RANCANGAN DAN IMPLEMENTASI JARINGAN VPN SIMULASI CISCO PAKET TRACER PADA PT.PUTRA PUTRIPERKASA

[1]Torando, [2]Irwansyah
[1]Teknik Komputer, Fakultas Vokasi, Universitas Bina Darma, irwansyah@binadarma.ac.id

Abstract – VPN (Virtual Private Network) in its implementation is divided into two types, namely remote access VPN and site-to-site VPN. VPN Remote access is a VPN that is used to safely remotely remote a private server or host over a public network. Meanwhile, site-to-site VPN is used to connect networks that are quite long distances through public networks so that they appear to be on one local network, for example between PT. Putra Putri Perkasa, KM.14 Branch, and Air Batu Branch. In this case, communication or data sharing occurs between PT. Putra Putri Perkasa, KM.14 Branch, and Air Batu Branch via site to site VPN (VirtualPrivate Network) technology, of course requires security to maintain the confidentiality of this data. The Internet Protocol Security (IPSec) security protocol is a security protocol capable of meeting security support criteria and having a better level of security which is most widely used to improve site to site VPN security at PT. Pertamina Ubeb Adera Pengabuan.

Keywords: **IPSec; VPN; Sharing; Host Private.**

***Abstrak* –** VPN (Virtual Private Network) dalam implementasinya terbagi dua jenis yaitu VPN remote access dan site-to-site VPN. VPN Remote access adalah VPN yang digunakan untuk meremote server atau host private dengan aman melalui jaringan publik. Sedangkan VPN site-to-site digunakan untuk menghubungkan jaringan yang memiliki jarak yang cukup jauh melalui jaringan publik sehingga seakan berada pada satu jaringan local, misal antara PT. Putra Putri Perkasa, Cabang KM.14, dan Cabang Air Batu. Dalam kasus ini terjadinya komunikasi atau sharing data antara PT. Putra Putri Perkasa, Cabang KM.14, dan Cabang Air Batu melalui teknologi VPN (VirtualPrivate Network) site to site, tentunya membutuhkan sebuah scurity(keamanan) untuk menjaga kerahasian data-data tersebut. Protokol keamanan Internet Protocol Security (IPSec) merupakan protokol keamanan mampu memenuhi kriteria dukungan keamanan dan mememiliki tingkat keamanan yang lebih baik yang paling banyak digunakan untuk meningkatkan keamanan VPN site to site yang ada di PT. Pertamina Ubeb Adera Pengabuan.

Kata Kunci : *Honeypot* , *Cowrie*, Keamanan Jaringan

1. Pendahuluan

Dengan semakin pesatnya perkembangan teknologi, bukan berarti mengurangi permasalahan yang terjadi pada jaringan komputer. Serperti yang terjadi di PT. Putra Putri Perkasa, sering terjadi permasahan jaringan komputer, di tambah dengan jarak yang jauh antara kantor pusat dan mitra kerja. Sehingga menyebabkan kendala ketika ada permasalahan jaringan yang terjadi sehingga tidak dapat di atasi dengan cepat. Masalah seperti ini dapet terjadi bagi perusahaan yang memiliki mitra kerja yang letaknya berjauhan dengan kantor pusat. Untuk itu pihak peruhasaan sangat mengharapkan ada sistem jaringan komputer yang aman agar dapat digunakan untuk mengontrol setiap pengiriman data-data penting ke semua mitra kerja. Dan mengatasi permasalahan jaringan yang ada di setiap perusahaan mitra kerja secara cepat

Sistem jaringan komputer yang aman dan dapat mengatasi hal ini adalah *Vitual Private Network* (VPN), yang dapat membuat dua jaringan yang lokasinya berjauhan untuk saling terkoneksi. Seakan-akan kedua jaringan tersebut di dalam suatu jaringan internet yang privasi Teknologi VPN (*Virtual Private Network*), suatu komunikasi dalam jaringan sendiri yang terpisah dari jaringan umum. Untuk mengirim data antara kantor pusat dan kantor mitra sehingga data yang di kirim dapat terjaga kemanan dan kerahasiaanya dari acaman orang yang tidak bertanggung jawab.

Oleh karna itu perlu dibangunya sebuah keamanan jaringan yang berbasisVPN (*Virtual Private Network*) di PT. Putra Putri Perkasa, sehingga dapat memudahkan para karyawan untuk menyelesaikan pekerjaanya tanpa harus menghawatirkan data yang dikirim ke mitra perusahaan dan hasil pekerjaan sesuai yang di harapkan. Untuk menjawab permasalahan di atas,maka penulis dalam tugas akhir ini akan menganalisa dan implementasi keamanan jaringan VPN pada PT. Putra Putri Perkasa [1].

2. Tinjauan Pustaka

2.1 *VPN (Virtual Private Network)*

VPN adalah suatu mekanisme menyambungkan sebuah titik (atau biasa dengan node) pada sebuah jaringan computer dengan titik yang lain melalui mediasi sebuah jaringan yang lain, sebuah titik dapat berupa sebuah jaringan komputer lokal (atau biasa disebut LAN) atau sebuah komputer. VPN adalah sebuah cara aman untuk mengakses local area network yang berada pada jangkauan dengan menggunakan internet atau jaringan umum lainnya untuk melakukan transmisi data paket secara pribadi dengan enkripsi perlu penerapan teknologi tertentu agar walaupun menggunakan medium yang umum, tetapi traffic (lalu lintas) antara remote-site tidak dapat disadap dengan mudah, juga tidak memungkinkan pihak lain untuk menyusupkan traffic yang tidaksemestinyakedalam remote-site[2].

1. VPN PPTP

singkatan dari *point-to-point tunneling protocol*(Protokol kanalisasi titik ke titik). Seperti nama yang disandang. VPN PPTP menciptakan kanal dan menangkap data. Nama yang cukup panjang untuk VPN yang paling umum digunakan. VPN PPTP digunakan oleh para pengguna jarak jauh untuk menyambungkan mereka dengan jaringan VPN menggunakan koneksi internet yang sudah ada.

2. VPN SITUS KE SITUS

juga disebut VPN dari *router-ke-router* dan paling banyak digunakan dalam oprasional berbasis perusahaan. Padanya keyantaanya bahwa perusahaan memiliki

kantor-kantor yang berlokasi baik nasional juga internasional, VPN situs ke situs dipakai untuk menyambungkan jaringan dari lokasi kantor utama ke banyak kantor.

3. VPN L2TP

singkatan dari *layer to tunneling protocol*(Protokol lapisan ke kanalisasi) yang dikembangkan oleh microsoft dan cisco. VPN L2PT merupakan VPN yang secara khusus digabungkan dengan protokol keamanan VPN lainnya guna membentuk koneksi VPN yang lebih aman.

2.2 Fungsi *VPN*

Fungsi *VPN* dibagi menjadi 3 jenis kategori [3]:

a. *Confidentiality (Kerahasian Data)*

Tenologi VPN memiliki sistem kerja mengenkripsi semua data yang lewat melaluinya. Dengan adanya teknologi ini maka kerahasian akan menjadi lebih terjaga. Biarpun ada pihak yang dapat menyadap data yang lalu-lalang, namun belum tentu mereka bisa membacanya dengan mudah kerna memang sudah di acak. Dengan menerapkan sistem ini, tidak ada satu pun oarang yang dapat mengakses dan membaca isi jaringan data dengan mudah.

b. Data *Integirty* (Keutuhan Data)

Data *Integrity* di tengah perjalanan data apapun bisa terjadi terhadap datanya baik itu hilang, rusak,bahkan di manipulasi isinya oleh orang-orang yang tidak bertanggung jawab.VPN memiliki teknoligi yang dapat menjaga keutuhan data yang akan di kirim agar sampai ke tujuannya tanpa cacat,hilang,rusak,atau pun dimanipulasi orang lain.

c. *Origin Authentication* (Authentik Sumber)

Teknologi VPN memiliki kemampuan untuk melakukan autentikasi terhadap sumber-sumber pengirim data yang akan diterima. VPN akan melakukan pemekrisaan terhadap semua data yang masuk dan mengambil informasi datanya. Kemudian alamat data akan disetujui jika proses autentikasinya berhasil. Dengan demikian, VPN menjamin semua data yang dikirim dan diterima oleh sumber yang semestinya. Tidak ada data yang di palsukan atau dikirimkan oleh pihak-pihak lain.

2.3 LAN Card

merupakan sebuah alat yang sangat penting dalam membangun sebuah jaringan, baik dalam skala kecil maupun besar. Alat ini dapat berupa kartu (card) atau melekat pada motherboard.Alat ini berfungsi untuk menghubungkan kabel dari hub ke komputer dan masing-masing komputer agar dapat saling berhubunganharus ada yang namanya LAN Card [1].

2.4 *Hub*

Suatu jenis perangkat jaringan komputer khusus yang disebut hub dapat ditemukan di banyak rumah dan jaringan bisnis kecil Hub adalah kotak persegipanjang kecil, biasanya terbuat dari plastik, yang menerima daya dari stop kontak pada dinding biasa. Hub menggabungkan beberapa komputer (atau perangkat jaringan lainnya) secara bersama-sama untuk membentuk network segment tunggal Pada segmen jaringan, semua komputer dapat berkomunikasi secara langsung dengan setiap hub.Hub mencakup serangkaian port yang masing-masing menerima kabel. jaringan, Hub jaringan kecil adalah empat komputer. Ada yang berisi 4atau 5 port, yaitu kelima port yang disediakan untuk "uplink" koneksi ke hub atau perangkat lain yang serupa. Hub yang lebih besar berisi 8, 12,16, bahkan 24 portHub digolongkan sebagai perangkat layer 1 pada model OSI. Pada lapisan fisik, hub dapat mendukung jaringan canggih, Hub ndak membaca data yang lewat melalui mereka dan tidak peduli sumber atau Tujuan Pada dasarnya, sebuah hub hanya menerima incomingpockets. atau mungkin menguatkan sinyal listrik, dan menyebarkan paket ini ke semua komputer dan perangkat pada jaringan,Secara teknis, hub terdiri dari tiga jenis, Passive ,Active, dan Intelligent [4].

2.5 Aspek-aspek Keamnanan Komputer

Inti dari keamanan komputer adalah melindungi komputer dan jaringannya dengan tujuan mengamankan informasi yang berada di dalamnya. Keamanan komputer sendiri meliputi beberapa aspek , antara lain[5] :

1. Authentication, penerima informasi dapat memastikan keaslian pesan, bahwa pesan itu datang dari orang yang dimintai informasi. Dengan kata lain informasi itu benar-beanr datang dari orang yang dikehendaki.
2. Integrity, keaslian pesan yang dikirim melalui jaringan dan dapat dipastikan bahwa informasi yang dikirim tidak dimodifikasi orang yang tidak berhak.
3. Non-repudiation, merupakan hal yang berhubungan dengan si pengirim. Pengirim tidak dapat mengelak bahwa dialah yang mengitim informasi tersebut
4. Authority, informasu yang berbeda pada sistem jaringan tidak dapar dimodifikasi oleh pihak yang tidak berhak untuk mengaksesnya.
5. Confidentiality, merupakan usaha untuk menjaga informasi dari orang yang tidak berhak mengaksesnya. Kerahasiaan ini biasanya berhubungan dengan informasi yang diberikan kepihak lain.
6. Privacy, lebih ke arah data data yang bersifat pribadi.

7. Availability, aspek availabilitas berhubungan dengan ketersediaan informasi ketika dibutuhkan. Sistem informasi yang diserang atau dijebol dapat menghambat atau maniadakan akses ke informasi.
8. Access control, aspek ini berhubungan dengan cara pengaturan akses ke informasi. Hal ini biasanya berhubungan dengan masalah otentikasi dan privasi. Kontrol akses seringkali dilakukan dengan menggunaka kombinasi user id dan password ataupun dengan mekanisme lain.

3. Metodologi Penelitian

3.1 Metode Penelitian

Dalam penelitian ini menggunakan metode eksperimental, adapun tahapan penelitian yang dilakukan dalam penyelesaian Tugas Akhir ini adalah dengan

1. Studi literatur dan pustaka dilakukan dengan mencari sumber-sumber pendukung. sumber yang dimaksud dapat berupa jurnal tugas akhir, buku, e-book yang membahas tentang *VPN.*
2. Menganalisis kebutuhan *VPN* yang diperlukan dalam penerapan jaringan *cisco paket tracer*.
3. Perancangan
4. Perancangan *VPN* menggunakan sistem simulasi Cisco Paket Tracer.
5. Kemudian implementasi dengan pengujian melakukan *ping terhadap cabang cabang perusahaan*.

4.1 Hasil

4.1.1 Konfigurasi Router *PT.Putra Putri Perkasa.*

Setting *ip addres* untuk masing-masing *router*

```
R1>enable
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#hostname Putra.Putri.Perkasa
Putra.Putri.Perkasa(config)#
```

Gambar 4.1 Konfigurasi Hostname

Kode Konfigurasi 1 merupakan perintah untuk mengaktifkan router, memasuki terminal router dan mengganti nama router, router pertama diberi dengan nama R1

```
Putra.Putri.Perkasa(config)#interface Serial0/0/0
Putra.Putri.Perkasa(config-if)#ip address 209.165.100.1 255.255.255.0
Putra.Putri.Perkasa(config-if)#
Putra.Putri.Perkasa(config-if)#exit
Putra.Putri.Perkasa(config)#interface GigabitEthernet0/1
Putra.Putri.Perkasa(config-if)#ip address 192.168.1.1 255.255.255.0
Putra.Putri.Perkasa(config-if)#ex
Putra.Putri.Perkasa(config)#access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
Putra.Putri.Perkasa(config)#access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
Putra.Putri.Perkasa(config)#
```

Gambar 4.2 Konfigurasi IP Address

Kode program 2 merupakan perintah untuk menambahkan ip address 192.168.1.1 ke router di interface Gig0/1 dan ip public 209.165.100.1 di interface Se0/0/0 perintah no shutdown berfungsi untuk mengaktifkan interface Gig0/1 dan Se0/0/0 di router, dan konfigurasi access-list permit.

```
Putra.Putri.Perkasa(config)#crypto isakmp policy 10
Putra.Putri.Perkasa(config-isakmp)# encryption aes 256
Putra.Putri.Perkasa(config-isakmp)# authentication pre-share
Putra.Putri.Perkasa(config-isakmp)# group 5
Putra.Putri.Perkasa(config-isakmp)#
```

Gambar 4.3 Konfigurasi Isakm Policy

Kode konfigurasi 3 merupakan perintah untuk mengaktifkan protocol isakmp, isakmp adalah protocol yang di gunakan untuk membentuk asosiasi keamanan dan kunci kriptografi, perintah cypto isakmp 10 berfungsi untuk konfigurasi dengan vpn dimana policy 10 adalah prioritasnya dan untuk perintah authentication berfungsi untuk menggunakan pre-share key, dimana kedua kunci harus sama antara R1 ke R2.

```
Putra.Putri.Perkasa#ena
Putra.Putri.Perkasa#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Putra.Putri.Perkasa(config)#crypto isakmp key secretkey address 209.165.200.1
```

Gambar 4.5 konfiguraso Isakmp Secretkey

Kode konfigurasi 4 merupakan perintah untuk koneksi, perintah isakmp key secret-key untuk memberikan kunci untuk koneksi router pertama menuju ke router kedua yang menggunakan ip publik

209.165.200.1. Perintah memberi access-list agar jaringan router pertama (R1) dan router (R2) bisa saling terkoneksi. Crypto ipsec berfungsi untuk setting ipsec dengan nama myset dan protocol yang digunakan adalah esp-sha-hmac.

```
Putra.Putri.Perkasa(config)#crypto isakmp key secretkey address 209.165.200.1
A pre-shared key for address mask 209.165.200.1 255.255.255.255 already exists!
Putra.Putri.Perkasa(config)#crypto ipsec transform-set R1-R3 esp-aes 256 esp-sha-hmac
Putra.Putri.Perkasa(config)#crypto ipsec transform-set Putra.Putri.Perkasa-Cab.KM14 esp-aes 256 esp-sha-hmac
Putra.Putri.Perkasa(config)#crypto ipsec transform-set Putra.Putri.Perkasa-Cab.Airbatu esp-aes 256 esp-sha-hmac
Putra.Putri.Perkasa(config)#crypto map IPSEC-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Putra.Putri.Perkasa(config-crypto-map)# set peer 209.165.200.1
Putra.Putri.Perkasa(config-crypto-map)# set pfs group5
Putra.Putri.Perkasa(config-crypto-map)# set security-association lifetime seconds 86400
Putra.Putri.Perkasa(config-crypto-map)# set transform-set Putra.Putri.Perkasa-Cab.KM14
Putra.Putri.Perkasa(config-crypto-map)# set transform-set Putra.Putri.Perkasa-Cab.Airbatu
Putra.Putri.Perkasa(config-crypto-map)# match address 100
Putra.Putri.Perkasa(config-crypto-map)#
```


Gambar 4.6 Konfigurasi IPSEC-MAP

Kode konfugurasi 5 merupakan perintah untuk setting crypto mapnya dengan nama mymap dengan no urut 10, dan perintah set peer berfungsi untuk set koneksi 209.165.200.1. dan perintah set transform-set R1-R2 untuk setting address router pertama dan kedua.

```
Putra.Putri.Perkasa(config-crypto-map)#int se0/0/0
Putra.Putri.Perkasa(config-if)#crypto map IPSEC-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Putra.Putri.Perkasa(config-if)#
```

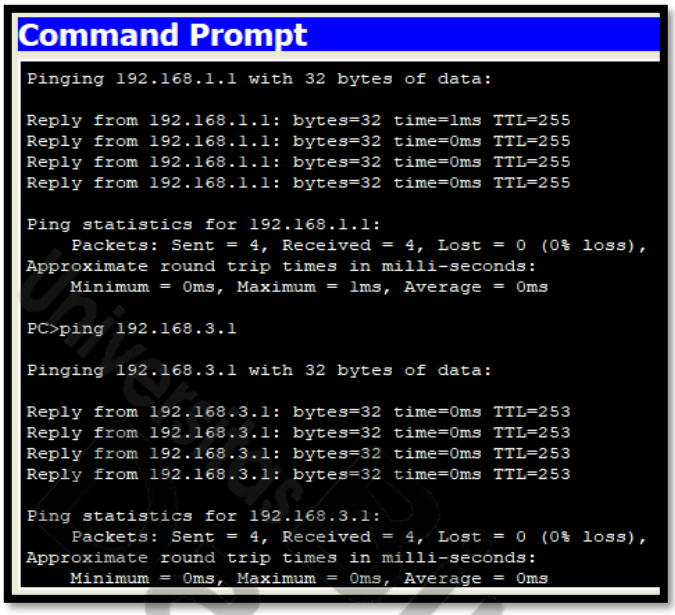
Gambar 4.7 Konfigurasi IPSEC-MAP

Kode konfigurasi 6 merupakan perintah untuk memberikan crypto mao di slot interface se0/0/0.

4.2 PEMBAHASAN

4.2.1 Paket Loss Tes

Pengujian packet loss dilakukan beberapa kali tes dengan perintah ‘ping’ ke IP tujuan menggunakan command prompt untuk melihat stabilitas koneksi di jaringan tanpa menggunakan.VPN. Dan didapatkan hasil



Gambar 4.21 Ping Paket Loss

Pada gambar hasil dari konektifitas komputer yang sudah terhubung atau berhasil dari masing-masing komputer yang menuju router R1 dan R2 dengan menggunakan fasilitas ping, ip address 192.168.1.1.

4.2.3 Penguji Pengiriman VPN

Pengiriman paket.

Gambar 4.7 Pengiriman Paket

Pada gambar 4.20 router pertama (R1) menerima hasil dari dua komputer yang saling mengirim paket satu sama lain dengan menggunakan fasilitas ping dirouter, pengirimannya belum melewati tunnel atau belum menggunakan VPN.

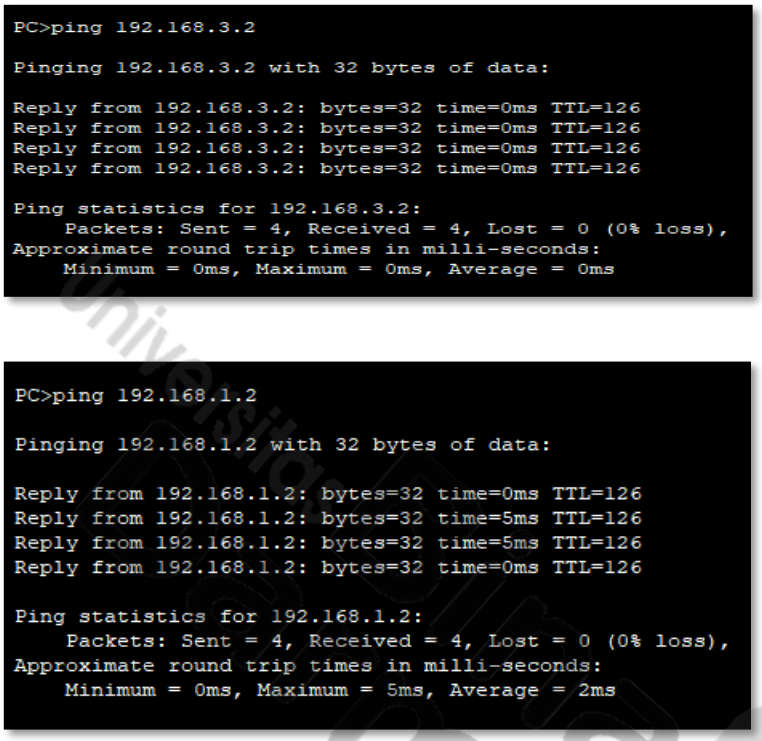
```
R2#show crypto ipsec sa

interface: GigabitEthernet0/0
    Crypto map tag: IPSEC-MAP, local addr 209.165.200.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   current_peer 209.165.100.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
   #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

     local crypto endpt.: 209.165.200.1, remote crypto
endpt.:209.165.100.1
     path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
     current outbound spi: 0x0(0)

     inbound esp sas:

 --More--
```

Gambar 4.8 Pengiriman Paket

Pada gambar 4.21 router kedua (R2) menerima hasil dari dua komputer yang saling mengirim paket satu sama lain dangan menggunakan fasilitas ping, pengirimannya belum melewati tunnel atau belum menggunakan VPN.

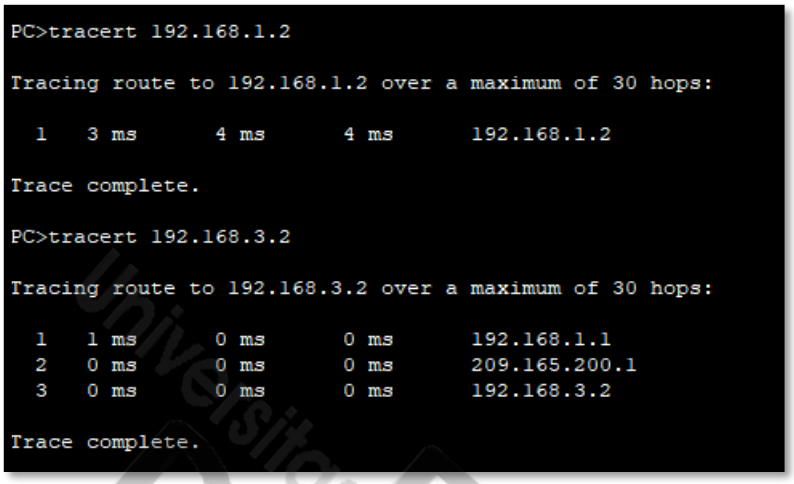
4.2.4 Pengujian Jaringan Akhir

Pengujian packet loss dilakukan beberapa kali tes dengan perintah ‘ping’ ke *IP* tujuan menggunakan *command prompt* untuk melihat stabilitas koneksi di jaringan menggunakan L2TP/IPSec VPN. Dan didapatkan hasil sebagai berikut.



Gambar 4.10 Packet Loss Jaringan VPN

Dari data diatas dapat kita lihat untuk data max dan *average round trip* suatu paket masih dalam nilai yang wajar. Dari percobaan 4 kiriman paket, max round trip = 1ms dan average round trip = 1ms untuk computer server, dan untuk computer client max round trip = 1ms dan average round trip = 1ms. Penulis juga melakukan *trace route* untuk melihat apakah paket yang dikirm sudah melewati (tunnel) jaringan L2TP/IPSEC yang dibuat. Dan seperti gambar, hasilnya adalah paket dikirim melalui komputer server IP 192.168.1.2 dan diteruskan ke IP VPN komputer *client* 192.168.3.2



Gambar 4.11 Trace Route VPN

5. Keismpulan

Konsep VPN terbagi atas dua macam koneksi yaitu *site-to-site* VPN dan remote access VPN. Dengan menggunakan L2TP/IPSec maka data yang dikirim ataupun diterima dalam kondisi aman dan sudah dienkripsi dengan baik dan akan dikirim melalui *tunnel.* Sehingga pihak-pihak yang tidak berhak mengakses tidak bisa melihat dan mengakses data tersebut. Karena L2TP/IPSec memberikan layanan keamanan yang sangat baik diantaranya layanannya yaitu data *integrity , confidentiality, authentication*, dan *anti replay*

.

Referensi

[1] Fariz Alwafi (2015). Analisa dan Implementasi Keamanan Jaringan
Pada PT. DAE MYUNG HIGHNES INDONESIA.

[2] Rasuanda, Moezes (2019) Perbandingan Performa VPN menggunakan
PPTP dan SSPT Over SSL Dengan Motode Quality of Service,Undergrate
Thesis, Universitas Internasioanal Batam.

[3] Hari, Ratmoko (2014) Analisis Implementasi Keamanan Jaringan
Virtual Private Network (VPN) Pada PT.Layar Sentosa Shipping
Corp. Skipsi ,Fakultas Ilmu komputer.

[4] Fatoni, Dedi Irawan (2015). Implementasi Jaringan VPN
(VIRTUAL PRIVATE NETWORK) Site to Site Mikrotik Route.
Jalan Jendral Ahmad Yani No.03 Palembang.

[5] Kuncoro Satrio (2015). Implementasi Autentikasi pada Virtual Private Network
(VPN) Menggunakan Kerberos. Salatiga.

[6] Anik Megawati (2018). Membangun jaringan VPN sederhana dengan AAA server
"packet tracer".Lamongan.

[7] Zaky Maulana Luthfansa,Ulla Delfana Rosiani (2021).
Pemanfaatan Wireshark Sniffing Komunukasi Data Berprotokol
HTTP pada jringan internet. Politiknik Negeri Malang.

[9] Donny Mahendra,Ema Utami,Abas Ali Pangeran. Perancangan dan Pegembangan
Keamanan Jaringan Enterprise dengan VPN. Jl. Ring road
Utara Condong Catur Depok Sleman Yogyakarta.

[10] Rivaldi Rachman (2021). Analisa Keamanan Jaringan Wiraless LAN (WLAN)
dengan metode penetration testing pada PT. PLN (PERSERO) sektor pengendalian pembangkit Pekanbaru. Universitas Islam Riau Pekanbaru .

[11] Sonny Rumalatur (2014). Analisa keamanan Jaringan Wireless (WLAN)

pada PT.PLN (Persero) Wilayah P2B Area Sorong. Depok 16424.

[12] Riana Febrianti,Sidik,Susafa,Ati,Esron, Rikardo Nainggolan,Ummu,Radiyah(2021).

Implementasi VPN Berbasis Point To Point Tunneling

Protocol (PPTP) Menggunakan Mikrotik Router Board.

Sekolah tinggi Manajemen Informatika dan Komputer Nusa Mandiri.

ISSN: 2654-5438