PRAKTIKUM
DESAIN DAN MANAJEMEN JARINGAN KOMPUTER

Nama	**Aliyah Rizky Al-Afifah Polanda**	**No. Modul**	**05**
NPM	**2206024682**	**Tipe**	**Tugas Pendahuluan**

1. VPN (*Virtual Private Network*) merupakan teknologi yang menciptakan koneksi terenkripsi melalui jaringan yang kurang aman (contohnya: jaringan publik). Bekerja dengan membentuk koneksi pribadi antara perangkat pengguna dengan server VPN yang berada di lokasi geografis yang berbeda. VPN digunakan untuk melindungi privasi dari pelanggan dan dapat juga digunakan untuk mengamankan komunikasi antara kantor pusat dengan kantor cabang.

   Keuntungan penggunaan VPN:

   a. Keamanan. VPN melakukan enkripsi terhadap lalu lintas internet antara perangkat pengguna dengan server VPN, sehingga data yang dipertukarkan tidak dapat dibaca oleh pihak ketiga.
   b. Penghematan biaya. Penggunaan VPN dapat membantu organisasi atau perusahaan menghemat biaya dengan meminimalkan pengeluaran untuk pembentukan koneksi antara kantor pusat dan cabang. Hal ini karena menggunakan koneksi virtual melalui VPN jauh lebih hemat daripada harus membangun infrastruktur fisik yang melibatkan pemasangan kabel dan perangkat keras tambahan.
   c. Privasi *online*. VPN melindungi privasi *online* pengguna dengan menyembunyikan alamat IP asli dan menggantinya dengan alamat IP dari server VPN. Hal ini menyulitkan pihak lain untuk melacak aktivitas *online* atau memantau lokasi dari pengguna VPN.
   d. Kompatibilitas. VPN kompatibel dengan berbagai jenis tautan WAN, termasuk teknologi *broadband* yang paling umum digunakan. Hal ini memungkinkan pekerja jarak jauh untuk memanfaatkan koneksi berkecepatan tinggi untuk mengakses jaringan perusahaan dengan aman.

   Referensi:

   - "What is VPN and How It Works?" geeksforgeeks.org, Mar. 2024. [Online]. Available: https://www.geeksforgeeks.org/what-is-vpn-and-how-it-works/. [Accessed Mar. 17, 2024].

2. *Site-to-site* VPN melakukan konfigurasi pada sebuah perangkat yang disebut sebagai VPN *gateway*, yang terletak di sisi pengguna, sehingga setiap pengguna yang terhubung ke VPN *gateway* tidak perlu melakukan konfigurasi tambahan untuk menggunakan VPN. Pengguna tidak mengetahui

bahwa VPN sedang digunakan. *Remote access* VPN mengharuskan setiap pengguna untuk melakukan konfigurasi agar dapat menggunakan VPN.

Perbedaan antara *site-to-site* dan *remote access* VPN adalah sebagai berikut:

Site-to-site VPN	Remote access VPN
Bertujuan untuk menghubungkan dua atau lebih LAN dengan koneksi yang aman.	Memungkinkan pengguna untuk mengakses sumber daya perusahaan secara *remote*.
Konfigurasi dilakukan pada perangkat jaringan di setiap lokasi.	Biasanya konfigurasi dilakukan pada server VPN di jaringan perusahaan.
Tidak memerlukan aplikasi klien VPN, karena semua konfigurasi dilakukan di VPN *gateway*.	Memerlukan aplikasi klien VPN di setiap perangkat pengguna.
Digunakan untuk mengamankan komunikasi antara LAN secara langsung.	Digunakan untuk mengamankan koneksi individu ke suatu server.
Contohnya adalah koneksi antara kantor pusat dan kantor cabang.	Contohnya adalah koneksi antara karyawan yang bekerja dari rumah dengan server perusahaan.

Referensi:

- "Types of Virtual Private Network (VPN) and its Protocols," geeksforgeeks.org, Jan. 2023. [Online]. Available: https://www.geeksforgeeks.org/types-of-virtual-private-network-vpn-and-its-protocols/. [Accessed Mar. 17, 2024].

3. GRE (*Generic Routing Encapsulation*) merupakan teknologi *tunneling* yang digunakan untuk melakukan enkapsulasi paket data dari berbagai jenis protokol jaringan. Termasuk dalam protokol serbaguna untuk membuat koneksi virtual *point-to-point* antara dua jaringan. IPSec (IP *Security*) merupakan protokol yang digunakan untuk mengamankan paket data dalam jaringan. IPSec sering digunakan dalam jaringan VPN untuk memastikan komunikasi yang dilakukan aman.

   Perbedaan antara GRE dan IPSec adalah sebagai berikut:

   a. GRE memiliki tujuan untuk membuat saluran virtual antara dua titik dalam jaringan. Sedangkan, IPSec memiliki tujuan untuk memberikan keamanan tambahan dalam koneksi antar jaringan.
   b. GRE tidak menyediakan keamanan bawaan, seperti enkripsi dan autentikasi, sehingga kurang aman jika GRE hanya diterapkan tanpa protokol tambahan. Sedangkan, IPSec memang dirancang untuk menyediakan keamanan pada komunikasi dalam jaringan IP. Fitur keamanan yang disediakan oleh IPSec adalah enkripsi, autentikasi, dan integritas data.

c. GRE cenderung memiliki *overhead* yang lebih rendah daripada IPSec karena tidak menyediakan fitur keamanan secara bawaan. Hal ini menyebabkan GRE dapat lebih cepat dalam mentransmisikan data. Di sisi lain, IPSec membutuhkan waktu pemrosesan tambahan untuk enkripsi dan dekripsi data, yang dapat menghasilkan *overhead* dan waktu tambahan.

d. GRE relatif lebih fleksibel terhadap protokol yang dapat dienkapsulasi dan cenderung lebih mudah untuk dikonfigurasi daripada IPSec.

e. GRE sering digunakan dalam kasus di mana prioritas utama adalah membentuk saluran virtual antara dua titik dalam jaringan, seperti dalam konfigurasi *site-to-site* VPN. Sedangkan, IPSec lebih umum digunakan dalam konteks keamanan, baik untuk memperkuat koneksi antara jaringan (*site-to-site*) maupun untuk memberikan akses jarak jauh yang aman (*remote access*).

Referensi:

- Md. Sajid. " Difference Between IPSec and GRE," tutorialspoint.com, Apr. 2023. [Online]. Available: https://www.tutorialspoint.com/difference-between-ipsec-and-gre. [Accessed Mar. 17, 2024].

4. Status *interface* dalam GRE *tunnel*:

a. Up/up.

Mengindikasikan bahwa GRE *tunnel* berfungsi dan siap untuk meneruskan *traffic*. Secara administratif, *tunnel* dan protokol pada *tunnel* aktif.

b. Administratively down/down.

Mengindikasikan bahwa *tunnel* dinonaktifkan secara administratif. Dalam status ini, tidak ada *traffic* yang akan diteruskan melalui *tunnel*.

c. Up/down.

Mengindikasikan bahwa *tunnel* telah aktif secara administratif, namun terdapat masalah yang menyebabkan *tunnel* menjadi *down*. Status ini dapat disebabkan oleh kesalahan konfigurasi dalam jaringan.

d. Reset/down.

Mengindikasikan bahwa *tunnel* telah direset oleh suatu perangkat lunak, biasanya karena terjadi perubahan konfigurasi atau pembaruan perangkat lunak.

Referensi:

- "Determine What Impacts GRE Tunnel Interface States, " cisco.com, Oct. 2023. [Online]. Available: https://www.cisco.com/c/en/us/support/docs/ip/generic-routing-encapsulation-gre/118361-technote-gre-00.html#toc-hId-1891593053. [Accessed Mar. 17, 2024].

5. Fitur-fitur keamanan dari IPSec:
   a. **Enkripsi**. IPSec menyediakan fitur enkripsi untuk melindungi kerahasiaan informasi yang dikirimkan menggunakan VPN. Enkripsi bekerja dengan cara mengubah data yang dikirim menjadi format yang tidak dapat dibaca tanpa kunci enkripsi yang tepat.
   b. **Autentikasi**. IPSec menyediakan fitur autentikasi untuk memastikan bahwa informasi yang diterima berasal dari sumber yang sah dan tidak dimodifikasi selama proses transmisi. Protokol autentikasi yang digunakan adalah HMAC (*Hash-based Message Authentication Code*).
   c. **Integritas data** dipastikan dengan menambahkan informasi tambahan ke setiap paket yang ditransmisikan. Informasi tambahan ini digunakan untuk verifikasi bahwa paket tidak dimodifikasi.
   d. **Key management**. Bertujuan untuk mengelola kunci kriptografi yang digunakan untuk melindungi data. IPSec memastikan bahwa kunci tersebut dijaga dengan aman sepanjang siklus hidupnya. Hal ini menjadi aspek penting dalam memastikan keamanan komunikasi yang terenkripsi.

   Referensi:

   - "IP security (IPSec)" geeksforgeeks.org, Apr. 2023. [Online]. Available: https://www.geeksforgeeks.org/ip-security-ipsec/. [Accessed Mar. 17, 2024].

6. Enkripsi merupakan proses mengubah format dari informasi yang akan dikirimkan melalui jaringan berdasarkan kunci tertentu, sehingga pihak ketiga tidak dapat membaca informasi tersebut. Terdapat dua metode berbeda yang dapat digunakan untuk melakukan enkrpsi, yaitu:
   a. *Symmetric encryption.*

      Merupakan metode enkripsi di mana proses enkripsi dan dekripsi informasi hanya dilakukan dengan satu kunci. Metode ini merupakan yang paling sederhana dan paling umum untuk digunakan. Karena sederhana, enkripsi simetris mudah untuk dikonfigurasi, namun memiliki kekurangan dari segi keamanan.
   b. *Asymmetric encryption.*

      Merupakan metode yang menggunakan dua kunci berbeda untuk proses enkripsi dan dekripsi. Hal ini didasarkan pada teknik kunci publik dan kunci privat. Kunci publik yang digunakan untuk enkripsi tersedia untuk semua orang, namun kunci privat yang digunakan untuk dekripsi hanya diketahui oleh penerima informasi.

   Perbedaan antara enkripsi simetris dan asimetris adalah sebagai berikut:

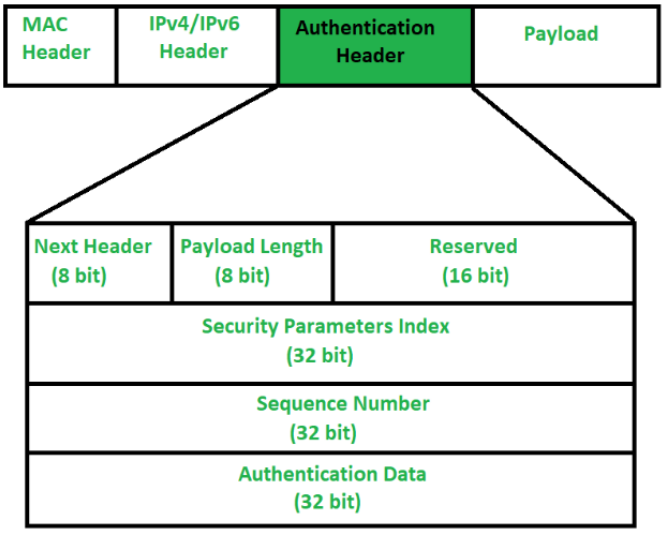
Symmetric Encryption	Asymmetric Encryption
Hanya membutuhkan satu kunci untuk enkripsi dan dekripsi.	Membutuhkan dua kunci berbeda untuk enkripsi dan dekripsi.
Hasil enkripsi (*cypher text*) berukuran sama atau lebih kecil dari teks asli.	Hasil enkripsi (*cypher text*) berukuran sama atau lebih besar dari teks asli.
Proses enkripsi dapat dilakukan dengan sangat cepat.	Proses enkripsi lebih lambat daripada enkripsi simetris.
Sesuai untuk diterapkan jika terdapat data berukuran besar yang ingin ditransmisikan.	Sesuai untuk diterapkan jika data yang ingin ditransmisikan berukuran kecil.
Hanya menyediakan kerahasiaan informasi.	Menyediakan kerahasiaan dan keaslian informasi, serta *non-repudiation*, yaitu mencegah atau menolak kemungkinan untuk menyangkal tindakan yang telah dilakukan oleh pengguna.
Panjang kunci yang digunakan adalah 128 atau 256 *bits*.	Panjang kunci yang digunakan adalah setidaknya 2048 bits
Karena hanya satu kunci yang digunakan, maka metode ini kurang aman.	Merupakan metode yang lebih aman.
Contohnya adalah AES (*Advanced Encryption Standard*).	Contohnya adalah RSA.

Referensi:

- "Difference Between Symmetric and Asymmetric Key Encryption," geeksforgeeks.org, May, 2023. [Online]. Available: https://www.geeksforgeeks.org/difference-between-symmetric-and-asymmetric-key-encryption/. [Accessed Mar. 17, 2024].
- "Difference between Symmetric encryption and Asymmetric encryption," javatpoint.com. [Online]. Available: https://www.javatpoint.com/symmetric-encryption-vs-asymmetric-encryption. [Accessed Mar. 17, 2024].

7. Ya, pada IPSec terdapat fitur keamanan untuk menjaga integritas data. Integritas data dalam IPSec dipertahankan dengan menerapkan *Authentication Header* (AH). AH memverifikasi asal data dan *payload* untuk mendeteksi modifikasi selama transmisi antara sumber dan tujuan. Hal ini dilakukan dengan menambahkan *Message Authentication Code* (MAC) ke dalam paket IPSec menggunakan fungsi *hash*. Penerima akan menggunakan kunci autentikasi yang sama untuk memverifikasi MAC

dan memastikan bahwa isi paket tidak dimodifikasi dalam perjalanan. AH terdiri dari beberapa bagian, yaitu:



a. *Next Header*: memiliki ukuran 8 bit dan digunakan untuk mengidentifikasi jenis *header* yang ada setelah AH.
b. *Payload Length*: merupakan panjang dari AH dalam skala 4, ukuran *header* asli dibagi 4 dan dikurangi oleh 2.
c. *Reserved*: biasanya diatur ke 0, karena berfungsi untuk penggunaan masa depan.
d. *Security Parameters Index* (SPI): merupakan bagian yang penting untuk mengidentifikasi semua paket yang termasuk dalam koneksi saat ini. Berupa nilai unik yang digunakan untuk memverifikasi asosiasi keamanan (AS) yang berkaitan dengan paket. Setiap AS memiliki SPI yang unik dan digunakan oleh penerima untuk menentukan keamanan dan kebijakan yang diterapkan pada paket yang diterima. SPI memungkinkan sistem untuk mengidentifikasi dan membedakan antara beberapa AS yang mungkin berlaku.
e. *Sequence Number*: digunakan untuk memberikan identifikasi unik pada setiap paket yang akan dikirimkan. *Sequence number* digunakan untuk mencegah serangan *replays*, di mana penyerang mencoba mengirimkan kembali paket yang sudah dikirim sebelumnya. Penerima IPSec menyimpan nomor urut paket yang diterima dalam rentang waktu tertentu. Sehingga jika penerima menerima paket dengan nomor urut yang sudah pernah diterima dalam rentang waktu tersebut, paket tersebut dianggap sebagai *replay* dan ditolak.
f. *Authentication Data*: berisi nilai ICV (*Integrity Check Value*) dari paket. Dengan menggunakan algoritma *hashing* dan kunci yang sama, pengirim dan penerima pesan akan membuat ringkasan pesan. Jika kedua ringkasan cocok, penerima akan menerima data. Jika tidak, pesan ditolak karena dianggap telah diubah selama pengiriman.

Referensi:

- "Internet Protocol Authentication Header," geeksforgeeks.org, Mar. 2023. [Online]. Available: https://www.geeksforgeeks.org/internet-protocol-authentication-header/. [Accessed Mar. 17, 2024].

8. Konfigurasi GRE *tunnel*:

   Router(config)#interface tunnel [nomor tunnel]

   Router(config-if)#ip address [alamat IP] [netmask]

   Router(config-if)#tunnel source [alamat IP sumber atau interface sumber]

   Router(config-if)#tunnel destination [alamat IP tujuan]

   Untuk memeriksa konfigurasi:

   Router#show interface tunnel [nomor tunnel]

   Contoh:

   Router(config)#interface tunnel 1

   Router(config-if)#ip address 10.10.10.1 255.255.255.0

   Router(config-if)#tunnel source G0/0

   Router(config-if)#tunnel destination 172.16.2.1

   Referensi:

   - "Generic Routing Encapsulation (GRE) Tunnel," study-ccnp.com. [Online]. Available: https://study-ccnp.com/generic-routing-encapsulation-gre-tunnel/. [Accessed Mar. 17, 2024].
   - "GRE Tunnel on Cisco IOS Router," networklessons.com. [Online]. Available: https://networklessons.com/cisco/ccie-routing-switching/how-to-configure-gre-tunnel-on-cisco-ios-router. [Accessed Mar. 17, 2024].

9. Perbedaan antara SSL (*Secure Sockets Layer*) dan IPSec dalam *remote access* VPN:
   a. SSL bekerja pada lapisan diantara *transport layer* dan *application layer* OSI model, sedangkan IPSec bekerja pada lapisan *internet layer*.
   b. SSL biasanya digunakan untuk mengamankan komunikasi antara klien dan server dalam lingkungan *web*. IPSec digunakan untuk mengamankan seluruh *traffic* dalam jairngan antara dua titik.
   c. *Remote access* VPN menggunakan SSL untuk memberikan akses ke sumber daya jaringan internal melalui *web browser* atau aplikasi khusus. Sedangkan, *remote access* VPN

menggunakan IPSec untuk memberikan akses ke jaringan internal melalui klien VPN yang terhubung secara langsung ke jaringan.

d. SSL memiliki konfigurasi yang lebih mudah dan lebih kompatibel dengan banyak perangkat. Sedangkan, IPSec membutuhkan aplikasi tambahan dalam konfigurasinya.

e. Proses SSL lebih lambat karena bekerja pada lapisan aplikasi,. Sedangkan proses IPSec lebih cepat karena bekerja pada *internet layer*.

Referensi:

- "Difference between IPSec and SSL," geeksforgeeks.org, Feb. 2023. [Online]. Available: https://www.geeksforgeeks.org/difference-between-ipsec-and-ssl/. [Accessed Mar. 17, 2024].
- P. Loshin. "IPsec vs. SSL VPN: Comparing speed, security risks and technology," techtarget.com, Jun. 2019. [Online]. Available: https://www.techtarget.com/searchsecurity/tip/IPSec-VPN-vs-SSL-VPN-Comparing-respective-VPN-security-risks. [Accessed Mar. 17, 2024].