PERENCANAAN DAN IMPLEMENTASI JARINGAN MENGGUNAKAN IPSEC VPN

Paulino Saldanha, Erna Kumalasari , Uning Lestari
[1]Teknik Informatika, FTI, IST AKPRIND, pausaldanha@gmail.com
[2]Teknik Informatika, FTI, IST AKPRIND, ernakumalasaridzilhag@gmmail.com
[3]Teknik Informatika, FTI, IST AKPRIND, uningl@yahoo.com

ABSTRACT

Central Bank Timor Leste is one of the bank belong to the country,who manage whole outcome of natural source energy of East Timor. Such as Oil, Marble, Cement and the others natural source energy were we have. And all of the outcome of that will distribute trough local Government for development insfrastructures and also to prosperous its peoples from poverty trough various mehcanisim by the Government of East Timor. So that the aim of that Thesis is to design and to analyze a certain network system among Client and Server to achieve an effectively and data integrity on internet. Some method that using for writing that Thesis including, field Research method, internet research, library research and the direct interviewed with correspondence. There are library research method and internet research method for helped to collect information about all references and literatures will be an important manual to finished this Thesis. Interviewed method with the correspondence lead to asking directly about what matters and obstacle where faced by Central Bank Of East Timor while doing daily banking jobs. So research method is very useful for researcher to define what kind of device and materials and also how much cost its need to implement a IPSec VPN networking system. Than having some analyze and comparison between IPSec VPN and Non-IPSec VPN. And if sure that using IPSec VPN, should to make sure that all the packet of data who send through this tunnel is securely due to all of them has been encrypted by using encapsulation method.
Keywords: IPSec VPN, Internet Security

INTISARI

Bank Central Timor Leste (BCTL) adalah salah satu Bank milik negara Timor leste,yang bergerak di bidang pengelolaan hasil sumber daya alam Timor Leste,seperti minyak,batu bara, marmer,semen dan lain sebagainya yang hasilnya akan disalurkan melalui pemerintah untuk pengembangan infrastruktur dan untuk mensejahterakan rakyatnya melalui mekanisme yang akan di implementasikan oleh pemerintahan setempat.sehingga tujuan dari penulisan ini adalah untuk menganalisa dan merancang suatu sistem jaringan antara client dan server dan dapat mencapai efektifitas dan integritas data di dalam jaringan internet. Metode yang digunakan dalam penulisan skripsi ini meliputi: metode field research,internet research,library research,interview dengan korespondensi. Metode library research dan internet research dilakukan untuk mengoleksi informasi tentang referensi dan literatur yang akan menjadi pedoman dalam menyelesaika skripsi ini. Metode interview dengan korespondensi ini dilakukan agar supaya peneliti mengetahui secara langsun masalah dan kendala apa saja yang di hadapi oleh Bank Central Timor Leste dalam melakukan dan mengerjakan kegiatan perbankan setiap hari. Metode research ini sangat penting dilakukan karena untuk mengetahui dan menentukan alat dan bahan serta berapa biaya yang akan diperlukan untuk mengimplementasikan suatu sistem jaringan dalam hal ini yaitu type jaringan dengan teknologi VPN IPSEC yang merupakan salah satu solusi yang baik untuk melakukan remote access dan site-to-site VPN, kemudian menganalisa apakah perbedaan mengunakan fasilitas jaringan IPSEC VPN dengan jaringan internet biasa, dan jikalau menggunakan IPSec VPN maka dapat memastikan bahwa semua paket data yang melewati jaringan ini terjamin aman dan utuh karena semuanya telah dienkripsi atau biasanya disebut dengan metode enkapsulasi data.
Kata kunci: ***IPSec VPN.***

PENDAHULUAN

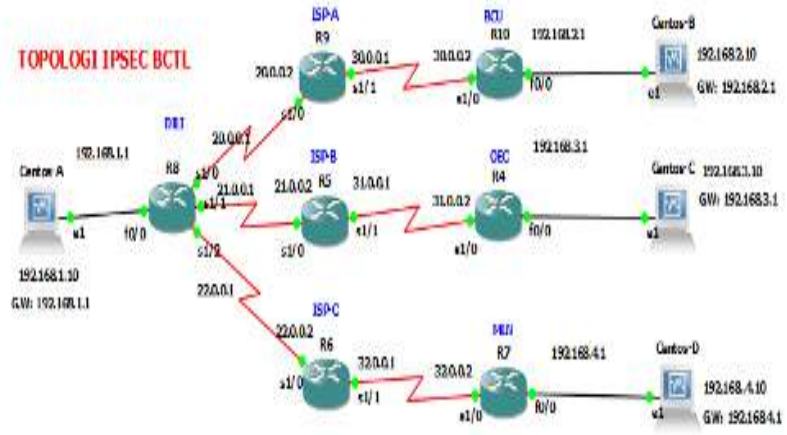
Bank Central Timor-Leste (BCTL) adalah salah satu bank milik negara yang bergerak di bidang investasi dan penanaman modal milik Negara yang berasal dari hasil minyak bumi dan pendapatan-pendapatan lainya. Oleh karena bank ini juga menggunakan jaringan public,sehingga hal ini sangat riskan terhadap kinerja dan serlukasi data yang ada,bahkan data dapat diakses oleh pihak yang tidak berwewenang dan tidak bertanggun jawab,seperti kita tahu bahwa era globalisasi saat ini, kemudahan akses terhadap informasimerupakan salah satu kunci untuk dapat bersaing dan memenangkan kompetisi,karena dengan adanya informasi yang cepat dan akurat dapat meningkatkankinerja suatu organisasi. Akses informasi yang cepat dan akurat salah satunyabisa didapatkan melalui Internet.Pemakaian Internet sebagai sarana jaringan publik untuk mendapatkan informasi maupun mengirimkan suatu informasi yang mempunyai resiko tersendiri, karenaInternet terbuka untuk umum, maka masalah kerahasiaan dan authentifikasi atasinformasi yang diterima dan dikirim pun juga terbuka. Oleh karenanyateknologi IPSec VPN dapat menjawab kebutuhan tersebut dan menjaminnya bahwa *IPSec* protokol dapat enkripsi data dengan tools-tools tertentu baik itu free maupun yang berlisensi tergantung dari kebutuhan organisasi agar supaya dapat tetap utuh sampai di tujuan. Hal yang tidak asing lagi yaitu ancaman terhadap kegiatan rutinitas semua Bank pada saat ini telah meningkat,baik itu Bank-Bank komersial maupun Non-komersial lainya, yang dalam aktivitas sehari-harinya melakukan transaksi antara Bank satu dengan Bank lain,Bank dengan Nasabah,seperti penyetoran Uang,penarikan Uang melalui buku tabungan Nasabah maupun melalui mesin ATM (Asyhincronous Transfer Mode),dan ancaman – ancaman itu berupa serangan-serangan yang dilakukan oleh kelompok atau individu tertentu atau biasanya disebut dengan kejahatan dunia maya (*Cyber crime*),dengan berbagai modus yang akan direncanakan oleh kelompok atau *individu* itu sendiri. dan mayoritas aktifitasnya adalah dengan tujuan yang negative atau jahat (destroy) terhadap target yang diiginkan,terutama pihak Bank dan Nasabah yang melakukan transaksi dalam bentuk uang dan laporan manajemen perbankan lainya pada waktu kapan dan dimana saja.hal ini menjadi trend yang sedang dibahas di dunia perbankan saat ini,tetapi tampa kita sadar bahwa kelalaian manusia itu sendiri merupakan salah satua factor utama yang akan memicu terjadinya kebocoran data transaksi kerahasiaan Bank dalam skala yang besar,dan kejadian ini sangat riskan sekali terhadap keamanan dan kenyamanan kinerja rutinitas Bank itu sendiri,inilah yang biasanya disebut dengan *Human error.*untuk mengatasi problem ini,maka pegawai Bank yang berkompeten kiranya meningkatkan sumber dayanya tersendiri di berbagai macam ilmu pengetahuan yang berkaitan dengan dunia perbankan demi mencegah,mengantisipasi dan menjaga integritas kinerja perbankan itu sendiri.berkaitan dengan menjaga integritas dan keamanan perbankan,sehingga dengan kehadiran teknologi IPSec *Virtual Private Network* (VPN) dapat membantu dan mengurangi hal-hal yang tidak diinginkan secara bersama. Baik dari pihak perbankan,nasabah maupun pemerintahan local mengenai serangan dan tindakan negative terhadap Bank bersangkutan.maka peneliti memamfaatkan momen teknologi tersebut IPSec (VPN) sebagai salah satu sarana alternative untuk memfasilitasi dan mendukung penuh segala aktifitas rutin perbankan. *Virtual Private Network* (VPN) merupakan sebuah jaringan private yang menghubungkan satu node jaringan ke node jaringan lainnya dengan menggunakan jaringan publik (internet). Data yang dilewatkan akan dibungkus (encapsulation) dan dienkripsi agar terjamin kerahasiaannya. Jaringan VPN dikoneksikan oleh penyedia jasa komunikasi (Internet Service Provider) melalui routernya ke router-router lain dengan menggunakan jalur internet yang telah dienkripsi diantara dua titik.disamping itu kita ketahui bahwa VPN merupakan suatu koneksi antar dua jaringan yang dibuat untuk mengkoneksikan kantor pusat, kantor cabang,suppliers dan rekan bisnis lainnya, ke dalam suatu jaringan dengan menggunakan access VPN untuk mengoneksikan jaringan jarak jauh untuk mengakses ke jaringan internet atau extranet di kantor cabang atau rekan kerja yang berbeda lokasi dengan kantor pusat,hal ini dilakukan dengan menggunakan mekanisme Tunneling (terowongan),sehingga memamfaatkan IPSec yang telah dicreateagar jaringan ini menjadi private.

TINJAUAN PUSTAKA

Virtual Private Network (VPN) merupakan sebuah jaringan private yang menghubungkan satu node jaringan ke node jaringan lainnya dengan menggunakan jaringan publik (internet). Sehingga data yang dilewatkan akan dibungkus (encapsulation) dan dienkripsi agar terjamin kerahasiaannya. Jaringan VPN dikoneksikan oleh penyedia jasa komunikasi (Internet Service Provider) melalui routernya ke router-router lain dengan menggunakan jalur internet yang telah dienkripsi diantara dua titik (Leon, 2010),Untuk merancang VPN perlu pengetahuan tentan jaringan komputer. VPN juga termasuk jaringan komputer yang bersifat private atau pribadi (bukan untuk akses umum yang menggunakan medium umum misalnya internet,untuk menghubunkan antar Remote-Site secara aman,walaupun menggunakan medium yang bersifat umum atau non-pribadi,pada umumnya sebuah jaringan VPN harus memiliki keamanan yang baik. Teori-teori dan penelitian mendasari yang telah melaksanakan sebelumnya,merupakan landasan bagi para peneliti agar dengan demikian dapat membahas dan mengali ilmu ini lebih detail lagi.

1. *perancangan jaringan dengan menggunakan ipsec vpn pada pt. great heart media Indonesia (febri,wijoyo, alvin agung,2010* Pada penelitian dan analisis ini tidak membahas mengenai Tunneling,yang mestinya menjadi bagian terpenting dalamVPN,sehingga pada pembahasan nanti akan membahas secara sederhana mengenai tunneling yangdimaksudkanini.
2. *perencanaan vpn sebagai komunikasi data pada perusahaan manufaktur telemor* (Aliudin, 2009) Perencanaan skripsi ini,cukup luas pembahasanya mengenai VoIP, L2TP tetapi namun masih belum membahas mengenai access VPN,sehingga diangap ini sebagai kekurangan yang akan dibahas dalam skripsi ini.

Pada Bab ini akan dibahas mengenai proses implementasi yang dilakukan pada rancangan jaringan pada Bank Central Timor Leste (BCTL). Pada bab ini juga akan dilakukan evaluasi menyeluruh terhadap hasil konfigurasi terhadap apa yang telah diimplementasikan sebelumnya. Hasil evaluasi tersebut terdiri dari segi keamanan,waktu respon, besar kecil paket data yang berpengaruh terhadap Bandwith, reliabilitas dari koneksi IPSec VPN yang telah diimplementasikan pada jaringan Bank Central Timor Leste (BCTL). Berikut ini adalah langkah-langkah implementasi IPSec VPN yang akan di analisis hasilnya. Pada bagian ini akan dibahas secara rinci mengenai implementasi dari perancangan IPSec VPN pada Bank Central Timor Leste (BCTL) secara menyeluruh. Penjelasan mengenai implementasi ini meliputi cara penggunaan, manfaat, hingga evaluasi dari IPSec VPN yang diimplementasikan pada Bank Central Timor Leste (BCTL). Menurut analisis dari hasil perancangan ini akan membuktikan bahwa memang terdapat perbedaan yang begitu kompleks antara jaringan yang menggunakan fasilitas IPSec VPN dan Non IPSec VPN, pada saat melakukan uji coba terhadahap hasil perancangan IPSec VPN tersebut. Adapun perencanaan jaringan yang akan diimplementasikan adalah sebagai berikut:



Gambar 1 Remote Site IPSec VPN Client dan Server

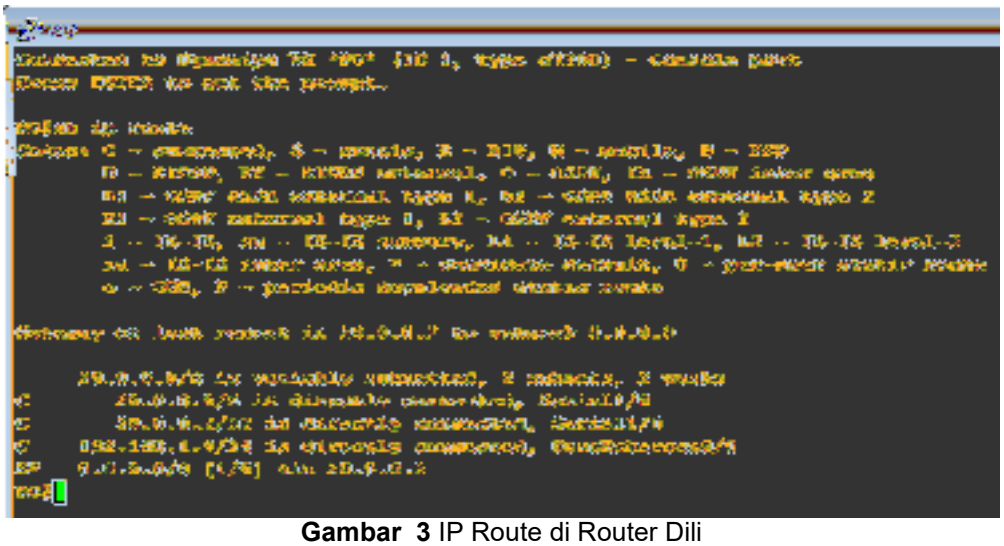
Pada gambar 1 adalah Konsep jaringan yang diimplemtasikan dengan kopnsep Remote Site IPSec VPN, pada gambar diatas menjelaskan bahwa suatu sistem jaringan memiliki fungsi tertentu, dia akan bekerja sesuai dengan peranya berdasarkan kebutuhan para user, Pada server IPSec VPN akan mengkonfigurasikan menggunakan metode autentikasi yaitu enkripsi dan dekripsi, dan juga di vpn client akan mengkonfigurasi layaknya client yang menggunakan fasilitas dan akses IPSec vpn, sehingga pada saat melakukan remote site antara kantor pusat dan kantor-kantor cabang maka semua data yang melewatinya telah terenkripsi dengn beberapa kunci enkripsi seperti algoritma MD5, Sha,Has, DES dan lain sebagainya. Oleh karena itu pada saat data diterima oleh vpn client, terlebih dahulu client vpn melakukan dekripsi terhadap data yang diterimanya dengan menggunakan beberapa kunci enkripsi yang telah digunakan oleh server IPSec vpn. Dengan demikian IPSec VPN ini selalu menjaga keamanan sistem jaringanya demi keutuhan data yang dimiliki oleh Bank tersebut.

```
[root@centos-minimal ~]# ping 192.168.2.10
PING 192.168.2.10 (192.168.2.10) 56(84) bytes of data.
64 bytes from 192.168.2.10: icmp_seq=1 ttl=61 time=62.0 ms
64 bytes from 192.168.2.10: icmp_seq=2 ttl=61 time=42.1 ms
64 bytes from 192.168.2.10: icmp_seq=3 ttl=61 time=47.5 ms
64 bytes from 192.168.2.10: icmp_seq=4 ttl=61 time=49.0 ms
64 bytes from 192.168.2.10: icmp_seq=5 ttl=61 time=41.9 ms
64 bytes from 192.168.2.10: icmp_seq=6 ttl=61 time=41.6 ms

--- 192.168.2.10 ping statistics ---
7 packets transmitted, 6 received, 14% packet loss, time 6002ms
rtt min/avg/max/mdev = 41.657/47.400/62.020/7.149 ms
[root@centos-minimal ~]# _
```

Gambar 2 Hasil Ping IPSec dari Centos-A ke Centos-B

Pada gambar 2 menyatakan bahwa hasil ping dari client di Centos-A ke client Centos-B adalah sukses. Hal ini membuktikan bahwa ipsec telah berjalan pada topologi di atas dengan traffic dari kantor pusat Dili ke kantor cabang di Baucau melalui isp-A dengan melakukan ip routing terlebih dahulu pada ketiga router yang ada yaitu Router Dili,ISP-A dan Router cabang Baucau.



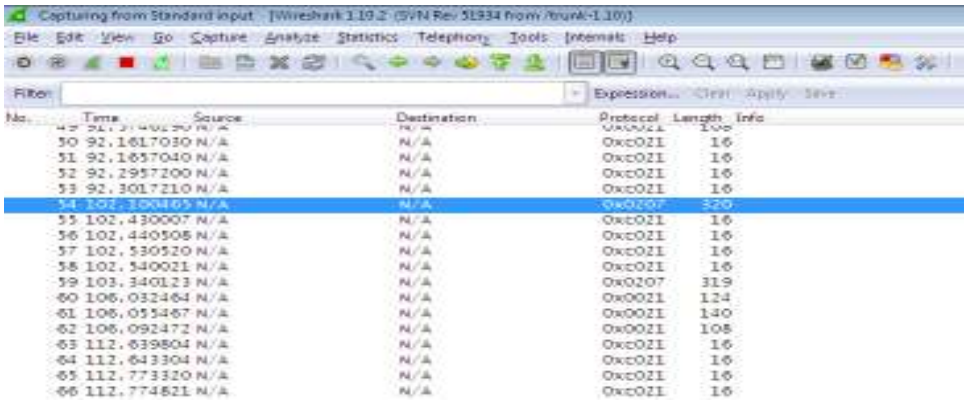
Gambar 3 IP Route di Router Dili

Seperti tampak pada hasil printscreen pada gambar 3, bahwa dari Centos-A (192.168.1.10) ke Centos-B (192.168.2.10) maka akan melewati ip gateway (20.0.0.2) di router ISP-A dengan port serial1/0. Dan sebaliknya dari Centos-B (192.168.2.10) ke Centos-A (192.168.1.10) maka akan melewati ip gateway (30.0.0.1) di router ISP-A dengan port serial 1/1.

```
[root@centos-minimal ~]# ftp 192.168.2.10
Connected to 192.168.2.10.
220 (vsFTPd 2.0.5)
530 Please login with USER and PASS.
530 Please login with USER and PASS.
KERBEROS_V4 rejected as an authentication type
Name (192.168.2.10:root): paulino
331 Please specify the password.
Password:
530 Login incorrect.
Login failed.
ftp> _
```

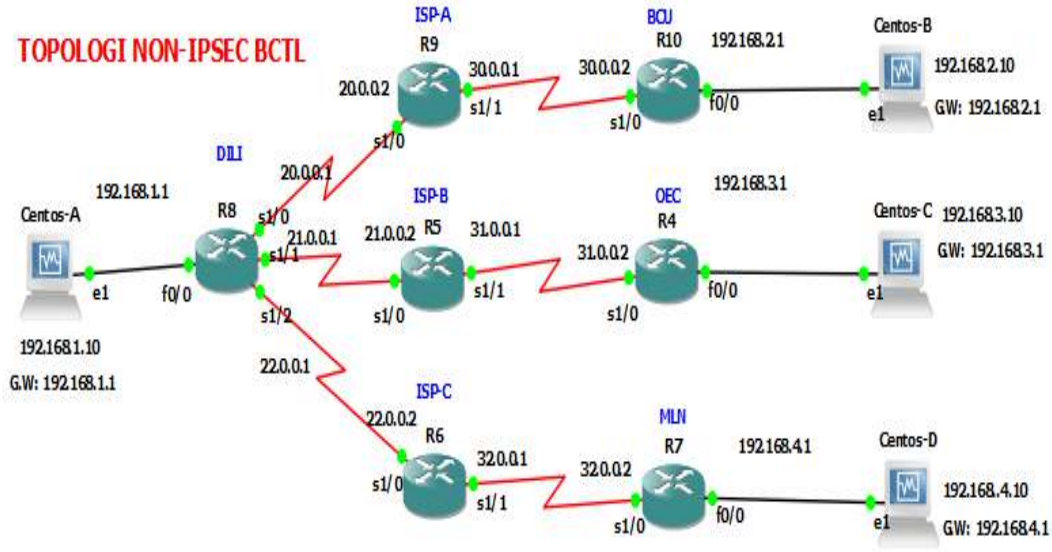
Gambar 4 FTP Server IPSec dari Centos-A ke Centos-B

Pada gambar 4 yaitu protocol FTP Server IPSec dari Centos-A ke Centos-B, jadi disini menggunakan protocol ini untuk melakukan login pada topologi IPSec sehingga meminta untuk memasukan User name dan password agar bisa membuktikan pada paket capturing nanti, apakah protocol ini di enkripsi atau tidak, dan hasil capturinya adalah terenkripsi karena saat melakukan login dengan user name dan password tidak terlihat di paket capturing.seperti pada gambar di bawah ini.



Gambar 5 Hasil IPSec Router ISP-A Serial 1/0

Pada gambar 5 membuktikan bahwa traffic data telah dienkripsi, sehingga saat melakukan ping menggunakan protocol FTP dari klient Centos-A ke klient di Centos-B tidak terlihat ip source dan destination termasuk juga user name dan password.



Gambar 6 Topologi Non-IPSec

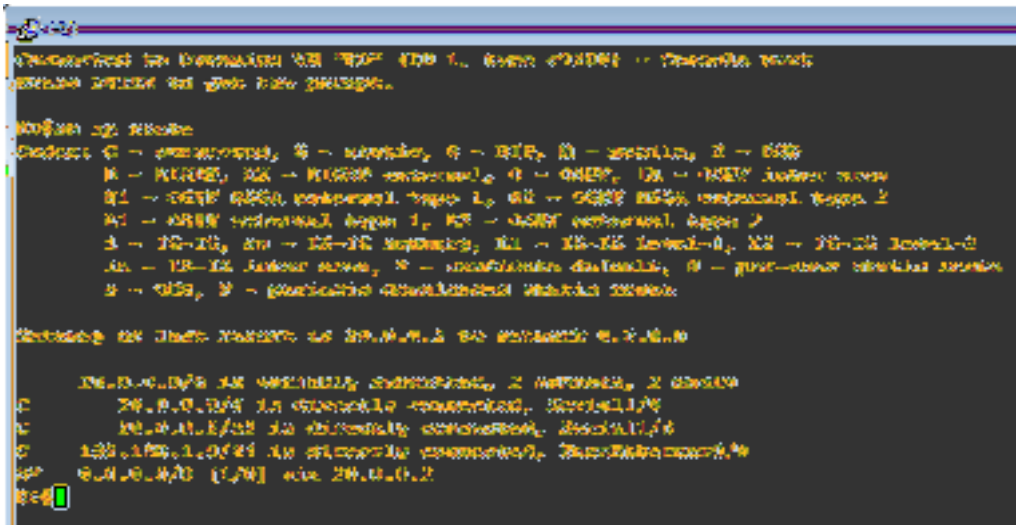
Seperti kita lihat pada gambar 6, dengan kehadiran topologi ini sehingga dapat memberi perbedaan untuk membuktikan bahwa, keamanan traffic data benar-benar ada dan tidaknya di antara dua tolopoli tersebut yaitu topologi IPSec VPN dan topologi Non-IPSec VPN, pada topologi ini juga memberi kontribusi kepada para user untuk melakukan pekerjaanya dengan baik sesuai dengan tujuan visi dan misi perbankan , namun dilihat dari sisi keamanan topologi ini belum bisa melindungi traffic data yang terus mengalir di setiap saatnya melewati jalur akses yang ada seperti dari kantor pusat ke kantor-kantor cabang. Berikut ini adalah hasil ping dan capturing dari topologi Non-IPSec.

```
[root@centos-minimal ~]# ping 192.168.2.10
PING 192.168.2.10 (192.168.2.10) 56(84) bytes of data.
64 bytes from 192.168.2.10: icmp_seq=1 ttl=61 time=62.0 ms
64 bytes from 192.168.2.10: icmp_seq=2 ttl=61 time=42.1 ms
64 bytes from 192.168.2.10: icmp_seq=3 ttl=61 time=47.5 ms
64 bytes from 192.168.2.10: icmp_seq=4 ttl=61 time=49.0 ms
64 bytes from 192.168.2.10: icmp_seq=5 ttl=61 time=41.9 ms
64 bytes from 192.168.2.10: icmp_seq=6 ttl=61 time=41.6 ms

--- 192.168.2.10 ping statistics ---
7 packets transmitted, 6 received, 14% packet loss, time 6002ms
rtt min/avg/max/mdev = 41.657/47.400/62.020/7.149 ms
[root@centos-minimal ~]# _
```

Gambar 7 Hasil Ping Non-IPsec dari Centos-A ke Centos-B

Pada gambar 7 menyatakan bahwa hasil ping dari client di Centos-A ke client Centos-B adalah sukses. Hal ini membuktikan bahwa ipsec telah berjalan pada topologi di atas dengan traffic dari kantor pusat Dili ke kantor cabang di Baucau melalui isp-A dengan melakukan ip routing terlebih dahulu pada ketiga router yang ada yaitu Router Dili,ISP-A dan Router cabang Baucau.



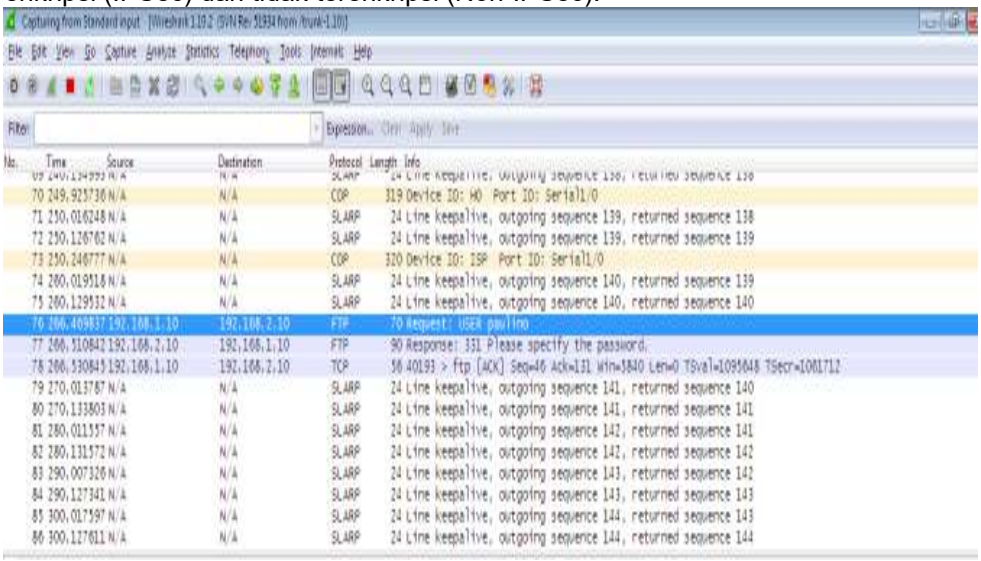
Gambar 8 IP Route di Router Dili

Pada gambar 8 adalah IP Route pada client di Router Dili dengan ip address 192.168.1.10 ke client di Router Baucau dengan ip address 192.168.2.10 yang melewati Router ISP-A dengan IP gateway 20.0.0.2. Jadi ip route ini untuk melanjutkan paket data yang dikirim dari suatu sumber ke tujuan yang benar.

Setting IP Route di Router Cabang Baucau

Gambar 9 FTP Server Non-IPSec dari Centos-A ke Centos-B

pada gambar 9 adalah melakukan ping menggunakan FTP dari Centos-A ke Centos-B, sehingga meminta untuk melakukan login yaitu dengan memasukan user name dan password yang akan membuktikan di paket capturing nanti, apakah user name dan password ini terenkripsi (IPSec) dan tidak terenkripsi (Non-IPSec).



Gambar 10 Hasil Non-IPSec di Router ISP Serial 1/0

Pada gambar 10 membuktikan bahwa traffic data tidak terenkripsi, sehingga saat melakukan ping menggunakan protocol FTP dari klient Centos-A ke klient di Centos-B dapat terlihat ip source dan destination termasuk juga user name dan password yang diggunakan saat melakukan login juga kelihatan, hal ini memudahkan para hacker untuk melakukan interupsi, sadap atau apapun itu bentuk seranganya saat traffic data sedang berjalan.dari Centos A ke Centos B untuk meminta informasi maka melaluilah ftp dengan ip address 192.168.2.10.

KESIMPULAN

Setelah melakukan simulasi uji coba dengan konfigurasi IPSec VPN, maka secara keseluruhan dapat menyimpulkan bahwa:

Simulasi IPSec VPN ini sangat membantu seorang network enginering untuk merancang dan membangun suatu jaringan komputer dengan baik dan aman akan keutuhan data karena semua data yang akan melintasi jaringan semua terenkripsi dan dilakukan dengan metode remote site ipsec vpn tunneling dan data sharing via ipsec vpn tunneling.

1. Bagi para peneliti yang akan mengembangkan konsep ini ke depanya, maka bagaimana perbandingan pengamanan jika memakai metode pengamanan data lain dengan menggunakan SSH dan Telnet.
2. Implementasikan di lapangan agar dapat melakukan perbandingan besar kecilnya paket data yang dikirim via jaringan konvensional dengan jaringan IPsec VPN.

DAFTAR PUSTAKA

WinkyF.,William B.W.,Alvin A.2010, *perancangan jaringan Dengan menggunkan IPSEC padaPT.GreatHeart Media Indonesia.*

Riscky.Vdan IndraP.2009*, telemor perencanaan vpn sebagai Komunikasi data pada Perusahaan ManufakturTelemor.*

Jonathan T., 2011, *pembatasan akses jaringan vpn dengan menggunakan iptables.*

Nanang S., 2009, *Mastering VPN Client Access di Windows Server 2008 Dan cara Konfigurasi IPSEC VPN.*

RizkiR., 2008, *Konsep Firewall Berbasis Paket Filtering dan metode perancangan IPSEC dengan menggunakan GNS3.*

Fauzi.P.,12 Agustus 2010, *Design and Management Network Computer* http://vtun.sourceforge.net/tun/.

Kalle V., 2008*, IPSEC VPN dengan konsep Remote Site IPSEC VPN Tunneling dan Data Sharing Via IPSEC VPN Tunneling.*

Dougless M. E., 1985 *IPSec VPN (singkatan dari IP Security).*