MODUL 2
PENGENALAN KONSEP VPC DAN JARINGAN KOMPUTER

3.1 Topik Pembahasan

1. Dasar-dasar jaringan
2. Amazon Virtual Private Cloud (Amazon VPC)
3. Jaringan VPC
4. Keamanan VPC
5. Amazon CloudFront

3.2 Tujuan Praktikum

1. Praktikan dapat memahami dasar-dasar jaringan
2. Praktikan dapat memahami Amazon Virtual Private Cloud (Amazon VPC)
3. Praktikan dapat memahami jaringan VPC
4. Praktikan dapat memahami Keamanan VPC
5. Praktikan dapat memahami Amazon CloudFront
6. Praktikan dapat membuat VPC

3.3 Alat dan Bahan

1. Laptop

3.4 Dasar Teori

3.4.1 Dasar-dasar jaringan

Jaringan komputer adalah dua mesin klien atau lebih yang terhubung bersama-sama untuk berbagi sumber daya. Sebuah jaringan dapat secara logis dipartisi menjadi subnet. Jaringan memerlukan perangkat jaringan (seperti perute atau switch) untuk menghubungkan semua klien bersama-sama dan memungkinkan komunikasi antar klien.

3.4.1.1 Model Open Systems Interconnection (OSI)

Model Open Systems Interconnection (OSI) adalah model konseptual yang digunakan untuk menjelaskan bagaimana data melalui jaringan. Model ini terdiri dari tujuh lapis dan menunjukkan protokol umum dan alamat yang digunakan untuk mengirim data pada setiap lapis.

Lapis	Nomor	Fungsi	Protokol/Alamat
Aplikasi	7	Cara aplikasi mengakses jaringan komputer	HTTP(S), FTP, DHCP, LDAP
Presentasi	6	• Memastikan bahwa lapis aplikasi dapat membaca data • Enkripsi	ASCI, ICA
Sesi	5	Memungkinkan pertukaran data secara teratur	NetBIOS, RPC
Transportasi	4	Menyediakan protokol untuk mendukung komunikasi antarhost	TCP, UDP
Jaringan	3	Perutean dan penerusan paket (perute)	IP
Tautan data	2	Memindahkan data di dalam jaringan LAN yang sama (hub dan switch)	MAC
Fisik	1	Transmisi dan penerimaan bitstream mentah melalui medium fisik	Sinyal (1 dan 0)

3.4.1.2 Alamat IP

Setiap mesin klien dalam jaringan memiliki alamat Internet Protocol (IP) yang unik yang mengidentifikasinya. Alamat IP adalah label numerik dalam format desimal. Mesin mengonversi angka desimal ke format biner. Alamat IP 32 bit disebut sebagai alamat IPv4. Alamat IP 128bit disebut sebagai IPV6, Alamat IPv6 dapat menampung lebih banyak perangkat pengguna dari pada IPV4.

3.4.2 Amazon Virtual Private Cloud (Amazon VPC)

Amazon Virtual Private cloud (Amazon VPC) adalah layanan virtual network yang memungkinkan Anda menyediakan bagian yang terisolasi secara logis dari AWS cloud (disebut virtual private cloud, atau VPC), VPC menjadi bagian dari satu Wilayah AWS dan dapat menjangkau beberapa Availability Zone.

Amazon VPC memberi kontrol atas sumber daya jaringan virtual, termasuk pilihan rentang alamat IP sendiri, pembuatan subnet, serta konfigurasi tabel rute, dan gateway jaringan.

3.4.2.1 Subnet dan VPC

VPC adalah sebuah jaringan virtual yang terisolasi secara logis dari jaringan virtual lainnya di AWS Cloud.Sebuah VPC didedikasikan untuk akun Anda. VPC menjadi bagian dari satu Wilayah AWS dan dapat menjangkau beberapa Availability Zone.

Setelah membuat VPC, Anda dapat membaginya menjadi satu subnet atau lebih. Subnet adalah rentang alamat IP dalam VPC.Subnet menjadi bagian dari satu Availability Zone. Anda dapat membuat subnet di Availability Zone yang berbeda untuk ketersediaan tinggi. Subnet umumnya diklasifikasikan sebagai publik atau privat.

3.4.2.2 Antar muka jaringan elastis

Antarmuka jaringan elastisadalah sebuah antarmuka jaringan virtual yang dapat Anda lampirkan atau lepaskan dari instans dalam VPC.Atribut antarmuka jaringan mengikutinya ketika dilampirkan kembali ke instans lain. Ketika Anda memindahkan antarmuka jaringan dari satu instans ke instans lainnya, lalu lintas jaringan dialihkan ke instans baru.

3.4.3 Jaringan VPC

3.4.3.1 Gateway Internet

Gateway internet adalah komponen VPC yang dapat diskalakan, redundan, dan tersedia dengan sangat baik yang memungkinkan komunikasi antara instans di VPC dan internet.

Gateway internet memiliki dua tujuan:

1. untuk memberikan target dalam tabel rute VPC untuk lalu lintas yang dapat dirutekan internet
2. untuk melakukan penerjemahan alamat jaringan untuk instans yang telah ditetapkan alamat IPv4 publik.

3.4.3.2 Gateway network address translation (NAT)

Gateway NAT adalah layanan Network Address Translation (NAT). Anda dapat menggunakan gateway NAT sehingga instans di subnet privat dapat terhubung ke layanan di luar VPC Anda tetapi layanan eksternal tidak dapat memulai koneksi dengan instans-instans tersebut.

3.4.3.3 Berbagi VPC

Manfaat berbagi VPC sebagai berikut:

1. Pemisahan tugas – Struktur VPC yang dikendalikan secara terpusat, perutean, alokasi alamat IP
2. Kepemilikan – Pemilik aplikasi terus memiliki sumber daya, akun, dan grup keamanan
3. Grup keamanan – peserta berbagi VPC dapat mereferensikan ID grup

keamanan satu sama lain

4. Efisiensi – Kepadatan yang lebih tinggi di subnet, penggunaan VPN dan AWS Direct Connect
5. Tanpa batas langsung – Batas langusng dapat dihindari—misalnya, 50antarmuka virtual per koneksi AWS Direct Connect melalui arsitektur jaringan yang disederhanakan
6. Pengoptimalan biaya - Biaya dapat dioptimalkan melalui penggunaan kembali gateway NAT, endpoint antarmuka VPC, dan lalu lintas antar-Availability Zone.

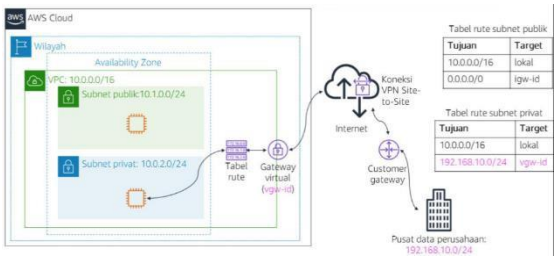
3.4.3.4 Peering VPC

peering VPC adalah koneksi jaringan antara dua VPC yang memungkinkan Anda merutekan lalu lintas di antaranya secara privat.Instans di masing-masing VPC dapat berkomunikasi dengan satu sama lain seakan-akan berada dalam jaringan yang sama. Anda dapat membuat koneksi peering VPC antar VPC Anda sendiri, dengan VPC di akun AWS yang lain, atau dengan VPC di wilayah AWS yang berbeda.

Peering VPC memiliki beberapa batasan:

1. Rentang alamat IP tidak dapat tumpang tindih
2. Peering transitif tidak didukung. Misalnya, Anda memiliki tiga VPC: A, B, dan C. VPC A terhubung ke VPC B, dan VPC A terhubung ke VPC C. Namun, VPC B tidakterhubung ke VPC C secara implisit. Untuk menghubungkan VPC B ke VPC C, Anda harus secara eksplisit menetapkan konektivitas tersebut.
3. Anda hanya dapat memiliki satu sumber daya peering antara dua VPC yang sama.

3.4.3.5 VPN AWS Site-to-Site



Virtual Machine yang diluncurkan ke VPC yang dibuat belum bisa langsung digunakan untuk berkomunikasi jarak jauh, dikarenakan VM yang tersedia masih di setting secara default. Untuk menghubungkan VPC ke jarak jauh dibutuhkan sebuah VPN

site-to-side dengan membuat virtual machine tambahan.

3.4.3.6 Endpoint VPC

Endpoint VPC adalah perangkat virtual yang memungkinkan Anda menghubungkan VPC ke layanan AWS yang didukung dan layanan endpoint VPC yang didukung oleh AWS PrivateLink. Koneksi ke layanan ini tidak memerlukan gateway internet, perangkat NAT, koneksi VPN, atau koneksi AWS Direct Connect.

Ada dua jenis endpoint VPC:

1. Endpoint VPC antarmuka(endpoint antarmuka)

   memungkinkan Anda terhubung ke layanan yang didukung oleh AWS PrivateLink.Layanan ini mencakup beberapa layanan AWS, layanan yang di-host oleh pelanggan AWS lainnya dan Partner AWS Partner Network (APN) di VPC mereka sendiri (disebut sebagai layanan endpoint), dan layanan AWS Marketplace APN Partner yang didukung.

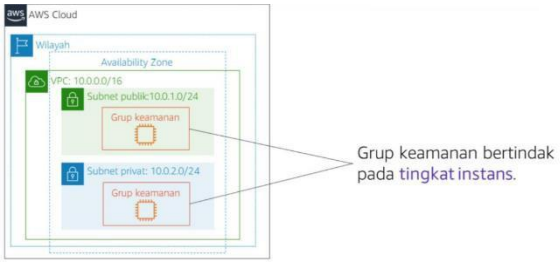
2. Endpoint gateway

   Penggunaan endpoint gateway tidak dikenakan biaya tambahan. Biaya standar untuk transfer data dan penggunaan sumber daya berlaku.

3.4.4 Keamanan VPC

Ada dua opsi firewall Amazon VPC yang dapat digunakan untuk mengamankan VPC seperti grup keamanan dan access control list jaringan (ACL jaringan).

3.4.4.1 Grup keamanan



AWS Grup keamanan bertindak sebagai firewall virtual bagi instans, serta mengontrol lalu lintas masuk dan keluar. Grup keamanan bertindak pada tingkat instans, bukan tingkat subnet. Oleh karena itu, setiap instans di subnet pada VPC dapat ditetapkan ke rangkaian grup keamanan yang berbeda.

Grup keamanan dibagi menjadi dua jenis yaitu:

a. Grup keamanan stateful

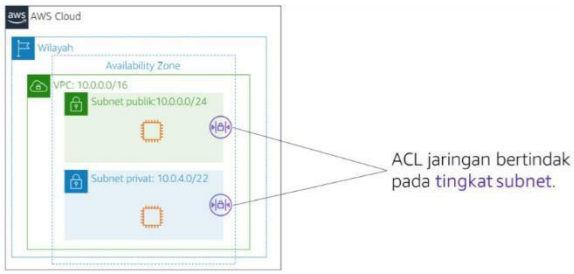
   yang berarti bahwa informasi status disimpan bahkan setelah

permintaan diproses. Karena itu, jika Anda mengirim permintaan dari instans Anda, lalu lintas respons untuk permintaan itu diizinkan masuk, terlepas dari aturan masuk grup keamanan. Respons terhadap lalu lintas masuk yang diizinkan tersebut diizinkan untuk keluar, terlepas dari aturan lalu lintas keluarnya.

b. Grup keamanan kustom

dapat menentukan aturan izinkan, tetapi tidak untuk aturan tolak. Semua aturan dievaluasi sebelum keputusan untuk mengizinkan lalu lintas. Access control list jaringan (ACL jaringan)

3.4.4.2 Access control list jaringan (ACL jaringan)



Access control list jaringan (ACL jaringan) adalah lapis keamanan opsional untuk Amazon VPC. Ini bertindak sebagai firewall untuk mengendalikan lalu lintas masuk dan keluar dari satu subnet atau lebih. Untuk menambahkan lapis keamanan lain ke VPC, Anda dapat mengatur ACL jaringan dengan aturan yang mirip dengan grup keamanan.

Setiap subnet di VPC Anda harus dikaitkan dengan ACL jaringan. Jika Anda tidak mengaitkan subnet dengan ACL jaringan secara eksplisit, subnet dikaitkan dengan ACL jaringan default secara otomatis.

3.4.4.3 Perbedaan grup keamanan dan ACL jaringan

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

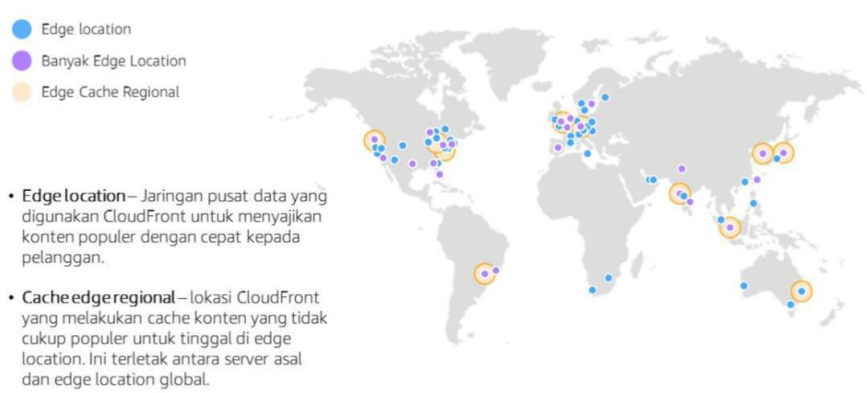
3.4.5 Amazon CloudFront

Amazon CloudFront adalah layanan CDN cepat yang memberikan data, video, aplikasi, dan antarmuka pemrograman aplikasi (API) dengan aman kepada pelanggan secara global dengan latensi rendah dan kecepatan transfer yang tinggi. Hal Ini juga menyediakan lingkungan yang ramah developer. Amazon CloudFront memberikan file ke pengguna melalui jaringan global edge location dan cache edge Regional. Amazon CloudFront berbeda dari solusi penyampaian konten tradisional karena memungkinkan Anda mendapatkan manfaat penyampaian konten kinerja tinggi dengan cepat tanpa kontrak negosiasi, harga tinggi, atau biaya minimum. Seperti layanan AWS lainnya, Amazon CloudFront adalah penawaran mandiri dengan harga bayar sesuai pemakaian.

3.4.3.1 Jaringan penyampaian konten (CDN)

Jaringan penyampaian konten (CDN) adalah sistem server pembuatan cache yang didistribusikan secara global. CDN menyimpan salinan file yang biasa diminta dalam cache (konten statis, seperti Hypertext Markup Language, atau HTML; Cascading Style Sheet, atau CSS; JavaScript; dan file gambar) yang di-host di server asal aplikasi. CDN memberikan salinan lokal dari konten yang diminta dari edge cache atau Point of Presence yang menyediakan pengiriman tercepat untuk pemohon.

3.4.3.2 Infrastruktur Amazon CloudFront



1. Amazon CloudFront menyampaikan konten melalui jaringan pusat data di seluruh dunia yang dikenal sebagai edge location.
2. Ketika pengguna mengajukan permintaan untuk konten yang disajikan melalui CloudFront, pengguna akan diarahkan ke edge location yang memberikan latensi (penundaan waktu) terendah, sehingga konten dapat disampaikan dengan kinerja terbaik.
3. Edge location CloudFront telah dirancang untuk menyajikan konten yang

populer dengan cepat kepada pemirsa Anda.

4. Jika suatu objek menjadi kurang populer, edge location individu dapat menghapus objek-objek tersebut untuk memberi ruang bagi konten yang lebih populer.
5. Untuk konten yang kurang populer, CloudFront memiliki cache edge Regional. Cache edge regional adalah lokasi CloudFront yang didistribusikan secara global dan ditempatkan berdekatan dengan pemirsa Anda. Mereka berada di antara server asal Anda dan edge location global yang menyajikan konten secara langsung kepada pemirsa.
6. Cache edge Regional memiliki kapasitas cache yang lebih besar dibandingkan edge location individu, sehingga objek dapat tetap ada dalam cache edge Regional untuk waktu yang lebih lama.
7. Dengan begitu, lebih banyak konten Anda akan tetap berada dalam jarak dekat dengan pemirsa, yang akan mengurangi kebutuhan CloudFront untuk mengakses server asal dan meningkatkan kinerja keseluruhan bagi pemirsa.

3.4.3.2 Manfaat Amazon Cloudfront

Amazon CloudFront memberikan manfaat sebagai berikut:

a. Cepat dan global

   Amazon CloudFront diskalakan secara masif dan didistribusikan secara global. Untuk mengirimkan konten ke pengguna akhir dengan latensi rendah, Amazon CloudFront menggunakan jaringan global yang terdiri dari edge location dan cache regional.

b. Keamanan di edge

   Amazon CloudFront menyediakan perlindungan tingkat jaringan dan tingkat aplikasi. Lalu lintas dan aplikasi Anda mendapatkan keuntungan melalui berbagai perlindungan bawaan seperti AWS Shield Standard, tanpa biaya tambahan. Anda juga dapat menggunakan fitur yang dapat dikonfigurasi seperti AWS Certificate Manager (ACM) untuk membuat dan mengelola sertifikat Secure Sockets Layer (SSL) kustom tanpa biaya tambahan.

c. Dapat diprogram sepenuhnya

   Fitur Amazon CloudFront dapat dikustomisasi untuk persyaratan aplikasi tertentu.

d. Terintegrasi secara mendalam dengan AWS

Amazon CloudFront terintegrasi dengan AWS, dengan lokasi fisik yang terhubung langsung ke Infrastruktur Global AWS, serta layanan AWS lain.

e. Hemat biaya

Amazon CloudFront hemat biaya karena tidak memiliki komitmen minimum dan biaya.