom tunel ID harus sama dengan Tunnel ID di cabang.



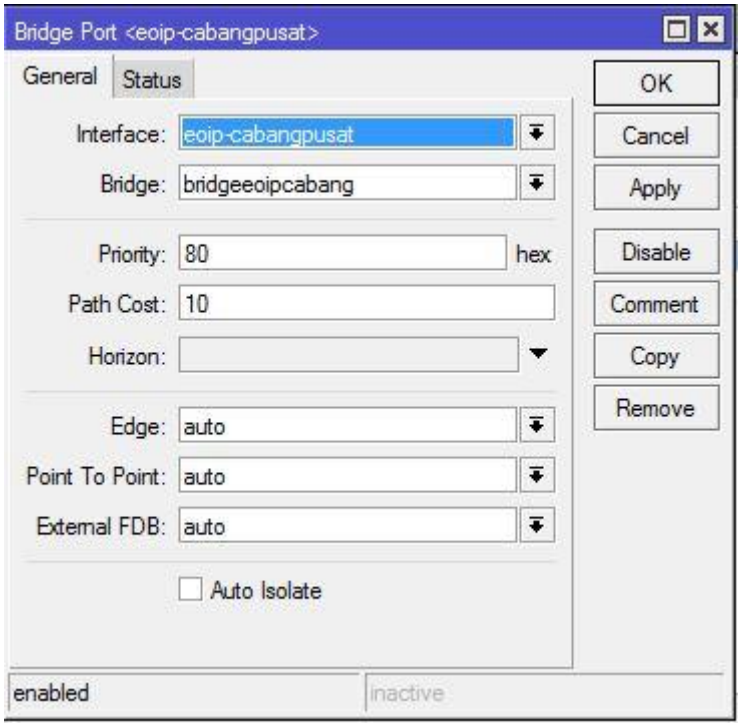
Gambar 4.13. Interface EOIP Cabang

Setelah membuat *interface* eoip, maka tahapan selanjutnya adalah membuat *bridge* antara *interface* LAN lokal dengan *Interface* EOIP yang baru dibuat.

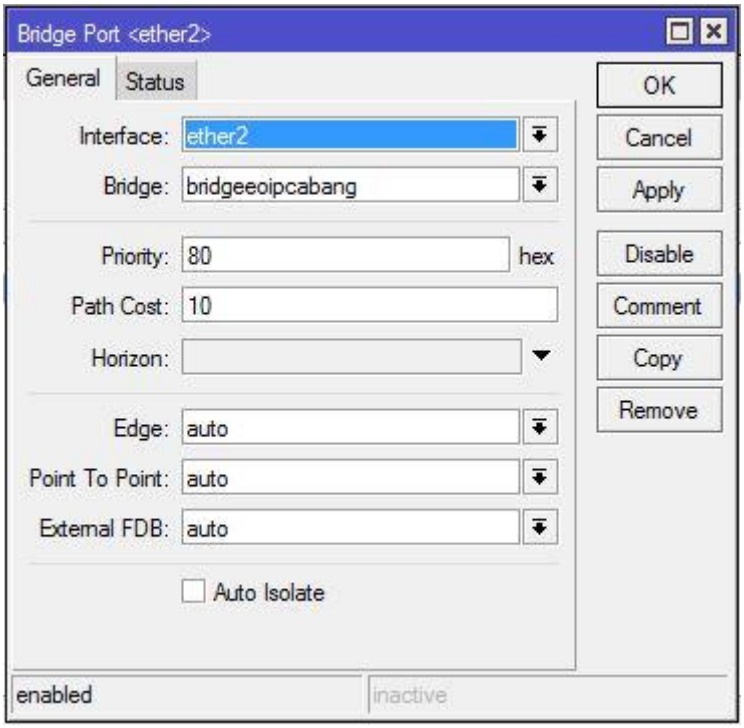


Gambar 4.14. *Bridge* EOIP Pusat

Setelah membuat *bridge* selanjutnya adalah menghubungkan *interface* LAN Lokal dengan EOIP



Gambar 4.15. *Bridge* Port EOIP Cabang



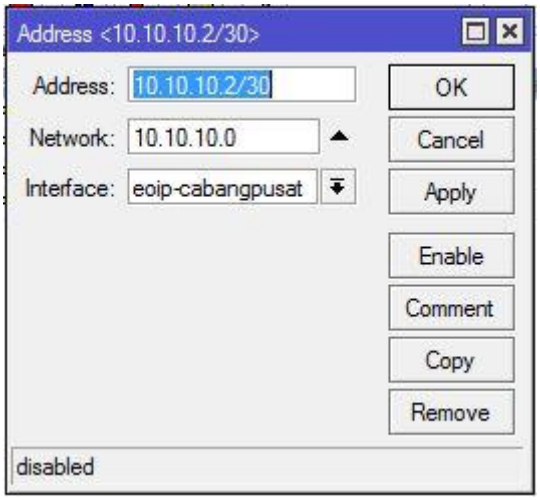
Gambar 4.16. *Bridge* Port LAN Lokal

Setelah *Bridge* selesai, maka port yang terhubung akan seperti pada gambar 4.17 dibawah ini.



Gambar 4.17. *Bridge* Port Cabang

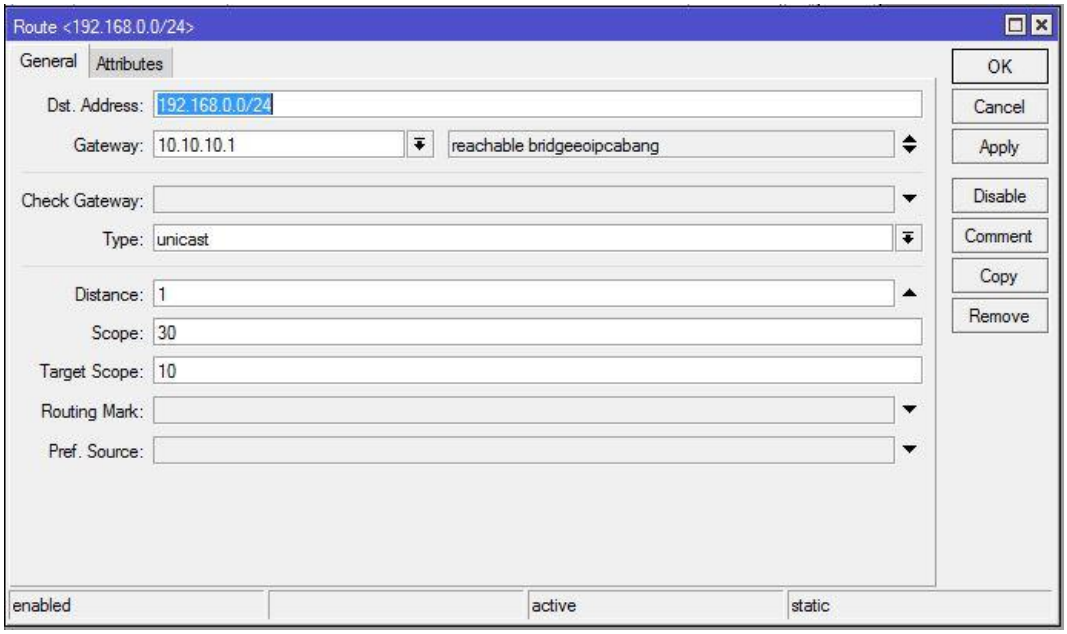
Setelah menkonfigurasi EOIP dan *Bridge* selanjutnya adalah menetapkan *route* dari LAN di kantor cabang ke LAN di kantor pusat melalui gateway EOIP yang sudah dibuat. Tahap pertama adalah dengan memberikan IP pada interface EOIP Cabang. IP yang digunakan pada EOIP Cabang harus dalam satu segmen dengan IP EOIP Pusat.



Gambar 4.18. IP Address EOIP Cabang

Setelah memberikan IP pada EOIP Cabang, selanjutnya adalah menentukan *route* agar LAN lokal cabang dapat berkomunikasi dengan

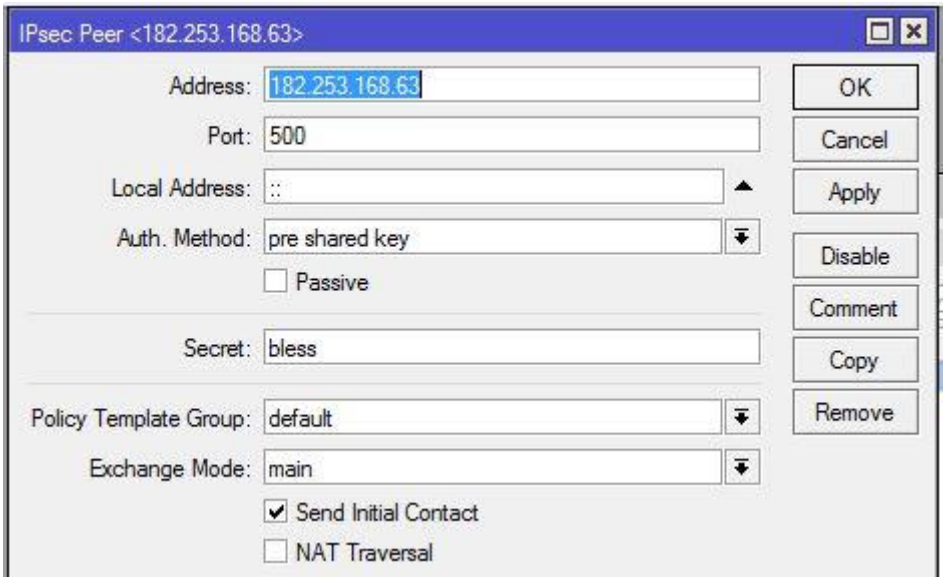
LAN lokal pusat. Konfigurasi dengan memasukan IP Segmen LAN Lokal di kantor pusat dengan gateway EOIP pusat.



Gambar 4.19. *Route* Cabang ke Pusat

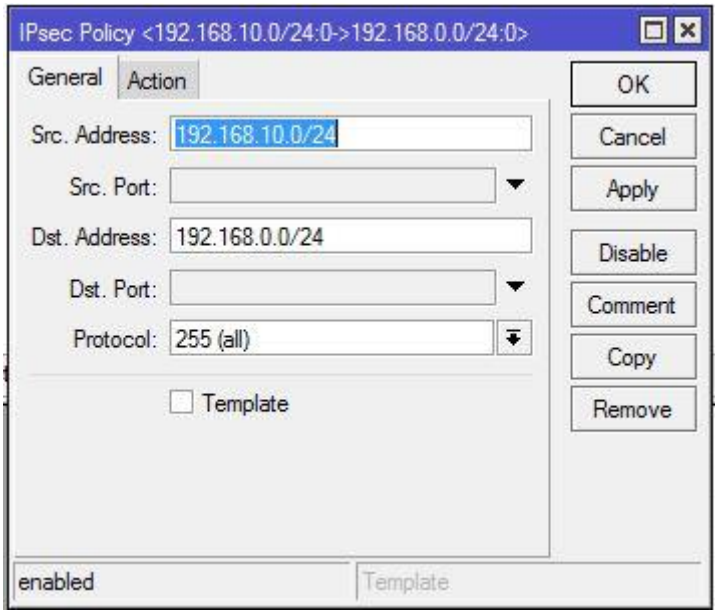
4.1.2.2.2 Konfigurasi IPSec di Kantor Cabang

Setelah konfigurasi setelah selanjutnya adalah mengkonfigurasi IPSec di kantor cabang yang terhubung ke kantor pusat. Tahapan pertama dalam mengkonfigurasi IPSec adalah menentukan *Peer* yang berarti kemana IPSec ini terhubung. Selain itu yang perlu diperhatikan disini adalah mengisi *secret*



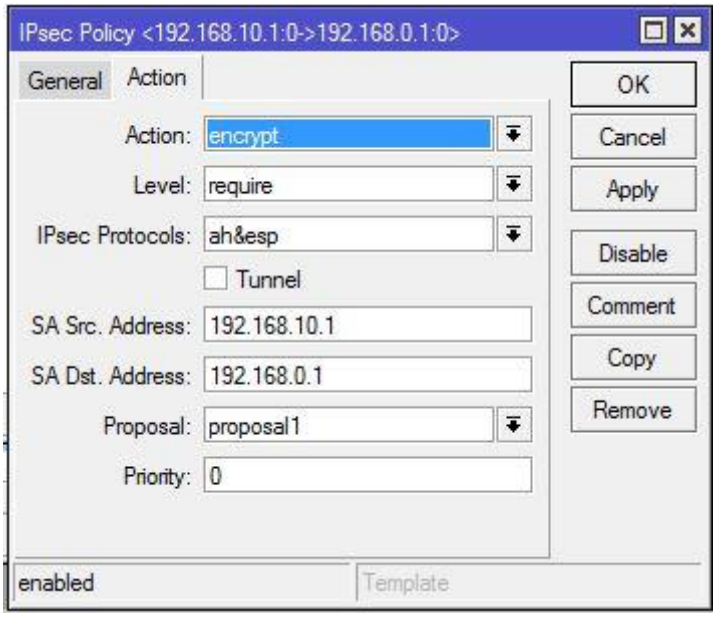
Gambar 4.20. IPSec *Peer* Cabang

Selanjutnya adalah menkonfigkurasi IPSec *Policy*. Pada bagian ini yang perlu diperhatikan adalah *src-address* yang diisi dengan IP LAN kantor cabang, *dst-address* yang diisi dengan IP LAN kantor pusat.



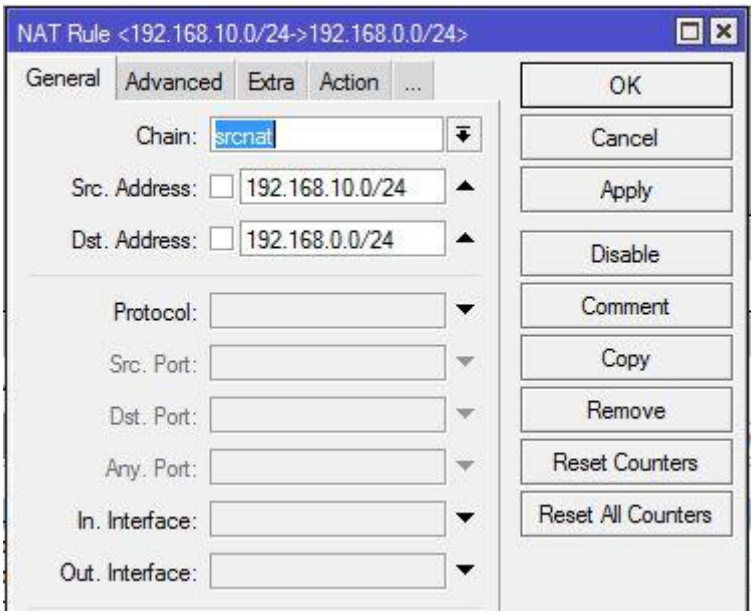
Gambar 4.21. IPSec *Peer General* Cabang

Kemudian konfigurasi IPSec *Policy* di tab *Action* dengan memperhatikan *SA Src-Address* yang diisi dengan IP Lokal di kantor cabang dan *SA Dst-Address* yang diisi dengan IP Lokal di kantor pusat. *Uncheck Tunnel* karena menggunakan EOIP sebagai metode *Tunnel* dan IPSec *Transport Mode.*

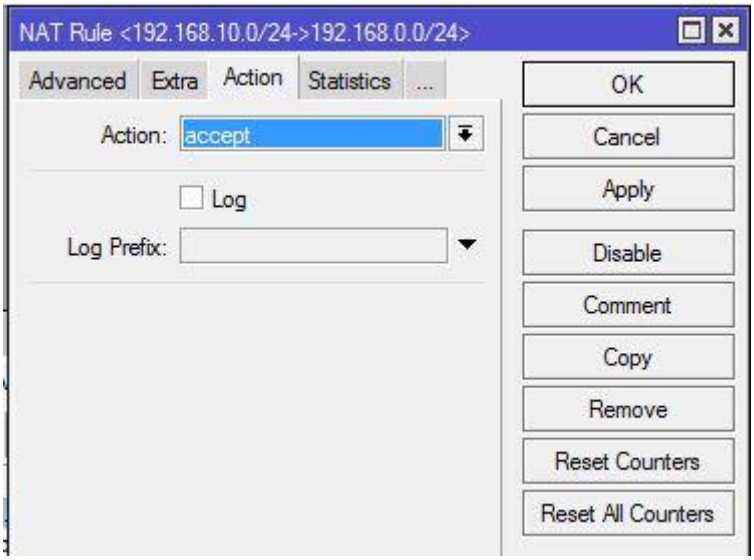


Gambar 4.22. IPSec *Peer Action* Cabang

Setelah menkonfigurasi IPSec, dikarenakan IPSec tidak dapat menembus NAT maka harus membuat rule dengan *chain* srcnat dengan *action Accept*



Gambar 4.23. NAT *General* IPSec Cabang



Gambar 4.24. NAT *Action* IPSec Cabang

4.2 Skenario Pengujian Sistem

Skenario pengujian sistem yang dilakukan adalah sebagai berikut :

a. Pengujian *ping*

Pengujian *ping* dilakukan untuk mengetahui apakah jaringan EOIP sudah terhubung secara lojik

b. Pengujian IPSec

Pengujian IPSec dilakukan untuk mengetahui apakah IPSec sudah berjalan dengan melihat *log* IPSec

c. Pengujian *Sniffing*

Pengujian Sniffing dilakukan untuk melihat apakah paket data yang dikirim benar-benar terenkripsi dan tak dapat dimanipulasi oleh pengguna yang tak berhak.

d. Pengujian Transfer Data

Pengujian transfer data dilakukan untuk mengetahui apakah sistem yang dibangun sudah berjalan sebagaimana mestinya.

e. Wawancara

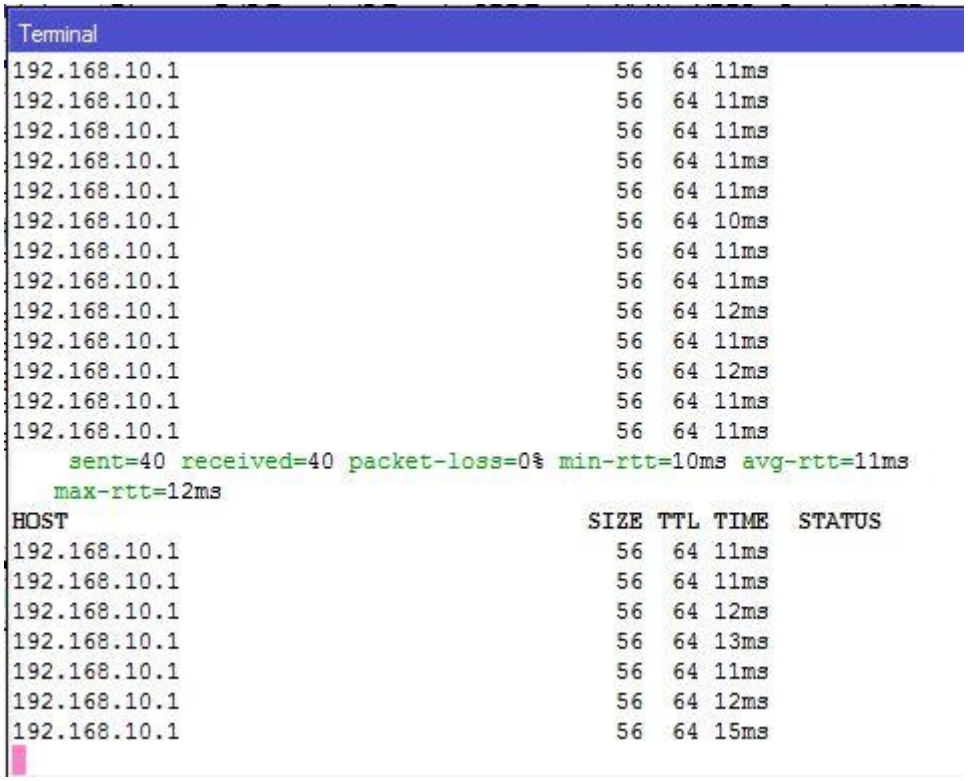
Wawancara dilakukan kepada Staf IT untuk mengetahui kinerja sistem yang dibangun. Selain itu wawancara dilakukan kepada bagian *accounting* sebagai pengguna utama sistem untuk mengetahui kepuasan pengguna.

4.3 Hasil Pengujian Sistem

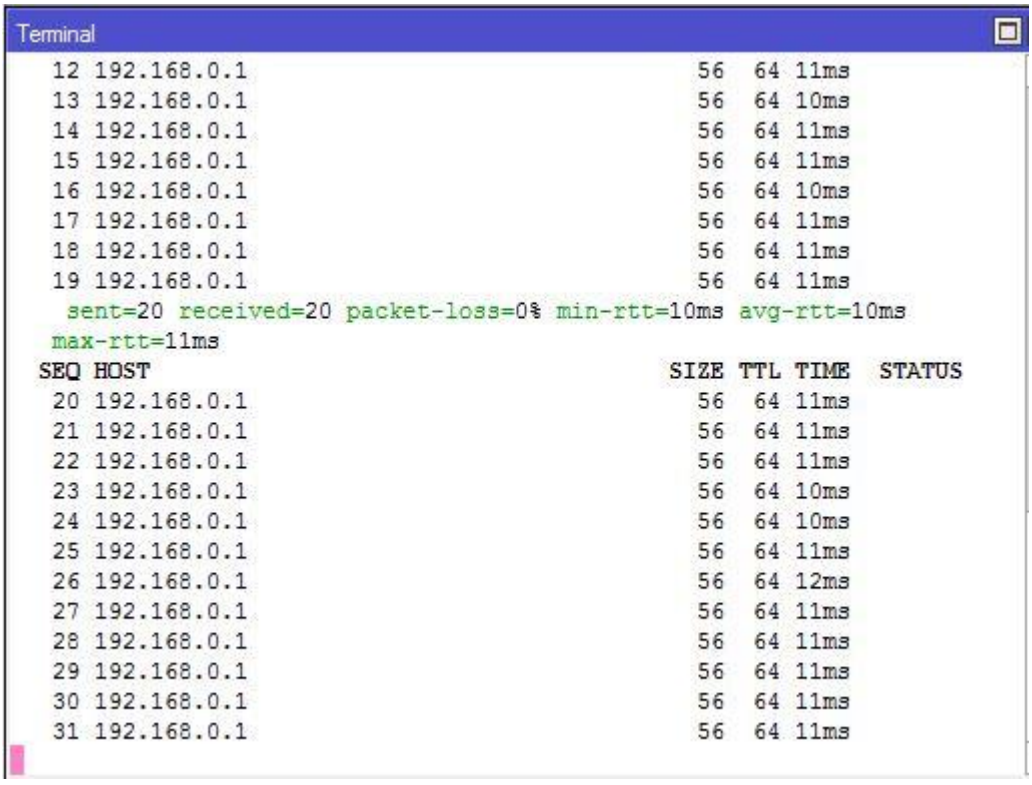
Pada bagian ini akan dipaparkan hasil pengujian terhadap sistem yang telah dibangun. Pengujian sistem itu sendiri terdiri dari hasil *ping*, uji IPSec, transfer file dan wawancara.

4.3.1 Hasil Uji *ping*

Berikut ini adalah hasil uji *ping* antara kantor pusat dan kantor pusat dengan menggunakan IP lokal masing-masing kantor. Hasil uji *ping* membuktikan bahwa jaringan telah dapat saling berkomunikasi.



Gambar 4.25. *Ping* pusat ke cabang

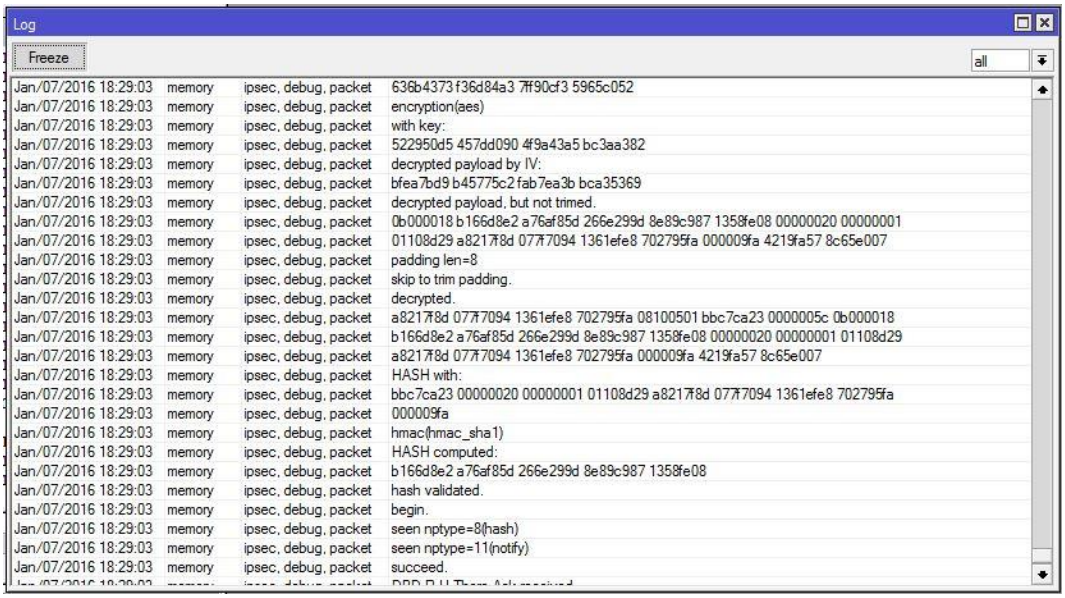


Gambar 4.26. *Ping* cabang ke pusat

Dari hasil uji *ping* diatas, membuktikan bahwa jaringan kantor cabang sudah dapat berkomunikasi dengan kantor cabang dan juga sebaliknya.

4.2.2 Hasil Uji IPSec

Berikut ini adalah *Log route*r selama komunikasi menggunakan IPSec.

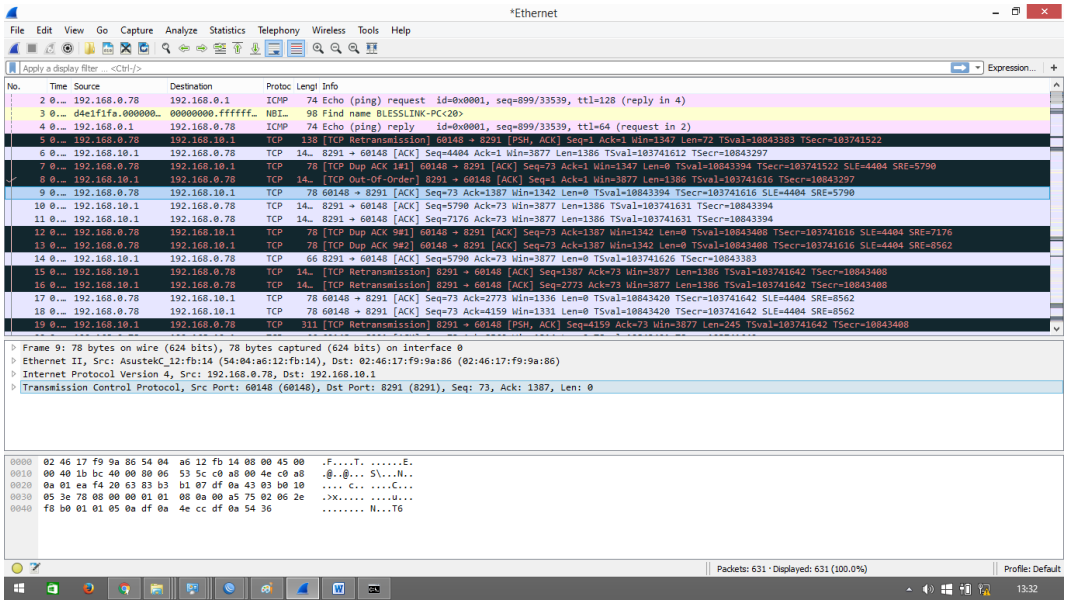


Gambar 4.27. Log IPSec

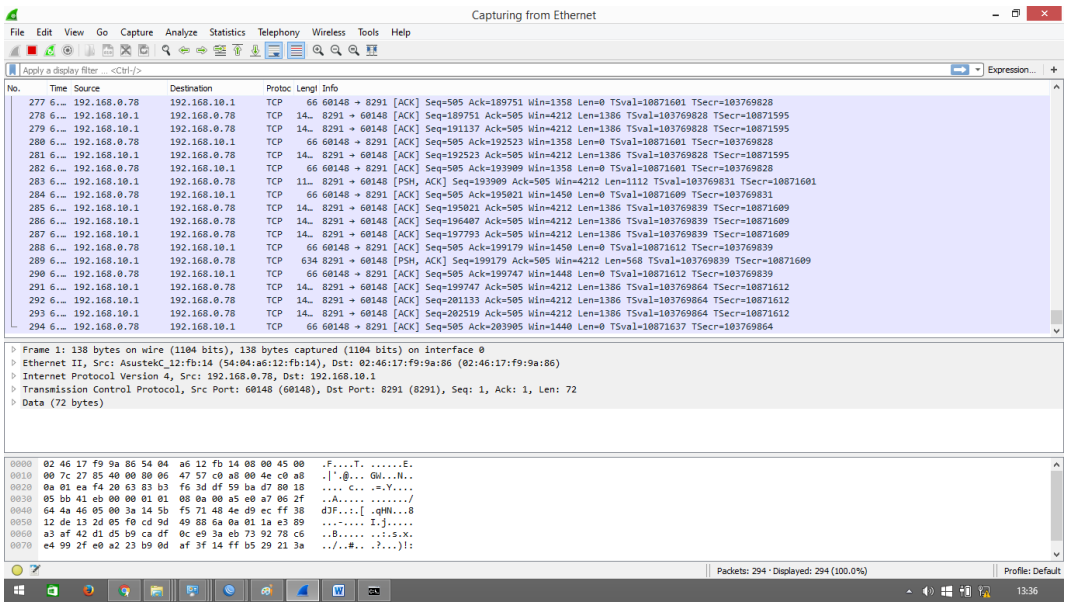
Pada gambar 4.27 menerangkan bahwa komunikasi yang terjadi telah menggunakan algoritma HASH SHA1 untuk autentifikasi dan enkripsi AES. Hal ini terlihat dari paket data yang terenkripsi diatas.

4.2.3 Hasil Uji *Sniffing*

Pengujian *sniffing* menggunakan *tool* wireshark untuk mengetahui apakah komunikasi data yang dibangun aman atau tidak. Dalam pengujian ini diperlihatkan beberapa transmisi data yang *vurneable* dan berbahaya yang ditandai dengan warna hitam.



Gambar 4.28. *Sniffing* tanpa IPSec



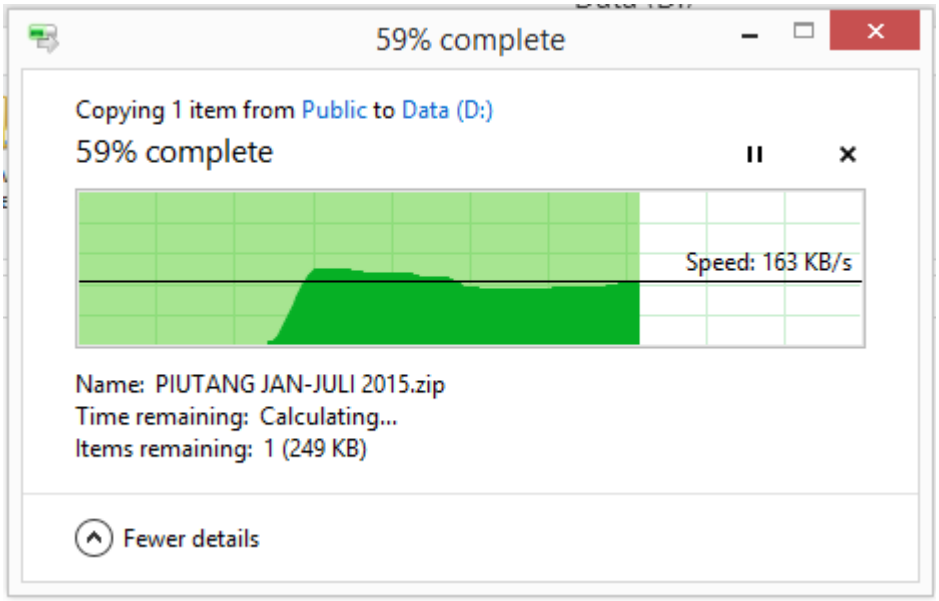
Gambar 4.29. Sniffing dengan IPSec

Dari hasil pengujian diatas bisa disimpulkan bahwa komunikasi sebelum menggunakan IPSec sangat berbahaya karena setiap paket data

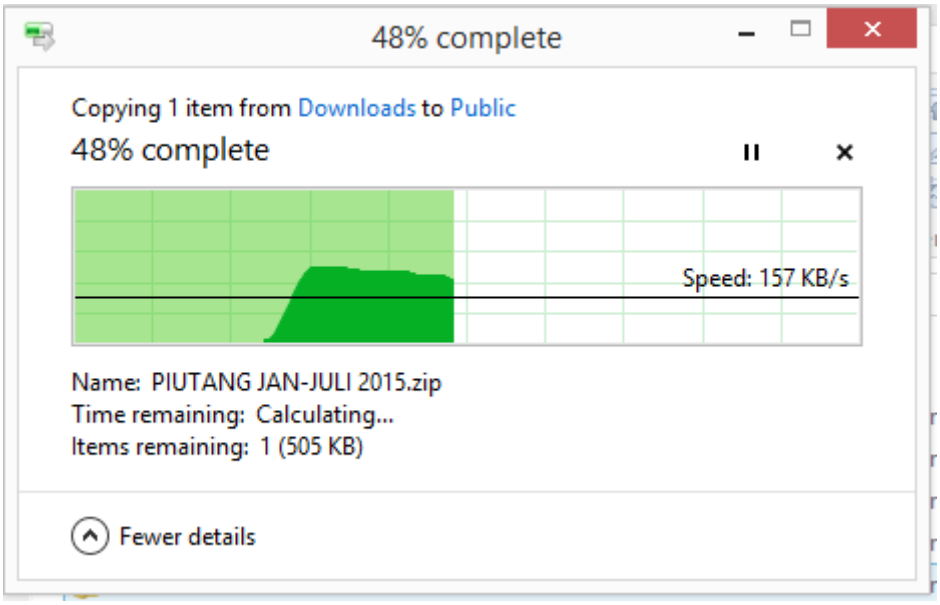
yang ditransmisikan dapat terlihat oleh *sniffer*. Sedangkan setelah menggunakan IPSec komunikasi data menjadi aman dari *sniffer*

4.2.4 Hasil Uji Transfer Data

Pengujian dilakukan dengan *Copy-paste* data antara komputer yang ada di kantor cabang dengan komputer yang ada dikantor pusat.



Gambar 4.30. Unduh data



Gambar 4.31. Unggah Data

Dari hasil uji transfer data diatas, membuktikan bahwa sistem EOIP sudah berjalan dan dapat digunakan untuk transfer data antara kantor cabang dan pusat.

4.2.5 Wawancara

Untuk mengetahui penilaian objektif terhadap sistem yang dibangun dan pengalaman pengguna yang menggunakannya, maka dilakukan wawancara terhadap staff IT untuk mengetahui pengalaman teknis terhadap sistem dan juga kepada bagian keuangan selaku pengguna yang akan menggunakan sistem ini.

Tabel 4.2. Wawancara dengan staff IT

1. Apakah anda kesulitan dalam mengelola jaringan EOIP yang telah dibangun?	
Jawaban Narasumber	Tidak, saya cukup mengerti dengan cara kerja sistem yang dibangun
2. Apakah dalam pembangunan sistem EOIP dan IPSec ini mengganggu	

jaringan yang adadi kantor?	
Jawaban Narasumber	Tidak, namun pernah sesekali jaringan terjadi masalah tapi sejauh ini tidak masalah
3. Bagaimana performansi sistem EOIP dan IPSec yang sudah dibangun ?	
Jawaban Narasumber	Baik, sejauh ini sistem yang dibangun memang dapat menghubungkan kedua kantor kami.
4. Apakah anda setuju bahwa EOIP dan IPSec akan membantu bagian keuangan dalam membutuhkan data dari kantor cabang?	
Jawaban Narasumber	Setuju, dengan sistem ini bagian keuangan tidak perlu mengirimkan data menggunakan Pos lagi dan keamanannya pun terjaga

Tabel 4.3. Wawancara bagian *accounting*

1. Apakah anda kesulitan dalam menggunakan sistem EOIP dan IPSec?	
Jawaban Narasumber	Tidak, sistem ini sama seperti file sharing yang biasa digunakan di kantor
2. Apakah sistem ini cukup cepat dalam transfer data yang dibutuhkan?	
Jawaban Narasumber	Ya, cukup cepat
3. Apakah direksi akan percaya dengan sistem yang dibangun ini untuk transfer data perusahaan?	
Jawaban Narasumber	Sepertinya iya, bila dilampirkan juga hasil laporan penelitian mengenai sistem ini