AWS Whitepaper

Pilihan Konektivitas Amazon Virtual Private Cloud

Pilihan Konektivitas Amazon Virtual Private Cloud: AWS Whitepaper

Table of Contents

Pilihan Konektivitas Amazon Virtual Private Cloud

Tanggal publikasi: 5 April 2023 () Revisi dokumen

Abstrak

Amazon Virtual Private Cloud (Amazon VPC) memungkinkan pelanggan menyediakan bagian pribadi dan terisolasi dari Amazon Web Services (AWS) Cloud tempat mereka dapat meluncurkan sumber daya AWS di jaringan virtual menggunakan rentang alamat IP yang ditentukan pelanggan. Amazon VPC memberi pelanggan beberapa opsi untuk menghubungkan jaringan virtual AWS mereka dengan jaringan jarak jauh lainnya. Dokumen ini menjelaskan beberapa opsi konektivitas jaringan umum yang tersedia bagi pelanggan kami. Ini termasuk opsi konektivitas untuk mengintegrasikan jaringan pelanggan jarak jauh dengan Amazon VPC dan menghubungkan beberapa VPCs Amazon ke jaringan virtual yang berdekatan.

Whitepaper ini ditujukan untuk arsitek dan insinyur jaringan perusahaan atau administrator VPC Amazon yang ingin meninjau opsi konektivitas yang tersedia. Ini memberikan gambaran tentang berbagai opsi untuk memfasilitasi diskusi konektivitas jaringan serta petunjuk ke dokumentasi dan sumber daya tambahan dengan informasi atau contoh yang lebih rinci.

Pengantar

Amazon VPC menyediakan beberapa opsi konektivitas jaringan untuk Anda gunakan, tergantung pada desain dan persyaratan jaringan Anda saat ini. Opsi konektivitas ini termasuk menggunakan internet atau AWS Direct Connect koneksi sebagai tulang punggung jaringan dan mengakhiri koneksi ke AWS atau titik akhir jaringan yang dikelola pengguna. Selain itu, dengan AWS, Anda dapat memilih cara perutean jaringan dikirimkan antara Amazon VPC dan jaringan Anda, memanfaatkan layanan AWS atau peralatan dan rute jaringan yang dikelola pengguna. Whitepaper ini mempertimbangkan opsi berikut dengan ikhtisar dan perbandingan tingkat tinggi masing-masing:

- Network-to-Amazon Opsi konektivitas VPC
  - AWS Site-to-Site VPN — Menjelaskan pembuatan koneksi IPsec VPN terkelola dari peralatan jaringan Anda di jaringan jarak jauh ke Amazon VPC.
  - AWS Transit Gateway + AWS Site-to-Site VPN — Menjelaskan pembuatan koneksi IPsec VPN terkelola dari peralatan jaringan Anda di jaringan jarak jauh ke hub jaringan regional untuk Amazon VPCs, menggunakan AWS Transit Gateway.
  - AWS Direct Connect- Menjelaskan membangun koneksi pribadi dan logis dari jaringan jarak jauh Anda ke Amazon VPC, menggunakan. AWS Direct Connect
  - AWS Direct Connect + AWS Transit Gateway— Menjelaskan membangun koneksi pribadi dan logis dari jaringan jarak jauh Anda ke hub jaringan regional untuk Amazon VPCs, menggunakan AWS Direct Connect dan AWS Transit Gateway.
  - AWS Direct Connect + AWS Site-to-Site VPN — Menjelaskan pembuatan koneksi pribadi dan terenkripsi dari jaringan jarak jauh Anda ke Amazon VPC, menggunakan dan Direct Connect AWS VPN. Site-to-Site
  - AWS Direct Connect AWS Transit Gateway + AWS Site-to-Site VPN— Menjelaskan pembuatan koneksi pribadi dan terenkripsi dari jaringan jarak jauh Anda ke hub jaringan regional untuk Amazon VPCs, menggunakan Direct Connect dan. AWS Transit Gateway
  - Site-to-Site VPN CloudHub— Menjelaskan pembuatan hub-and-spoke model untuk menghubungkan kantor cabang jarak jauh.
  - Perangkat Lunak VPN— Menjelaskan membuat koneksi VPN dari peralatan Anda di jaringan jarak jauh ke perangkat lunak VPN yang dikelola pengguna yang berjalan di dalam VPC Amazon.
  - AWS Transit Gateway + Solusi SD-WAN- Menjelaskan integrasi solusi jaringan area luas yang ditentukan perangkat lunak (SD-WAN) untuk menghubungkan beberapa lokasi terpencil ke

hub jaringan regional untuk Amazon VPCs, menggunakan AWS tulang punggung atau internet sebagai jaringan transit.

- Opsi VPC-to-Amazon konektivitas Amazon VPC
  - Peering VPC— Menjelaskan menghubungkan Amazon di VPCs dalam dan di seluruh wilayah menggunakan fitur peering VPC Amazon.
  - AWS Transit Gateway— Menjelaskan menghubungkan Amazon di VPCs dalam dan di seluruh wilayah menggunakan AWS Transit Gateway dalam hub-and-spoke model.
  - AWS PrivateLink— Menjelaskan menghubungkan Amazon VPCs dengan titik akhir antarmuka VPC dan layanan titik akhir VPC.
  - Perangkat Lunak VPN— Menjelaskan menghubungkan Amazon VPCs menggunakan koneksi VPN yang dibuat antara perangkat lunak VPN yang dikelola pengguna yang berjalan di dalam setiap VPC Amazon.
  - Perangkat Lunak VPN-to-AWS Site-to-Site VPN— Menjelaskan menghubungkan Amazon VPCs dengan koneksi VPN yang dibuat antara perangkat lunak VPN yang dikelola pengguna di satu VPC Amazon dan AWS Site-to-Site VPN yang terpasang ke VPC Amazon lainnya.
- Opsi konektivitas access-to-Amazon VPC jarak jauh perangkat lunak
  - AWS Client VPN— Menjelaskan menghubungkan akses jarak jauh perangkat lunak ke Amazon VPC, memanfaatkan AWS Client VPN.
  - Perangkat lunak klien VPN— Menjelaskan menghubungkan akses jarak jauh perangkat lunak ke Amazon VPC, memanfaatkan peralatan VPN perangkat lunak yang dikelola pengguna.
- Transit VPC- Menjelaskan membangun jaringan transit global di AWS menggunakan VPN perangkat lunak bersama dengan VPN yang dikelola AWS.
- AWS Cloud WAN- Menjelaskan pembentukan jaringan area luas terkelola (WAN) untuk dengan mudah membangun, mengelola, dan memantau interkoneksi global antara sumber daya di Amazon VPCs, pusat data, dan cabang jarak jauh.

Network-to-Amazon Opsi konektivitas VPC

Bagian ini menyediakan pola desain untuk menghubungkan jaringan jarak jauh dengan lingkungan Amazon VPC Anda. Opsi ini berguna untuk mengintegrasikan sumber daya AWS dengan layanan di tempat Anda yang ada (misalnya, pemantauan, otentikasi, keamanan, data, atau sistem lainnya) dengan memperluas jaringan internal Anda ke AWS Cloud. Ekstensi jaringan ini juga memungkinkan pengguna internal Anda untuk terhubung dengan mulus ke sumber daya yang dihosting di AWS seperti sumber daya internal lainnya.

Konektivitas VPC ke jaringan pelanggan jarak jauh paling baik dicapai saat menggunakan rentang IP yang tidak tumpang tindih untuk setiap jaringan yang terhubung. Misalnya, jika Anda ingin menghubungkan satu atau lebih VPCs ke jaringan perusahaan Anda, pastikan mereka dikonfigurasi dengan rentang Classless Inter-Domain Routing (CIDR) yang unik. Kami merekomendasikan untuk mengalokasikan satu blok CIDR yang berdekatan, tidak tumpang tindih untuk digunakan oleh setiap VPC. Untuk informasi tambahan tentang perutean dan kendala Amazon VPC, lihat Pertanyaan yang Sering Diajukan VPC Amazon.

Opsi	Kasus Penggunaan	Keuntungan	Batasan
AWS Site-to-Site VPN	AWS mengelola koneksi IPsec VPN melalui internet ke VPC individual	Gunakan kembali peralatan dan proses VPN yang ada Gunakan kembali koneksi internet yang ada AWS mengelola layanan VPN ketersediaan tinggi Mendukung rute statis atau kebijakan peering dan routing Border Gateway Protocol (BGP) dinamis	Latensi jaringan, variabilitas, dan ketersediaan tergantung pada kondisi internet Anda bertanggung jawab untuk menerapkan redundansi dan failover (jika diperlukan) Perangkat jarak jauh harus mendukung BGP single-hop (saat memanfaatkan

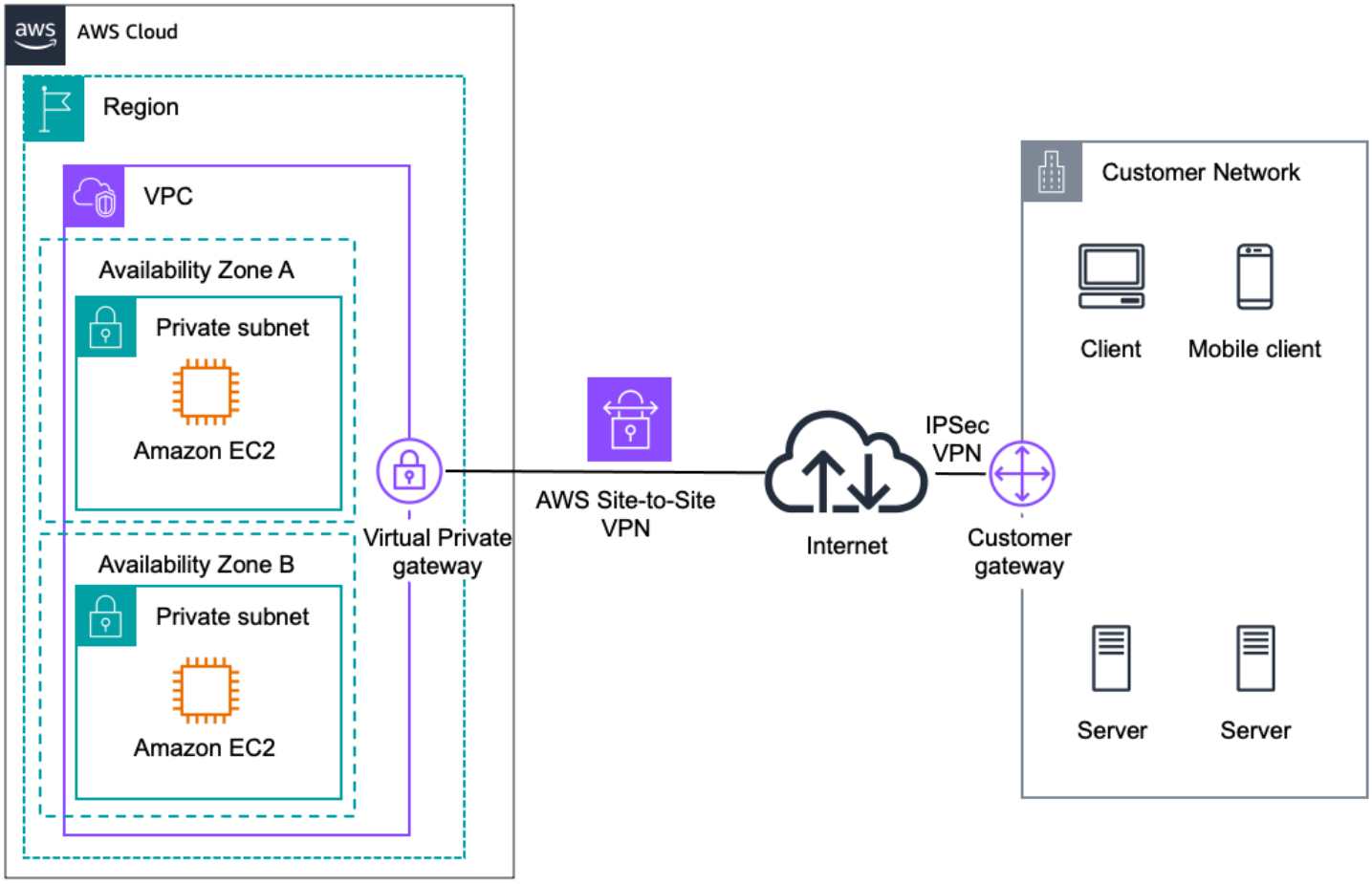
Opsi	Kasus Penggunaan	Keuntungan	Batasan
			BGP untuk perutean dinamis)
AWS Transit Gateway + AWS Site-to-Site VPN	AWS mengelola koneksi IPsec VPN melalui internet ke router regional untuk beberapa VPCs	Sama seperti opsi sebelumnya AWS mengelola hub jaringan regional ketersediaan dan skalabilitas tinggi hingga 5.000 lampiran	Sama seperti opsi sebelumnya
AWS Direct Connect	Koneksi jaringan khusus melalui jalur pribadi	Kinerja jaringan yang lebih dapat diprediksi Mengurangi biaya bandwidth Mendukung kebijakan peering dan routing BGP	Mungkin memerlukan hubungan penyedia telekomunikasi dan hosting tambahan atau sirkuit jaringan baru untuk disediakan
AWS Direct Connect + AWS Transit Gateway	Koneksi jaringan khusus melalui jalur pribadi ke router regional untuk beberapa VPCs	Sama seperti opsi sebelumnya AWS mengelola hub jaringan regional ketersediaan dan skalabilitas tinggi hingga 5.000 lampiran	Sama seperti opsi sebelumnya

Opsi	Kasus Penggunaan	Keuntungan	Batasan
AWS Direct Connect + AWS Site-to-Site VPN	IPsec Koneksi VPN melalui jalur pribadi	Kinerja jaringan yang lebih dapat diprediksi Mengurangi biaya bandwidth Mendukung kebijakan peering dan routing BGP pada AWS Direct Connect Gunakan kembali peralatan dan proses VPN yang ada AWS mengelola layanan VPN ketersediaan tinggi Mendukung rute statis atau kebijakan peering dan routing Border Gateway Protocol (BGP) dinamis pada koneksi VPN	Mungkin memerlukan hubungan penyedia telekomunikasi dan hosting tambahan atau sirkuit jaringan baru untuk disediakan Anda bertanggung jawab untuk menerapkan redundansi dan failover (jika diperlukan) Perangkat jarak jauh harus mendukung BGP single-hop (saat memanfaatkan BGP untuk perutean dinamis)
AWS Direct Connect AWS Transit Gateway + AWS Site-to-Site VPN	IPsec Koneksi VPN melalui jalur pribadi ke router regional untuk beberapa VPCs	Sama seperti opsi sebelumnya AWS mengelola hub jaringan regional ketersediaan dan skalabilitas tinggi hingga 5.000 lampiran	Sama seperti opsi sebelumnya

Opsi	Kasus Penggunaan	Keuntungan	Batasan
Site-to-Site VPN CloudHub	Connect kantor cabang jarak jauh dalam hub-and-spoke model untuk konektivitas primer atau cadangan	Gunakan kembali koneksi dan Site-to-Site VPN koneksi internet yang ada AWS mengelola layanan VPN ketersediaan tinggi Mendukung BGP untuk bertukar rute dan prioritas routing	Latensi jaringan, variabilitas, dan ketersediaan tergantung pada internet Endpoint kantor cabang yang dikelola pengguna bertanggung jawab untuk menerapkan redundansi dan failover (jika diperlukan)
AWS Transit Gateway + Solusi SD-WAN	Connect cabang dan kantor jarak jauh dengan jaringan area luas yang ditentukan perangkat lunak dengan menggunakan AWS backbone atau internet sebagai jaringan transit.	Mendukung beragam vendor, produk, dan protokol SD-WAN Beberapa solusi vendor memiliki integrasi dengan layanan asli AWS.	Anda bertanggung jawab untuk menerapkan HA (ketersediaan tinggi) peralatan SD-WAN jika ditempatkan di VPC Amazon.
Perangkat Lunak VPN	Koneksi VPN berbasis perangkat lunak melalui internet	Mendukung beragam vendor, produk, dan protokol VPN Solusi yang dikelola pelanggan sepenuhnya	Anda bertanggung jawab untuk menerapkan solusi HA (ketersediaan tinggi) untuk semua titik akhir VPN (jika diperlukan)

AWS Site-to-Site VPN

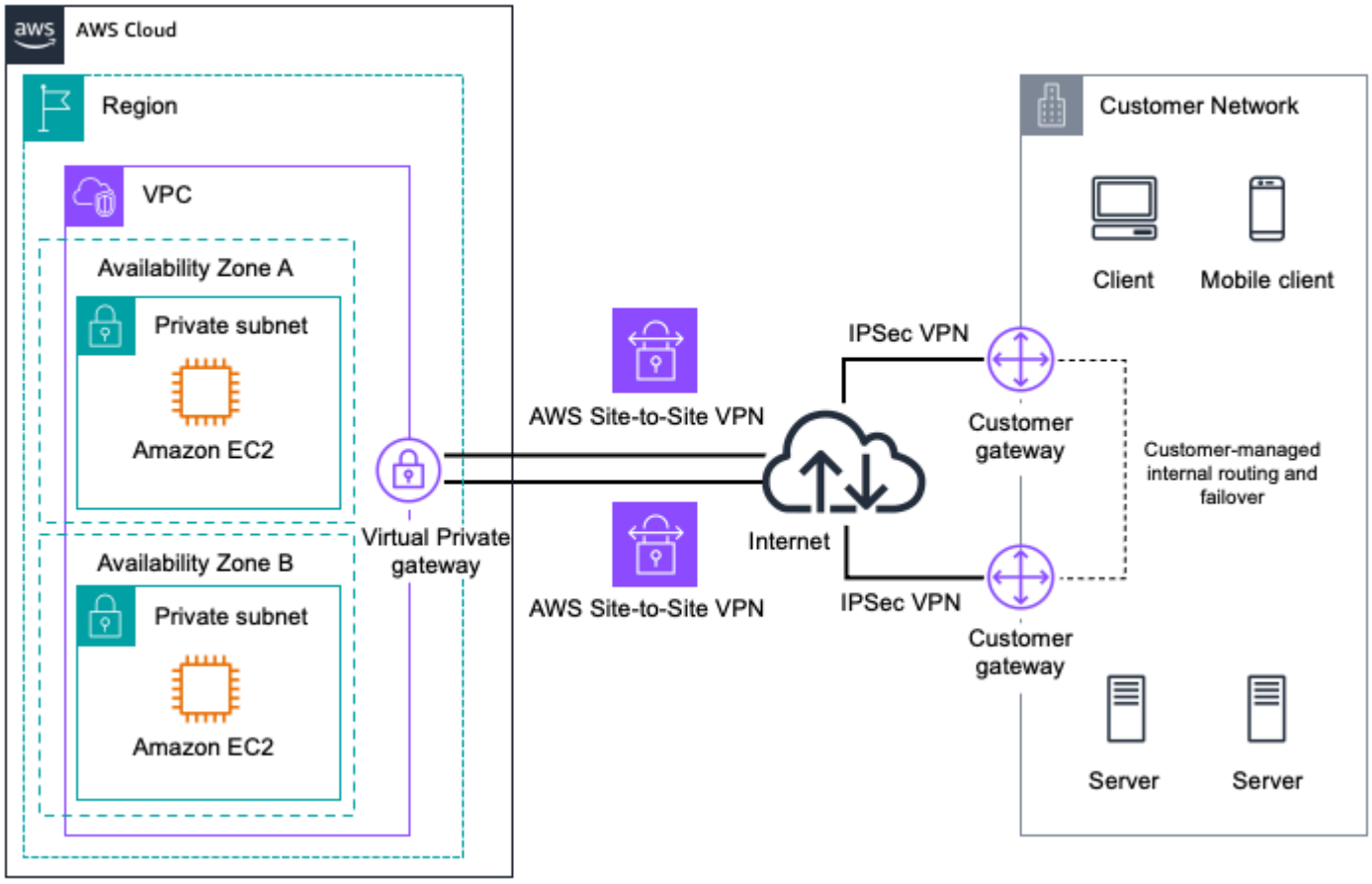
Amazon VPC menyediakan opsi untuk membuat koneksi IPsec VPN antara jaringan jarak jauh Anda dan Amazon VPC melalui internet, seperti yang ditunjukkan pada gambar berikut.



AWS Managed VPN

Pertimbangkan untuk mengambil pendekatan ini ketika Anda ingin memanfaatkan titik akhir VPN yang dikelola AWS yang mencakup redundansi otomatis dan failover yang terpasang di sisi AWS koneksi VPN.

Gateway pribadi virtual juga mendukung dan mendorong beberapa koneksi gateway pengguna sehingga Anda dapat menerapkan redundansi dan failover di sisi koneksi VPN Anda, seperti yang ditunjukkan pada gambar berikut.



Redundant AWS Site-to-Site VPN Connections

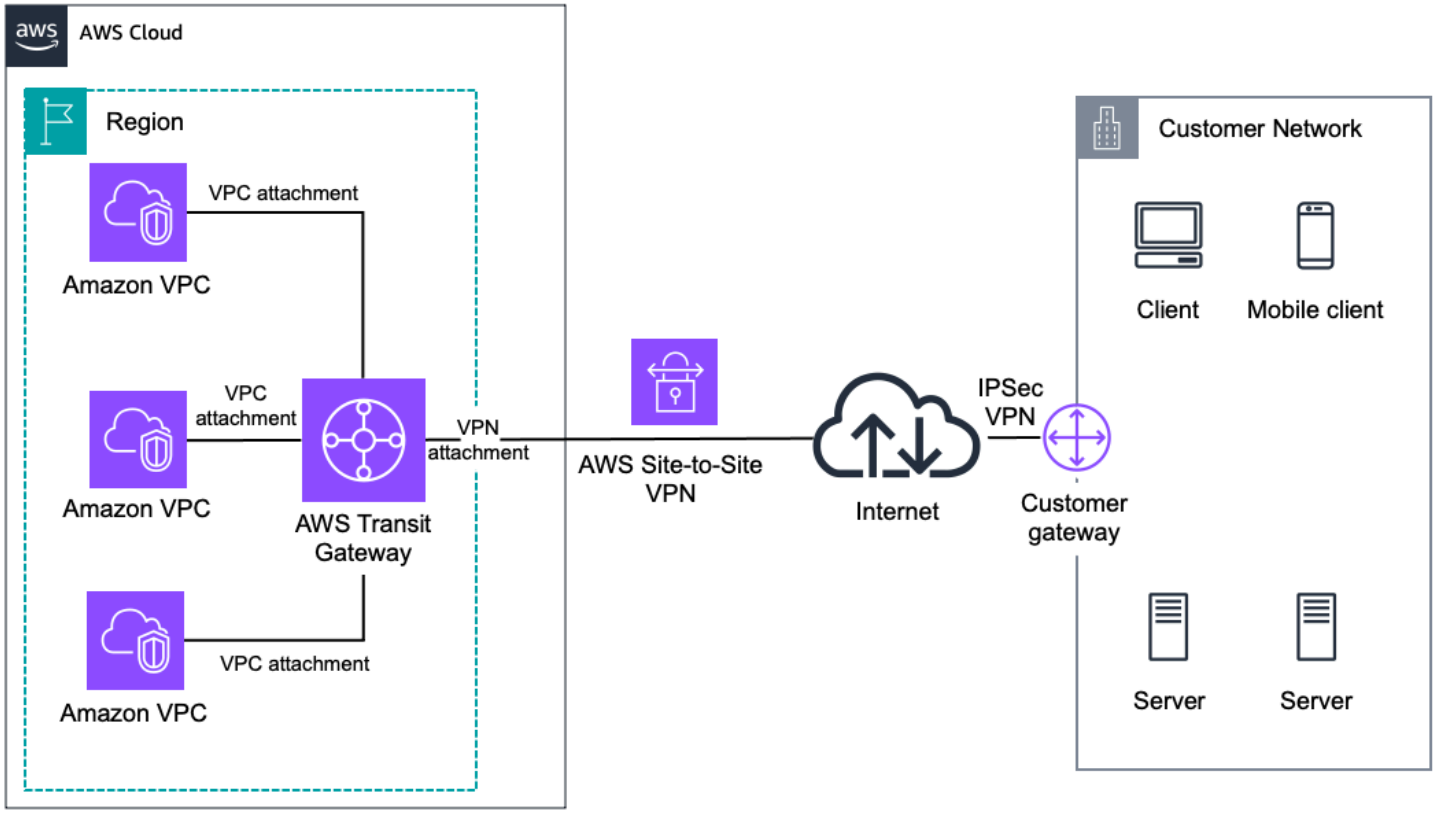
Opsi perutean dinamis dan statis disediakan untuk memberi Anda fleksibilitas dalam konfigurasi perutean Anda. Perutean dinamis menggunakan peering BGP untuk bertukar informasi perutean antara AWS dan titik akhir jarak jauh ini. Dengan perutean dinamis, Anda juga dapat menentukan prioritas perutean, kebijakan, dan bobot (metrik) dalam iklan BGP Anda dan memengaruhi jalur jaringan antara jaringan Anda dan AWS. Penting untuk dicatat bahwa ketika Anda menggunakan BGP, sesi BGP IPsec dan BGP harus dihentikan pada perangkat gateway pengguna yang sama, sehingga harus mampu menghentikan sesi keduanya dan BGP. IPsec

Sumber daya tambahan

- Panduan Pengguna AWS Site-to-Site VPN
- Persyaratan untuk perangkat gateway pelanggan
- Perangkat gateway pelanggan diuji dengan Amazon VPC

AWS Transit Gateway + AWS Site-to-Site VPN

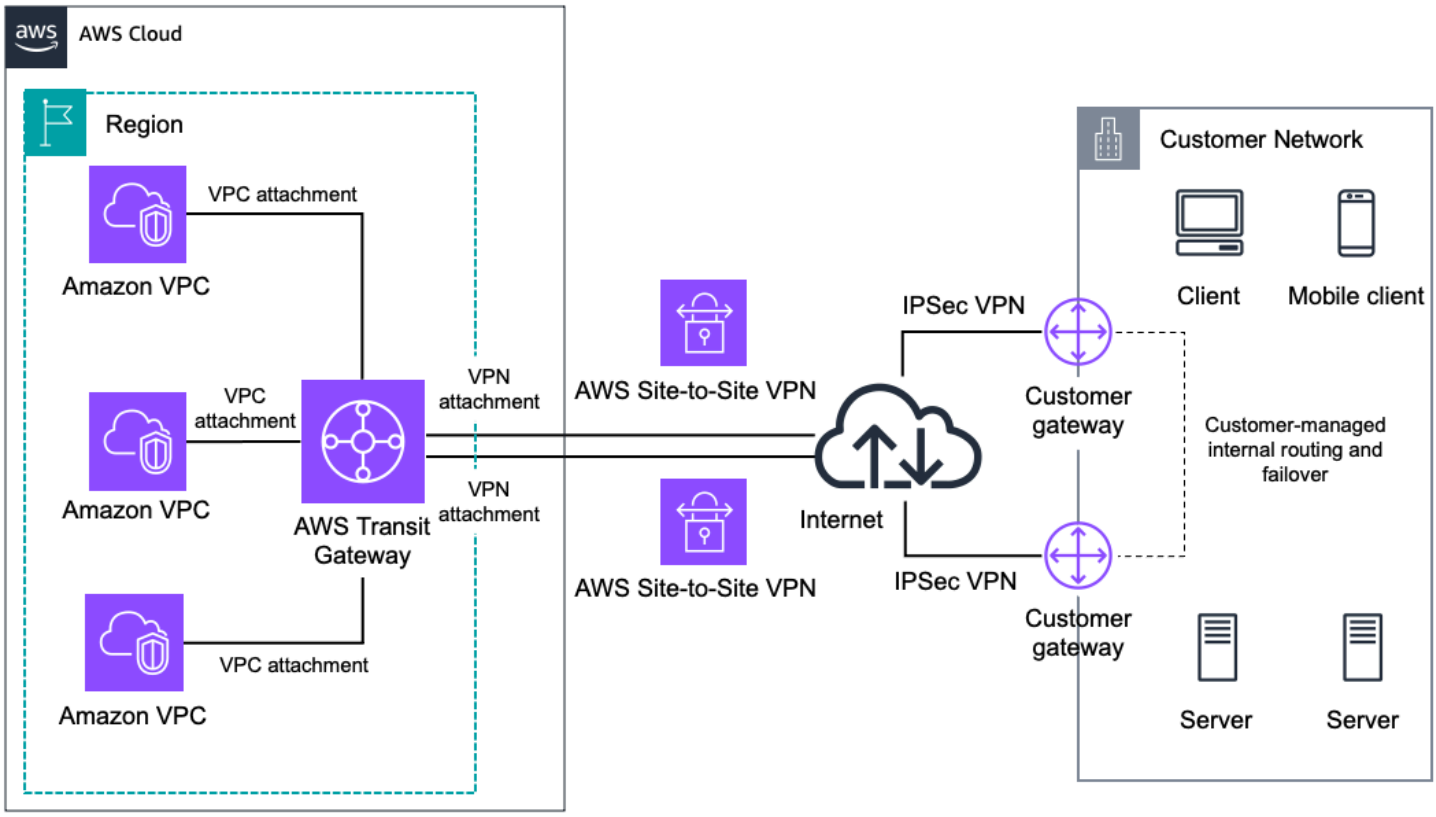
AWS Transit Gateway adalah hub transit jaringan regional dengan ketersediaan tinggi dan skalabilitas AWS yang digunakan untuk interkoneksi VPCs dan jaringan pelanggan. AWS Transit Gateway + VPN, menggunakan lampiran Transit Gateway VPN, menyediakan opsi untuk membuat koneksi IPsec VPN antara jaringan jarak jauh Anda dan Gateway Transit melalui internet, seperti yang ditunjukkan pada gambar berikut.



AWS Transit Gateway and AWS Site-to-Site VPN

Pertimbangkan untuk menggunakan pendekatan ini ketika Anda ingin memanfaatkan titik akhir VPN yang dikelola AWS untuk menghubungkan ke beberapa VPCs di wilayah yang sama tanpa biaya tambahan dan pengelolaan beberapa koneksi IPsec VPN ke beberapa Amazon. VPCs

AWS Transit Gateway juga mendukung dan mendorong beberapa koneksi gateway pengguna sehingga Anda dapat menerapkan redundansi dan failover di sisi koneksi VPN Anda seperti yang ditunjukkan pada gambar berikut.



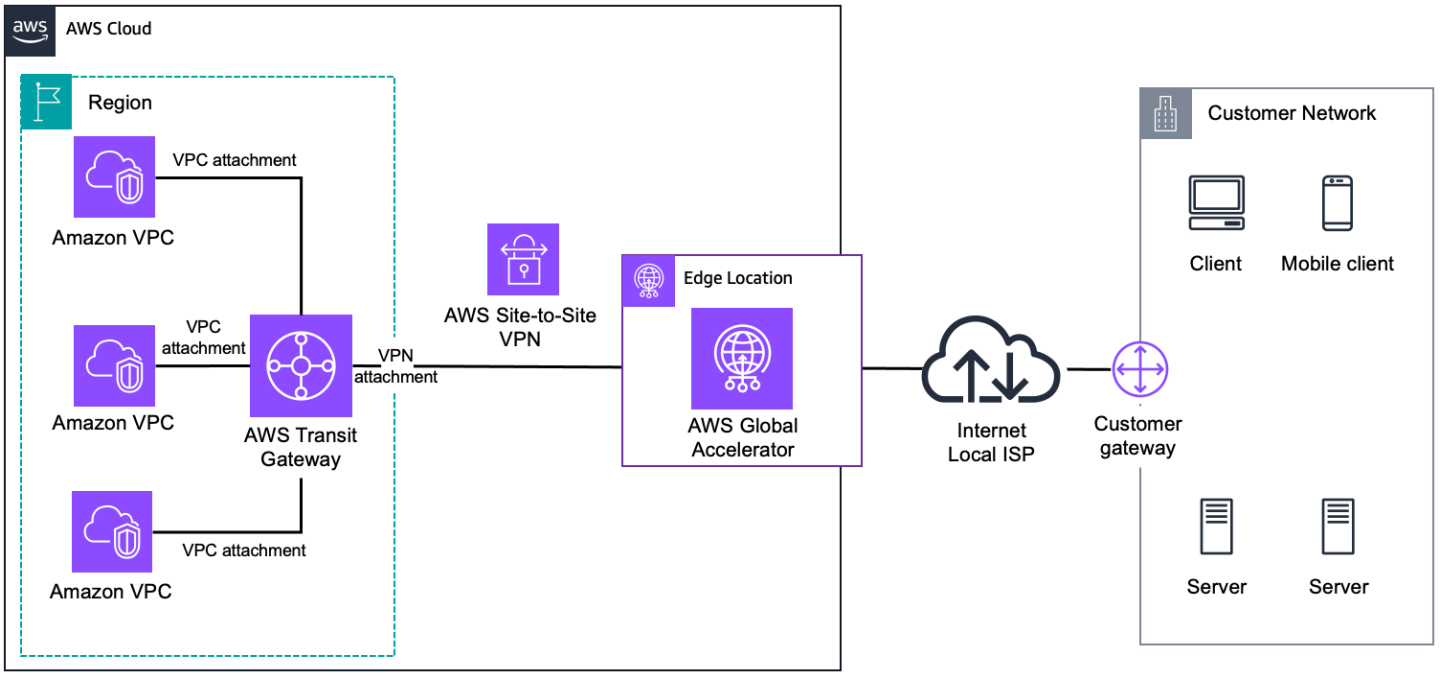
AWS Transit Gateway and Redundant VPN

Opsi perutean dinamis dan statis disediakan untuk memberi Anda fleksibilitas dalam konfigurasi perutean Anda pada lampiran VPN IPsec Transit Gateway. Perutean dinamis menggunakan peering BGP untuk bertukar informasi perutean antara AWS dan titik akhir jarak jauh ini. Dengan perutean dinamis, Anda juga dapat menentukan prioritas perutean, kebijakan, dan bobot (metrik) dalam iklan BGP Anda dan memengaruhi jalur jaringan antara jaringan Anda dan AWS. Penting untuk dicatat bahwa ketika Anda menggunakan BGP, sesi BGP IPsec dan BGP harus dihentikan pada perangkat gateway pengguna yang sama, sehingga harus mampu menghentikan sesi keduanya dan BGP. IPsec

Per koneksi VPN, Anda dapat mencapai 1,25 Gbps throughput dan 140.000 paket per detik. Saat mengakhiri koneksi VPN di Transit Gateway, Anda dapat menggunakan perutean Equal Cost Multi-Path (ECMP) untuk mendapatkan bandwidth VPN yang lebih tinggi dengan menggabungkan beberapa terowongan VPN. Untuk menggunakan ECMP, Anda perlu mengonfigurasi perutean dinamis dalam koneksi VPN — ECMP tidak didukung menggunakan perutean statis.

Selain itu, Anda dapat mengaktifkan akselerasi dalam koneksi AWS Site-to-Site VPN Anda. Koneksi VPN yang dipercepat menggunakan AWS Global Accelerator untuk merutekan lalu lintas dari jaringan Anda ke lokasi AWS edge yang paling dekat dengan perangkat gateway pelanggan Anda.

Anda dapat menggunakan opsi ini untuk menghindari gangguan jaringan yang mungkin terjadi ketika lalu lintas dialihkan melalui internet publik. Akselerasi hanya didukung untuk koneksi VPN yang terpasang ke Transit Gateway, seperti yang ditunjukkan pada gambar berikut:



Accelerated AWS Site-to-Site VPN

Terakhir, mengenai pengalamatan IP, koneksi Site-to-Site VPN pada AWS Transit Gateway dukungan keduanya IPv4 dan IPv6 lalu lintas. Aturan-aturan berikut berlaku:

- IPv6 hanya didukung untuk alamat IP bagian dalam terowongan VPN. Alamat IP luar untuk AWS titik akhir adalah IPv4 alamat publik. Alamat IP gateway pelanggan harus berupa IPv4 alamat publik.
- Koneksi Site-to-Site VPN tidak dapat mendukung keduanya IPv4 dan IPv6 lalu lintas. Jika konektivitas hybrid Anda memerlukan komunikasi dual-stack, Anda harus membuat terowongan VPN yang berbeda untuk lalu lintas dan lalu lintas. IPv4 IPv6

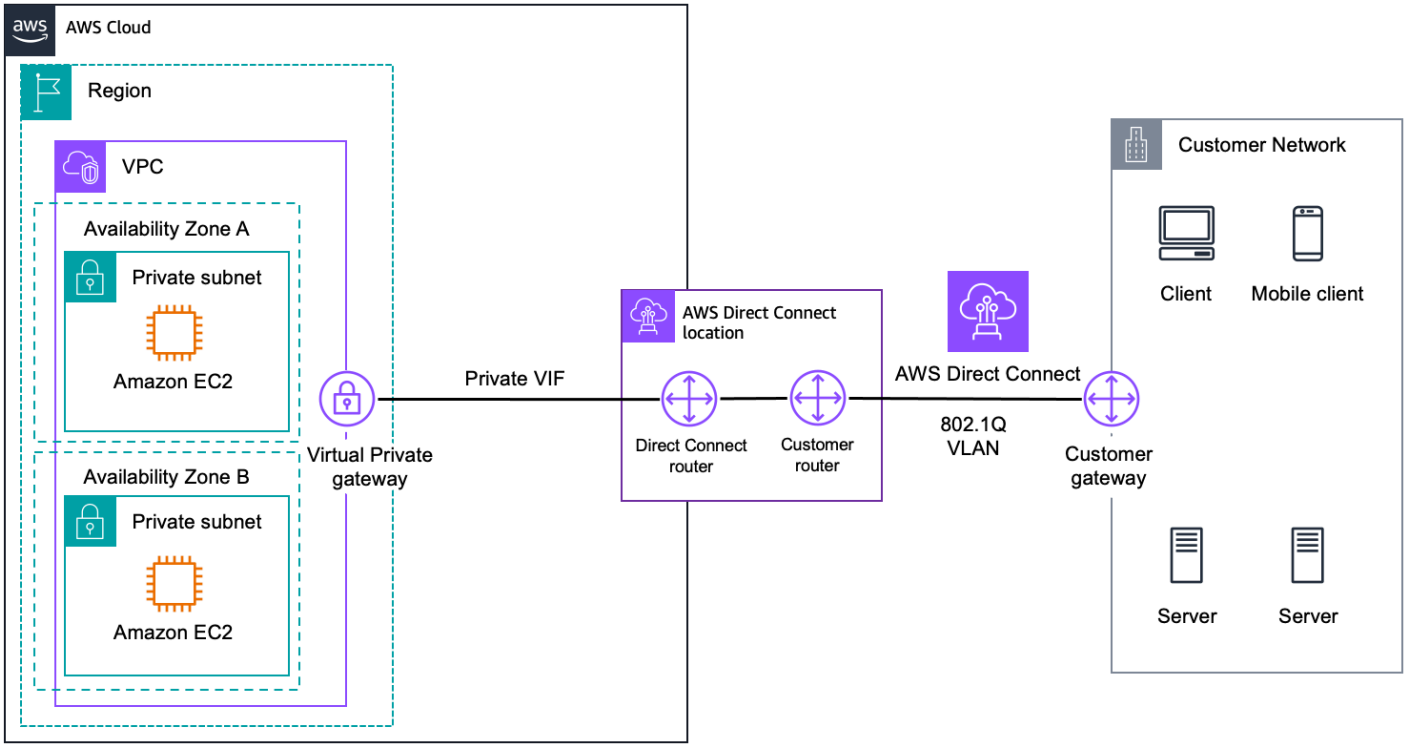
Sumber daya tambahan

- Lampiran Transit gateway VPN
- Gateway pelanggan
- Bekerja dengan Site-to-Site VPN
- Koneksi Site-to-Site VPN yang dipercepat

AWS Direct Connect

AWS Direct Connectmembuatnya mudah untuk membuat koneksi khusus dari jaringan lokal ke satu atau lebih VPCs. Direct Connect Dapat mengurangi biaya jaringan, meningkatkan throughput bandwidth, dan memberikan pengalaman jaringan yang lebih konsisten daripada koneksi berbasis internet. Ini menggunakan 802.1Q standar industri untuk terhubung VLANs ke Amazon VPC menggunakan alamat IP pribadi. VLANs Ini dikonfigurasi menggunakan antarmuka virtual (VIFs), dan Anda dapat mengonfigurasi tiga jenis VIFs:

- Antarmuka virtual publik - Membangun konektivitas antara titik akhir AWS publik dan pusat data, kantor, atau lingkungan colocation Anda.
- Antarmuka virtual transit - Membangun konektivitas pribadi antara AWS Transit Gateway dan pusat data, kantor, atau lingkungan colocation Anda. Opsi konektivitas ini tercakup dalam bagian???.
- Antarmuka virtual pribadi - Membangun konektivitas pribadi antara sumber daya Amazon VPC dan pusat data, kantor, atau lingkungan colocation Anda. Penggunaan pribadi VIFs ditunjukkan pada gambar berikut.



AWS Direct Connect

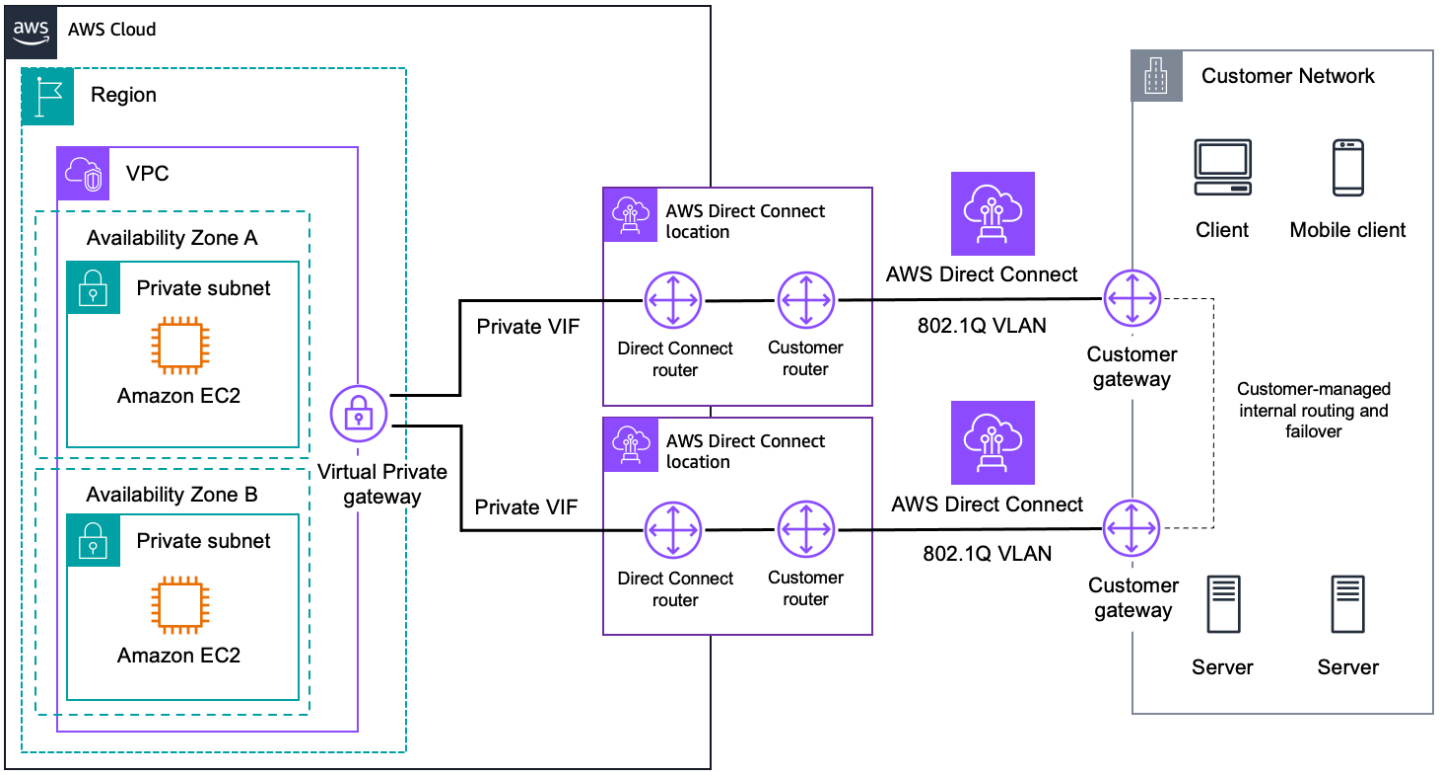
Anda dapat membangun konektivitas ke AWS tulang punggung menggunakan AWS Direct Connect dengan membuat sambungan silang ke AWS perangkat di lokasi Direct Connect. Anda dapat mengakses AWS Wilayah mana pun dari salah satu lokasi Direct Connect kami (kecuali Tiongkok). Jika Anda tidak memiliki peralatan di suatu lokasi, Anda dapat memilih dari ekosistem penyedia layanan WAN untuk mengintegrasikan AWS Direct Connect titik akhir Anda di AWS Direct Connect lokasi dengan jaringan jarak jauh Anda.

Dengan AWS Direct Connect, Anda memiliki dua jenis koneksi:

- Koneksi khusus, di mana koneksi ethernet fisik dikaitkan dengan satu pelanggan. Anda dapat memesan kecepatan port 1, 10, atau 100 Gbps. Anda mungkin perlu bekerja dengan mitra dalam Program AWS Direct Connect Mitra untuk membantu Anda membangun sirkuit jaringan antara AWS Direct Connect koneksi dan pusat data, kantor, atau lingkungan colocation Anda.
- Koneksi yang di-host, di mana koneksi ethernet fisik disediakan oleh AWS Direct Connect Mitra dan dibagikan dengan Anda. Anda dapat memesan kecepatan port antara 50 Mbps dan 10 Gbps. Pekerjaan Anda dengan Mitra dalam Direct Connect koneksi yang mereka buat dan sirkuit jaringan antara AWS Direct Connect koneksi dan pusat data, kantor, atau lingkungan colocation Anda.

Untuk koneksi khusus, Anda juga dapat menggunakan grup agregasi tautan (LAG) untuk menggabungkan beberapa koneksi pada satu AWS Direct Connect titik akhir. Anda memperlakukan mereka sebagai koneksi tunggal yang terkelola. Anda dapat menggabungkan hingga empat koneksi 1- atau 10-Gbps, dan hingga dua koneksi 100-Gbps.

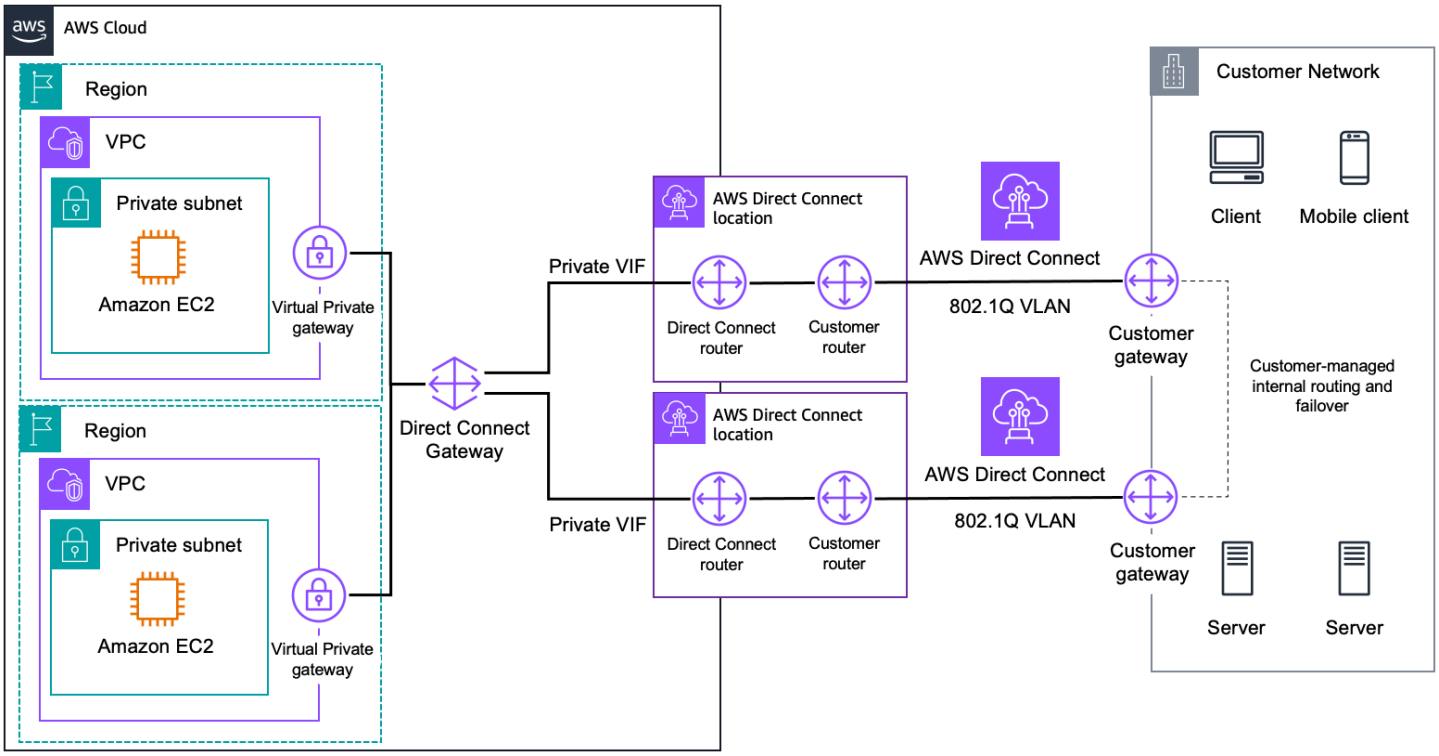
Saat membahas ketersediaan tinggi di AWS Direct Connect, kami sarankan untuk menggunakan Direct Connect koneksi tambahan. The Direct Connect Resiliency Toolkit menawarkan panduan dalam membangun koneksi jaringan yang sangat tangguh antara AWS dan pusat data, kantor, atau lingkungan colocation Anda. Gambar berikut menunjukkan contoh opsi konektivitas ketahanan tinggi, dengan dua Direct Connect koneksi diakhiri di dua lokasi berbeda. Direct Connect



Redundan AWS Direct Connect

AWS Direct Connect tidak dienkripsi secara default. Untuk koneksi khusus 10 atau 100 Gbps, Anda dapat menggunakan MAC security (MACsec) sebagai opsi enkripsi. Untuk koneksi 1 Gbps atau kurang, Anda dapat membuat terowongan VPN di atas koneksi — opsi ini tercakup dalam AWS Direct Connect + AWS Site-to-Site VPN dan AWS Direct Connect AWS Transit Gateway + AWS Site-to-Site VPN bagian.

Salah satu sumber daya penting AWS Direct Connect adalah gateway Direct Connect, yang merupakan sumber daya yang tersedia secara global untuk mengaktifkan koneksi ke beberapa Amazon VPCs atau Gateway Transit di berbagai Wilayah atau AWS akun. Sumber daya ini juga memungkinkan Anda untuk terhubung ke VPC atau Transit Gateway yang berpartisipasi dari satu VIF pribadi atau VIF transit, mengurangi AWS Direct Connect manajemen, seperti yang ditunjukkan pada gambar berikut.



AWS Direct Connect Gateway

Mengenai pengalamatan IP, antarmuka AWS Direct Connect virtual mendukung keduanya IPv4 dan sesi IPv6 BGP untuk operasi dual-stack.

- VIFs IPv4 Konfigurasi pribadi dan transit menggunakan IPv4 alamat atau alamat yang dibuat AWS yang dikonfigurasi oleh Anda. Untuk peering VIFs IPv4 BGP publik, Anda harus menentukan IPv4 CIDR /31 publik unik yang Anda miliki (atau mengirimkan permintaan agar blok CIDR ditetapkan).
- Untuk semua jenis peering VIFs IPv6 BGP, AWS menetapkan /125 CIDR, yang tidak dapat dikonfigurasi.

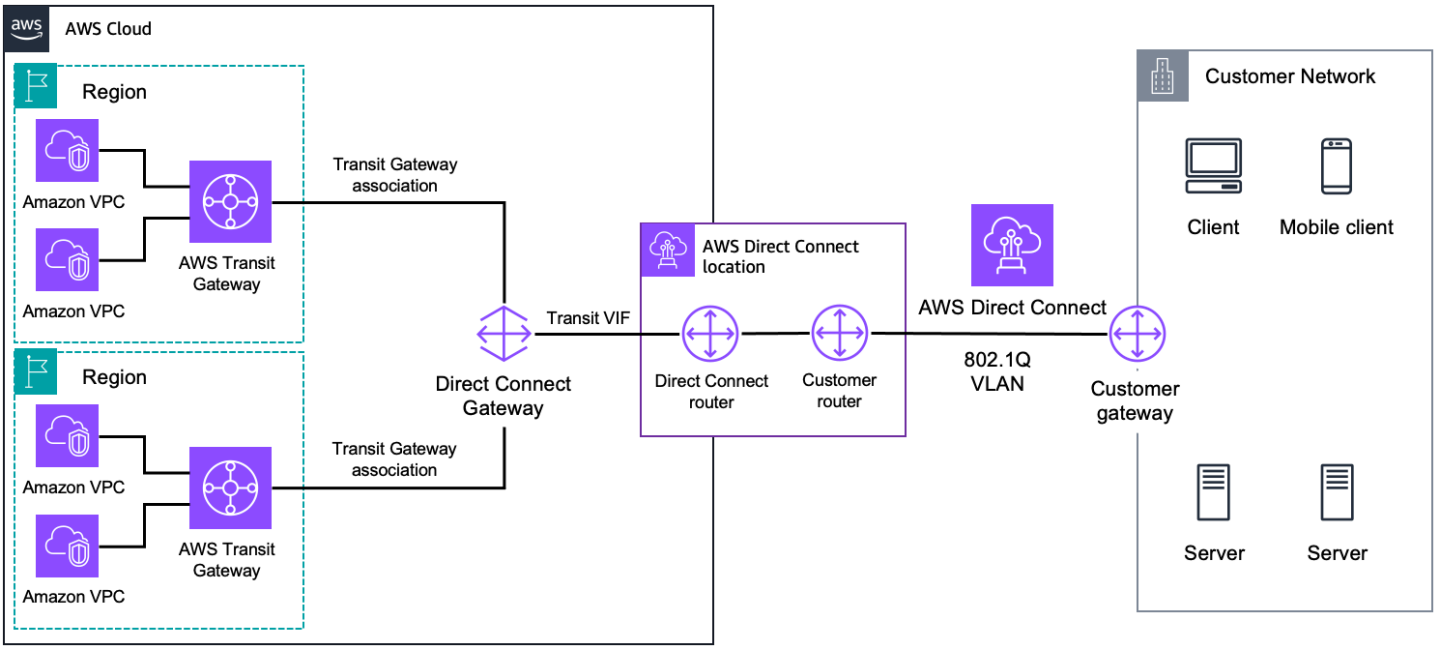
Sumber daya tambahan

- AWS Direct Connect Panduan Pengguna
- AWS Direct Connect antarmuka virtual
- AWS Direct Connect gerbang
- AWS Direct Connect Toolkit Ketahanan
- AWS Direct Connect Keamanan MAC
- AWS Direct Connect lokasi

- AWS Direct Connect Mitra Pengiriman

AWS Direct Connect + AWS Transit Gateway

AWS Direct Connect+ AWS Transit Gateway, menggunakan lampiran VIF transit ke gateway Direct Connect, memungkinkan jaringan Anda menghubungkan beberapa router terpusat regional melalui koneksi khusus pribadi. Diagram berikut menunjukkan menghubungkan ke dua router.



AWS Direct Connect and AWS Transit Gateway

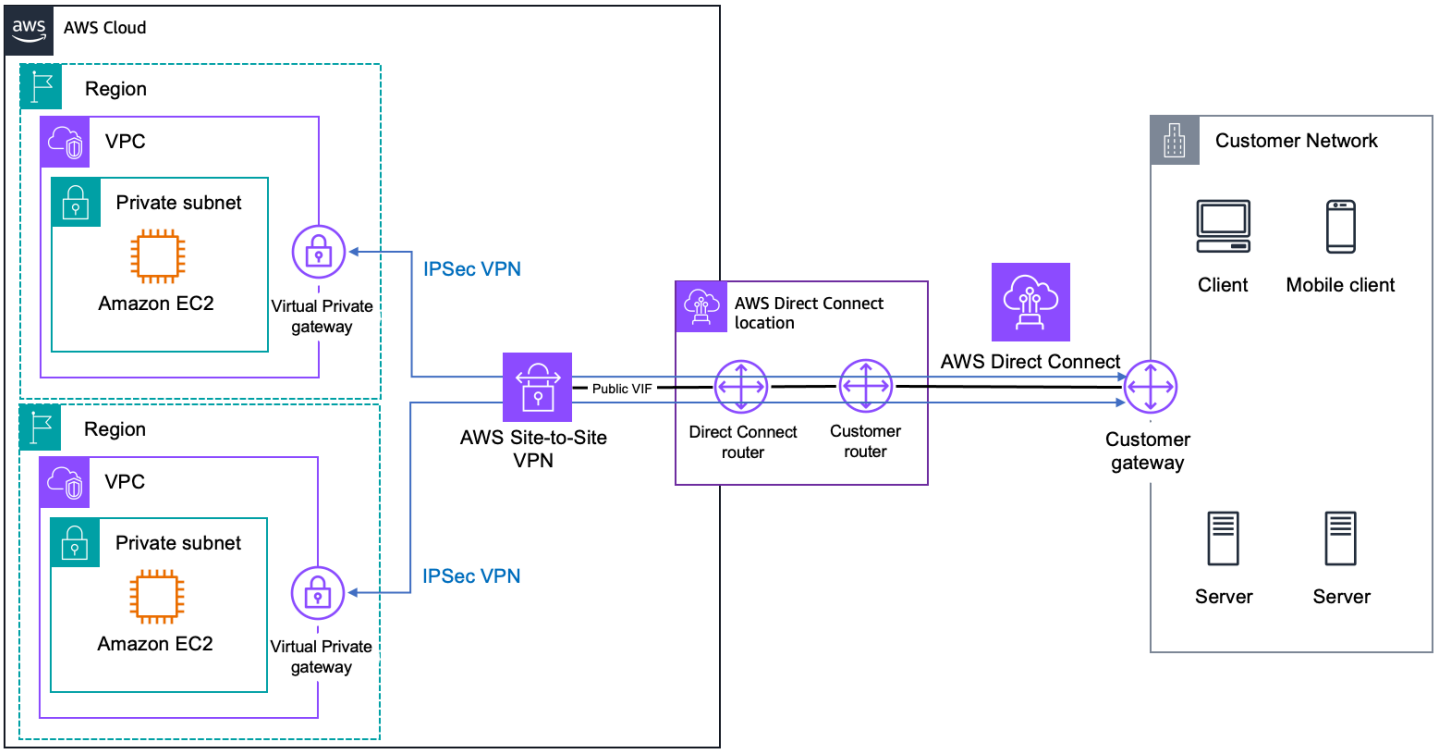
Masing-masing AWS Transit Gateway adalah hub transit jaringan untuk interkoneksi VPCs di wilayah yang sama, mengkonsolidasikan konfigurasi perutean Amazon VPC di satu tempat. Solusi ini menyederhanakan pengelolaan koneksi antara VPC Amazon dan jaringan Anda melalui koneksi pribadi yang dapat mengurangi biaya jaringan, meningkatkan throughput bandwidth, dan memberikan pengalaman jaringan yang lebih konsisten daripada koneksi berbasis internet.

Sumber daya tambahan

- Panduan Pengguna AWS Direct Connect
- Tautkan grup agregasi di AWS Direct Connect
- Posting blog: Mengintegrasikan koneksi host sub-1 Gbps dengan AWS Transit Gateway

AWS Direct Connect + AWS Site-to-Site VPN

Dengan AWS Direct Connect+ AWS Site-to-Site VPN, Anda dapat menggabungkan AWS Direct Connect koneksi dengan solusi VPN yang dikelola AWS. AWS Direct Connect public VIFs membuat koneksi jaringan khusus antara jaringan Anda dan sumber daya AWS publik seperti titik akhir AWS Site-to-Site VPN. Setelah Anda membuat koneksi ke layanan, Anda dapat membuat IPsec koneksi ke gateway pribadi virtual Amazon VPC yang sesuai. Gambar berikut menggambarkan opsi ini.



AWS Direct Connect and AWS Site-to-Site VPN

Solusi ini menggabungkan manfaat IPsec koneksi end-to-end aman dengan latensi rendah dan peningkatan bandwidth AWS Direct Connect untuk memberikan pengalaman jaringan yang lebih konsisten daripada koneksi VPN berbasis internet. Sesi koneksi BGP dibuat antara AWS Direct Connect dan router Anda di VIF publik. Sesi BGP lain atau rute statis akan dibuat antara gateway pribadi virtual dan router Anda di terowongan IPsec VPN.

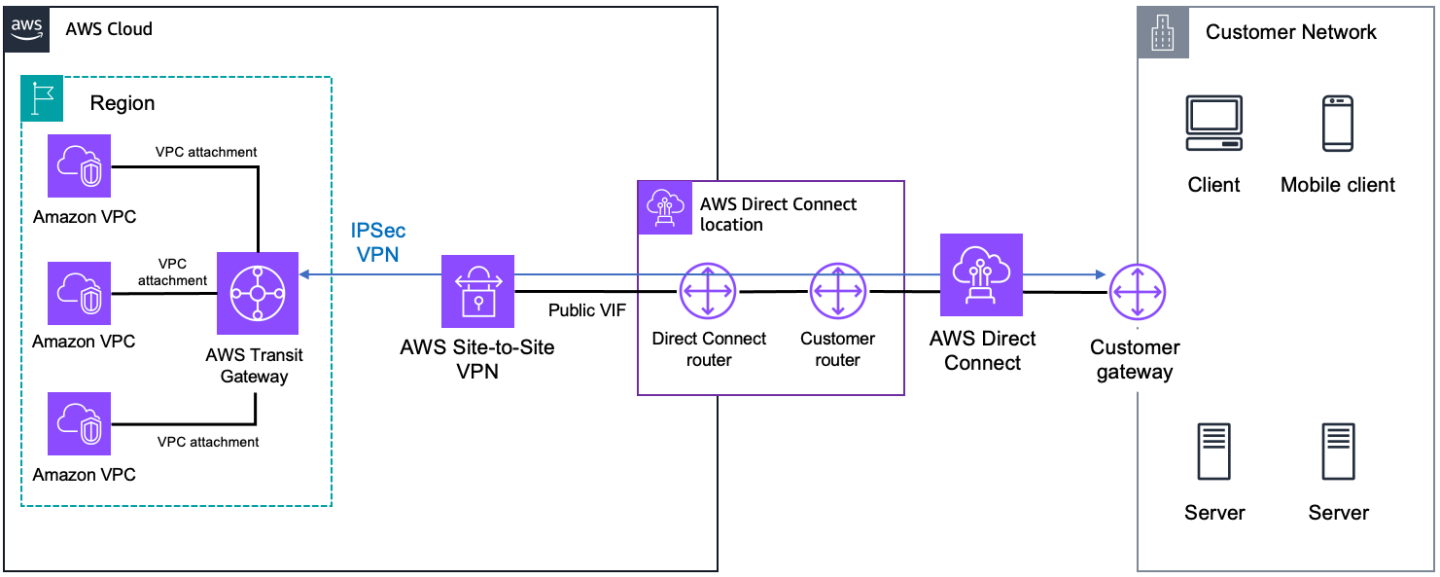
Sumber daya tambahan

- AWS Direct Connect
- AWS Direct Connect antarmuka virtual
- Panduan Pengguna AWS Site-to-Site VPN

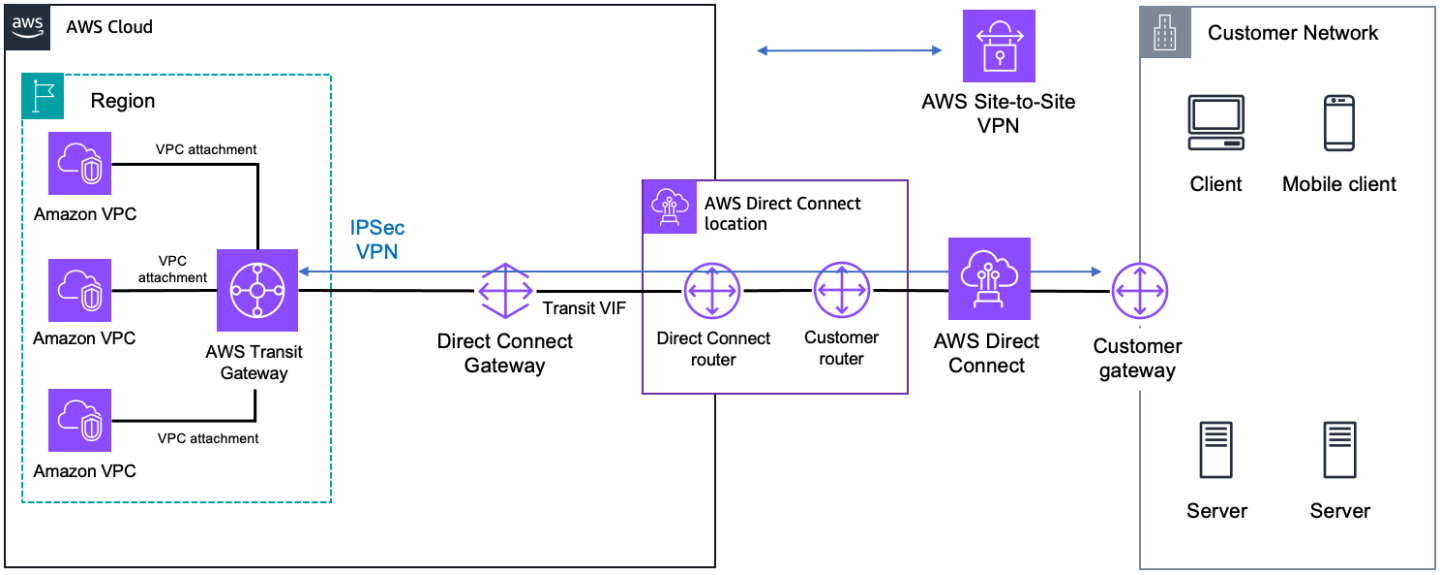
AWS Direct Connect AWS Transit Gateway + AWS Site-to-Site VPN

Dengan AWS Direct ConnectAWS Transit Gateway+AWS Site-to-Site VPN, Anda dapat mengaktifkan koneksi end-to-end IPsec terenkripsi antara jaringan Anda dan router terpusat regional untuk Amazon VPCs melalui koneksi khusus pribadi.

Anda dapat menggunakan AWS Direct Connect public VIFs untuk terlebih dahulu membuat koneksi jaringan khusus antara jaringan Anda ke sumber daya AWS publik, seperti titik akhir AWS Site-to-Site VPN. Setelah koneksi ini dibuat, Anda dapat membuat IPsec koneksi ke AWS Transit Gateway. Gambar berikut menggambarkan opsi ini.



AWS Direct Connect, AWS Transit Gateway, and AWS Site-to-Site VPN (public VIF)



AWS Direct Connect, AWS Transit Gateway, and AWS Site-to-Site VPN (transit VIF)

Pertimbangkan untuk mengambil pendekatan ini ketika Anda ingin menyederhanakan manajemen dan meminimalkan biaya koneksi IPsec VPN ke beberapa Amazon VPCs di wilayah yang sama, dengan latensi rendah dan pengalaman jaringan yang konsisten manfaat dari koneksi khusus pribadi melalui VPN berbasis internet. Sesi BGP dibuat antara AWS Direct Connect dan router Anda menggunakan VIF publik atau transit. Sesi BGP lain atau rute statis akan dibuat antara AWS Transit Gateway dan router Anda di terowongan IPsec VPN.

Sumber daya tambahan

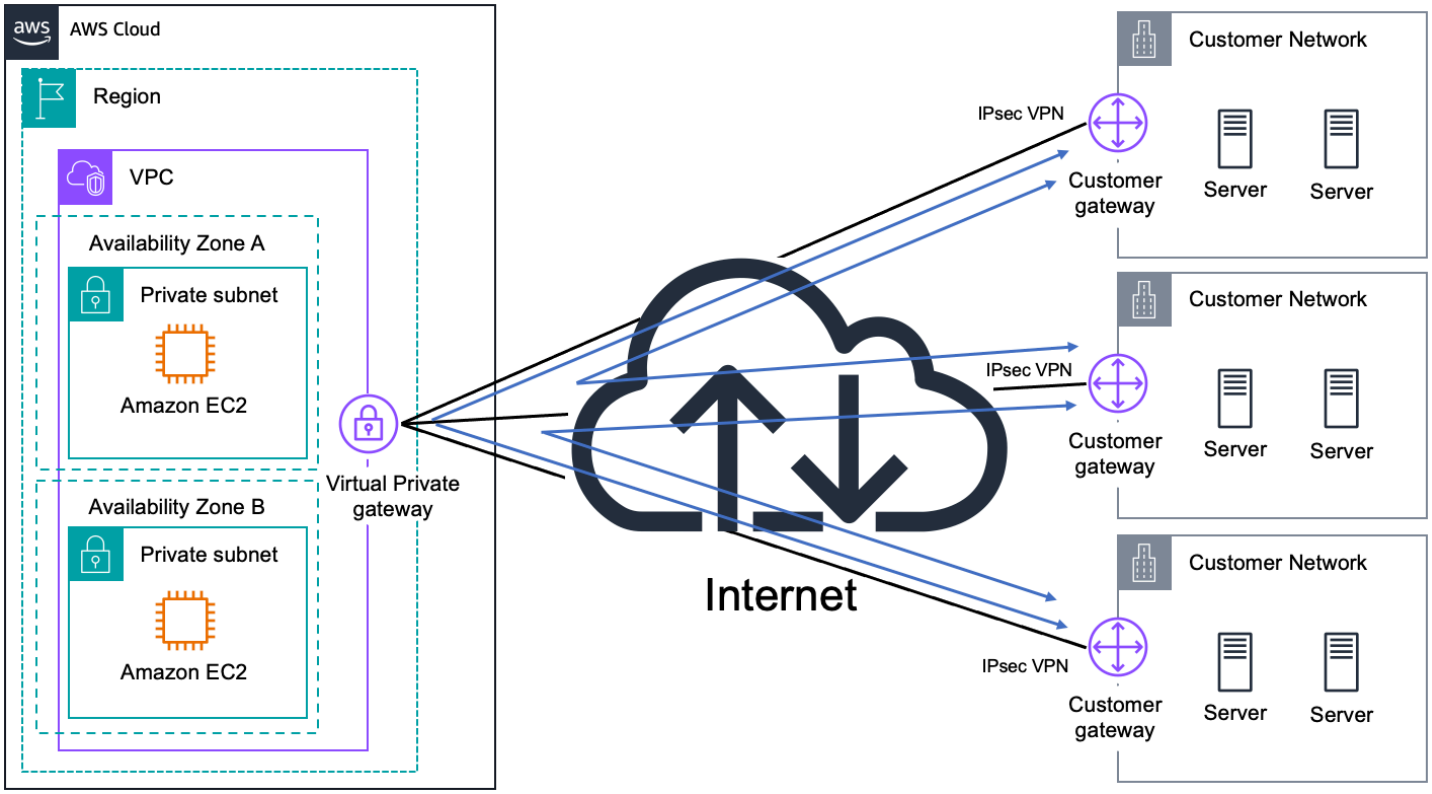
- Antarmuka virtual AWS Direct Connect
- Lampiran Transit gateway VPN
- Persyaratan untuk perangkat gateway pelanggan
- Perangkat gateway pelanggan diuji dengan Amazon VPC
- AWS Site-to-Site VPN — VPN IP Pribadi dengan AWS Direct Connect

Site-to-Site VPN CloudHub

Berdasarkan opsi AWS managed VPN yang dijelaskan sebelumnya, Anda dapat berkomunikasi dengan aman dari satu situs ke situs lainnya menggunakan. Site-to-Site VPN CloudHub Site-to-Site VPN CloudHub Beroperasi pada hub-and-spoke model sederhana yang dapat Anda gunakan dengan atau tanpa VPC. Gunakan pendekatan ini jika Anda memiliki beberapa kantor cabang dan

koneksi internet yang ada dan ingin menerapkan hub-and-spoke model yang nyaman dan berpotensi berbiaya rendah untuk konektivitas primer atau cadangan antara kantor jarak jauh ini.

Gambar berikut menunjukkan Site-to-Site VPN CloudHub arsitektur, dengan garis yang menunjukkan lalu lintas jaringan antara situs terpencil yang diarahkan melalui Site-to-Site VPN koneksi mereka.



Site-to-Site VPN CloudHub

Site-to-Site VPN CloudHub menggunakan gateway pribadi virtual VPC Amazon dengan beberapa gateway pelanggan, masing-masing menggunakan nomor sistem otonom BGP yang unik (). ASNs Situs jarak jauh tidak boleh memiliki rentang IP yang tumpang tindih. Gateway Anda mengiklankan rute yang sesuai (awalan BGP) melalui koneksi VPN mereka. Iklan routing ini diterima dan diiklankan kembali ke setiap peer BGP sehingga setiap situs dapat mengirim data ke dan menerima data dari situs lain.

Sumber daya tambahan

- Menyediakan komunikasi yang aman antar situs menggunakan VPN CloudHub
- Panduan Pengguna AWS Site-to-Site VPN
- Persyaratan untuk perangkat gateway pelanggan

- Perangkat gateway pelanggan diuji dengan Amazon VPC

AWS Transit Gateway + Solusi SD-WAN

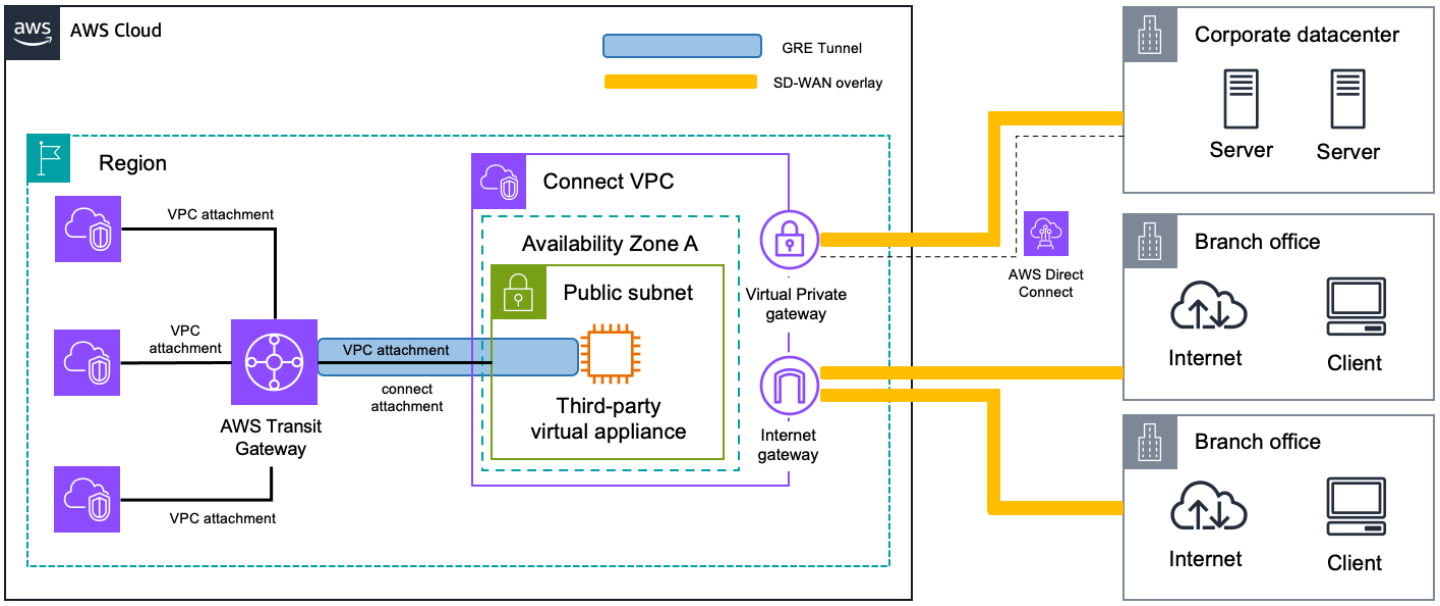
Software Defined Wide Area Networks (SD-WANs) digunakan untuk menghubungkan pusat data, kantor, atau lingkungan colocation Anda melalui jaringan transit yang berbeda (seperti internet publik, jaringan MPLS, atau menggunakan tulang punggung AWS AWS Direct Connect), mengelola lalu lintas secara otomatis dan dinamis di seluruh jalur yang paling tepat dan efisien berdasarkan kondisi jaringan, jenis aplikasi, atau persyaratan kualitas layanan (QoS).

Gunakan pendekatan ini jika Anda memiliki topologi jaringan yang kompleks, dengan beberapa pusat data, kantor, atau lingkungan kolokasi yang perlu berkomunikasi antara mereka sendiri dan dengan AWS. Solusi SD-WAN dapat membantu Anda mengelola jenis jaringan ini secara efisien.

Saat berbicara tentang koneksi jaringan SD-WAN ke AWS, AWS Transit Gateway sediakan hub transit jaringan regional yang dikelola dengan sangat tersedia dan dapat diskalakan untuk VPCs interkoneksi dan jaringan SD-WAN Anda. Lampiran Transit Gateway connect menyediakan cara asli untuk menghubungkan infrastruktur dan peralatan SD-WAN Anda dengan AWS. Ini memudahkan untuk memperluas SD-WAN Anda ke AWS tanpa harus mengaturnya. IPsec VPNs

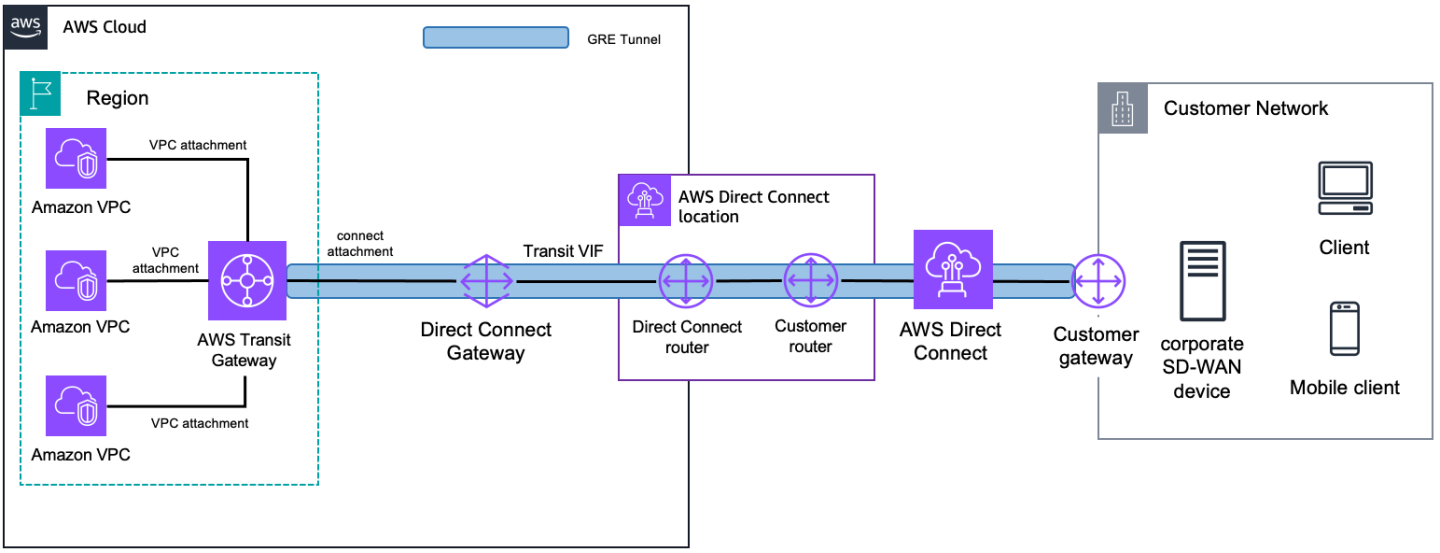
Transit Gateway menghubungkan attachment mendukung Generic Routing Encapsulation (GRE) untuk kinerja bandwidth yang lebih tinggi dibandingkan dengan koneksi VPN. Ini mendukung Border Gateway Protocol (BGP) untuk routing dinamis, dan menghilangkan kebutuhan untuk mengkonfigurasi rute statis. Ini menyederhanakan desain jaringan dan mengurangi biaya operasional terkait. Selain itu, integrasinya dengan Transit Gateway Network Manager memberikan visibilitas lanjutan melalui topologi jaringan global, metrik kinerja tingkat lampiran, dan data telemetri.

Saat mengintegrasikan jaringan SD-WAN Anda ke Transit Gateway menggunakan lampiran sambung, Anda memiliki dua pola umum. Yang pertama adalah menempatkan peralatan virtual jaringan SD-WAN di VPC dalam AWS. Kemudian, Anda menggunakan lampiran VPC sebagai transportasi dasar untuk lampiran sambungan Transit Gateway antara peralatan virtual dan Gateway Transit, seperti yang dapat ditunjukkan pada gambar berikut.



SD-WAN connectivity with AWS Transit Gateway (virtual appliance in AWS)

Atau, Anda dapat memperluas dan mengelompokkan lalu lintas SD-WAN Anda ke AWS tanpa menambahkan infrastruktur tambahan. Anda dapat membuat lampiran sambungan Transit Gateway menggunakan AWS Direct Connect koneksi sebagai transport yang mendasari, seperti yang dapat ditunjukkan pada gambar berikut.



SD-WAN connectivity with AWS Transit Gateway (Direct Connect as transport)

Ada beberapa pertimbangan yang harus diperhatikan saat menggunakan lampiran koneksi Transit Gateway:

- Anda dapat membuat lampiran sambung di Gateway Transit yang ada.

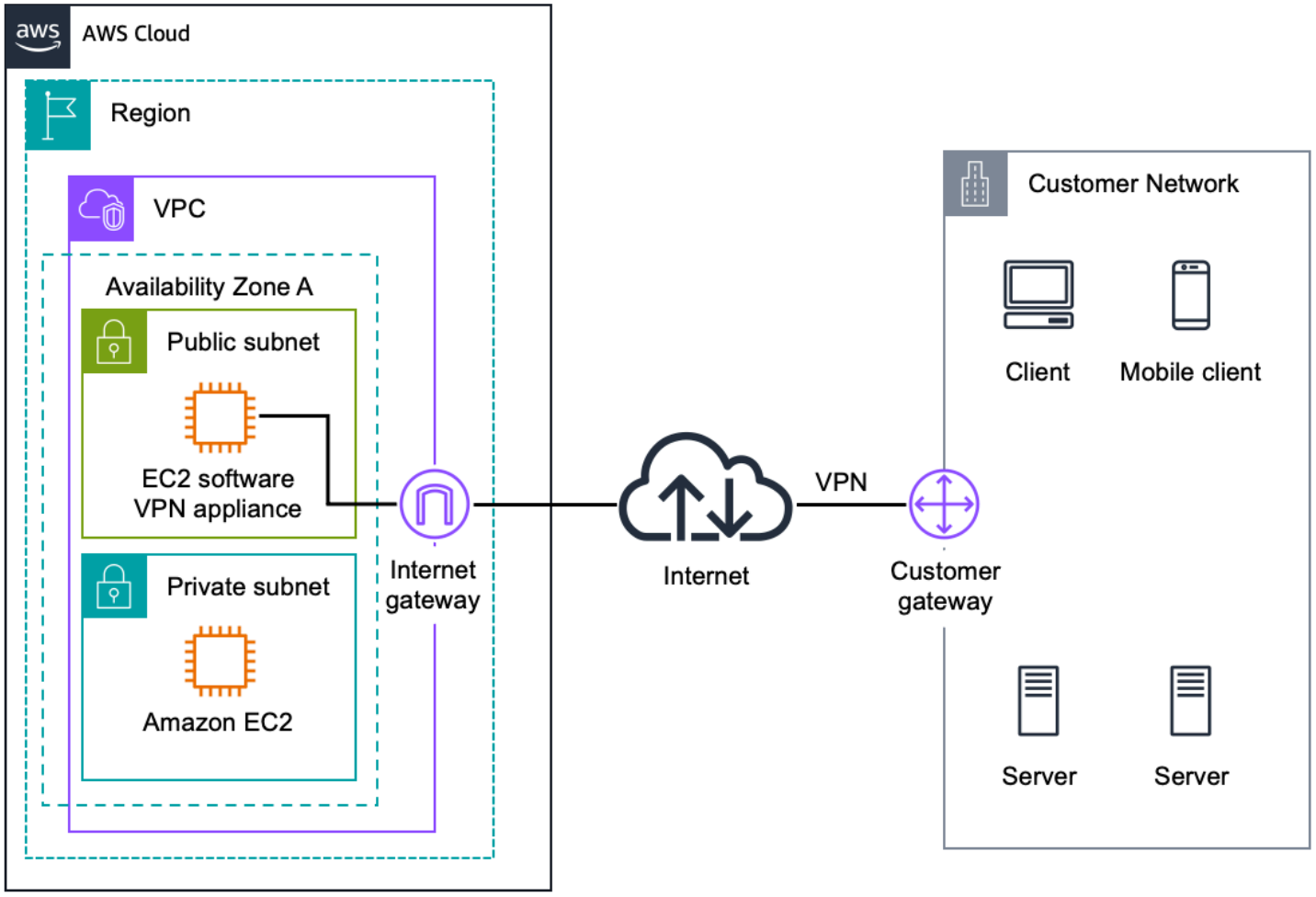
- Peralatan pihak ketiga harus dikonfigurasi dengan terowongan GRE untuk mengirim dan menerima lalu lintas dari Transit Gateway menggunakan lampiran sambungan. Alat harus dikonfigurasi dengan BGP untuk pembaruan rute dinamis dan pemeriksaan kesehatan.
- Connect attachment tidak mendukung rute statis.
- Transit Gateway menghubungkan attachment mendukung bandwidth maksimum lima Gbps per terowongan GRE. Bandwidth di atas lima Gbps dapat dicapai dengan mengiklankan awalan yang sama di beberapa Connect peer (terowongan GRE) untuk lampiran Connect yang sama.
- Maksimal empat rekan Connect didukung untuk setiap lampiran koneksi.
- Transit Gateway menghubungkan dukungan lampiran IPv6 dan iklan rute dinamis melalui Ekstensi Multiprotocol untuk BGP (MBGP atau MP-BGP).

Sumber daya tambahan

- Lampiran transit gateway peering
- Persyaratan dan pertimbangan
- Posting blog: Sederhanakan konektivitas SD-WAN dengan AWS Transit Gateway Connect

Perangkat Lunak VPN

Amazon VPC menawarkan fleksibilitas untuk sepenuhnya mengelola kedua sisi konektivitas VPC Amazon Anda dengan membuat koneksi VPN antara jaringan jarak jauh Anda dan perangkat lunak perangkat lunak VPN yang berjalan di jaringan VPC Amazon Anda. Opsi ini disarankan jika Anda harus mengelola kedua ujung koneksi VPN, baik untuk tujuan kepatuhan atau untuk memanfaatkan perangkat gateway yang saat ini tidak didukung oleh solusi VPN Amazon VPC. Gambar berikut menunjukkan opsi ini.



Perangkat Lunak Site-to-Site VPN

Anda dapat memilih dari ekosistem beberapa mitra dan komunitas sumber terbuka yang telah menghasilkan perangkat lunak perangkat lunak VPN yang berjalan di Amazon EC2. Seiring dengan pilihan ini muncul tanggung jawab bahwa Anda harus mengelola perangkat lunak, termasuk konfigurasi, tambalan, dan peningkatan.

Perhatikan bahwa desain ini memperkenalkan satu titik kegagalan potensial ke dalam desain jaringan karena perangkat lunak VPN berjalan pada satu EC2 instans Amazon. Untuk informasi tambahan, lihat Lampiran A: Arsitektur HA Tingkat Tinggi untuk instance VPN perangkat lunak Arsitektur untuk Instans VPN Perangkat Lunak.

Sumber daya tambahan

- Peralatan VPN tersedia di AWS Marketplace
- Tech Brief - Menghubungkan Cisco ASA ke EC2 VPC Instance () IPsec

- Tech Brief - Menghubungkan Beberapa VPCs dengan EC2 Instance () IPsec
- Tech Brief - Menghubungkan Beberapa VPCs dengan EC2 Instans (SSL)

Opsi VPC-to-Amazon konektivitas Amazon VPC

Gunakan pola desain ini saat Anda ingin mengintegrasikan beberapa Amazon VPCs ke dalam jaringan virtual yang lebih besar. Ini berguna jika Anda memerlukan beberapa VPCs karena keamanan, penagihan, kehadiran di beberapa wilayah, atau persyaratan pengisian kembali internal, untuk lebih mudah mengintegrasikan sumber daya AWS di antara Amazon. VPCs Anda juga dapat menggabungkan pola-pola ini dengan opsi konektivitas VPC jaringan—untuk—Amazon untuk membuat jaringan perusahaan yang mencakup jaringan jarak jauh dan beberapa. VPCs

Konektivitas VPC antara paling baik VPCs dicapai saat menggunakan rentang IP yang tidak tumpang tindih untuk setiap VPC yang terhubung. Misalnya, jika Anda ingin menghubungkan beberapa VPCs, pastikan setiap VPC dikonfigurasi dengan rentang Classless Inter-Domain Routing (CIDR) yang unik. Oleh karena itu, kami menyarankan Anda untuk mengalokasikan satu blok CIDR yang berdekatan, tidak tumpang tindih untuk digunakan oleh setiap VPC. Untuk informasi tambahan tentang perutean dan kendala Amazon VPC, lihat Pertanyaan yang Sering Diajukan VPC Amazon.

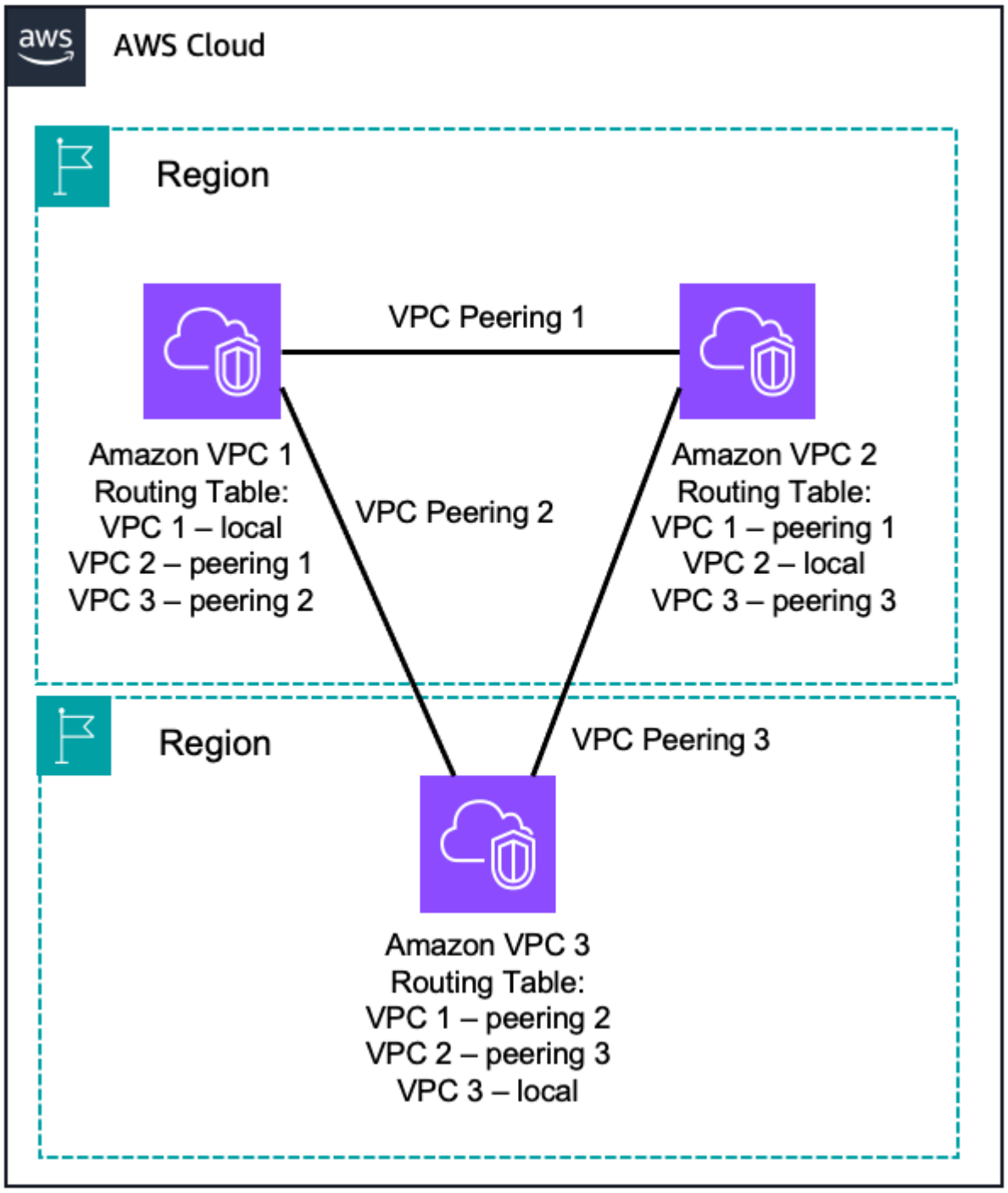
Opsi	Kasus Penggunaan	Keuntungan	Batasan
Peering VPC	Konektivitas jaringan yang disediakan AWS antara dua. VPCs	Memanfaatkan infrastruktur jaringan terukur yang dikelola AWS	Pengintip VPC tidak mendukung hubungan peering transitif Sulit dikelola dalam skala
AWS Transit Gateway	Konektivitas router regional yang disediakan AWS untuk VPCs	AWS mengelola layanan ketersediaan dan skalabilitas tinggi Hub jaringan regional hingga 5.000 lampiran	Transit Gateway peering hanya mendukung rute statis
AWS PrivateLink	Konektivitas jaringan yang disediakan AWS antara dua VPCs menggunakan titik akhir antarmuka	Memanfaatkan infrastruktur jaringan terukur yang dikelola AWS	Layanan VPC Endpoint hanya tersedia di wilayah AWS tempat layanan tersebut dibuat

Opsi	Kasus Penggunaan	Keuntungan	Batasan
Perangkat Lunak VPN	Koneksi VPN berbasis perangkat lunak antara VPCs	Mendukung beragam vendor, produk, dan protokol VPN Dikelola sepenuhnya oleh Anda	Anda bertanggung jawab untuk menerapkan solusi HA untuk semua titik akhir VPN (jika diperlukan) Instans VPN bisa menjadi hambatan jaringan
Perangkat Lunak VPN-to-AWS Site-to-Site VPN	Alat perangkat lunak untuk koneksi VPN antara VPCs	AWS mengelola koneksi VPC VPN ketersediaan tinggi Mendukung beragam vendor VPN dan produk yang dikelola oleh Anda Mendukung rute statis dan kebijakan peering dan routing BGP dinamis	Anda bertanggung jawab untuk menerapkan solusi HA untuk perangkat lunak titik akhir VPN (jika diperlukan) Instans VPN bisa menjadi hambatan jaringan IPsec Protokol VPN hanya untuk AWS Managed VPN

Peering VPC

Koneksi peering VPC adalah koneksi jaringan antara dua VPCs yang memungkinkan perutean menggunakan alamat IP pribadi masing-masing VPC seolah-olah mereka berada di jaringan yang sama. Koneksi peering VPC dapat dibuat antara Anda sendiri VPCs atau dengan VPC di akun AWS lain. Peering VPC juga mendukung peering antar wilayah.

Lalu lintas yang menggunakan VPC Peering antar wilayah selalu berada di tulang punggung AWS global dan tidak pernah melintasi internet publik, sehingga mengurangi vektor ancaman, seperti eksploitasi umum dan serangan S. DDo



VPC-to-VPC Peering

AWS menggunakan infrastruktur VPC yang ada untuk membuat koneksi peering VPC dan tidak bergantung pada perangkat keras fisik yang terpisah. Oleh karena itu, mereka tidak memperkenalkan

satu titik kegagalan atau hambatan bandwidth jaringan di antaranya. VPCs Selain itu, tabel routing VPC, grup keamanan, dan daftar kontrol akses jaringan dapat dimanfaatkan untuk mengontrol subnet atau instance mana yang dapat memanfaatkan koneksi peering VPC.

Amazon VPCs tidak mendukung peering transitif, artinya Anda tidak dapat mengkomunikasikan dua VPCs yang tidak secara langsung diintip menggunakan VPC ketiga sebagai transit. Jika Anda ingin semua berkomunikasi satu sama lain menggunakan VPC peering, Anda harus membuat koneksi peering VPC 1:1 di antara mereka masing-masing. VPCs Atau, Anda dapat menggunakan AWS Transit Gateway AWS Cloud WAN untuk bertindak sebagai hub transit jaringan.

Keduanya IPv4 dan IPv6 lalu lintas didukung dalam koneksi peering VPC. Namun, dua VPCs tidak dapat diintip jika blok IPv4 CIDR utamanya tumpang tindih, terlepas dari blok sekunder IPv4 atau IPv6 CIDR yang digunakan. Pertimbangkan hal ini saat menetapkan blok CIDR utama ke Anda VPCs jika Anda berencana untuk menggunakan VPC mengintip di antara mereka.

Sumber daya tambahan

- Pengintip VPC Amazon
- Apa itu VPC peering?

AWS Transit Gateway

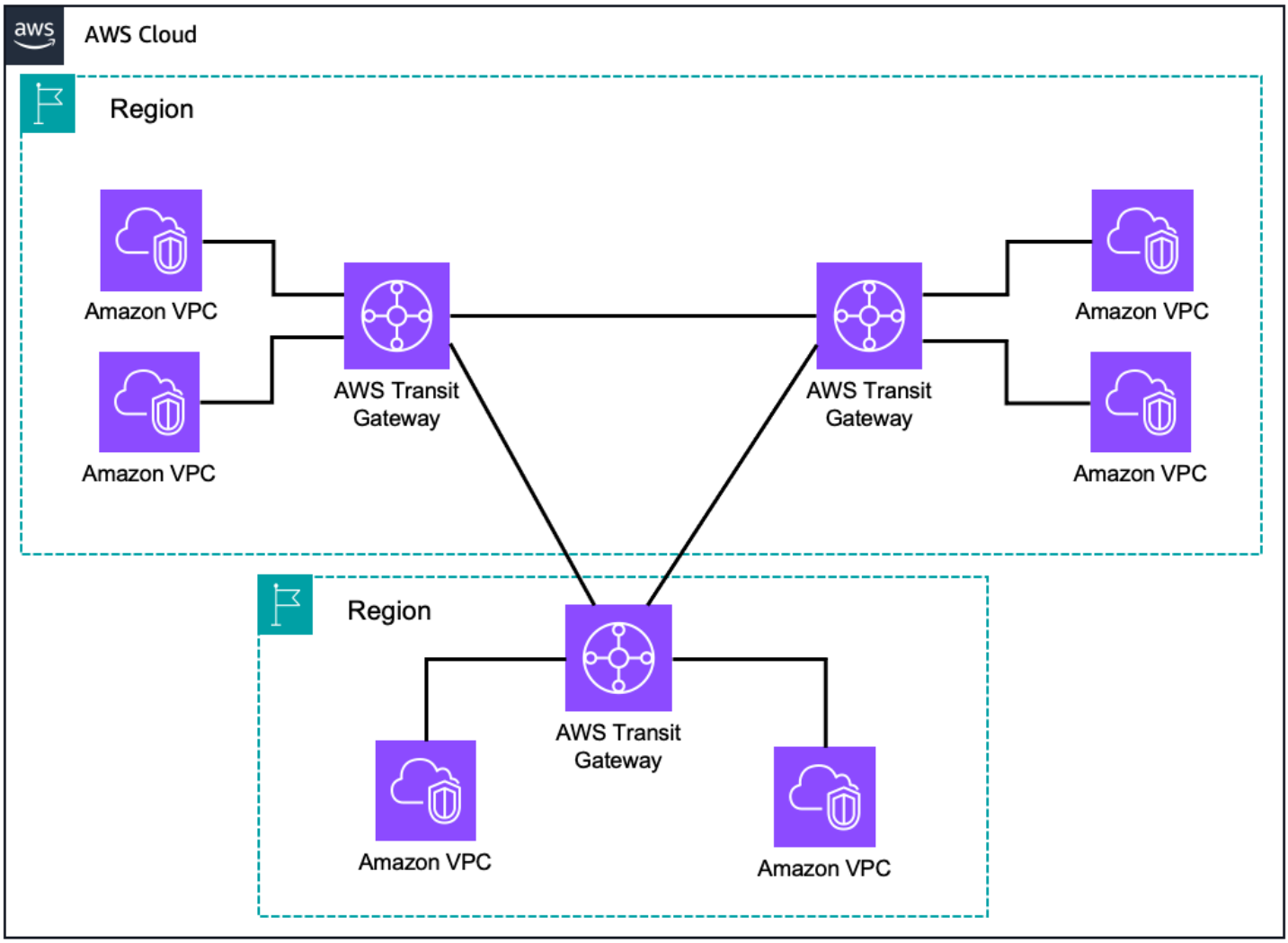
AWS Transit Gateway adalah layanan yang sangat tersedia dan dapat diskalakan untuk mengkonsolidasikan konfigurasi perutean AWS VPC untuk wilayah dengan arsitektur. hub-and-spoke Setiap VPC spoke hanya perlu terhubung ke Transit Gateway untuk mendapatkan akses ke koneksi lain. VPCs Keduanya IPv4 dan IPv6 lalu lintas didukung di AWS Transit Gateway.

Anda dapat memanfaatkan beberapa tabel rute Transit Gateway, asosiasi, dan propagasi untuk mengelompokkan lalu lintas Anda dalam Transit Gateway yang sama. Anda akan dapat mengelola domain routing yang berbeda (misalnya, lalu lintas produksi dan non-produksi) dari satu titik manajemen, memastikan bahwa domain routing ini tidak akan dapat berkomunikasi antara satu sama lain.

Anda juga dapat memanfaatkan hub-and-spoke arsitektur yang dibuat oleh Transit Gateway untuk memusatkan akses ke layanan bersama seperti inspeksi lalu lintas, akses titik akhir VPC antarmuka, atau lalu lintas keluar melalui gateway NAT atau instans NAT. Sentralisasi ini menyederhanakan kompleksitas pengelolaan sumber daya ini di beberapa sumber daya VPCs, dan memungkinkan kontrol yang lebih baik saat Anda memperluas jejak Anda di AWS.

Transit Gateway dapat diintip satu sama lain dalam Wilayah AWS yang sama atau di antara Wilayah AWS yang berbeda. AWS Transit Gateway Lalu lintas selalu berada di tulang punggung AWS global dan tidak pernah melintasi internet publik, sehingga mengurangi vektor ancaman seperti eksploitasi umum dan serangan S. DDo

Dengan jumlah yang besar VPCs, Transit Gateway menyediakan manajemen VPC-to-VPC komunikasi yang lebih sederhana melalui VPC Peering, seperti yang ditunjukkan pada gambar berikut.



AWS Transit Gateway

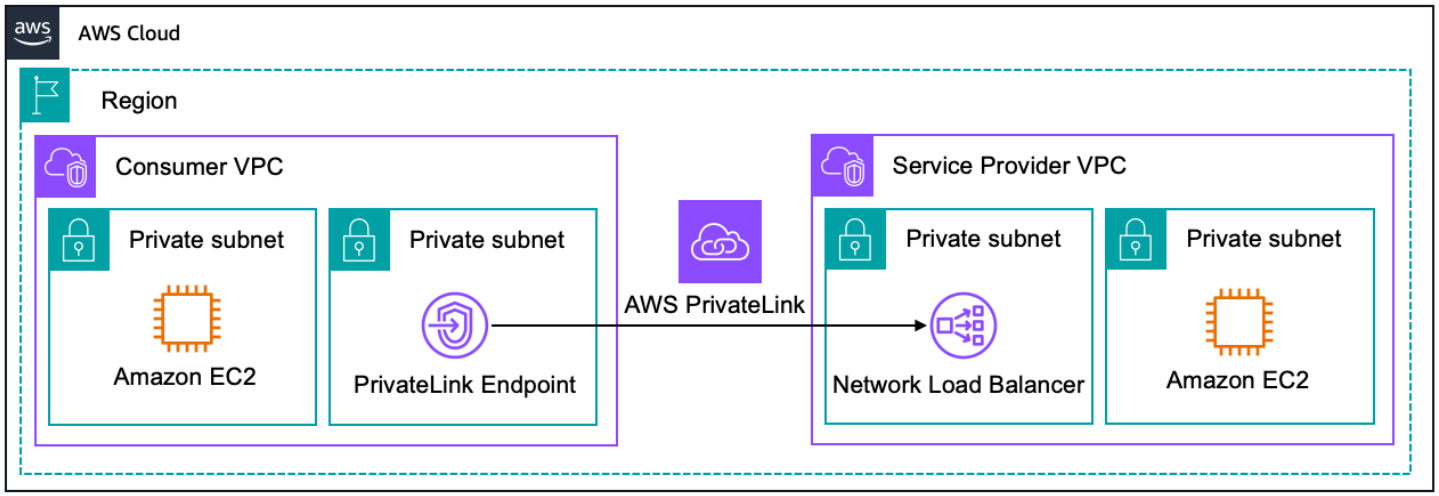
Untuk visibilitas pusat lalu lintas IP yang menuju dan dari Gateway Transit Anda, Anda dapat mempublikasikan Log Aliran Gateway Transit ke CloudWatch Log Amazon dan Amazon S3. Data log alur dikumpulkan di luar jalur lalu lintas jaringan Anda, dan oleh karena itu tidak mempengaruhi throughput atau latensi jaringan.

Sumber daya tambahan

- Gerbang transit Amazon VPC
- Lampiran transit gateway peering
- Bekerja dengan Transit Gateway
- Mencatat lalu lintas jaringan menggunakan Log Aliran Transit Gateway

AWS PrivateLink

AWS PrivateLink memungkinkan Anda untuk terhubung ke beberapa layanan AWS, layanan yang dihosting oleh akun AWS lainnya (disebut sebagai layanan titik akhir), dan layanan AWS Marketplace mitra yang didukung, melalui alamat IP pribadi di VPC Anda. Titik akhir antarmuka dibuat langsung di dalam VPC Anda, menggunakan antarmuka jaringan elastis dan alamat IP di subnet VPC Anda. Itu berarti bahwa Grup Keamanan VPC dapat digunakan untuk mengelola akses ke titik akhir.



AWS PrivateLink

Kami merekomendasikan pendekatan ini jika Anda ingin menggunakan layanan yang ditawarkan oleh VPC lain dengan aman dalam jaringan AWS, menggunakan alamat IP pribadi. Atau, AWS PrivateLink adalah solusi yang baik ketika VPCs telah tumpang tindih alamat IP.

AWS PrivateLink sepenuhnya mendukung IPv6, tetapi kedua tujuan VPCs, Subnet VPC, Network Load Balancer, dan nama DNS harus diaktifkan atau dimodifikasi untuk menggunakan dual-stack. Setelah prasyarat ini terpenuhi, IPv6 dapat diaktifkan pada konfigurasi layanan untuk titik akhir.

Kontrol akses ke AWS PrivateLink

Titik akhir antarmuka dibuat langsung di dalam VPC Anda dengan menggunakan antarmuka jaringan elastis dan alamat IP di subnet VPC Anda. Itu berarti bahwa Grup Keamanan VPC dapat digunakan untuk mengelola akses jaringan ke titik akhir.

Saat membuat titik akhir antarmuka atau titik akhir gateway, Anda juga dapat melampirkan kebijakan titik akhir. Kebijakan endpoint mengontrol prinsip AWS (akun AWS, pengguna IAM, dan peran) yang dapat menggunakan titik akhir VPC untuk mengakses layanan titik akhir.

Anda tidak dapat melampirkan lebih dari satu kebijakan ke titik akhir. Namun, Anda dapat memodifikasi kebijakan endpoint kapan saja.

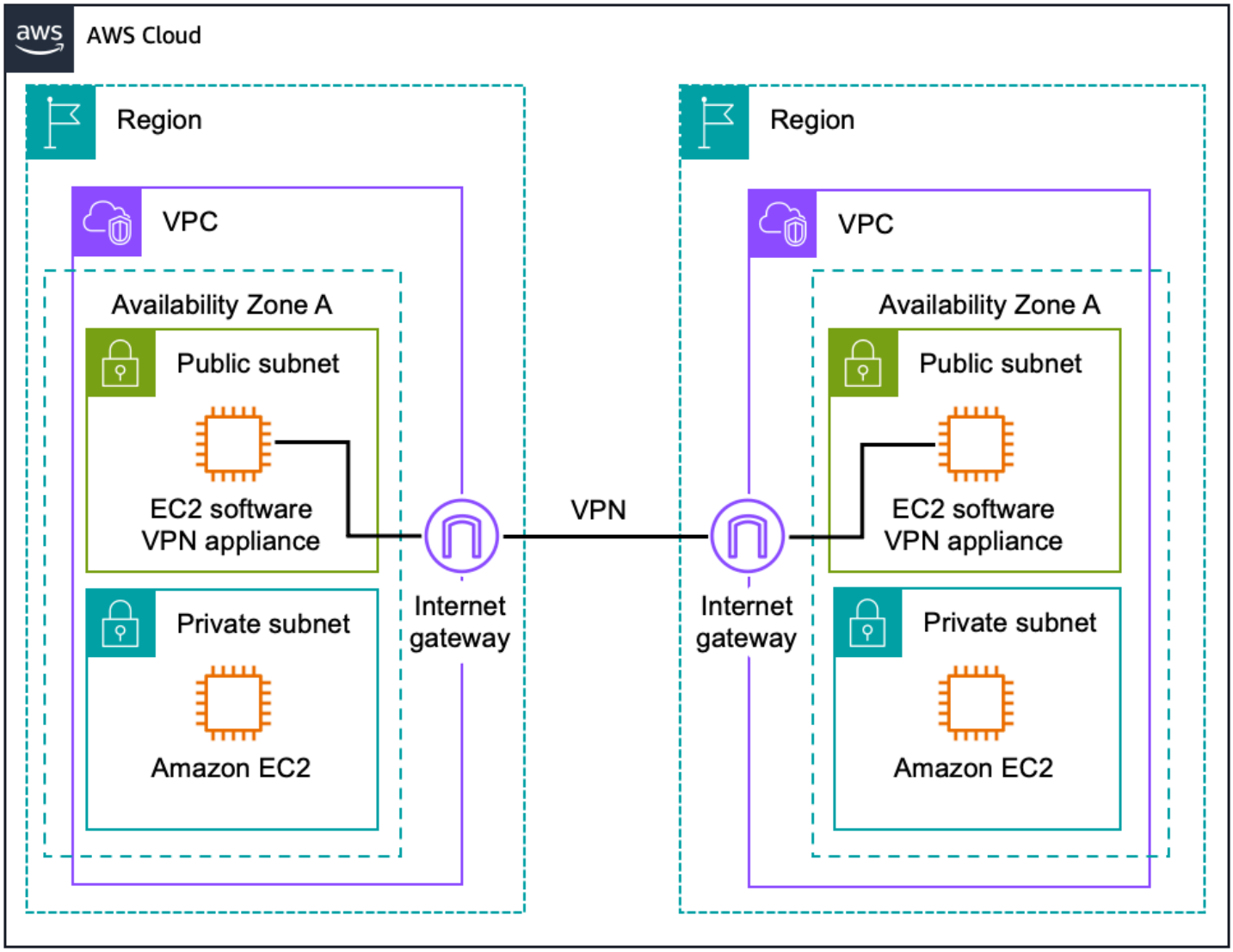
Kebijakan endpoint tidak mengesampingkan atau mengganti kebijakan pengguna IAM atau kebijakan khusus layanan (seperti kebijakan bucket Amazon S3). Jika Anda menggunakan titik akhir antarmuka untuk terhubung ke Amazon S3, Anda juga dapat menggunakan kebijakan bucket Amazon S3 untuk mengontrol akses ke bucket dari titik akhir tertentu atau spesifik. VPCs

Sumber daya tambahan

- Antarmuka titik akhir VPC ()AWS PrivateLink
- Layanan titik akhir VPC ()AWS PrivateLink
- Posting blog: Percepat IPv6 adopsi Anda dengan PrivateLink layanan dan titik akhir
- Posting blog: Menghubungkan Jaringan dengan Rentang IP yang Tumpang Tindih
- AWS PrivateLink Mitra

Perangkat Lunak VPN

Amazon VPC menyediakan fleksibilitas perutean jaringan. Ini termasuk kemampuan untuk membuat terowongan VPN aman antara dua atau lebih perangkat lunak perangkat lunak VPN untuk menghubungkan beberapa VPCs ke jaringan pribadi virtual yang lebih besar sehingga instance di setiap VPC dapat terhubung dengan mulus satu sama lain menggunakan alamat IP pribadi. Opsi ini disarankan ketika Anda ingin mengelola kedua ujung koneksi VPN menggunakan penyedia perangkat lunak VPN pilihan Anda. Opsi ini menggunakan gateway internet yang terpasang pada setiap VPC untuk memfasilitasi komunikasi antara perangkat lunak perangkat lunak VPN.



Software Site-to-Site VPN VPC-to-VPC Routing

Anda dapat memilih dari ekosistem beberapa mitra dan komunitas open source yang telah menghasilkan perangkat lunak perangkat lunak VPN yang berjalan di Amazon EC2. Seiring dengan pilihan ini datang tanggung jawab bagi Anda untuk mengelola perangkat lunak termasuk konfigurasi, patch, dan upgrade.

Perhatikan bahwa desain ini memperkenalkan satu titik kegagalan potensial ke dalam desain jaringan karena perangkat lunak VPN berjalan pada satu EC2 instans Amazon. Untuk informasi tambahan, lihat Lampiran A: Arsitektur HA Tingkat Tinggi untuk instance VPN perangkat lunak.

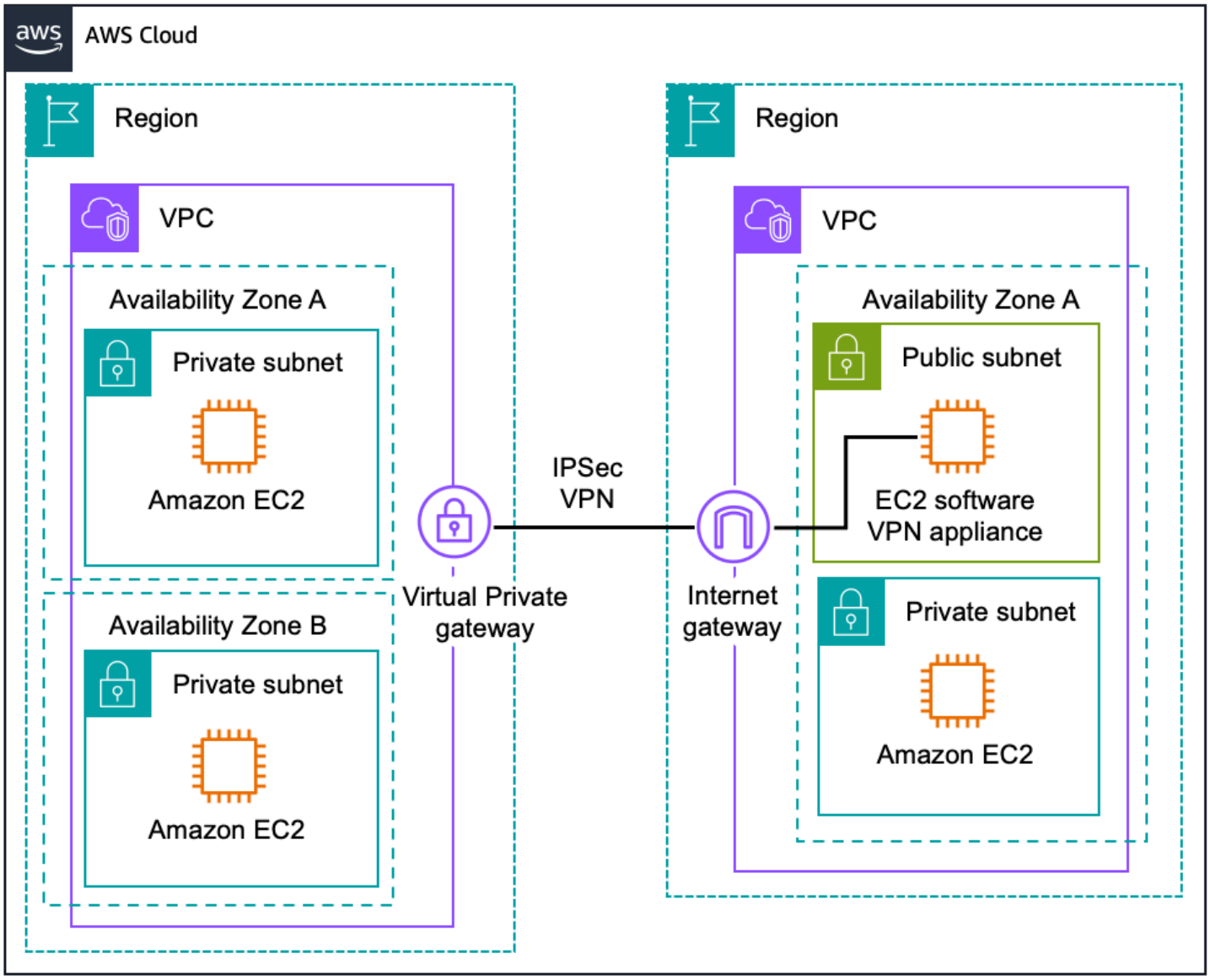
Sumber daya tambahan

- Peralatan VPN tersedia dari AWS Marketplace

- Tech Brief - Menghubungkan Beberapa VPCs dengan EC2 Instance () IPsec
- Tech Brief - Menghubungkan Beberapa VPCs dengan EC2 Instans (SSL)

Perangkat Lunak VPN-to-AWS Site-to-Site VPN

Amazon VPC memberikan fleksibilitas untuk menggabungkan VPN terkelola AWS dan opsi VPN perangkat lunak untuk menghubungkan beberapa opsi. VPCs Dengan desain ini, Anda dapat membuat terowongan VPN aman antara perangkat lunak VPN dan gateway pribadi virtual, memungkinkan instance di setiap VPC terhubung dengan mulus satu sama lain menggunakan alamat IP pribadi. Opsi ini menggunakan gateway pribadi virtual di satu VPC Amazon dan kombinasi gateway internet dan perangkat lunak perangkat lunak VPN di VPC Amazon lainnya, seperti yang ditunjukkan pada gambar berikut.



Software VPN to AWS Site-to-Site VPN VPC-to-VPC Routing

Perhatikan bahwa desain ini memperkenalkan satu titik kegagalan potensial ke dalam desain jaringan. Untuk informasi tambahan, lihat Lampiran A: Arsitektur HA Tingkat Tinggi untuk instance VPN perangkat lunak.

Sumber daya tambahan

- Peralatan VPN tersedia dari AWS Marketplace
- Panduan Pengguna AWS Site-to-Site VPN
- Persyaratan untuk perangkat gateway pelanggan

Opsi konektivitas access-to-Amazon VPC jarak jauh perangkat lunak

Dengan VPN akses jarak jauh perangkat lunak, Anda dapat memanfaatkan layanan berbiaya rendah, elastis, dan aman untuk menerapkan solusi akses jarak jauh sekaligus memberikan pengalaman tanpa batas terhubung ke sumber daya yang dihosting AWS. Opsi ini biasanya disukai oleh perusahaan kecil dengan jaringan jarak jauh yang kurang luas atau yang belum membangun dan menerapkan solusi akses jarak jauh untuk karyawan mereka.

Anda dapat menggabungkan pola-pola ini dengan opsi Network-to-Amazon Opsi konektivitas VPC konektivitas dan Opsi VPC-to-Amazon konektivitas Amazon VPC untuk membuat jaringan yang mencakup jaringan jarak jauh dan beberapa VPCs.

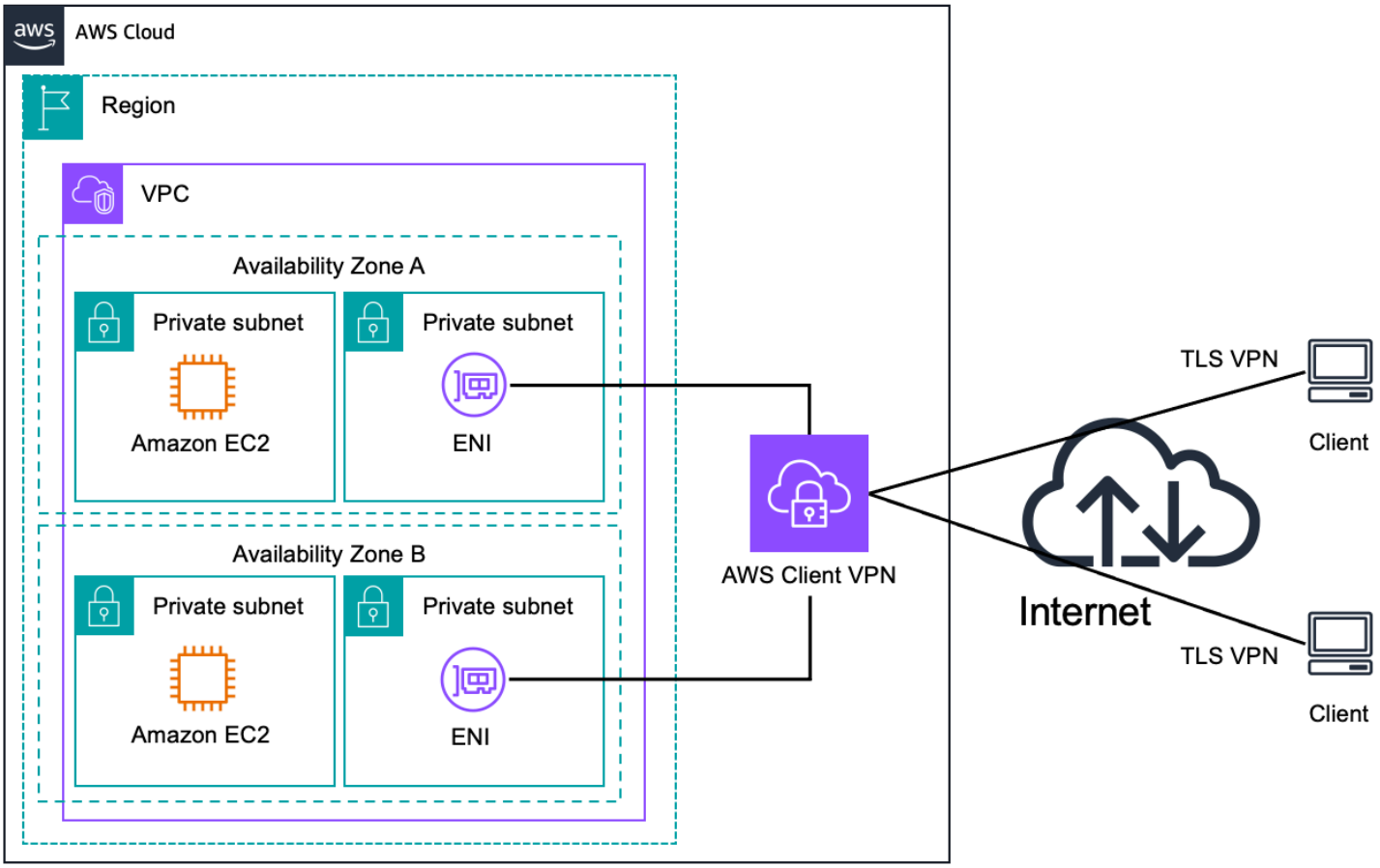
Tabel berikut menguraikan kelebihan dan keterbatasan opsi ini.

Opsi	Kasus Penggunaan	Keuntungan	Batasan
AWS Client VPN	AWS mengelola solusi akses jarak jauh ke Amazon VPC dan/atau jaringan internal	AWS mengelola layanan ketersediaan dan skalabilitas tinggi	Hanya klien OpenVPN
Perangkat lunak klien VPN	Perangkat lunak VPN solusi akses jarak jauh ke jaringan internal Amazon VPC and/or	Mendukung beragam vendor, produk, dan protokol VPN Solusi yang dikelola pelanggan sepenuhnya	Anda bertanggung jawab untuk menerapkan solusi HA

AWS Client VPN

AWS Client VPN adalah layanan ketersediaan dan skalabilitas tinggi yang dikelola AWS yang memungkinkan akses jarak jauh perangkat lunak yang aman. Ini menyediakan opsi untuk membuat

koneksi TLS aman antara klien jarak jauh dan Amazon Anda VPCs, untuk mengakses sumber daya AWS dan lokal secara aman melalui internet, seperti yang ditunjukkan pada gambar berikut.



AWS Client VPN Remote Access

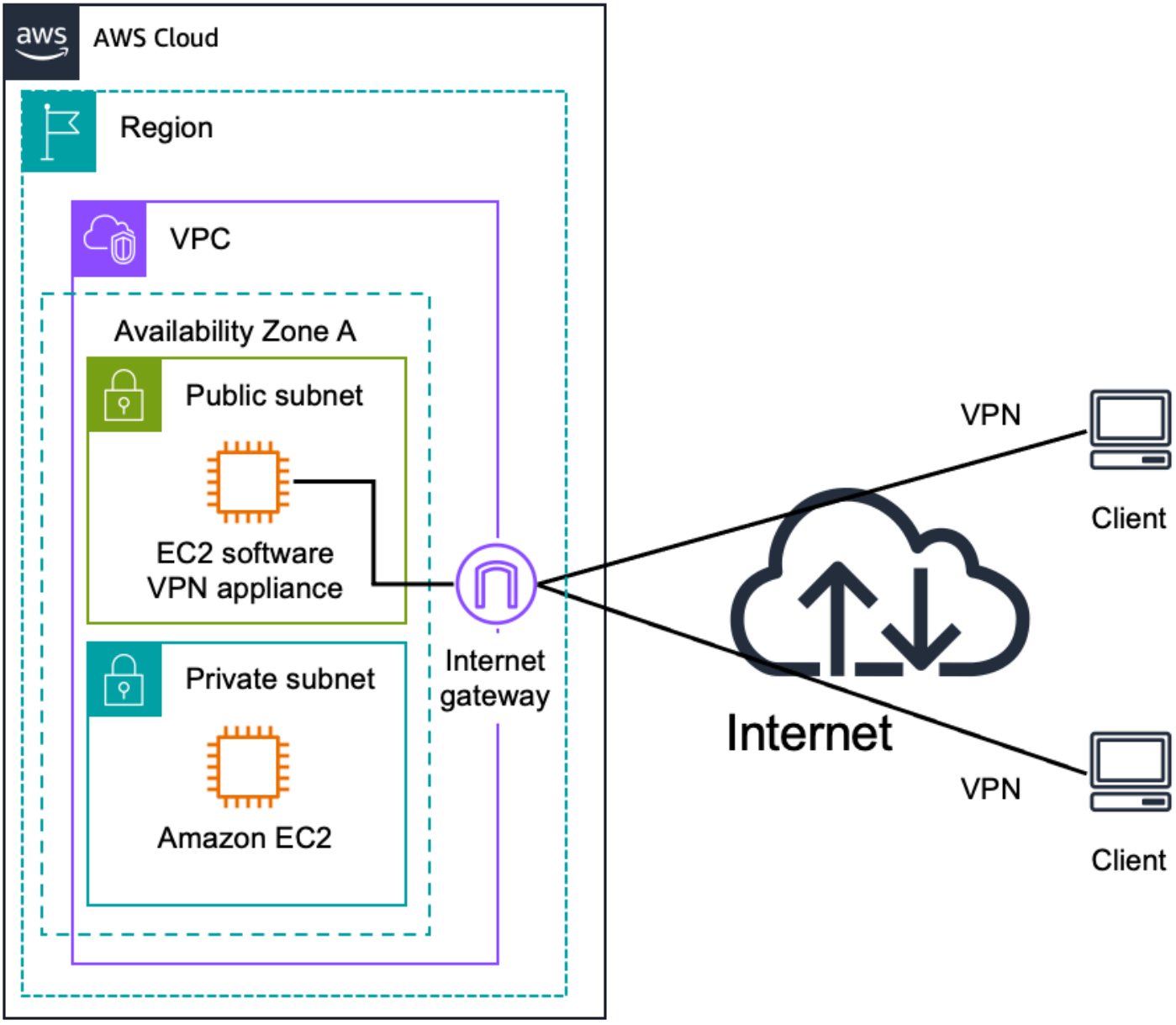
Klien jarak jauh dapat berupa AWS Client VPN for Desktop, atau klien VPN OpenVPN pihak ketiga, dengan autentikasi oleh Active Directory atau otentikasi sertifikat timbal balik.

Sumber daya tambahan

- Panduan Administrator AWS Client VPN

Perangkat lunak klien VPN

Anda dapat memilih dari ekosistem beberapa mitra dan komunitas open source yang telah menghasilkan solusi akses jarak jauh yang berjalan di Amazon EC2. Solusi ini memberikan fleksibilitas besar pada penggunaan protokol keamanan untuk akses jarak jauh ke Amazon Anda VPCs, untuk mengakses sumber daya AWS secara aman dan lokal melalui internet, seperti yang ditunjukkan pada gambar berikut.



Software Client VPN Remote Access

Solusi akses jarak jauh berkisar dalam kompleksitas, mendukung beberapa opsi otentikasi klien (termasuk otentikasi multifaktor) dan dapat diintegrasikan dengan Amazon VPC atau solusi manajemen identitas dan akses yang dihosting dari jarak jauh (memanfaatkan salah satu network-to-Amazon opsi VPC) seperti Microsoft Active Directory atau solusi otentikasi LDAP/Multifaktor lainnya.

Anda bertanggung jawab untuk mengelola perangkat lunak akses jarak jauh termasuk manajemen pengguna, konfigurasi, tambalan, dan peningkatan. Desain ini memperkenalkan satu titik kegagalan potensial ke dalam desain jaringan karena server akses jarak jauh berjalan pada satu instans

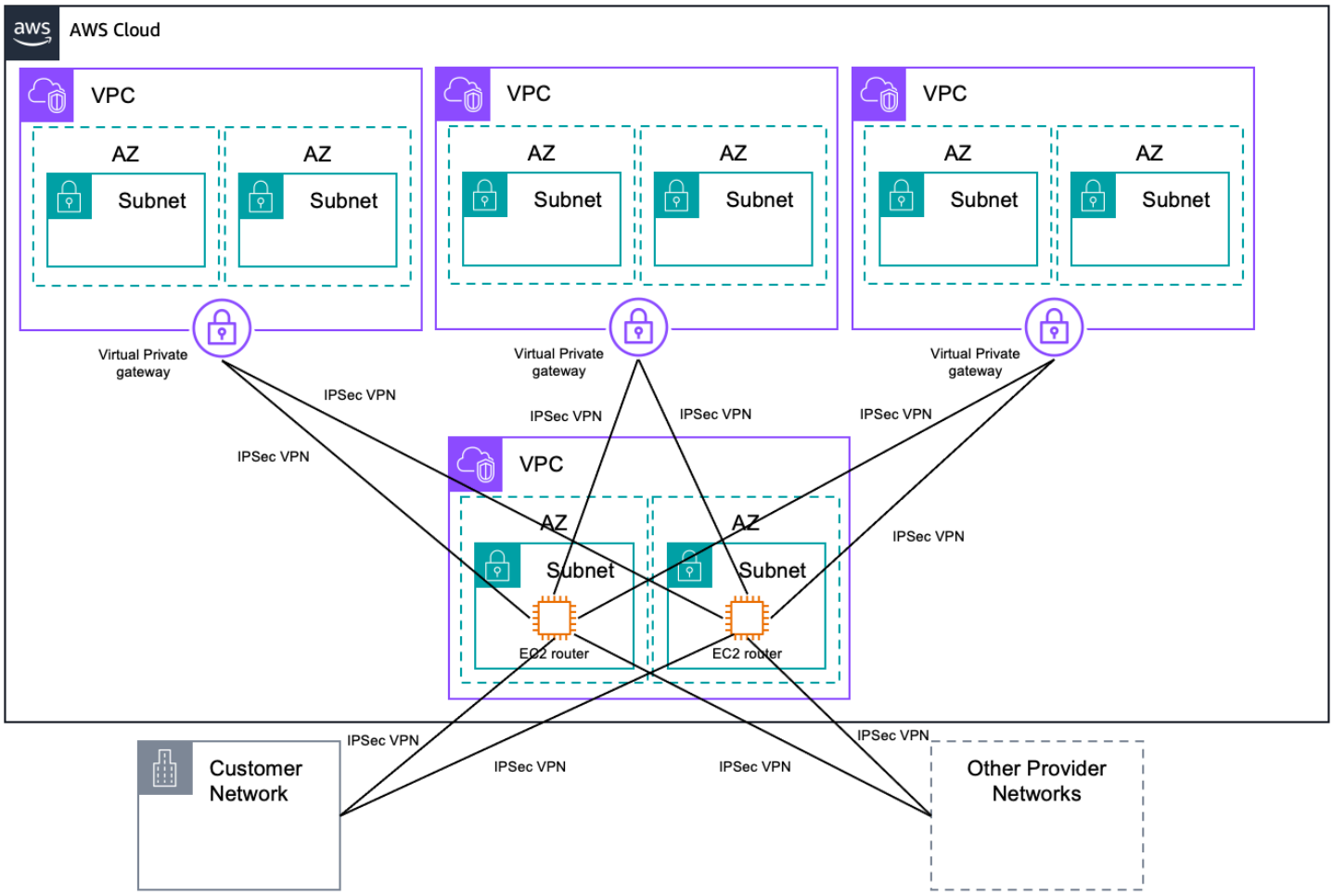
Amazon EC2. Untuk informasi tambahan, lihat Lampiran A: Arsitektur HA Tingkat Tinggi untuk instance VPN perangkat lunak.

Sumber daya tambahan

- Peralatan VPN tersedia dari AWS Marketplace
- Panduan Memulai Cepat Server Akses OpenVPN

Transit VPC

Berdasarkan desain VPN Perangkat Lunak yang disebutkan di atas, Anda dapat membuat jaringan transit global di AWS. VPC transit adalah strategi umum untuk menghubungkan beberapa jaringan yang tersebar secara geografis VPCs dan jarak jauh untuk menciptakan pusat transit jaringan global. VPC transit menyederhanakan manajemen jaringan dan meminimalkan jumlah koneksi yang diperlukan untuk menghubungkan beberapa VPCs jaringan dan jarak jauh. Gambar berikut menggambarkan desain ini.



Transit VPC

Selain menyediakan perutean jaringan langsung antara VPCs dan jaringan lokal, desain ini juga memungkinkan VPC transit untuk menerapkan aturan perutean yang lebih kompleks, seperti terjemahan alamat jaringan antara rentang jaringan yang tumpang tindih, atau untuk menambahkan penyaringan atau inspeksi paket tingkat jaringan tambahan. Desain VPC transit dapat digunakan untuk mendukung kasus penggunaan penting seperti, jaringan pribadi, konektivitas bersama, dan penggunaan AWS lintas akun.

Sumber daya tambahan

- AWS Transit Gateway
- Cisco Catalyst 8000V untuk SD-WAN & Perutean di AWS Marketplace

AWS Cloud WAN

AWS Cloud WAN adalah jaringan area luas terkelola (WAN) yang digerakkan oleh maksud, dijelaskan oleh kebijakan yang Anda tetapkan yang menyatukan pusat data, cabang, dan jaringan AWS Anda. Meskipun Anda dapat membuat jaringan global Anda sendiri dengan menghubungkan beberapa Transit Gateway di seluruh Wilayah, Cloud WAN menyediakan fitur otomatisasi, segmentasi, dan manajemen konfigurasi bawaan yang dirancang khusus untuk membangun dan mengoperasikan jaringan global, berdasarkan kebijakan jaringan inti Anda. Cloud WAN telah menambahkan fitur seperti lampiran VPC otomatis, pemantauan kinerja terintegrasi, dan konfigurasi terpusat.

Kebijakan jaringan inti ditulis dalam bahasa deklaratif yang mendefinisikan segmen, perutean Wilayah AWS, dan bagaimana lampiran harus dipetakan ke segmen. Dengan kebijakan jaringan inti, Anda dapat menjelaskan maksud Anda untuk kontrol akses dan perutean lalu lintas, sementara AWS Cloud WAN menangani detail konfigurasi jaringan.

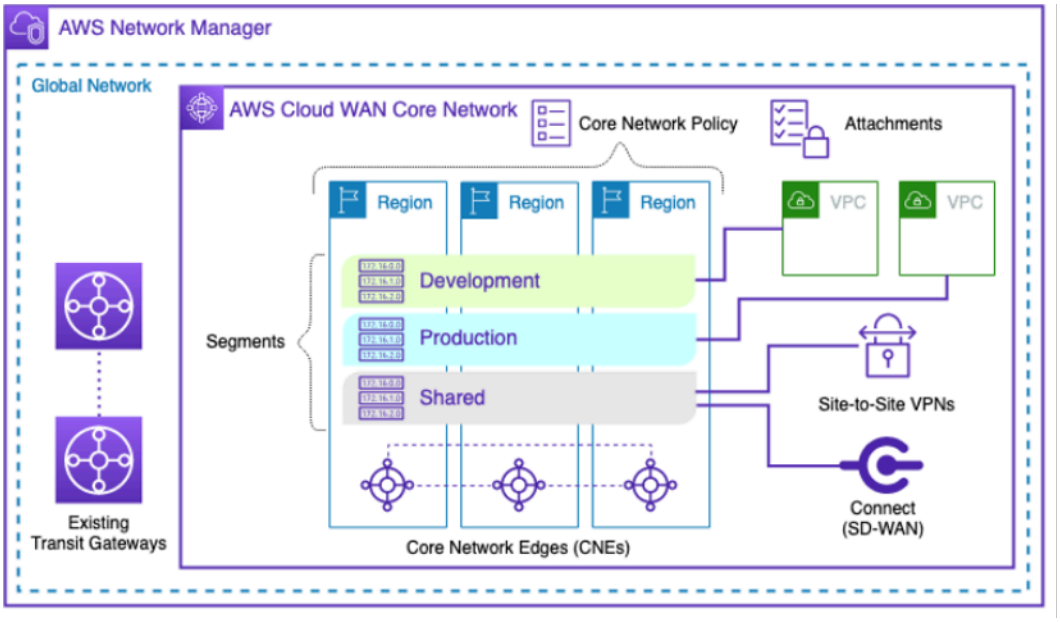
Cloud WAN dikelola dalam AWS Network Manager, yang memungkinkan Anda mengelola dan memvisualisasikan jaringan inti Cloud WAN dan jaringan Transit Gateway Anda secara terpusat di seluruh akun AWS, Wilayah, dan lokasi lokal. Network Manager memberi Anda beberapa visualisasi dasbor untuk membantu Anda melihat dan memantau semua aspek jaringan global Anda. Beberapa dasbor meliputi:

- Peta dunia yang menunjukkan dengan tepat di mana sumber daya jaringan Anda, seperti lokasi tepi, perangkat, dan lampiran, berada.
- Pemantauan yang menggunakan CloudWatch Acara untuk melacak statistik senilai 15 bulan, memberi Anda perspektif yang lebih baik tentang kinerja jaringan Anda.
- Pelacakan peristiwa yang mengalirkan peristiwa real-time ke dasbor acara.
- Diagram topologi dan logis dari jaringan gateway transit dan gateway transit Anda.

Transit Gateway dan Cloud WAN memungkinkan konektivitas terpusat antara VPCs dan lokasi lokal. Transit Gateway adalah hub konektivitas jaringan regional dan optimal untuk pelanggan yang beroperasi di beberapa Wilayah AWS, ingin mengelola konfigurasi peering dan routing mereka sendiri, atau lebih suka menggunakan otomatisasi mereka sendiri. Cloud WAN optimal untuk pelanggan yang ingin mendefinisikan jaringan global mereka melalui kebijakan dan memiliki layanan mengimplementasikan komponen yang mendasarinya secara otomatis.

Hal yang perlu diketahui

- CNE (Core network edge) mewarisi banyak karakteristik Transit Gateway, seperti throughput per lampiran VPC.
- Cloud WAN mendukung keduanya IPv4 dan IPv6.
- Untuk jaringan besar dengan banyak perubahan, pertimbangkan untuk membuat pengembangan terpisah dan pengujian jaringan global di mana Anda dapat memvalidasi perubahan.



AWS Cloud WAN

Sumber daya tambahan

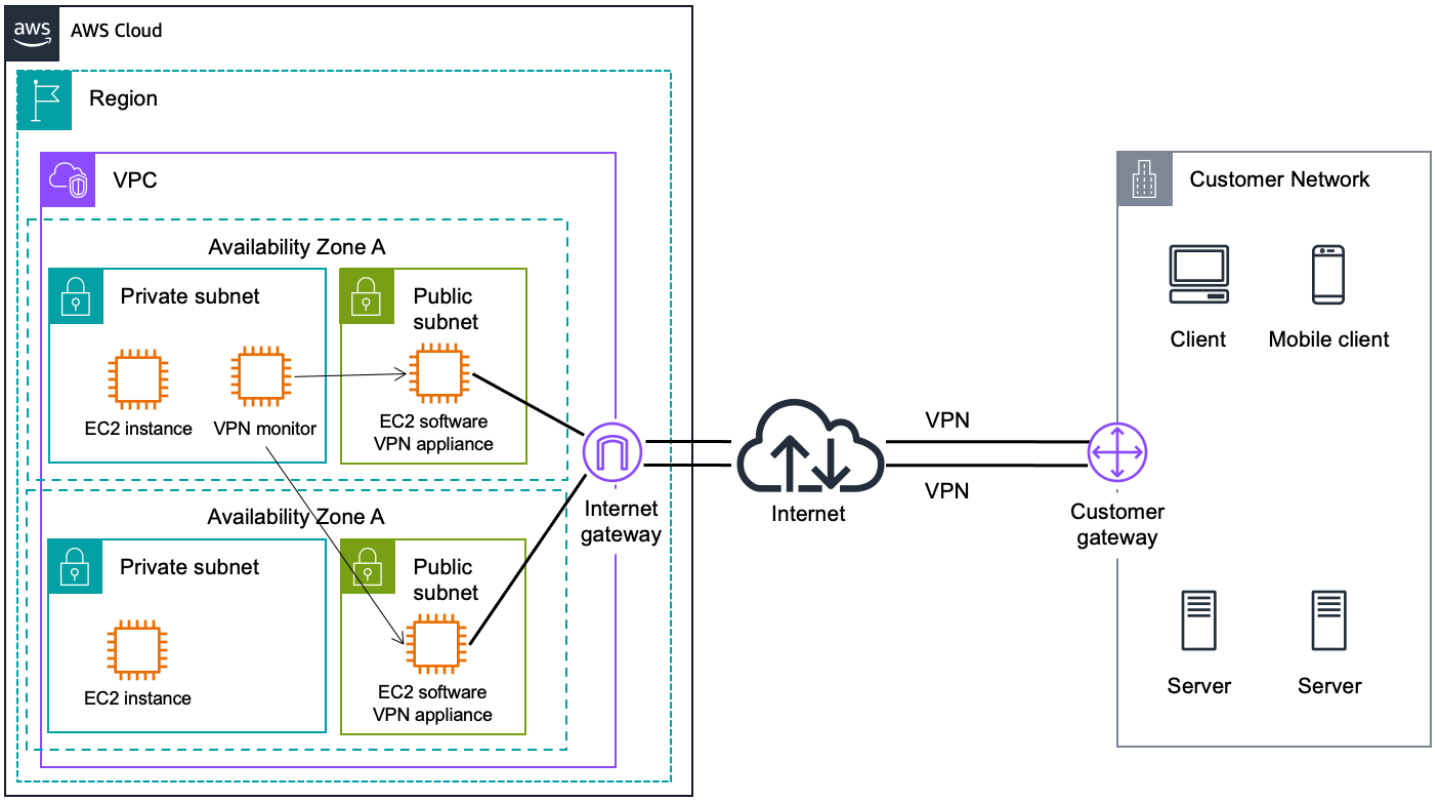
- Dokumentasi AWS Cloud WAN
- Posting blog: Pola migrasi dan interoperabilitas AWS Cloud WAN dan AWS Transit Gateway

Kesimpulan

AWS menyediakan sejumlah opsi konektivitas yang efisien dan aman untuk membantu Anda memaksimalkan AWS saat mengintegrasikan jaringan jarak jauh Anda dengan Amazon VPC. Opsi yang disediakan dalam whitepaper ini menyoroti beberapa opsi dan pola konektivitas yang telah digunakan pelanggan untuk berhasil mengintegrasikan jaringan jarak jauh mereka atau beberapa jaringan VPC Amazon. Anda dapat menggunakan informasi yang disediakan di sini untuk menentukan mekanisme yang paling tepat untuk menghubungkan infrastruktur yang diperlukan untuk menjalankan bisnis Anda terlepas dari di mana secara fisik berada atau dihosting.

Lampiran A: Arsitektur HA Tingkat Tinggi untuk instance VPN perangkat lunak

Membuat koneksi VPC yang sepenuhnya tangguh untuk instans VPN perangkat lunak memerlukan pengaturan dan konfigurasi beberapa instance VPN dan instance pemantauan untuk memantau kesehatan koneksi VPN.



Perangkat Lunak Tingkat Tinggi VPN HA

Sebaiknya konfigurasi tabel rute VPC Anda untuk memanfaatkan semua instans VPN secara bersamaan dengan mengarahkan lalu lintas dari semua subnet dalam satu Availability Zone melalui instans VPN masing-masing di Availability Zone yang sama. Setiap instans VPN kemudian menyediakan konektivitas VPN untuk instance yang berbagi Availability Zone yang sama.

Pemantauan VPN

Untuk memantau perangkat lunak berbasis VPN Anda dapat membuat Monitor VPN. Monitor VPN adalah contoh khusus yang Anda perlukan untuk menjalankan skrip pemantauan VPN. Instans ini dimaksudkan untuk menjalankan dan memantau keadaan koneksi VPN dan instance VPN. Jika

instance VPN atau koneksi mati, monitor harus menghentikan, menghentikan, atau memulai ulang instance VPN sambil juga mengalihkan lalu lintas dari subnet yang terpengaruh ke instance VPN yang berfungsi sampai kedua koneksi berfungsi kembali. Karena persyaratan pelanggan berbeda-beda, AWS saat ini tidak memberikan panduan preskriptif untuk menyiapkan instance pemantauan ini. Namun, contoh skrip untuk mengaktifkan HA antara instance NAT dapat digunakan sebagai titik awal untuk membuat solusi HA untuk instance VPN Perangkat Lunak. Kami menyarankan Anda memikirkan logika bisnis yang diperlukan untuk memberikan pemberitahuan atau mencoba memperbaiki konektivitas jaringan secara otomatis jika terjadi kegagalan koneksi VPN.

Selain itu, Anda dapat memantau terowongan AWS Managed VPN menggunakan CloudWatch metrik Amazon, yang mengumpulkan titik data dari layanan VPN menjadi metrik hampir real-time yang dapat dibaca. Setiap koneksi VPN mengumpulkan dan menerbitkan berbagai metrik terowongan ke Amazon. CloudWatch Metrik ini memungkinkan Anda memantau kesehatan terowongan, aktivitas, dan membuat tindakan otomatis.

Kontributor

Para kontributor untuk dokumen ini antara lain:

- Daniel Yu, Manajer Akun Teknis Senior, AWS Enterprise Support
- Garvit Singh, Pembuat Solusi, Arsitektur Solusi AWS
- Steve Morad, Manajer Senior, Pembangun Solusi, Arsitektur Solusi AWS
- Sohaib Tahir, Arsitek Solusi, Arsitektur Solusi AWS
- Fiona Armada, Arsitek Solusi Utama, Arsitektur Solusi AWS
- Pablo Sánchez Carmona, Arsitek Solusi Spesialis Jaringan, Arsitektur Solusi AWS
- Tony Hawke, Manajer Akun Teknis Spesialis Jaringan Senior, AWS Enterprise Support

Revisi dokumen

Untuk mengetahui jika ada perubahan pada laporan resmi ini, Anda dapat berlangganan umpan RSS.

Perubahan	Deskripsi	Tanggal
Laporan resmi diperbarui	Menambahkan AWS Cloud WAN dan Transit Gateway menghubungkan opsi lampiran, diagram yang diperbarui, dan informasi di seluruh bagian.	5 April 2023
Laporan resmi diperbarui	Menambahkan opsi AWS Transit Gateway dan AWS Client VPN, diagram dan informasi yang diperbarui.	Juni 6, 2020
Pembaruan kecil	Perubahan kecil untuk memperbaiki referensi ke perangkat lunak perangkat lunak VPN.	20 Mei 2020
Laporan resmi diperbarui	Informasi yang diperbarui di seluruh. Fokus pada desain/ fitur berikut: transit VPC, gateway Direct Connect, dan. AWS PrivateLink	Januari 1, 2018
Publikasi awal	Opsi Konektivitas Amazon Virtual Private Cloud diterbitk an.	1 Juli 2014

Pemberitahuan

Pelanggan bertanggung jawab untuk membuat penilaian independen mereka sendiri atas informasi dalam dokumen ini. Dokumen ini: (a) hanya untuk tujuan informasi, (b) mewakili penawaran dan praktik produk AWS saat ini, yang dapat berubah tanpa pemberitahuan, dan (c) tidak membuat komitmen atau jaminan apa pun dari AWS dan afiliasinya, pemasok, atau pemberi lisensinya. Produk atau layanan AWS disediakan “sebagaimana adanya” tanpa jaminan, pernyataan, atau ketentuan dalam bentuk apa pun, baik tersurat maupun tersirat. Tanggung jawab dan kewajiban AWS kepada pelanggannya dikendalikan oleh perjanjian AWS, dan dokumen ini bukan bagian dari, juga tidak mengubah, perjanjian apa pun antara AWS dan pelanggannya.

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.