Cyberspace: Jurnal Pendidikan Teknologi Informasi
Volume 5, Nomor 1, Maret 2021, 16-21

Implementation Of Generic Routing Encapsulation Using CISCO Packet Tracer

Muhammad Kahfi Aulia, Djuniadi

Ilmu Komputer, Fakultas Matematika dan Ilmu Pengetahuan Alam,
Universitas Negeri Semarang
E-mail: kahfiaulia39@students.unnes.ac.id, djunaidi@mail.unnes.ac.id

Abstract

Virtual Private Network (VPN) is a technology that offers low-cost remote access solutions for companies. The IPSec protocol provides cryptography services and network security for data transmission. Generic Routing Encapsulation (GRE) tunnel exists to encapsulate multicast and broadcast packets into unicast packets. This is very usable which IPSec does not support encryption of multicast and broadcast packets. The target of this simulation is that Router 1 shows that the network is protected by GRE. The first thing to do is set the network topology. Here, for example, there are two offices that want to transmit data to each other. Each of these offices has a switch, FTP server, DNS server, router, and PC. Then set the IP address of each device and connect it with cables. Router 2 and Router 3 function to connect the two offices in one WAN network. Each of these data transmissions is IPSec protected for data encryption protection then GRE coated for transmission encapsulation. From simulation results, we can conclude that both network can be connected and communicated each other with protection from GRE tunnel.

Keywords: *GRE, CISCO Packtet Tracer, Network Security*

Abstrak

Virtual Private Network (VPN) merupakan teknologi yang menawarkan solusi remote access murah untuk perusahaan. Protokol IPSec menyediakan jasa kriptografi dan keamanan jaringan untuk transmisi data. Generic Routing Encapsulation (GRE) ada untuk mengenkapsulasi paket multicast dan broadcast menjadi unicast. Ini sangat dapat digunakan karena IPSec tidak mendukung pengenkripsian paket multicast dan broadcast. Target dari simulasi ini adalah dua jaringan dapat terhubung dalam dengan keamanan tunnel GRE dan dapat berkomunikasi satu sama lain, Router 1 menunjukkan bahwa jaringan telah dilindungi oleh GRE. Pertama-tama yang harus dilakukan adalah mengatur topologi jaringannya. Disini umpamanya ada dua kantor yang ingin saling mentransmisikan data. Masing-masing kantor ini memiliki switch, server FTP, server DNS, router, dan PC. Kemudian mengatur alamat IP dari masing-masing perangkat dan dihubungkan dengan kabel-kabel. Router 2 dan Router 3 berfungsi menghubungkan kedua kantor dalam satu jaringan WAN. Masing-masing transmisi data ini dilindungi oleh IPSec untuk perlindungan enkripsi data kemudian dilapisi GRE untuk enkapsulasi transmisi. Dari hasil simulasi dapat kita simpulkan bahwa kedua jaringan tersebut bisa terhubung dan bisa saling berkomunikasi dengan lindungan tunnel GRE.

Kata Kunci: *GRE, CISCO Packet Tracer, Keamanan Jaringan*

1. Pendahuluan

Dilatarbelakangi oleh perkembangan teknologi informasi yang makin modern dan maju di zaman sekarang ini, teknologi informasi banyak digunakan oleh perusahaan untuk mengembangkan ranah bisnisnya ke jenjang internasional. Kemajuan teknologi informasi untuk kepentingan perusahaan, di sisi lain terdapat kemajuan penyerangan jaringan yang semakin modern pula. Oleh karena itu dibutuhkan metode keamanan jaringan untuk melindungi perusahaan atau organisasi dari berbagai jenis serangan.

Jaringan komputer adalah suatu sistem yang terdiri atas berbagai piranti keras serta piranti lunak yang saling terhubung satu sama lain. Manfaat dari adanya jaringan komputer ini adalah, piranti-piranti itu dapat saling komunikasi dan dapat saling berbagi informasi satu sama lain [1].

VPN (Virtual Private Network) adalah teknologi yang memanfaatkan suatu jaringan, terutama jaringan publik seperti internet, untuk membangun jaringan pribadi khusus, dan itu adalah "line in the line". Data disebarkan melalui "terowongan terenkripsi" yang aman di jaringan publik. Membangun jalur komunikasi khusus antara dua atau lebih perusahaan Intranet terletak di bagian yang berbeda untuk menghubungkan Internet, sama seperti membuat jalur khusus. Tetapi tidak perlu membuat garis fisik nyata seperti kabel optik. Perusahaan hanya perlu menyewa jalur data khusus lokal dan menghubungkannya ke Internet, sehingga lembaga dapat mengirimkan informasi satu sama lain [2].

Namun, meningkatkan tingkat keamanan dalam jaringan publik dapat mempengaruhi kegunaan sistem dan meningkatkan kompleksitas dalam hal routing jaringan informasi. Terutama karena header dan fitur tambahan yang ditambahkan pada paket yang ditransmisikan. Selain itu kompleksitas pengguna dan organisasi yang menggunakan jaringan publik juga ikut terpengaruhi. Misalnya jika suatu perusahaan meminta semua karyawannya untuk menginstal aplikasi VPN dan mengotentikasi akses secara terus menerus akan sangat merepotkan dan dapat memengaruhi produktivitas. Dengan demikian, penerapan mekanisme keamanan harus memperhatikan kegunaan sistem. Eksploitasi protokol keamanan, metode tunneling, dan teknik enkapsulasi diatur untuk memfasilitasi interoperabilitas antar jaringan sambil mengoptimalkan kegunaan layanan jaringan [3].

Teknologi terowongan (tunneling) adalah suatu teknologi diciptakan untuk menyediakan koneksi dari sumber ke tujuannya, koneksi ini juga disebut dengan koneksi point-to-point (titik ke titik). Koneksi point-to-point tersebut terbentuk dengan melintasi jaringan public yaitu internet, tetapi koneksi tersebut tidak melihat paket-paket data milik orang lain yang juga menggunakan jaringan publik tersebut. Koneksi ini juga hanya melakukan transportasi data dari pemilik data [4]. Ada banyak protokol tunneling yang sudah digunakan, beberapanya yaitu Layer 2 Tunneling Protocol (L2TP), Point-To-Point Tunnelling Protocol (PPTP),), IP-in-IP (IPIP), Ethernet over IP (EoIPIPSec (Internet Protocol Security) [5].

Generic Routing Encapsulation adalah standar enkapsulasi 3 lapis internasional dalam RFC 2784 oleh Internet Engineering Task Force. Sejumlah proposal berbeda seperti RFC 1234, RFC 1226 saat ini ada untuk enkapsulasi satu protokol di atas protokol lain. Jenis enkapsulasi lain seperti RFC 1241, SDRP, RFC 1479 telah diusulkan untuk mengangkut IP melalui IP untuk tujuan kebijakan. [6] Protokolnya digunakan untuk mengenkapsulasi paket IP untuk transmisi di berbagai jenis jaringan.

Mekanisme enkapsulasi dari protokol GRE disederhanakan seperti ada sebuah

header yang ditambahkan di paket awal. Enkapsulasi datagram dari protokol lapisan jaringan tertentu dan GRE mampu mengenkapsulasi datagram untuk ditransmisikan ke protokol lapisan jaringan lain. Kanal transmisi dari jaringan heterogen disebut tunnel (terowongan). Sebagai salah satu metode enkapsulasi, GRE sangat kuat dan sering digunakan di VPN, tetapi GRE sendiri tidak mendukung enkripsi data. Spesifikasi ini mendefinisikan opsi GRE Key yang akan digunakan untuk negosiasi mode enkapsulasi GRE dan pertukaran kunci GRE uplink dan downlink. Tombol GRE downlink dan uplink yang dinegosiasikan dapat digunakan untuk menandai lalu lintas downlink dan uplink untuk sesi mobilitas tertentu. Selain itu, spesifikasi ini memungkinkan gateway akses seluler dan jangkar mobilitas lokal untuk menegosiasikan penggunaan mode enkapsulasi GRE tanpa menukar tombol GRE [7][8][9][10]. RFC2784 menentukan checksum GRE opsional, dan [RFC2890] menentukan kolom kunci GRE dan nomor urut opsional. Bidang opsional ini tidak terlalu berguna untuk enkapsulasi MPLS-in-GRE. Nomor urut dan bidang checksum tidak diperlukan, karena tidak ada bidang yang sesuai di paket MPLS asli yang sedang disalurkan [11]. GRE mendukung Ipv4 [12] maupun IPv6 [13].

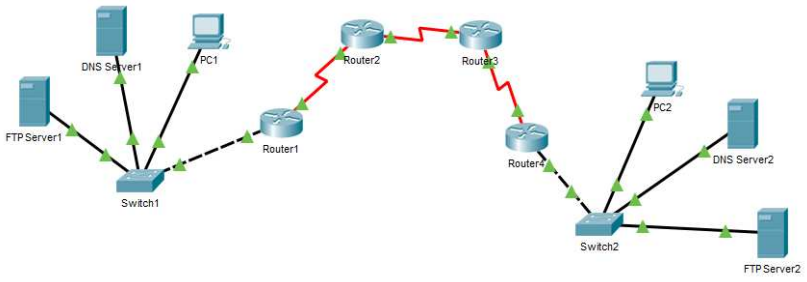
Bingkai GRE yang memenuhi kondisi multiplexing yang telah ditentukan diatur dalam muatan dari satu frame Protokol Internet (IP) luar sesuai dengan informasi header bingkai multiplexing yang diperoleh dari frame GRE. Dengan cara ini, untuk bingkai data dengan muatan kecil, biaya enkapsulasi yang tidak perlu dikurangi, dan efisiensi transmisi bingkai data ditingkatkan. Dengan demikian, sumber daya bandwidth jaringan disimpan, dan kinerja transmisi sistem ditingkatkan [14].

Keamanan jaringan ada untuk menjaga integritas dan validitas data pada suatu sistem informasi, dan menjamin ketersediaan layanan terutama berkaitan dengan keamanan untuk penggunanya. Sistem jaringan komputer sangat rentan untuk diserang, maka dari itu sistem sebaik mungkin harus diproteksi dari berbagai serangan dan usaha penyusupan dari luar atau dalam [15]. Solusi keamanan dari Generic Routing Encapsulation adalah enkapsulasi dari transmisi data antar protokol lapisan jaringan sehingga transmisi data menjadi lebih aman.

Berdasarkan penjelasan diatas maka tujuan dari simulasi implementasi Generic Routing Encapsulation menggunakan CISCO Packet Tracer adalah dua jaringan dapat terhubung dan dapat berkomunikasi satu sama lain dilindungi oleh GRE ini.

2. Metode Penelitian

Simulasi untuk Generic Routing Encapsulation ini menggunakan aplikasi CISCO Packet Tracer. Diumpamakan ada induk perusahaan dan anak perusahaan yang ingin terhubung oleh suatu jaringan dan dilindungi oleh Generic Routing Encapsulation. Induk maupun anak perusahaan dimisalkan memiliki 1 server FTP, 1 server DNS, 1 PC, 1 Switch. Kemudian dibuatlah desain topologi jaringan seperti ini



Gambar 1. Topologi jaringan.

Konfigurasi alamat IP:

1) Alamat IP PC1 diatur menjadi 222.17.244.2, subnet masknya 255. 255. 255. 0, dan alamat gateway diatur menjadi 222.17.244.1.

2) Alamat IP DNS Server1 diatur menjadi 222.17.244.3, subnet masknya 255. 255. 255. 0, dan alamat gateway diatur menjadi 222.17. 244.1.

3) Alamat IP FTP Server1 diatur menjadi 222.17.244.4, subnet masknya 255. 255. 255. 0, dan alamat gateway diatur menjadi 222.17.244.1.

4) Alamat IP PC2 diatur menjadi 222.17.245.2, subnet masknya 255. 255. 255. 0, dan alamat gateway diatur menjadi 222.17.245.1.

5) Alamat IP DNS Server2 diatur menjadi 222.17.245.3, subnet masknya 255. 255. 255. 0, dan alamat gateway diatur menjadi 222.17. 245.1.

6) Alamat IP FTP Server2 diatur menjadi 222.17.245.4, subnet masknya 255. 255. 255. 0, dan alamat gateway diatur menjadi 222.17.245.1.

3. Hasil dan Pembahasan

Target dari simulasi ini adalah adanya terowongan (tunnel) secara fisikal pada jaringan publik. Pertama-tama yang harus dilakukan adalah mengatur topologi jaringannya. Disini umpamanya ada dua kantor yang ingin saling mentransmisikan data. Masing-masing kantor ini memiliki switch, server FTP, server DNS, router, dan PC. Kemudian mengatur alamat IP dari masing-masing perangkat dan dihubungkan dengan kabel-kabel. Router 2 dan Router 3 berfungsi menghubungkan kedua kantor dalam satu jaringan WAN. Masing-masing transmisi data ini dilindungi oleh IPSec untuk perlindungan enkripsi data kemudian dilapisi GRE untuk enkapsulasi transmisi.

Pengujian untuk mengetahui apakah GRE sudah terpasang dengan baik adalah dengan menggunakan perintah "show ip route" pada Router 1. Hasil yang didapatkan adalah sebagai berikut

```
Gateway of last resort is 188.128.5.2 to network 0.0.0.0
          188.128.0.0/24 is subnetted, 1 subnets
C       188.128.5.0 is directly connected, Serial0/0/1
C    192.168.1.0/24 is directly connected, Tunnel0
C    222.17.244.0/24 is directly connected, FastEthernet0/0
          S* 0.0.0.0/0 [1/0] via 188.128.5.0
```

Gambar 2. Hasil perintah "show ip route" pada Router 1.

Kemudian kita gunakan perintah "show interface tunnel 0" dan hasilnya adalah sebagai berikut

```
Tunnel0 is up, line protocol is up (connected)
                Hardware is Tunnel
          Internet address is 192.168.1.1/24
      MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
       reliability 255/255, txload 1/255, rxload 1/255
          Encapsulation TUNNEL, loopback not set
                Keepalive not set
Tunnel source 188.128.5.1 (Serial0/0/1), destination 52.1.1.2
          Tunnel protocol/transport GRE/I
```

Gambar 3. Hasil perintah "show ip route" pada Router 1.

Perhatikan gambar 3 ada "Tunnel protocol/transport GRE/IP" yang berarti jaringan sudah dilindungi oleh GRE sehingga transmisi data sudah aman.

4. Kesimpulan

Berdasarkan hasil simulasi dapat disimpulkan bahwa Generic Routing Encapsulation bisa dilakukan pada dua jaringan yang terhubung dengan router dalam lingkup WAN sehingga semua perangkat pada kedua jaringan itu dapat terhubung dan bisa saling berkomunikasi satu sama lain. Hal ini bisa kita implementasikan di perusahaan utama dengan perusahaan cabang sehingga pekerjaan akan selesai lebih efektif dan aman. Selain itu, diharapkan kedepannya GRE ini bisa digunakan secara masif di berbagai jaringan internet. Saran untuk penelitian selanjutnya adalah GRE bisa digabungkan dengan metode tunneling ataupun metode keamanan yang lain sehingga keamanan jaringan menjadi lebih baik.

Referensi

1. Komputer, W., 2010. Cara Mudah Membangun Jaringan Komputer & Internet. MediaKita.
2. Wang, C. and Chen, J.Y., 2014, May. Implementation of GRE over IPsec VPN enterprise network based on Cisco packet tracer. In 2nd International Conference on Soft Computing in Information Communication Technology. Atlantis Press.
3. Ogudo, K.A., 2019, August. Analyzing Generic Routing Encapsulation (GRE) and IP Security (IPSec) Tunneling Protocols for Secured Communication over Public Networks. In 2019 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD) (pp. 1-9). IEEE.
4. Hendriana, Y. and Widyawan, S.T., 2012. Evaluasi Implementasi Keamanan Jaringan Virtual Private Network (VPN)(Studi Kasus pada CV. Pangestu Jaya) (Doctoral dissertation, [Yogyakarta]: Universitas Gadjah Mada).
5. Warman, I. and Hanafi, A., 2019. Analisa Perbandingan kinerja Generic routing encapsulation (GRE) tunnel dengan point to point protocol over ethernet (PPPoE) tunnel mikrotik routeros. Jurnal TeknoIf, 7(1).
6. Hanks, S., Li, T., Farinacci, D. and Traina, P., 1994. RFC1701: Generic Routing Encapsulation (GRE).
7. Farinacci, D., Li, T., Hanks, S., Meyer, D. and Traina, P., 2000. Generic routing encapsulation (GRE). RFC 2784, March.
8. Hanks, S., Li, T., Farinacci, D. and Traina, P., 1994. Generic routing encapsulation (GRE). RFC 1701, October.
9. Muhanna, A., Khalil, M., Gundavelli, S. and Leung, K., 2010. Generic Routing Encapsulation (GRE) Key Option for Proxy Mobile IPv6. IETF RFC 5845 (Proposed Standard).
10. Farinacci, D., Li, T., Hanks, S., Meyer, D. and Traina, P., 2000. RFC2784: Generic routing encapsulation (GRE).
11. Rosen, E., 2005. Encapsulating MPLS in IP or Generic Routing Encapsulation (GRE).
12. Hanks, S., 1994. Generic routing encapsulation over IPv4 networks. RFC1702.
13. Pignataro, C., Bonica, R. and Krishnan, S., 2015. IPv6 Support for Generic Routing Encapsulation (GRE). RFC7676, October.

14. He, J., Huawei Technologies Co Ltd, 2011. Generic routing encapsulation bearing method, apparatus and system. U.S. Patent Application 12/944,178.
15. Aziz, Saiful dan Bambang Eka Purnama. 2012. Sistem Keamanan Jaringan Komputer Dengan Firewall dan Intrusion Detection System (IDS). Jurnal Speed 13, Volume 9. No. 2, Agustus 2012: 1-6.