PRAKTIKUM
CLOUD COMPUTING

MODUL 2
PENGENALAN AMAZON VIRTUAL PRIVATE CLOUD (VPC)

2.1 Topik Pembahasan

1. Konsep Dasar Jaringan Komputer
2. Amazon Virtual Private Cloud (Amazon VPC)
3. Subnet VPC dan Komponen Jaringan VPC

2.2 Tujuan Praktikum

1. Praktikan dapat memahami dasar-dasar jaringan
2. Praktikan dapat memahami dan menjelaskan Amazon Virtual Private Cloud (Amazon VPC)
3. Praktikan dapat memahami dan mempraktikan Keamanan Jaringan menggunakan Amazon VPC
4. Praktikan dapat Mendesain arsitektur jaringan sederhana menggunakan Amazon VPC

2.3 Alat dan Bahan

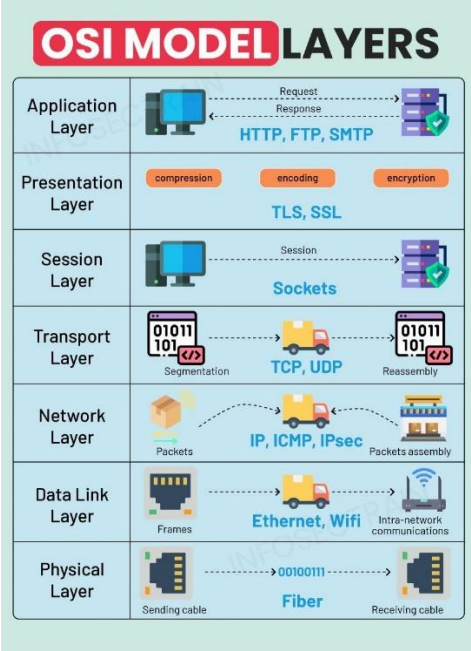
1. Laptop
2. Hotspot
3. Kertas Folio
4. Alat Tulis

2.4 Dasar Teori

2.4.1 Pengenalan Dasar Jaringan

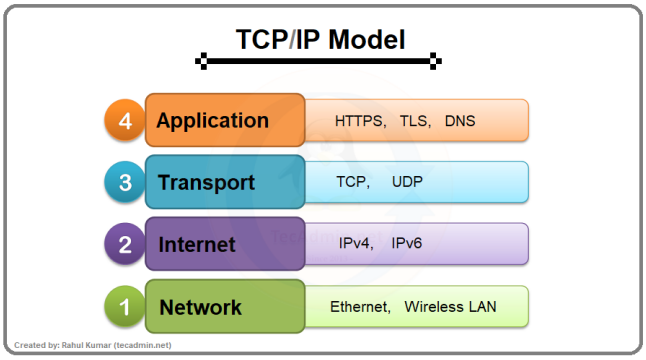
Dalam jaringan komputer, terdapat dua model utama yang digunakan dalam distribusi data antara satu perangkat ke perangkat lain yaitu model OSI dan model TCP/IP.

Model OSI (Open Systems Interconnection) merupakan model jaringan yang terdiri dari tujuh lapisan dimana setiap lapisan punya tugas khusus, misalnya mengatur alamat, membuat koneksi, sampai menampilkan data. OSI Layer sering digunakan untuk memberi gambaran detail tentang alur komunikasi data.



Gambar 2.4.1 Ketujuh Lapisan Model OSI

Sedangkan model TCP/IP merupakan model jaringan yang lebih sederhana dan bukti penerapan dapat dilihat pada kehidupan nyata, terutama di internet. Model ini hanya punya empat lapisan utama: network interface, internet, transport, dan application. TCP/IP adalah dasar dari jaringan internet modern yang memungkinkan semua perangkat bisa saling terhubung.



Gambar 2.4.1 Model TCP/IP

2.4.2 Pengalamatan Jaringan (IP Address, Subnet, dan CIDR)

Dalam sebuah jaringan komputer, setiap perangkat harus memiliki alamat saling berkomunikasi yang disebut sebagaii **IP Address (Internet Protocol Address)** dan berfungsi seperti nomor rumah pada sebuah jalan: tanpa alamat, data tidak akan tahu harus dikirim ke mana.

IP Address memiliki dua versi utama:

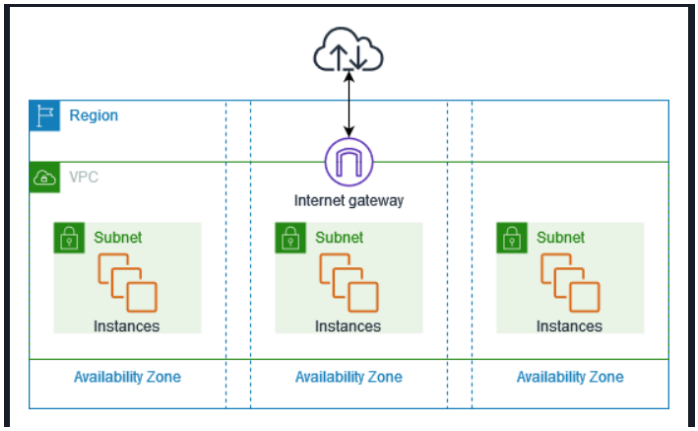
- **IPv4** (32 bit, ditulis dalam format desimal, contoh: 192.168.1.1).
- **IPv6** (128 bit, ditulis dalam format heksadesimal, contoh: 2001:db8::1).

Sedangkan untuk membuat jaringan lebih teratur dibutuhkan pembagian alamat IP menjadi kelompok-kelompok kecil yang disebut sebgai **subnet/subnetting** dengan subnet memungkinkan dalam memisahkan jaringan besar menjadi beberapa bagian lebih kecil untuk keperluan berupa (Database,User dan Server).

Lalu untuk menentukan ukuran subnet, digunakan konsep **CIDR (Classless Inter-Domain Routing)**. CIDR ditulis dengan menambahkan garis miring dan angka di belakang alamat IP, misalnya **192.168.1.0/24**. Angka **/24** menunjukkan berapa banyak bit yang digunakan sebagai network ID.

2.4.3 Amazon Virtual Private Cloud (Amazon VPC)

Amazon Virtual Private Cloud (Amazon VPC) adalah layanan jaringan virtual di AWS yang memungkinkan kita menjalankan resource, seperti server (EC2), di dalam lingkungan jaringan yang terisolasi secara logis. Artinya, jaringan tersebut hanya milik kita dan tidak bercampur dengan pengguna AWS lain. Konsepnya mirip dengan jaringan tradisional yang biasa digunakan di data center perusahaan, misalnya ada subnet, routing, dan firewall. Bedanya, VPC berjalan di atas infrastruktur AWS yang berskala besar, fleksibel, dan mudah disesuaikan. Dalam sebuah VPC, kita bisa membuat subnet di beberapa Availability Zone, menaruh instance EC2 di dalam subnet tersebut, dan menambahkan Internet Gateway supaya resource di dalam VPC dapat berkomunikasi dengan internet. Dengan cara ini, VPC memberikan kontrol penuh terhadap arsitektur jaringan, sekaligus keamanan dan skalabilitas yang disediakan AWS.



Gambar 2.4.3 Jaringan Amazon VPC

2.4.4 Subnet dan VPC

Amazon Virtual Private Cloud (VPC) adalah jaringan virtual pribadi di AWS. VPC bersifat terisolasi secara logis dari pengguna lain dan hanya dapat diakses oleh akun kita. Setiap VPC berada dalam satu wilayah AWS, namun bisa mencakup beberapa Availability Zone.

Di dalam VPC, kita bisa membuat **subnet**, yaitu bagian kecil dari jaringan dengan rentang IP tertentu. Subnet hanya dapat berada pada satu Availability Zone. Umumnya ada dua jenis subnet:

- **Subnet Publik**: dapat diakses langsung dari internet (misalnya untuk web server).
- **Subnet Privat**: tidak langsung ke internet, lebih aman untuk resource sensitif seperti database.

Gambar 2.4.3 Subnet pada Amazon VPC

2.4.5 Komponen Jaringan dalam VPC

2.4.6 Internet Gateway

Internet Gateway adalah komponen VPC yang berfungsi sebagai pintu keluar-masuk agar subnet publik dapat terhubung dengan internet. Internet Gateway digunakan untuk:

1. Menjadi target routing menuju internet.
2. Memberikan alamat IPv4 publik pada instance agar bisa diakses dari luar.

2.4.7 NAT Gateway

NAT Gateway memungkinkan resource di subnet privat mengakses internet, tetapi tetap tidak dapat diakses langsung dari luar. Ini penting misalnya untuk database atau server aplikasi yang butuh update software, namun harus tetap terlindungi dari akses publik. Dengan NAT Gateway, keamanan tetap terjaga tanpa mengorbankan kebutuhan konektivitas keluar.

2.4.8 VPC Sharing

VPC Sharing adalah fitur AWS yang memungkinkan beberapa akun berbeda menggunakan satu VPC yang sama. Dengan cara ini, organisasi bisa membangun satu arsitektur jaringan utama, lalu membagi penggunaannya ke berbagai tim atau departemen tanpa harus membuat banyak VPC terpisah.Keuntungannya antara lain:

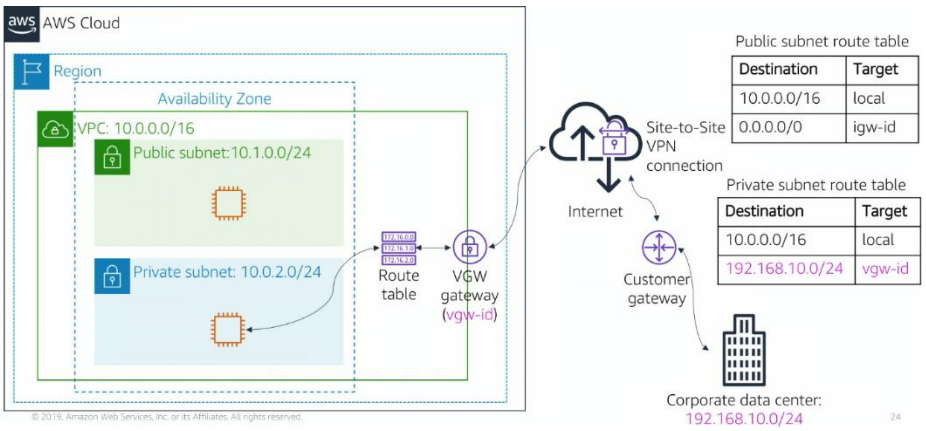
- Pengelolaan jaringan lebih mudah karena terpusat.
- Resource tetap dimiliki oleh masing-masing akun.
- Hemat biaya, misalnya dengan berbagi NAT Gateway atau VPC Endpoint.

2.4.9 VPC Peering

VPC Peering adalah koneksi langsung antar VPC sehingga resource di dalamnya bisa saling berkomunikasi secara privat. VPC Peering cocok untuk aplikasi yang dipisahkan ke beberapa VPC tapi tetap harus saling terhubung.

2.4.10 VPN Site-to-Site

VPN Site-to-Site digunakan untuk menghubungkan VPC dengan jaringan lokal (*on-premises*) melalui koneksi terenkripsi di internet. Dengan VPN ini, organisasi bisa membuat **hybrid cloud**, di mana sebagian layanan ada di data center sendiri dan sebagian lagi di AWS.



Gambar 2.4.10 Skenario VPN Site-to-Site

2.4.11 VPC Endpoint

VPC Endpoint memungkinkan komunikasi privat dari VPC ke layanan AWS tanpa harus menggunakan IGW, NAT, atau VPN.

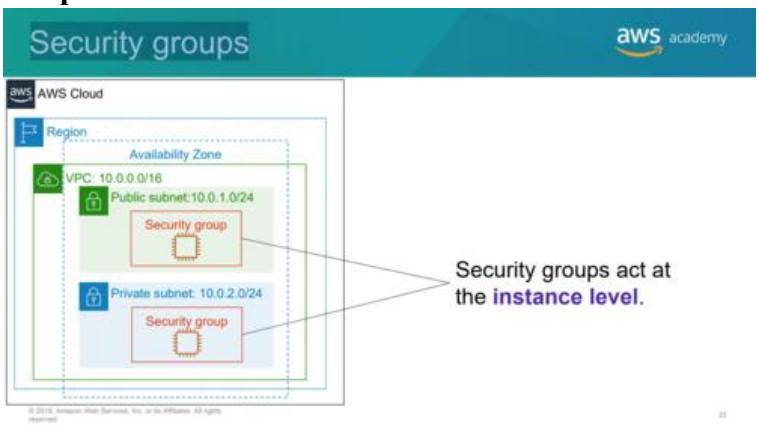
- **Interface Endpoint**: menggunakan AWS PrivateLink untuk menghubungkan layanan AWS atau pihak ketiga.
- **Gateway Endpoint**: biasanya digunakan untuk layanan populer seperti Amazon S3 dan DynamoDB.

  Dengan VPC Endpoint, lalu lintas lebih aman karena tidak melewati internet publik.

2.5.1 Keamanan VPC

Guna merancang suatu jaringan VPC yang aman selama perancangan dibutuhkan aspek keamanan yang kuat lewat dua mekanisme utama untuk melindungi resource, yaitu **Security Group** dan **Network ACL (NACL)** yang telah di sediakan oleh AWS

2.5.1 Security Group



Security Group adalah firewall virtual pada tingkat instance. Security Group bersifat *stateful*, artinya jika kita mengizinkan koneksi keluar, maka balasan otomatis diizinkan masuk tanpa perlu aturan tambahan.

- **Karakteristik:**
    - Berlaku pada level instance.
    - Mendukung aturan izin (*allow*) saja, tidak ada aturan tolak (*deny*).
    - Aturan outbound dan inbound saling melengkapi.
- **Contoh penggunaan:**
    - Mengizinkan HTTP (port 80) dan HTTPS (port 443) untuk web server.
    - Membatasi SSH (port 22) hanya dari alamat IP administrator.

Dengan Security Group, kita bisa memastikan setiap instance hanya membuka port yang memang diperlukan.

2.5.1 Network ACL (NACL)

Network Access Control List (NACL) adalah firewall pada tingkat subnet. Berbeda dengan Security Group, NACL bersifat *stateless*: setiap aturan inbound dan outbound harus ditentukan secara eksplisit.

- **Karakteristik:**
    - Berlaku pada level subnet.
    - Mendukung aturan izin (*allow*) dan tolak (*deny*).
    - Balasan trafik harus diatur manual.
- **Contoh penggunaan:**
    - Menolak akses dari alamat IP tertentu yang dianggap berbahaya.
    - Membatasi trafik hanya untuk port tertentu pada seluruh subnet.

Atribut	Grup Keamanan	ACL jaringan
Cakupan	Tingkat instans	Tingkat subnet
Aturan yang Didukung	Hanya aturan izinkan	Aturan izinkan dan tolak
Status	Stateful (lalu lintas kembali diizinkan secara otomatis, terlepas dari aturan)	Stateless (lalu lintas kembali harus diizinkan oleh aturan secara eksplisit)
Urutan Aturan	Semua aturan dievaluasi sebelum keputusan untuk mengizinkan lalu lintas	Aturan dievaluasi dalam urutan angka sebelum keputusan untuk mengizinkan lalu lintas

Gambar 2.5.3 Perbandingan Security Groups dan ACL