PENERAPAN METODE IPSEC UNTUK OPTIMALISASI KONEKSI JARINGAN di PT. OTO MULTIARTHA

Oleh:
Prionggo Hendradi, Braja Santosa
Fakultas Teknik, Teknik Informatika
Universitas Satya Negara Indonesia
Email: prionggo.hendradi@gmail.com

ABSTRAK

Penerapan Metode IPSec Untuk Optimalisasi Koneksi Jaringan di PT. OTO Multiartha. Dibawah bimbingan Prionggo Hendradi, S.Kom, MMSI dan Faizal Zuli, S.Kom., M.Kom, MTA. PT. OTO Multiartha adalah salah satu perusahaan yang bergerak dibidang pembiayaan keuangan (leasing). kemajuan perusahaan tersebut sangat pesat karena memiliki komitmen dan integritas yang tinggi, sehingga sampai sekarang sudah memiliki banyak cabang yang tersebar di seluruh Indonesia. Dengan banyaknya cabang yang tersebar tersebut, PT. OTO Multiartha memiliki kewajiban penuh untuk melayani cabang-cabang tesebut, baik dari segi pertukaran data, atau pun komunikasi lainnya. Oleh sebab itu PT. OTO Multiartha harus memiliki jaringan yang sangat baik, agar bias memenuhi kebutuhan cabang-cabang tersebut. Maka dengan itu dibutuhkan sebuah jaringan cadangan guna untuk membackup ketika jaringan utama mati, maka dibuatlah sebuah jaringan private pada jaringan internet public dengan menggunakan IPSec sebagai metodenya, karena metode IPSec tersebut sangat menjamin untuk melindungi komunikasi antar cabang dan head office PT. OTO Multiartha.

Kata Kunci : IPSEC, Optimalisasi Jaringan, Security Jaringan

ABSTRACT

Application of IPSec Method For Optimizing Conection Network at PT. OTO Multiartha. Under the guidance of Prionggo Hendradi, S.Kom, MMSI and Faizal Zuli, S.Kom., M.Kom, MTA. PT. OTO Multiartha is one company engaged in financial financing (leasing). The company's progress very rapidly because it has a high commitment and integrity, so that up to now have many branches spread all over Indonesia. With many branches, PT. OTO Multiartha have full obligation to serve the branches proficiency level, both in terms of data exchange, or any other communication. Therefore PT. OTO Multiartha must have a very good network, in order to meet the needs of bias those branches. So with that needed a backup network in order to backup when the main network down, then made a private network to the public Internet network using IPSec as a method, because the method is so warrant IPSec to protect communications between branches and head office of PT. OTO Multiartha.

Keywords: *IPSEC, Network Optimization, Network Security*

PENDAHULUAN

A. Latar Belakang

PT. OTO Multiartha adalah salah satu perusahaan yang bergerak dibidang pembiayaan keuangan (leasing) yang memiliki komitmen dan integritas tinggi, sehingga sampai saat ini perusahaan ini berkembangan dengan pesat serta memiliki cabang-cabang yang tersebar diseluruh indonesia.

Dengan banyaknya cabang tersebut, PT. OTO Multiartha memiliki kewajiban penuh untuk melayani cabang-cabang tesebut, baik dari segi pertukaran data, atau pun komunikasi lainnya. Oleh sebab itu PT. OTO Multiartha harus memiliki jaringan yang sangat baik, agar bisa memenuhi kebutuhan komunikasi cabang-cabang tersebut.

Pada dasarnya PT. OTO Multiartha sudah memiliki jaringan utama dengan menggunakan Multiprotocol Label Switching (MPLS), mengingat koneksi jaringan internet di Indonesia belum stabil maka diperlukan koneksi jaringan internet public untuk menjamin komunikasi jaringan tetap terkoneksi. Dengan demikian diperlukan jaringan cadangan untuk tetap membackup secara otomatis ketika jaringan utama mati.

Internet public adalah solusi yang tepat untuk mengatasi permasalahan tersebut, namun mengingat internet public banyak ancaman dari pihak luar yang tidak bertanggung jawab, sehingga dibutuhkan jaringan private untuk melindungi komunikasi dan kerahasian pertukaran data antar cabang dan head office.

Berdasarkan permasalahan diatas penulis mengambil kesimpulan untuk mengambil judul : "*Penerapan Metode IPSec Untuk Optimalisasi Koneksi Jaringan di PT. OTO Multiartha"*

B. Rumusan Masalah

Dalam penulisan skripsi ini, dapat dirumuskan masalah bagaimana penerapan metode IPSec untuk optimalisasi jaringan di PT. OTO Multiartha

C. Tujuan Penelitian

Dengan penerapan metode IPSec pada jaringan public yang digunakan oleh PT. OTO Multiartha dalam transaksi data dan informasi antara head office dan cabang, akan menjamin tingkat keamanan baik disisi pengirim maupun penerima informasi.

LANDASAN TEORI

A. Jaringan Komputer

Jaringan komputer merupakan penggabungan teknologi komputer dan komunikasi yang merupakan sekumpulan komputer berjumlah banyak yang terpisah-pisah akan tetapi saling berhubungan dalam melaksanakan tugasnya

B. Protokol Jaringan

Protokol adalah suatu kumpulan dari aturan-aturan yang berhubungan dengan komunikasi data antara alat-alat komunikasi supaya komunikasi data dapat

dilakukan dengan benar. Protokol biasanya berbentuk sebuah *software* yang mengatur komunikasi data tersebut.

C. Topologi Jaringan

1. Topologi Ring
   Pada topologi ring setiap komputer di hubungkan dengan komputer lain dan seterusnya sampai kembali lagi ke komputer pertama, dan membentuk lingkaran sehingga disebut ring, topologi ini berkomunikasi menggunakan data token untuk mengontrol hak akses komputer untuk menerima data,
2. Topologi Bus
   Topologi jaringan komputer bus tersusun rapi seperti antrian dan menggunakan cuma satu kabel coaxial dan setiap komputer terhubung ke kabel menggunakan konektor BNC, dan kedua ujung dari kabel coaxial harus diakhiri oleh terminator
3. Topologi Star
   Topologi ini membentuk seperti bintang karena semua komputer di hubungkan ke sebuah hub atau switch dengan kabel UTP, sehingga hub/switch lah pusat dari jaringan dan bertugas untuk mengontrol lalu lintas data.
4. Topologi Mesh
   Pada topologi ini setiap komputer akan terhubung dengan komputer lain dalam jaringannya menggunakan kabel tunggal, jadi proses pengiriman data akan langsung mencapai komputer tujuan tanpa melalui komputer lain ataupun switch atau hub.
5. Topologi Tree
   Topologi jaringan komputer Tree merupakan gabungan dari beberapa topologi star yang dihubungan dengan topologi bus, jadi setiap topologi star akan terhubung ke topologi star lainnya menggunakan topologi bus, biasanya dalam topologi ini terdapat beberapa tingkatan jaringan, dan jaringan yang berada pada tingkat yang lebih tinggi dapat mengontrol jaringan yang berada pada tingkat yang lebih rendah.

D. TCP/IP

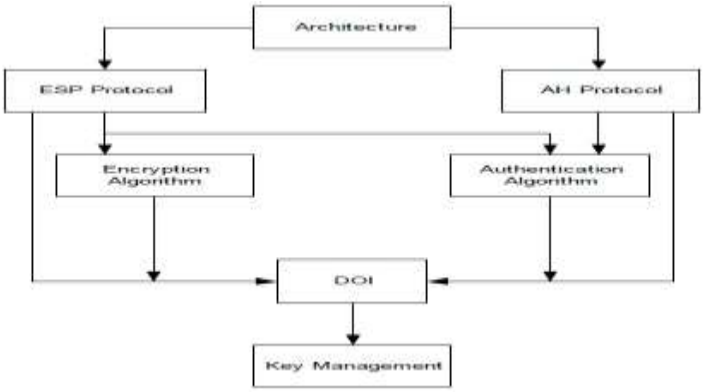
Protokol TCP/IP adalah standar komunikasi data yang digunakan oleh komunitas internet dalam proses tukar-menukar data dari satu komputer ke komputer lain di dalam jaringan Internet. Protokol ini tidaklah dapat berdiri sendiri, karena memang protokol ini berupa kumpulan protokol (protocol suite). Protokol ini juga merupakan protokol yang paling banyak digunakan saat ini. Data tersebut diimplementasikan dalam bentuk perangkat lunak (software) di sistem operasi. Istilah yang diberikan kepada perangkat lunak ini adalah TCP/IP stack.

Protokol TCP/IP dikembangkan pada akhir dekade 1970-an hingga awal 1980-an sebagai sebuah protokol standar untuk menghubungkan komputer-komputer dan jaringan untuk membentuk sebuah jaringan yang luas (WAN). TCP/IP merupakan sebuah standar jaringan terbuka yang bersifat independen terhadap mekanisme transport jaringan fisik yang digunakan, sehingga dapat digunakan di mana saja. Protokol ini menggunakan skema pengalamatan yang

sederhana yang disebut sebagai alamat IP (IP Address) yang mengizinkan hingga beberapa ratus juta komputer untuk dapat saling berhubungan satu sama lainnya di Internet. Protokol ini juga bersifat routable yang berarti protokol ini cocok untuk menghubungkan sistem-sistem berbeda (seperti Microsoft Windows dan keluarga UNIX) untuk membentuk jaringan yang heterogen.

E. IPSec (*Internet Protokol Security)*

IPSec adalah standart keamanan untuk penggunaan komunikasi berbasis internet protokol (IP) dengan cara enkripsi atau authentikasi semua paket IP yang lewat. (Aris Wendy: 2008). IPSec menyediakan keamanan pada level network layer, IPSec didesain sebagai cryptographic protokol yang berfungsi untuk keamanan data dan key exchange. Protokol IPSec diimplementasikan kedalam network layer, yaitu layer ketiga pada OSI layer yang mengerjakan layan network routing, flow control, segmentation (desegmentation) dan error control functions.



Gambar 2.1 Arsitektur IPSec

F. Cara Kerja IPSec

IPSec menggunakan dua protokol untuk menyediakan layanan keamanan lalulintas yaitu *Authentication Header* (AH) and *Encapsulating Security Payload* (ESP). Implementasi IPSec harus mendukung ESP dan juga AH. Protokol AH menyediakan integritas hubungan, authentifikasi data asal dan layanan anti jawaban.

a. Protokol Pada IPsec
   Berdasarkan fungsinya didalam IPSec terdapat dua protokol yang berjalan di belakang IPsec, yaitu:
   - Authentication Header (AH), menyediakan layanan authentication, integrity, replay protection pengamanan pada header IP, namun tidak menyediakan layanan confidentiality. Next Header berisi TCP, UDP, dan sebagainya. Berikut ini adalah gambar paket header dari AH.
   - Encapsulating Security Payload (ESP), menyediakan layanan Authentication, integrity, replays protection dan confidentiality terhadap data (ESP melakukan pengamanan data terhadap segala sesuatu dalam paket data setelah header). Berikut ini adalah gambar paket header dari ESP.

G. OSI Layer

Model referensi jaringan terbuka OSI atau OSI Reference Model for open networking adalah sebuah model arsitektural jaringan yang dikembangkan oleh badan International Organization for Standardization (ISO) di Eropa pada tahun 1977. OSI sendiri merupakan singkatan dari Open System Interconnection. Model ini disebut juga dengan model "Model tujuh lapis OSI" (OSI seven layer model). OSI Reference Model pun akhirnya dilihat sebagai sebuah model ideal dari koneksi logis yang harus terjadi agar komunikasi data dalam jaringan dapat berlangsung. Beberapa protokol yang digunakan dalam dunia nyata, semacam TCP/IP, DECnet dan IBM System Network Architecture (SNA) memetakan tumpukan protokol (protokol stack) mereka ke OSI Reference Model. OSI Reference Model pun digunakan sebagai titik awal untuk mempelajari bagaimana beberapa protokol jaringan di dalam sebuah kumpulan protokol dapat berfungsi dan berinteraksi (Iwan Sofana, 2012, CISCO CCNA & Jaringan Komputer). OSI Reference Model memiliki tujuh lapis, yakni sebagai berikut:

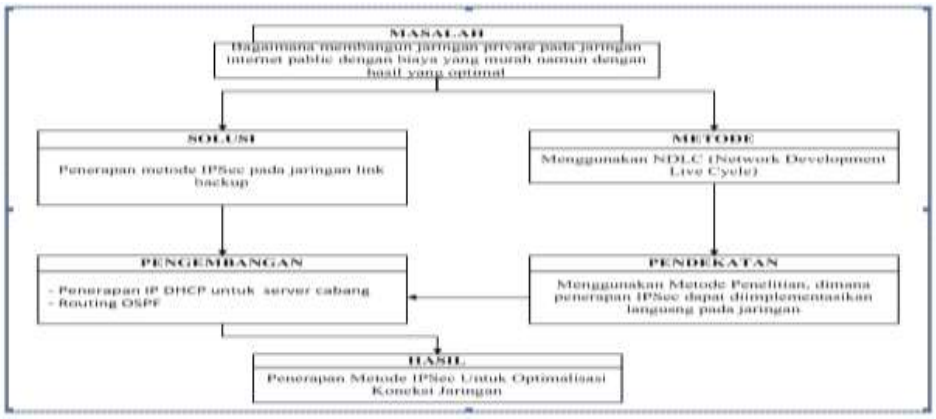
Gambar 2.13 Struktur Lapisan OSI Layer

H. *Security Association*

Bagian ini akan menjelaskan kebutuhan manajemen untuk implementasi Ipv4 yang mengimplementasikan AH, ESP atau keduanya. Konsep "*Security Association*" adalah pokok dari IPSec. Semua implementasi dari AH dan ESP harus mendukung konsep Security Association seperti yang dijelaskan dibawah

I. Kerangka Berpikir

Merupakan suatu gambaran secara jelas akan pembahasan yang akan dipecahkan hingga mendapatkan suatu solusi yang baik. Adapun kerangka berpikir sebagai berikut :



Gambar 2.15 Kerangka berpikir suatu permasalahan

METODOLOGI PENELITIAN

A. Tempat dan Waktu penelitian

Penelitian ini dilaksanakan dari bulan Maret sampai dengan Agustus 2015 yang bertempat di PT. OTO Multiartha Jl. Jend. Sudirman Kav 61-62 Jakarta 12190 Indonesia gedung Summit Mas II penelitian dilakukan di departemen IT Network dan Security yang berada dilantai 17.

B. Alat dan Bahan Penelitian

Berikut alat dan bahan-bahan yang digunakan oleh penulis untuk melakukan penelitian, diantaranya sebagai berikut :

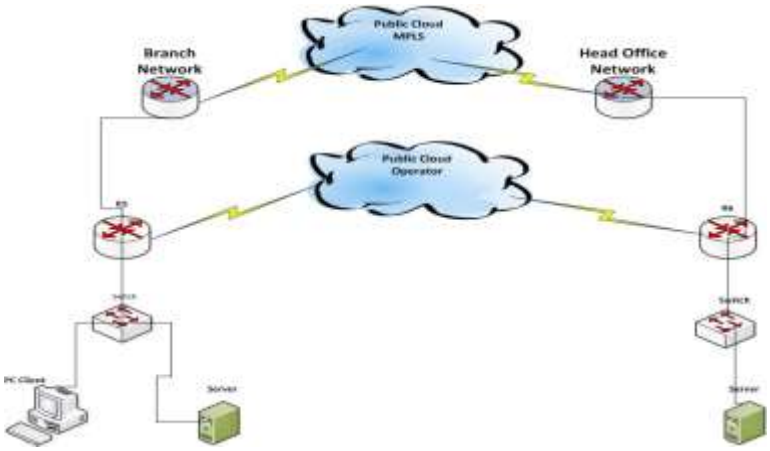
a. Perangkat Lunak
   System Oprasi Linux (linux-microcore), IOS Router C3640, Firewall, GNS 3 (Aplikasi simulasi jaringan).
b. Perangkat Keras
   Komputer server dengan spesifikasi Intel Core 2 Quad 2,4 GHz, Harddisk 500 GB, DVD RW, memori DDR3 4 GB, kartu jaringan dan monitor, Komputer client dengan spesifikasi Intel Core 2 Duo 2,4 GHz, Harddisk 250 GB, DVD RW, memori DDR3 2GB, dan monitor 14Inc, Firewall VPN, Kabel Ethernet CAT 5E, Router Cisco dan Switch

C. Metode Pengumpulan Data

Untuk mendapatkan informasi yang valid sebagai dasar penelitian, penulis melakukan riset terlebih dahulu di departemen IT Network dan Security, berikut adalah langkah-langkah yang dilakukan penulis dalam mengumpulkan data-data yang valid di PT. Oto Multiartha tersebut.

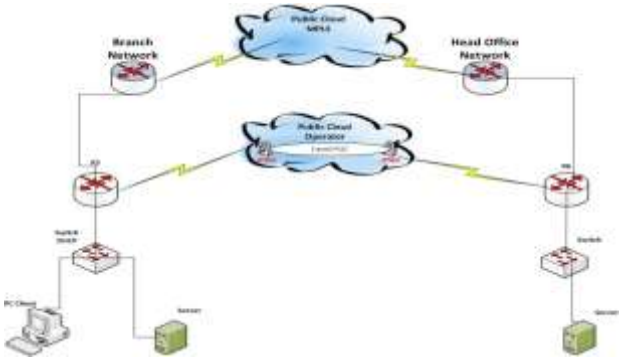
D. Analisa Jaringan yang Berjalan

Berdasarkan hasil dari studi lapangan dapat diketahui gambaran topologi jaringan yang digunakan saat ini, pada dasarnya PT. OTO Multiartha menggunakan topologi star, ini dapat dilihat dari semua server utama berada pada head office tersebut. Dan jaringan private berpusat pada head office.



Gambar 3.2 Topologi jaringan sebelum diimplementasikan IPSec

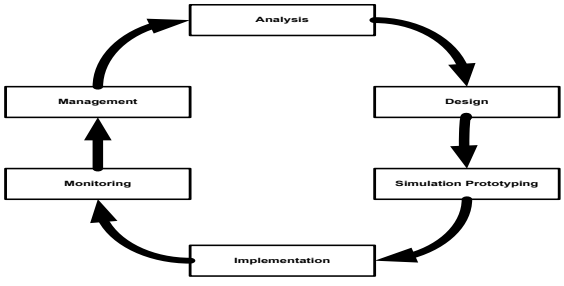
E. Jaringan yang diusulkan



Gambar 4.11 Topologi jaringan yang sudah diimplementasikan IPSec

F. Metode Pengembangan

Metode yang digunakan dalam pengembangan ini adalah metode Network Development Life Cycle (NDLC), dengan beberapa tahapan-tahapan yaitu: Analisis dan Design, Simulasi, Implemetasi, Manajemen dan Monitoring.(James E. Goldman,2005).



Gambar 3.3 *Network Development Life Cycle*

HASIL DAN PEMBAHASAN

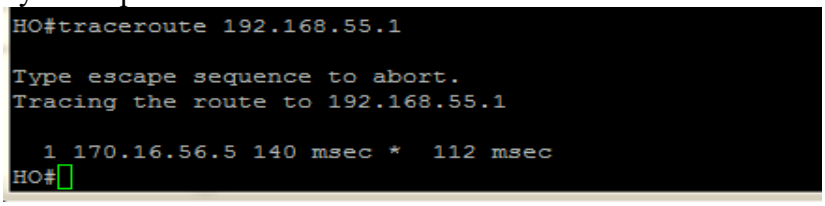
A. Hasil Pengujian

Dari hasil penelitian dan simulasi pada bab sebelumnya, maka dapat dihasilkan sebuah metode keamanan jaringan dengan memanfaatkan private

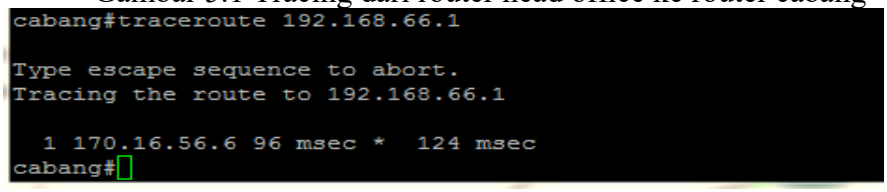
jaringan pada internet public dari router head office ke router cabang dan sebaliknya dengan menggunakan IPSec sebagai metode keamanannya.

1. Hasil Pengujian Tunneling

   Berikut adalah hasil pengujian tunneling dari router head office ke router cabang, dengan menggunakan printah Traceroute pada router tersebut, dengan melalui jaringan private via internet public yang sudah dikonfigurasi sebelumnya oleh penulis.



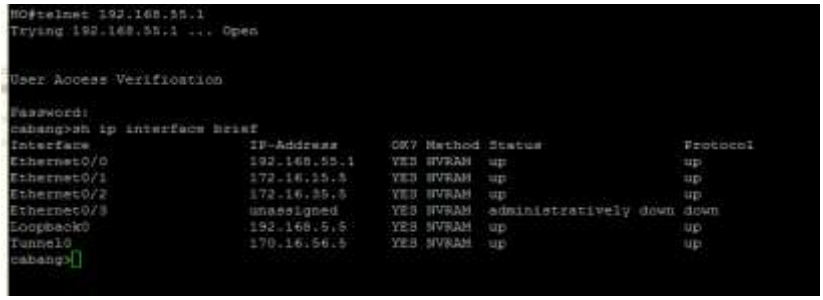
Gambar 5.1 Tracing dari router head office ke router cabang



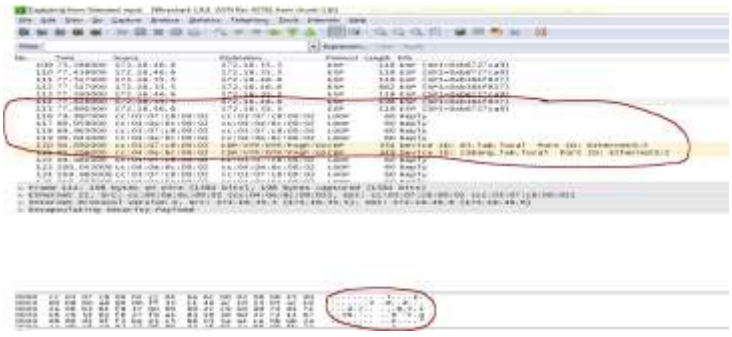
Gambar 5.2 Tracing dari router cabang ke router head office

2. Hasil Pengujian IPSec

   Berikut adalah bagian dimana penulis akan menjelaskan cara kerja IPSec pada jaringan PT. Oto Multiartha via jaringan private di internet public dengan menggunakan telnet dan Wireshark sebagai tool untuk capture setiap paket data yang lewat pada jaringan tersebut. Dan untuk percobaan transfer datanya menggunakan Telnet untuk melakukan komunikasi antar ke-dua router tersebut.



Gambar 5.3 Telnet dari router head office ke router cabang



Gambar 5.4 Hasil capture wireshark

Gambar 5.4 Berikut menjelaskan hasil dari capture Wireshark menggunakan telnet sebagai contoh paket data yang akan lewat jaringan tersebut, sebelumnya akan di enkripsi terlebih dahulu oleh dua protokol untuk Authentication Header pada paket yang membawa security identifier, data mengenai integrity control, dan informasi keamanan lainnya.

Sehingga setiap paket data yang lewat tidak akan bisa diketahui oleh pihak luar yang tidak bertanggung jawab, karena paket data tersebut sudah di enkrisi sebanyak 256 kali dengan menggunakan algoritma kriptografi sehingga paket data akan dijamin tingkat kerahasiannya,

B. Implementasi

Setelah melakukan proses analisa dan simulasi penulis akan melakukan implementasi pada jaringan yang sebenarnya, dengan tahapannya sama seperti proses simulasi, implementasi ini tidak akan mengganggu aktivitas office karena dilakukan pada interface router liannya.

1. Konfigurasi Router Head Office

   Pada bagian ini penulis akan melakukan konfigurasi router head office, karena jaringan sudah terhubung dengan baik, maka penulis hanya melakukan konfigurasi tunneling dan IPSec disetiap interface yang akan terkoneksi kerouter cabang, berikut langkah-langkah konfigurasinya :

```
HO#sh ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Ethernet0/0                192.168.66.1    YES NVRAM  up                    up
Ethernet0/1                172.16.26.6     YES NVRAM  up                    up
Ethernet0/2                172.16.46.6     YES NVRAM  up                    up
Ethernet0/3                unassigned      YES NVRAM  administratively down down
Loopback0                  192.168.6.6     YES NVRAM  up                    up
Tunnel0                    170.16.56.6     YES NVRAM  up                    up
HO#
```

Gambar 5.5 IP interface head office

```
HO#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     170.16.0.0/24 is subnetted, 1 subnets
C       170.16.56.0 is directly connected, Tunnel0
     172.16.0.0/24 is subnetted, 4 subnets
C       172.16.46.0 is directly connected, Ethernet0/2
S       172.16.99.0 [1/0] via 172.16.46.4
C       172.16.26.0 is directly connected, Ethernet0/1
O       172.16.12.0 [110/20] via 172.16.26.2, 00:33:08, Ethernet0/1
C    192.168.66.0/24 is directly connected, Ethernet0/0
C    192.168.6.0/24 is directly connected, Loopback0
S    192.168.0.0/16 [1/0] via 170.16.56.5
```

Gambar 5.6 IP Routing

```
HO#sh ip ospf interface brief
Interface    PID   Area            IP Address/Mask    Cost  State Nbrs F/C
Et0/2        1     0               172.16.46.6/24     10    DR    0/0
Et0/1        1     0               172.16.26.6/24     10    DR    1/1
Et0/0        1     0               192.168.66.1/24    10    DR    0/0
Lo0          1     6               192.168.6.6/24     1     LOOP  0/0
HO#
```

Gambar 5.7 IP OSPF

```
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 5
crypto isakmp key RAHASIA address 172.16.35.5
!
!
crypto ipsec transform-set MYTRANS esp-aes esp-sha-hmac
!
crypto ipsec profile MY_ENCAP
 set transform-set MYTRANS
```

Gambar 5.8 Konfigurasi IPSec

```
interface Tunnel0
 ip address 170.16.56.6 255.255.255.0
 tunnel source 172.16.46.6
 tunnel destination 172.16.35.5
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile MY_ENCAP
```

Gambar 5.10 Interface Tunneling

```
line vty 0 4
 password 12345
 login
```

Gambar 5.12 Konfigurasi login

2. Konfigurasi Router Cabang

   Karena router dicabang sudah terpasang dan terkoneksi sehingga memudahkan penulis untuk melakukan konfigurasi disetiap interface yang akan terkoneksi, konfigurasi dilakukan tidak jauh berbeda dengan konfigurasi yang dilakukan di router head office. Berikut konfigurasi disetiap masing-masing interfacenya :

```
cabang#sh ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Ethernet0/0                192.168.55.1    YES NVRAM  up                    up
Ethernet0/1                172.16.15.5     YES NVRAM  up                    up
Ethernet0/2                172.16.35.5     YES NVRAM  up                    up
Ethernet0/3                unassigned      YES NVRAM  administratively down down
Loopback0                  192.168.5.5     YES NVRAM  up                    up
Tunnel0                    170.16.56.5     YES NVRAM  up                    up
cabang#
```

Gambar 5.13 IP interface

```
cabang#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 170.16.56.6 to network 0.0.0.0

     170.16.0.0/24 is subnetted, 1 subnets
C       170.16.56.0 is directly connected, Tunnel0
     172.16.0.0/24 is subnetted, 3 subnets
S       172.16.46.0 [1/0] via 172.16.35.3
C       172.16.35.0 is directly connected, Ethernet0/2
C       172.16.15.0 is directly connected, Ethernet0/1
C    192.168.55.0/24 is directly connected, Ethernet0/0
     192.168.5.0/32 is subnetted, 1 subnets
C       192.168.5.5 is directly connected, Loopback0
S*   0.0.0.0/0 [1/0] via 170.16.56.6
cabang#
```

Gambar 5.14 IP Routing

```
cabang#sh ip OSPF interface brief
Interface    PID   Area            IP Address/Mask    Cost  State Nbrs F/C
Et0/1        1     0               172.16.15.5/24     10    DR    0/0
Et0/0        1     0               192.168.55.1/24    10    DR    0/0
Lo0          1     5               192.168.5.5/32     1     LOOP  0/0
cabang#
```

Gambar 5.15 IP OSPF

```
ip dhcp pool 1
   network 192.168.55.0 255.255.255.0
   default-router 192.168.55.1
!
```

Gambar 5.16 IP DHCP

```
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 5
crypto isakmp key RAHASIA address 172.16.46.6
!
!
crypto ipsec transform-set MYTRANS esp-aes esp-sha-hmac
!
crypto ipsec profile MY_ENCAP
 set transform-set MYTRANS
```

Gambar 5.17 Konfigurasi IPSec

```
interface Loopback0
 ip address 192.168.5.5 255.255.255.255
 ip ospf 1 area 5
```

Gambar 5.18 Interface Loopback

```
interface Tunnel0
 ip address 170.16.56.5 255.255.255.0
 tunnel source 172.16.35.5
 tunnel destination 172.16.46.6
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile MY_ENCAP
```

Gambar 5.19 Interface tunneling

```
router ospf 1
 router-id 5.5.5.5
 log-adjacency-changes
 network 172.16.15.5 0.0.0.0 area 0
```

Gambar 5.20 Route ospf area 1

```
line vty 0 4
 password Holiday1
 login
```

Gambar 5.21 Konfigurasi password

```
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 5
crypto isakmp key RAHASIA address 172.16.46.6
!
!
crypto ipsec transform-set MYTRANS esp-aes esp-sha-hmac
!
crypto ipsec profile MY_ENCAP
 set transform-set MYTRANS
```

Gambar 5.17 Konfigurasi IPSec

C. Monitoring

Pada tahap ini penulis melakukan monitoring pada jaringan internal dan jaringan external PT. OTO Multiartha, karena metode IPSec sangat tergantung pada jaringan internet public, untuk pengamatannya menggunakan tools sebagai berikut :

a. MRTG sebagai tool monitoring

b. Perangkat jaringan untuk melihat paket data yang berjalan
c. Tools lainnya yang digunakan untuk mengamati jaringan dan komunikasi secara umum secara terpusat atau tersebar

D. Manajemen

Pada proses ini semua hasil monitoring menjadi bahan acuan penulis untuk mendokumentasikan semua aktivitas jaringan yang sedang berjalan, selama kurung waktu beberapa minggu, guna untuk memastikan apakah metode yang diterapkan berjalan baik atau sebaliknya.

KESIMPULAN DAN SARAN

A. Kesimpulan

1. Penulis telah berhasil mengimplementasi IPSec pada jaringan PT. OTO Multiartha
2. Dengan menggunakan metode IPSec komunikasi jaringan private yang melewati jaringan internet public akan lebih aman dibandingkan hanya menggunakan davice firewall.
3. Jaringan yang digunakan saat ini di PT. OTO Multiartha sudah baik namun belum menjamin jaringan tersebut tetap terkoneksi, sehingga dibutuhkan jaringan private dengan menggunakan metode IPSec sebagai keamanan pada jaringan internet public

B. Saran

Penulis menyadari bahwa metode IPSec yang digunakan ini belum sempurna, mengingat keterbatasannya kemampuan yang dimiliki penulis, berikut beberapa saran yang diusulkan oleh penulis, diantaranya sebagai berikut :

1. Agar menggunakan operator internet yang memiliki konektivitas yang setabil dan bandwidth yang besar membuat kinerja IPSec lebih optimal
2. Dengan menggunakan device firewall disetiap getway interface perangkat jaringan membuat tingkat keamanan lebih terjamin.

DAFTAR PUSTAKA

Roger S. Pressman, 1997. Rekayasa Perangkat Lunak, 502-510, Penerbit : Andi, Yogyakarta.

Rafiudin, Rahmat, 2003. Panduan Membangun Jaringan Komputer Untuk Pemula. PT Elex Media Komputindo : Jakarta.

Sukmaaji Anjik, 2008. Jaringan Komputer : 46-50, Jakarta.

Sunyoto, Wendy, Aris, 2006. VPN Sebuah Konsep Teori dan Implementasi, "BukuWeb Networking", Surabaya.

Stallings William, 2003. Cryptography And Network Security, IV Edition : 640 673, Canada .

Sofana, Iwan, 2004. CISCO CCNA & Jaringan Komputer, 305-32, Bandung.

Winarno, Sugeng, 2006. Jaringan Komputer dengan TCP/IP, Informatika, Bandung.