AWS Whitepaper

Membangun Infrastruktur Multi VPC AWS Jaringan yang Skalabel dan Aman

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Membangun Infrastruktur Multi VPC AWS Jaringan yang Skalabel dan Aman: AWS Whitepaper

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Merek dagang dan tampilan dagang Amazon tidak boleh digunakan sehubungan dengan produk atau layanan apa pun yang bukan milik Amazon, dengan cara apa pun yang dapat menyebabkan kebingungan di antara pelanggan, atau dengan cara apa pun yang menghina atau mendiskreditkan Amazon. Semua merek dagang lain yang tidak dimiliki oleh Amazon merupakan properti dari masing-masing pemilik, yang mungkin berafiliasi, terkait dengan, atau disponsori oleh Amazon, atau tidak.

Table of Contents

Membangun Infrastruktur Jaringan AWS Multi-VPC yang Dapat Diskalakan dan Aman

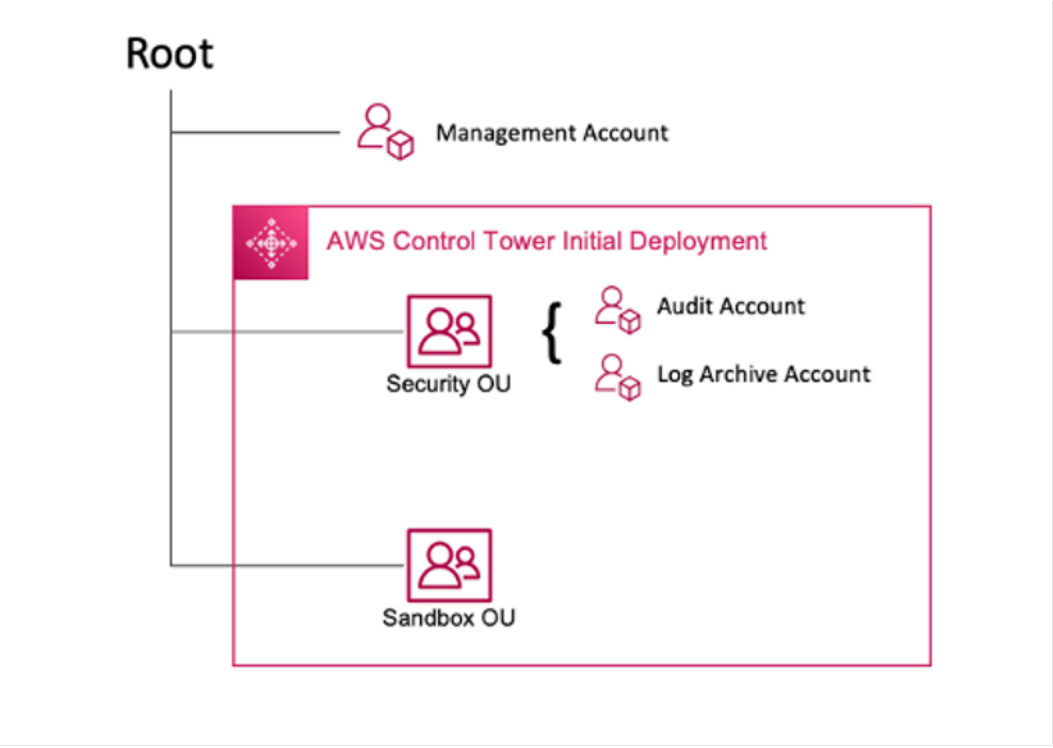
Tanggal publikasi: 17 April 2024 () Riwayat dokumen

Pelanggan Amazon Web Services (AWS) sering mengandalkan ratusan akun dan virtual private cloud (VPC) untuk mengelompokkan beban kerja mereka dan memperluas jejak mereka.Tingkat skala ini sering menimbulkan tantangan seputar berbagi sumber daya, konektivitas antar-VPC, dan fasilitas lokal ke konektivitas VPC.

Whitepaper ini menjelaskan praktik terbaik untuk membuat arsitektur jaringan yang dapat diskalakan dan aman dalam jaringan besar menggunakan AWS layanan seperti Amazon Virtual Private Cloud (Amazon VPC),,,,, AWS PrivateLinkGateway AWS Direct ConnectLoad Balancer AWS Transit Gateway, dan Amazon Route 53. AWS Network Firewall Ini menunjukkan solusi untuk mengelola infrastruktur yang berkembang — memastikan skalabilitas, ketersediaan tinggi, dan keamanan sambil menjaga biaya overhead tetap rendah.

Pengantar

AWS pelanggan memulai dengan membangun sumber daya dalam satu AWS akun yang mewakili batas manajemen yang mengelompokkan izin, biaya, dan layanan. Namun, seiring pertumbuhan organisasi pelanggan, segmentasi layanan yang lebih besar diperlukan untuk memantau biaya, mengontrol akses, dan menyediakan pengelolaan lingkungan yang lebih mudah. Solusi multi-akun memecahkan masalah ini dengan menyediakan akun khusus untuk layanan TI dan pengguna dalam suatu organisasi. AWS menyediakan beberapa alat untuk mengelola dan mengkonfigurasi infrastruktur ini, termasuk AWS Control Tower.



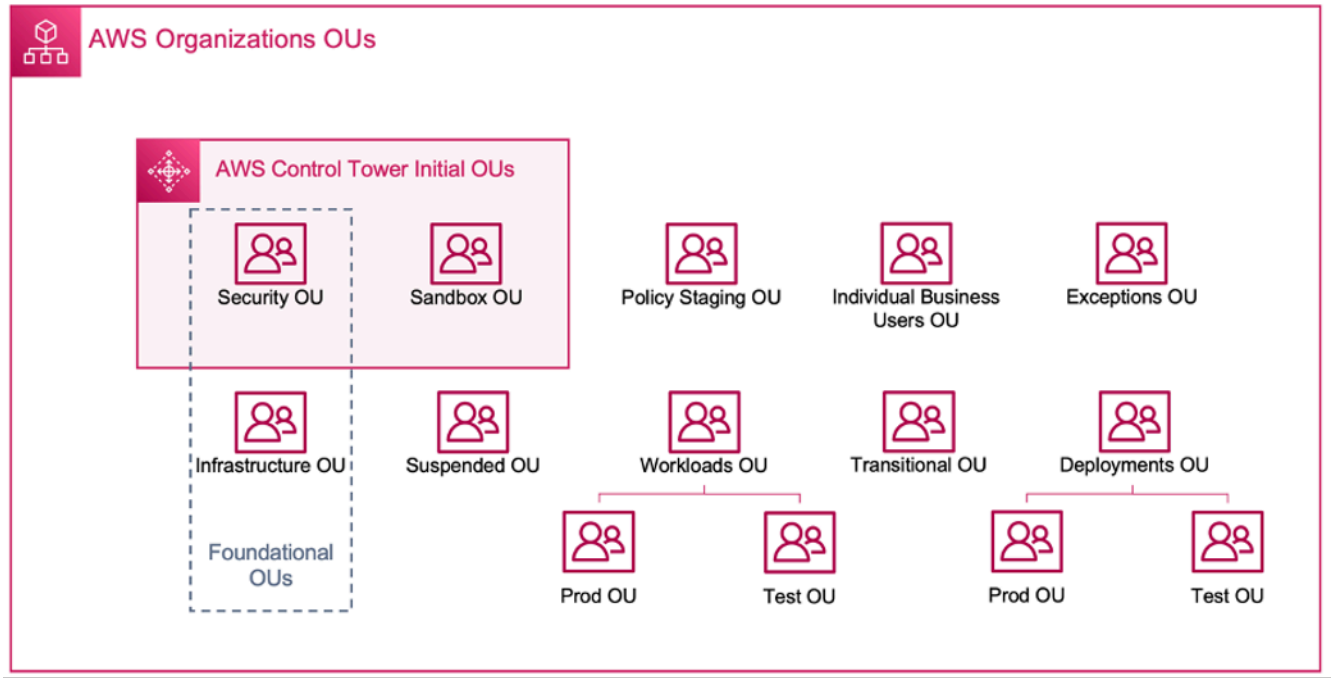
AWS Penyebaran awal Control Tower

Ketika Anda mengatur lingkungan multi-akun Anda menggunakan AWS Control Tower, itu menciptakan dua Unit Organisasi (OU):

- Keamanan OU - Dalam OU ini, AWS Control Tower membuat dua akun:
- Arsip Log
- Audit (Akun ini sesuai dengan akun Tooling keamanan yang dibahas sebelumnya dalam panduan.)
- Sandbox OU - OU ini adalah tujuan default untuk akun yang dibuat di dalamnya AWS Control Tower. Ini berisi akun tempat pembangun Anda dapat menjelajahi dan bereksperimen dengan AWS layanan, serta alat dan layanan lainnya, tunduk pada kebijakan penggunaan yang dapat diterima tim Anda.

AWS Control Tower memungkinkan Anda untuk membuat, mendaftar, dan mengelola OU tambahan untuk memperluas lingkungan awal untuk menerapkan panduan.

Diagram berikut menunjukkan OU yang awalnya digunakan oleh AWS Control Tower. Anda dapat memperluas AWS lingkungan Anda untuk menerapkan salah satu dari OU yang direkomendasikan termasuk dalam diagram, untuk memenuhi kebutuhan Anda.



AWS OU organisasi

Untuk detail lebih lanjut tentang penggunaan lingkungan multi-akun AWS Control Tower, lihat Lampiran E di whitepaper Mengatur AWS Lingkungan Anda Menggunakan Beberapa Akun.

> **Note**
>
> Dalam whitepaper ini, “Control Tower” adalah istilah luas untuk pengaturan Multi-akun/Multi-VPC yang dapat diskalakan, aman, dan berkinerja baik di mana Anda menerapkan beban kerja Anda. Pengaturan ini dapat dibangun menggunakan alat yang berbeda. Anda dapat menemukan informasi selengkapnya tentang praktik terbaik, prinsip desain, dan manfaat fondasi cloud multi-akun di whitepaper Mengatur AWS Lingkungan Anda Menggunakan Beberapa Akun.

Sebagian besar pelanggan memulai dengan beberapa VPC untuk menyebarkan infrastruktur mereka. Jumlah VPC yang dibuat pelanggan biasanya terkait dengan jumlah akun, pengguna, dan lingkungan bertahap mereka (produksi, pengembangan, pengujian, dan sebagainya). Seiring bertambahnya penggunaan cloud, jumlah pengguna, unit bisnis, aplikasi, dan Wilayah yang berinteraksi dengan pelanggan juga tumbuh, yang mengarah pada penciptaan VPC baru.

Seiring bertambahnya jumlah VPC, manajemen lintas VPC menjadi penting untuk pengoperasian jaringan cloud pelanggan. Whitepaper ini mencakup praktik terbaik untuk tiga area spesifik dalam konektivitas lintas-VPC dan hybrid:

- Konektivitas jaringan — Menghubungkan VPC dan jaringan lokal dalam skala besar.
- Keamanan jaringan — Membangun titik keluar terpusat untuk mengakses internet dan titik akhir seperti gateway terjemahan alamat jaringan (NAT), titik akhir VPC,,, dan Gateway Load Balancer. AWS PrivateLinkAWS Network Firewall
- Manajemen DNS — Menyelesaikan DNS dalam Control Tower dan DNS hybrid.

Perencanaan dan manajemen alamat IP

Untuk membangun desain jaringan multi-VPC multi-akun yang dapat diskalakan, perencanaan dan manajemen alamat IP sangat penting. Skema pengalamatan IP yang baik perlu mempertimbangkan kebutuhan jaringan Anda saat ini dan masa depan. Skema alamat IP IP Anda harus mencakup beban kerja lokal Anda, beban kerja cloud Anda, dan juga harus memungkinkan ekspansi masa depan (misalnya, penambahan unit bisnis baru Wilayah AWS, dan merger atau akuisisi). Ini juga harus mencegah tim Anda secara tidak sengaja membuat CIDR IP yang tumpang tindih. Jika CIDR IP yang tumpang tindih diinginkan seperti untuk beban kerja yang terisolasi atau terputus, keputusan ini perlu disadari dan harus memperhitungkan implikasi pada perutean, keamanan, dan biaya. Anda mungkin juga perlu mempertimbangkan untuk membuat proses persetujuan yang diperlukan untuk pengecualian tersebut. Skema pengalamatan IP yang baik juga membantu menyederhanakan desain jaringan dan konfigurasi perutean Anda.

Pertimbangan utama:

- Rencanakan skema pengalamatan IP Anda (IP publik dan pribadi) di depan dan pilih alat manajemen alamat IP untuk mengalokasikan, mengelola, dan melacak penggunaan alamat IP di semua beban kerja Anda.
- Gunakan skema pengalamatan IP hierarkis dan diringkas.
- Merencanakan penugasan IP yang konsisten berdasarkan lingkungan Wilayah AWS, organisasi, atau unit bisnis.
- Tentukan CIDR IP yang berbeda (IPv4 dan IPv6) untuk jaringan lokal dan cloud.
- Secara proaktif mencegah dan melacak CIDR IP yang tumpang tindih.
- Ukur CIDR IP Anda dengan tepat untuk memungkinkan penskalaan dan pertumbuhan masa depan.

- Aktifkan beban kerja Anda untuk IPv6 atau kompatibilitas dual-stack untuk mengurangi konflik IP dan mengatasi penipisan ruang IPv4.

Anda dapat menggunakan Amazon VPC IP Address Manager (IPAM) untuk menyederhanakan perencanaan, pelacakan, dan pemantauan alamat IP publik dan pribadi untuk beban kerja Anda. AWS IPAM memungkinkan Anda untuk mengatur, mengalokasikan, memantau, dan berbagi ruang alamat IP di beberapa Wilayah AWS dan. Akun AWS Ini juga membantu alokasi otomatis CIDR ke VPC menggunakan aturan bisnis tertentu.

Lihat Praktik Terbaik Manajer Alamat IP VPC Amazon, Mengelola kumpulan IP di seluruh VPC dan Wilayah menggunakan Manajer Alamat IP VPC Amazon VPC, dan Manajemen Alamat IP untuk posting AWS Control Tower blog guna mempelajari praktik terbaik pengalamatan IP dan cara menggunakan IPAM untuk mengelola kumpulan IP di seluruh VPC,, dan. Wilayah AWS AWS Control Tower

Apakah Anda sudah Well-Architected?

Kerangka Kerja AWS Well-Architected membantu Anda memahami pro dan kontra dari keputusan yang Anda buat saat membangun sistem di cloud. Enam pilar dari Kerangka Kerja ini memungkinkan Anda mempelajari praktik terbaik arsitektural untuk merancang dan mengoperasikan sistem yang andal, aman, efisien, hemat biaya, dan berkelanjutan. Dengan menggunakan AWS Well-Architected Tool, tersedia tanpa biaya di AWS Management Console, Anda dapat meninjau beban kerja Anda terhadap praktik terbaik ini dengan menjawab serangkaian pertanyaan untuk setiap pilar.

Untuk panduan lebih lanjut dari para ahli dan praktik terbaik untuk arsitektur cloud Anda—referensi penerapan arsitektur, diagram, dan laporan resmi—lihat Pusat Arsitektur AWS.

Konektivitas VPC ke VPC

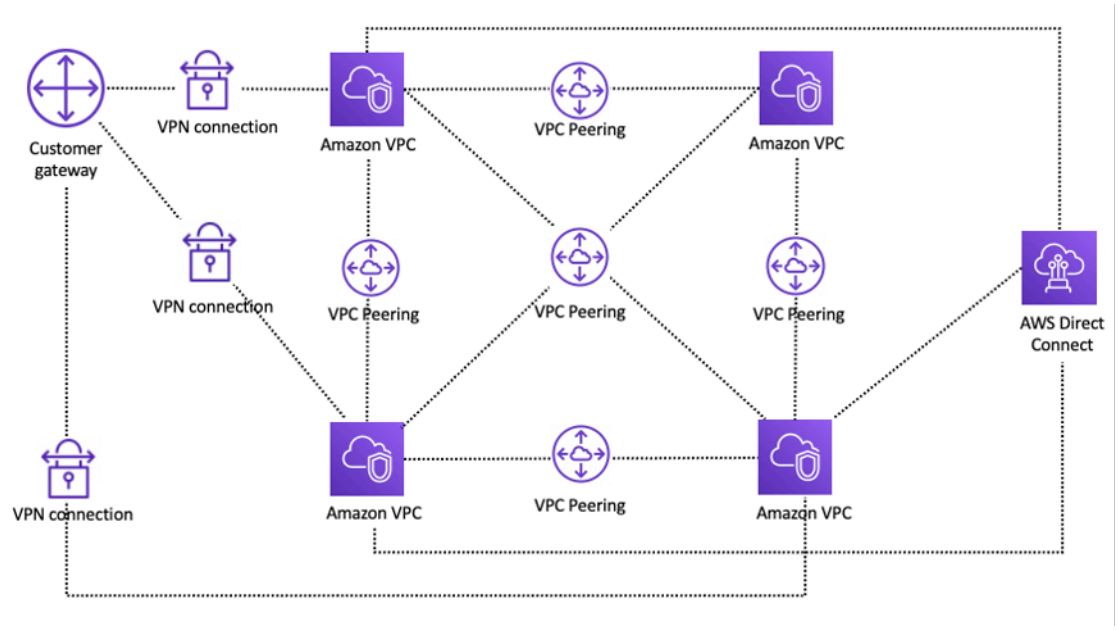
Pelanggan dapat menggunakan dua pola konektivitas VPC yang berbeda untuk mengatur lingkungan multi-VPC: banyak ke banyak, atau hub dan bicara. Dalam many-to-many pendekatannya, lalu lintas antara setiap VPC dikelola secara individual antara setiap VPC. Dalam hub-and-spoke model, semua lalu lintas antar-VPC mengalir melalui sumber daya pusat, yang merutekan lalu lintas berdasarkan aturan yang ditetapkan.

Peering VPC

Cara pertama untuk menghubungkan dua VPC adalah dengan menggunakan VPC peering. Dalam pengaturan ini, koneksi memungkinkan konektivitas dua arah penuh antara VPC. Koneksi peering ini digunakan untuk merutekan lalu lintas antar VPC. VPC di berbagai akun dan Wilayah AWS juga dapat diintip bersama. Semua transfer data melalui koneksi peering VPC yang tetap berada dalam Availability Zone gratis. Semua transfer data melalui koneksi peering VPC yang melintasi Availability Zone dibebankan pada kecepatan transfer data dalam wilayah standar. Jika VPC diintip di seluruh Wilayah, biaya transfer data antar wilayah standar akan berlaku.

VPC peering adalah point-to-point konektivitas, dan tidak mendukung perutean transitif. Misalnya, jika Anda memiliki koneksi peering VPC antara VPC A dan VPC B dan antara VPC A dan VPC C, instance di VPC B tidak dapat transit melalui VPC A untuk mencapai VPC C. Untuk merutekan paket antara VPC B dan VPC C, Anda diminta untuk membuat koneksi peering VPC langsung.

Pada skala besar, ketika Anda memiliki puluhan atau ratusan VPC, menghubungkannya dengan pengintip dapat menghasilkan ratusan atau ribuan koneksi pengintip. Sejumlah besar koneksi bisa sulit untuk dikelola dan ditingkatkan. Misalnya, jika Anda memiliki 100 VPC dan Anda ingin mengatur peering mesh penuh di antara mereka, dibutuhkan 4.950 koneksi peering [n(n-1)/2] di mana n jumlah total VPC. Ada batas maksimum 125 koneksi peering aktif per VPC.



Pengaturan jaringan menggunakan peering VPC

Jika Anda menggunakan peering VPC, konektivitas lokal (VPN dan/atau Direct Connect) harus dilakukan ke setiap VPC. Sumber daya dalam VPC tidak dapat menjangkau lokal menggunakan konektivitas hybrid dari VPC peered, seperti yang ditunjukkan pada gambar sebelumnya.

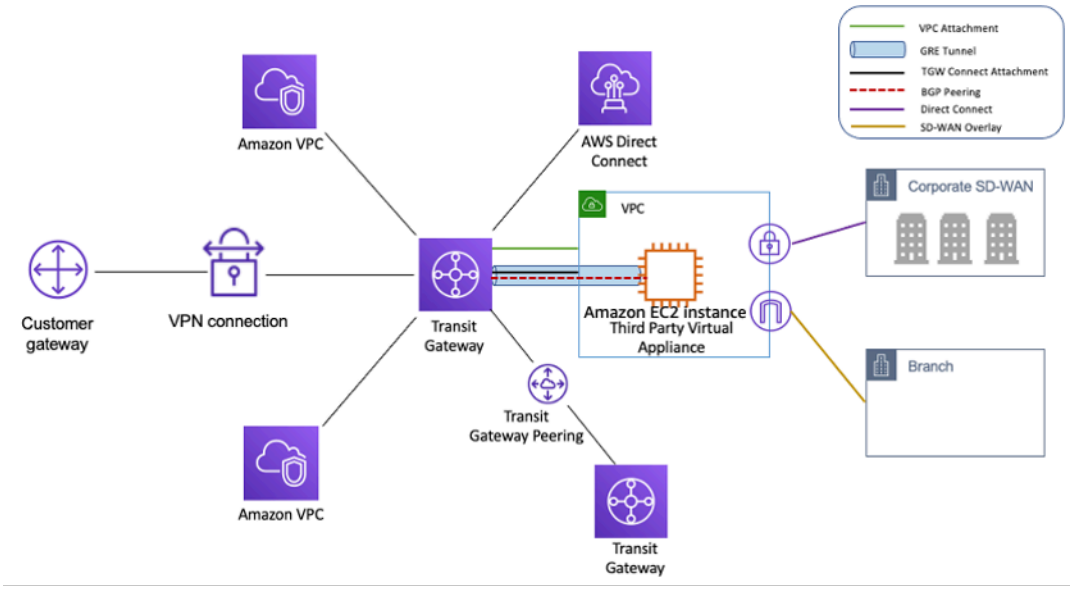
Peering VPC paling baik digunakan ketika sumber daya dalam satu VPC harus berkomunikasi dengan sumber daya di VPC lain, lingkungan kedua VPC dikendalikan dan diamankan, dan jumlah VPC yang akan dihubungkan kurang dari 10 (untuk memungkinkan manajemen individu dari setiap koneksi). VPC peering menawarkan biaya keseluruhan terendah dan kinerja agregat tertinggi jika dibandingkan dengan opsi lain untuk konektivitas antar-VPC.

AWS Transit Gateway

AWS Transit Gatewaymenyediakan desain hub dan spoke untuk menghubungkan VPC dan jaringan lokal sebagai layanan yang dikelola sepenuhnya tanpa mengharuskan Anda menyediakan peralatan virtual pihak ketiga. Tidak diperlukan hamparan VPN, dan AWS mengelola ketersediaan dan skalabilitas tinggi.

Transit Gateway memungkinkan pelanggan untuk menghubungkan ribuan VPC. Anda dapat melampirkan semua konektivitas hybrid Anda (koneksi VPN dan Direct Connect) ke satu gateway, mengkonsolidasikan dan mengendalikan seluruh konfigurasi AWS perutean organisasi Anda di satu tempat (lihat gambar berikut). Transit Gateway mengontrol bagaimana lalu lintas dirutekan di

antara semua jaringan spoke yang terhubung menggunakan tabel rute. hub-and-spoke Model ini menyederhanakan manajemen dan mengurangi biaya operasional karena VPC hanya terhubung ke instance Transit Gateway untuk mendapatkan akses ke jaringan yang terhubung.



Desain hub dan bicara dengan AWS Transit Gateway

Transit Gateway adalah sumber daya Regional dan dapat menghubungkan ribuan VPC dalam satu sama Wilayah AWS. Anda dapat menghubungkan beberapa gateway melalui satu koneksi Direct Connect untuk konektivitas hybrid. Biasanya, Anda dapat menggunakan hanya satu instance Transit Gateway yang menghubungkan semua instance VPC Anda di Wilayah tertentu, dan menggunakan tabel perutean Transit Gateway untuk mengisolasinya di mana pun diperlukan. Perhatikan bahwa Anda tidak memerlukan gateway transit tambahan untuk ketersediaan tinggi, karena gateway transit sangat tersedia secara desain; untuk redundansi, gunakan satu gateway di setiap Wilayah. Namun, ada kasus yang valid untuk membuat beberapa gateway untuk membatasi radius ledakan miskonfigurasi, memisahkan operasi bidang kontrol, dan administrasi. ease-of-use

Dengan mengintip Transit Gateway, pelanggan dapat mengintip instans Transit Gateway mereka dalam Wilayah yang sama atau beberapa dan merutekan lalu lintas di antara mereka. Ini menggunakan infrastruktur dasar yang sama seperti pengintip VPC, dan karena itu dienkripsi. Untuk informasi selengkapnya, lihat Membangun jaringan global menggunakan AWS Transit Gateway Inter-Region peering dan AWS Transit Gateway sekarang mendukung Intra-Region Peering.

Tempatkan instance Transit Gateway organisasi Anda di akun Layanan Jaringannya. Ini memungkinkan manajemen terpusat oleh insinyur jaringan yang mengelola akun layanan Jaringan. Gunakan AWS Resource Access Manager (RAM) untuk berbagi instans Transit Gateway untuk menghubungkan VPC di beberapa akun di AWS Organization Anda dalam Wilayah yang sama.AWS

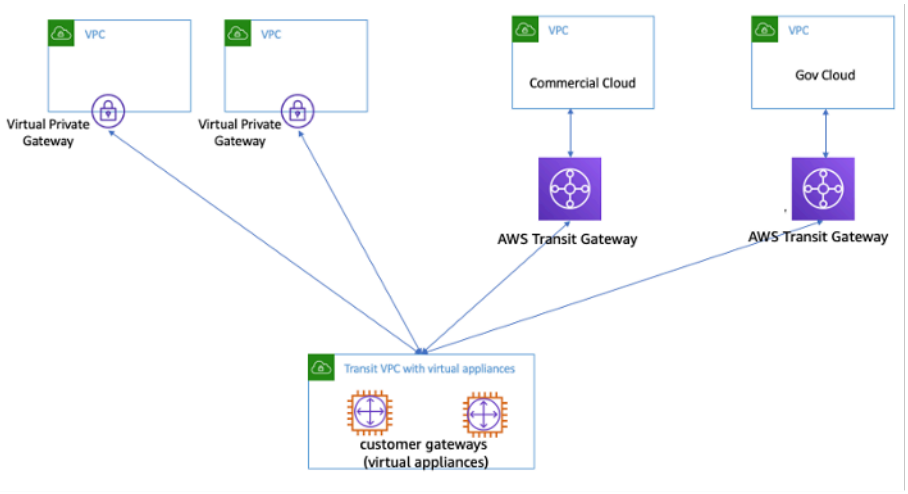
RAM memungkinkan Anda berbagi AWS sumber daya dengan mudah dan aman dengan apa pun Akun AWS, atau di dalam AWS Organization Anda. Untuk informasi selengkapnya, lihat lampiran AWS Transit Gateway Otomatis ke gateway transit di posting blog akun pusat.

Transit Gateway juga memungkinkan Anda untuk membangun konektivitas antara infrastruktur SD-WAN dan AWS menggunakan Transit Gateway Connect. Gunakan lampiran Transit Gateway Connect dengan Border Gateway Protocol (BGP) untuk perutean dinamis dan protokol terowongan Generic Routing Encapsulation (GRE) untuk kinerja tinggi, memberikan bandwidth total hingga 20 Gbps per lampiran Connect (hingga empat rekan Transit Gateway Connect per lampiran Connect). Dengan menggunakan Transit Gateway Connect, Anda dapat mengintegrasikan infrastruktur SD-WAN lokal atau peralatan SD-WAN yang berjalan di cloud melalui lampiran atau AWS Direct Connect lampiran VPC sebagai lapisan transport yang mendasarinya. Lihat Sederhanakan konektivitas SD-WAN dengan AWS Transit Gateway Connect untuk arsitektur referensi dan konfigurasi terperinci.

Solusi VPC Transit

Transit VPC dapat menciptakan konektivitas antar VPC dengan cara yang berbeda dari VPC peering dengan memperkenalkan desain hub dan spoke untuk konektivitas antar-VPC. Dalam jaringan VPC transit, satu VPC pusat (hub VPC) terhubung dengan setiap VPC lainnya (spoke VPC) melalui koneksi VPN yang biasanya memanfaatkan BGP melalui IPsec. VPC pusat berisi instans Amazon Elastic Compute Cloud (Amazon EC2) yang menjalankan peralatan perangkat lunak yang merutekan lalu lintas masuk ke tujuan mereka menggunakan hamparan VPN. Transit VPC peering memiliki keuntungan sebagai berikut:

- Perutean transitif diaktifkan menggunakan jaringan VPN overlay — memungkinkan desain hub dan spoke.
- Saat menggunakan perangkat lunak vendor pihak ketiga pada instans EC2 di VPC transit hub, fungsionalitas vendor seputar keamanan tingkat lanjut (lapisan 7 Firewall/Intrusion Prevention System (IPS) /Intrusion Detection System (IDS)) dapat digunakan. Jika pelanggan menggunakan perangkat lunak yang sama di tempat, mereka mendapat manfaat dari pengalaman operasional/pemantauan terpadu.
- Arsitektur VPC Transit memungkinkan konektivitas yang mungkin diinginkan dalam beberapa kasus penggunaan. Misalnya, Anda dapat menghubungkan GovCloud instans AWS dan VPC Wilayah Komersil atau instans Gateway Transit ke VPC Transit dan mengaktifkan konektivitas antar-VPC antara kedua Wilayah. Evaluasi persyaratan keamanan dan kepatuhan Anda saat mempertimbangkan opsi ini. Untuk keamanan tambahan, Anda dapat menerapkan model inspeksi terpusat menggunakan pola desain yang dijelaskan nanti dalam whitepaper ini.



Transit VPC dengan peralatan virtual

Transit VPC hadir dengan tantangannya sendiri, seperti biaya yang lebih tinggi untuk menjalankan peralatan virtual vendor pihak ketiga di EC2 berdasarkan ukuran/keluarga instans, throughput terbatas per koneksi VPN (hingga 1,25 Gbps per terowongan VPN), dan konfigurasi tambahan, manajemen, dan overhead ketahanan (pelanggan bertanggung jawab untuk mengelola HA dan redundansi instans EC2 yang menjalankan peralatan virtual vendor pihak ketiga).

Pengintip VPC vs Transit VPC vs Gerbang Transit

Tabel 1 - Perbandingan konektivitas

Kriteria	Peering VPC	Transit VPC	Transit Gateway	PrivateLink	Awan WAN	Kisi VPC
Cakupan	Regional/ Global	Regional	Regional	Regional	Global	Regional
Arsitektur	Jala penuh	Berbasis VPN hub-and-spoke	Berbasis lampiran hub-and-spoke	Model Penyedia atau Konsumen	Berbasis lampiran, multi-wilayah	Konektivitas Aplikasi ke Aplikasi
Penskalaan	125 rekan aktif/VPC	Tergantung pada virtual router/EC2	5000 lampiran per Wilayah	Tidak ada batasan	5000 lampiran per jaringan inti	500 asosiasi VPC per layanan

Kriteria	Peering VPC	Transit VPC	Transit Gateway	PrivateLink	Awan WAN	Kisi VPC
Segmentasi	Grup keamanan	Pelanggan dikelola	Tabel rute Transit Gateway	Tidak ada segmentasi	Segmen	Kebijakan jaringan layanan dan layanan
Latensi	Terendah	Ekstra, karena overhead enkripsi VPN	Transit Gateway tambahan hop	Lalu lintas tetap berada di tulang punggung AWS, pelanggan harus menguji	Menggunakan jalur data yang sama dengan Transit Gateway	Lalu lintas tetap berada di tulang punggung AWS, pelanggan harus menguji
Batas bandwidth	Batas per instance, tidak ada batas agregat	Tunduk pada batas bandwidth instans EC2 berdasarkan ukuran/keluarga	Hingga 100 Gbps (burst) / attachment	10 Gbps per Availability Zone, secara otomatis menskalakan hingga 100 Gbps	Hingga 100 Gbps (burst) / attachment	10 Gbps per Zona Ketersediaan

Kriteria	Peering VPC	Transit VPC	Transit Gateway	PrivateLink	Awan WAN	Kisi VPC
Visibilitas	Log Alur VPC	Log dan Metrik Aliran VPC CloudWatch	Manajer Jaringan Transit Gateway, Log Aliran VPC, Metrik CloudWatch	CloudWatch Metrik	Manajer Jaringan, Log Aliran VPC, Metrik CloudWatch	CloudWatch Akses Log
Grup keamanan referensi silang	Didukung	Tidak didukung	Tidak didukung	Tidak didukung	Tidak didukung	Tidak berlaku
Dukungan IPv6	Didukung	Tergantung pada alat virtual	Didukung	Didukung	Didukung	Didukung

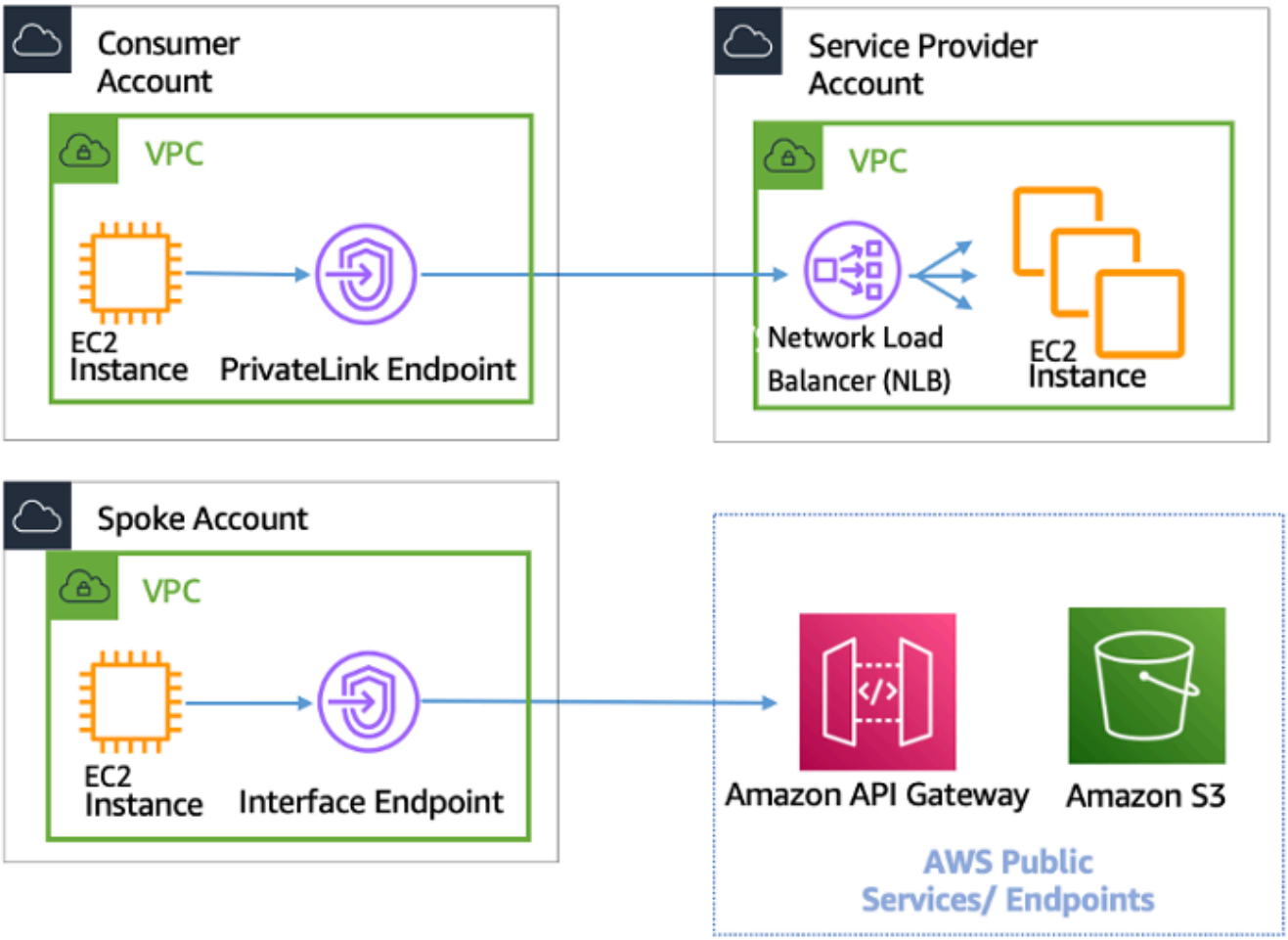
AWS PrivateLink

AWS PrivateLinkmenyediakan konektivitas pribadi antara VPC, layanan AWS, dan jaringan lokal Anda tanpa mengekspos lalu lintas Anda ke internet publik. Endpoint VPC antarmuka, didukung oleh AWS PrivateLink, memudahkan untuk terhubung ke AWS dan layanan lain di berbagai akun dan VPC untuk menyederhanakan arsitektur jaringan Anda secara signifikan. Hal ini memungkinkan pelanggan yang mungkin ingin secara pribadi mengekspos layanan/aplikasi yang berada di satu VPC (penyedia layanan) ke VPC lain (konsumen) dengan cara yang hanya VPC konsumen Wilayah AWS yang memulai koneksi ke VPC penyedia layanan. Contohnya adalah kemampuan aplikasi pribadi Anda untuk mengakses API penyedia layanan.

Untuk menggunakannya AWS PrivateLink, buat Network Load Balancer untuk aplikasi Anda di VPC Anda, dan buat konfigurasi layanan titik akhir VPC yang mengarah ke penyeimbang beban tersebut. Konsumen layanan kemudian membuat titik akhir antarmuka ke layanan Anda. Ini menciptakan

elastic network interface (ENI) di subnet konsumen dengan alamat IP pribadi yang berfungsi sebagai titik masuk untuk lalu lintas yang ditujukan untuk layanan. Konsumen dan layanan tidak diharuskan berada dalam VPC yang sama. Jika VPC berbeda, VPC konsumen dan penyedia layanan dapat memiliki rentang alamat IP yang tumpang tindih. Selain membuat titik akhir VPC antarmuka untuk mengakses layanan di VPC lain, Anda dapat membuat titik akhir VPC antarmuka untuk mengakses layanan AWS yang didukung secara pribadi, seperti yang ditunjukkan pada gambar berikut AWS PrivateLink.

Dengan Application Load Balancer (ALB) sebagai target NLB, Anda sekarang dapat menggabungkan kemampuan routing lanjutan ALB dengan. AWS PrivateLink Lihat Grup Target Tipe Application Load Balancer untuk Network Load Balancer untuk arsitektur referensi dan konfigurasi terperinci.



AWS PrivateLink untuk konektivitas ke VPC dan AWS Services lainnya

Pilihan antara Transit Gateway, VPC peering, dan tergantung pada AWS PrivateLink konektivitas.

- AWS PrivateLink— Gunakan AWS PrivateLink ketika Anda memiliki klien/server yang diatur di mana Anda ingin mengizinkan satu atau lebih VPC konsumen akses searah ke layanan tertentu atau serangkaian instance di VPC penyedia layanan atau layanan tertentu. AWS Hanya klien dengan akses di VPC konsumen yang dapat memulai koneksi ke layanan di VPC atau layanan penyedia layanan. AWS Ini juga merupakan pilihan yang baik ketika klien dan server di dua VPC memiliki alamat IP yang tumpang tindih karena AWS PrivateLink menggunakan ENI dalam VPC klien dengan cara yang memastikan bahwa tidak ada konflik IP dengan penyedia layanan. Anda dapat mengakses AWS PrivateLink titik akhir melalui VPC peering, VPN, Transit Gateway, Cloud WAN, dan. AWS Direct Connect
- Peering VPC dan Transit Gateway — Gunakan peering VPC dan Transit Gateway saat Anda ingin mengaktifkan konektivitas IP layer-3 antar VPC.

  Arsitektur Anda akan berisi campuran teknologi ini untuk memenuhi kasus penggunaan yang berbeda. Semua layanan ini dapat digabungkan dan dioperasikan satu sama lain. Misalnya, AWS PrivateLink menangani konektivitas client-server gaya API, peering VPC untuk menangani persyaratan konektivitas langsung di mana grup penempatan mungkin masih diinginkan dalam konektivitas Wilayah atau Antar wilayah, dan Transit Gateway untuk menyederhanakan konektivitas VPC dalam skala besar serta konsolidasi tepi untuk konektivitas hybrid.

Pembagian VPC

Berbagi VPC berguna ketika isolasi jaringan antar tim tidak perlu dikelola secara ketat oleh pemilik VPC, tetapi pengguna dan izin tingkat akun harus. Dengan VPC Bersama, beberapa akun AWS membuat sumber daya aplikasinya (seperti instans Amazon EC2) dalam VPC Amazon bersama yang dikelola secara terpusat. Dalam model ini, akun yang memiliki VPC (pemilik) berbagi satu atau lebih subnet dengan akun lain (peserta). Setelah subnet dibagikan, peserta dapat melihat, membuat, mengubah, dan menghapus sumber daya aplikasi mereka di subnet yang dibagikan dengan mereka. Peserta tidak dapat melihat, mengubah, atau menghapus sumber daya milik peserta lain atau pemilik VPC. Keamanan antara sumber daya dalam VPC bersama dikelola menggunakan grup keamanan, daftar kontrol akses jaringan (NACL), atau melalui firewall antara subnet.

Manfaat berbagi VPC:

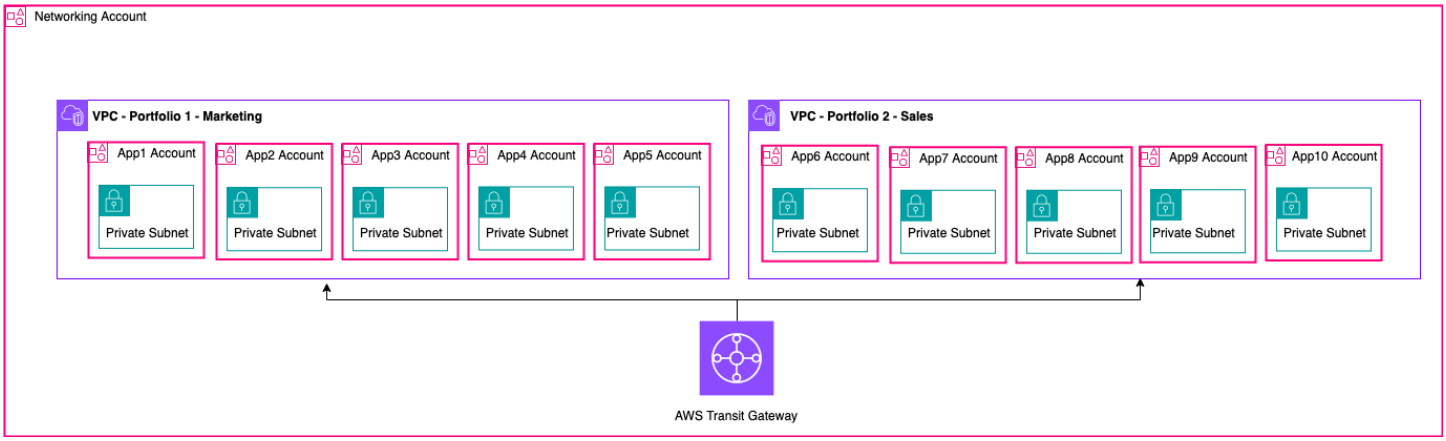
- Desain yang disederhanakan - tidak ada kerumitan seputar konektivitas antar-VPC
- Lebih sedikit VPC yang dikelola
- Pemisahan tugas antara tim jaringan dan pemilik aplikasi

- Pemanfaatan alamat IPv4 yang lebih baik
- Biaya lebih rendah — tidak ada biaya transfer data antar instans milik akun berbeda dalam Availability Zone yang sama

> **Note**
>
> Ketika Anda berbagi subnet dengan beberapa akun, peserta Anda harus memiliki beberapa tingkat kerja sama karena mereka berbagi ruang IP dan sumber daya jaringan. Jika perlu, Anda dapat memilih untuk berbagi subnet yang berbeda untuk setiap akun peserta. Satu subnet per peserta memungkinkan ACL jaringan untuk menyediakan isolasi jaringan selain kelompok keamanan.

Sebagian besar arsitektur pelanggan akan berisi beberapa VPC, banyak di antaranya akan dibagikan dengan dua atau lebih akun. Transit Gateway dan VPC peering dapat digunakan untuk menghubungkan VPC bersama. Misalnya, Anda memiliki 10 aplikasi. Setiap aplikasi memerlukan akun AWS sendiri. Aplikasi dapat dikategorikan menjadi dua portofolio aplikasi (aplikasi dalam portofolio yang sama memiliki persyaratan jaringan yang sama, Aplikasi 1-5 di 'Pemasaran' dan Aplikasi 6-10 di 'Penjualan').

Anda dapat memiliki satu VPC per portofolio aplikasi (total dua VPC), dan VPC dibagikan dengan akun pemilik aplikasi yang berbeda dalam portofolio itu. Pemilik aplikasi menyebarkan aplikasi ke VPC bersama masing-masing (dalam hal ini, dalam subnet yang berbeda untuk segmentasi dan isolasi rute jaringan menggunakan NACL). Kedua VPC bersama terhubung melalui Transit Gateway. Dengan pengaturan ini, Anda bisa beralih dari harus menghubungkan 10 VPC menjadi hanya dua, seperti yang terlihat pada gambar berikut.

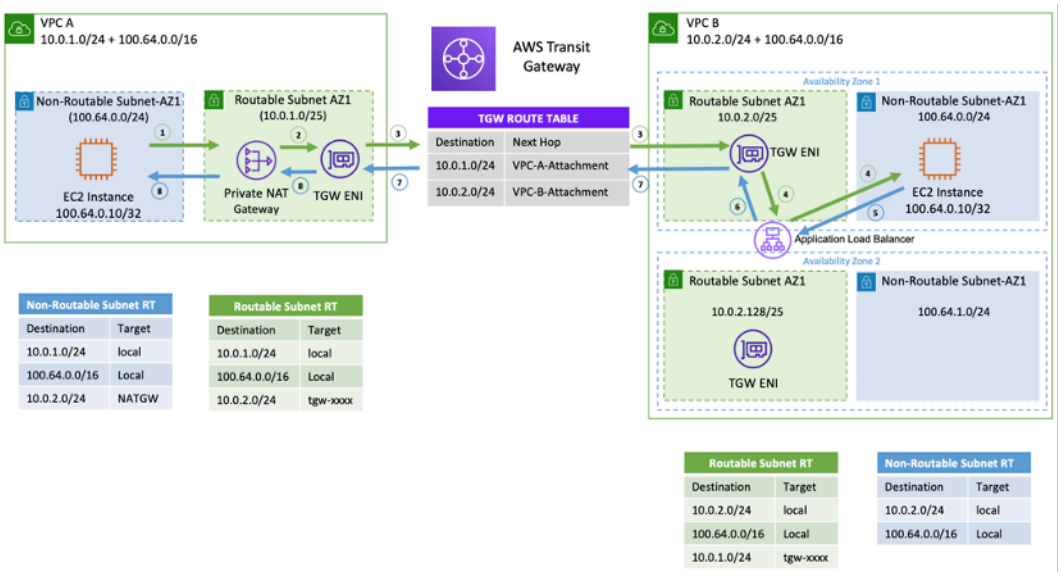


Contoh pengaturan - VPC bersama

> **Note**
>
> Peserta berbagi VPC tidak dapat membuat semua sumber daya AWS di subnet bersama. Untuk informasi selengkapnya, lihat bagian Batasan di dokumentasi Berbagi VPC.
> Untuk informasi lebih lanjut tentang pertimbangan utama dan praktik terbaik untuk berbagi VPC, lihat berbagi VPC: pertimbangan utama dan praktik terbaik posting blog.

Gerbang NAT Pribadi

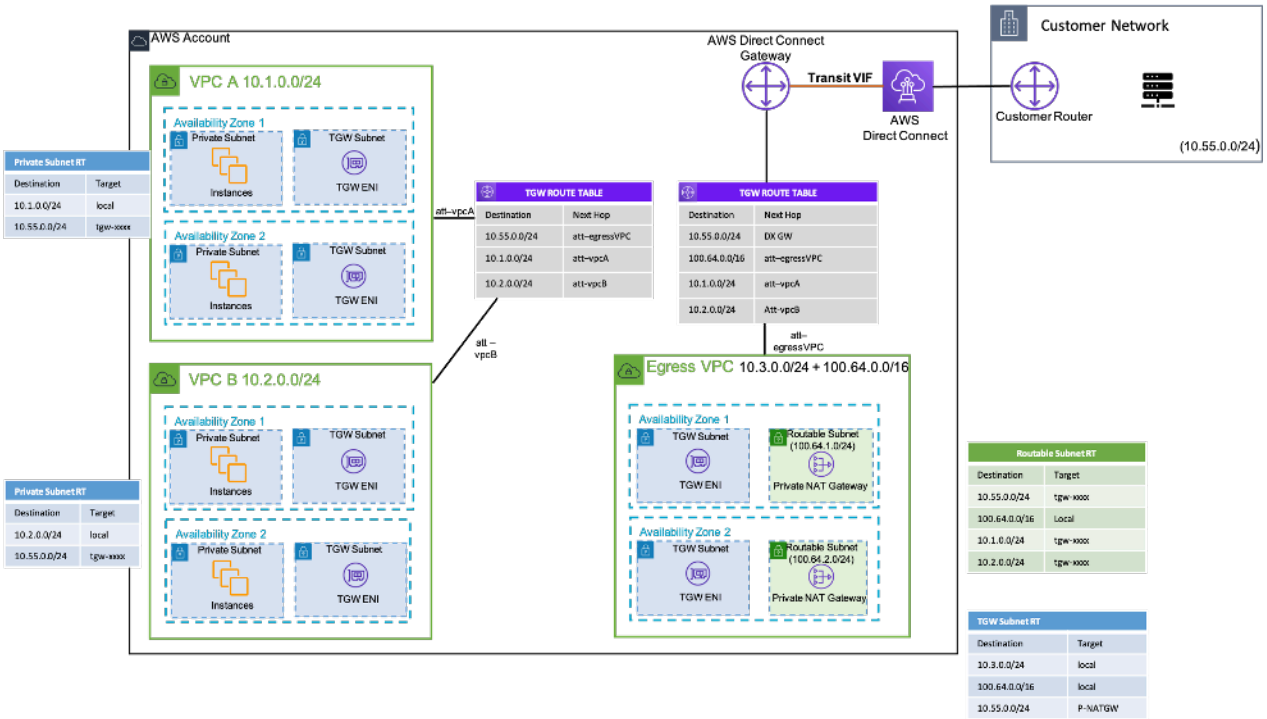
Tim sering bekerja secara independen dan mereka mungkin membuat VPC baru untuk sebuah proyek, yang mungkin memiliki blok routing antar-domain (CIDR) tanpa kelas yang tumpang tindih. Untuk integrasi, mereka mungkin ingin mengaktifkan komunikasi antara jaringan dengan CIDR yang tumpang tindih, yang tidak dapat dicapai melalui fitur seperti peering VPC dan Transit Gateway. Gateway NAT pribadi dapat membantu kasus penggunaan ini. Gateway NAT pribadi menggunakan alamat IP pribadi yang unik untuk melakukan NAT sumber untuk alamat IP sumber yang tumpang tindih, dan ELB melakukan NAT tujuan untuk alamat IP tujuan yang tumpang tindih. Anda dapat merutekan lalu lintas dari gateway NAT pribadi Anda ke VPC lain atau jaringan lokal menggunakan Transit Gateway atau gateway pribadi virtual.



Contoh pengaturan - Gateway NAT pribadi

Gambar sebelumnya menunjukkan dua subnet non-routable (overlapping CIDR,) di VPC A dan B. Untuk membuat koneksi di antara keduanya, Anda dapat menambahkan CIDR sekunder non-overlapping/routable (`100.64.0.0/16`subnet routable, dan) ke VPC A dan B, masing-masing. `10.0.1.0/24` `10.0.2.0/24` CIDR yang dapat dirutekan harus dialokasikan oleh tim manajemen jaringan yang bertanggung jawab atas alokasi IP. Gateway NAT pribadi ditambahkan ke subnet yang dapat dirutekan di VPC A dengan alamat IP. `10.0.1.125` Gateway NAT pribadi melakukan terjemahan alamat jaringan sumber pada permintaan dari instance di subnet VPC A (`100.64.0.10`) yang tidak dapat dirutekan sebagai`10.0.1.125`, ENI dari gateway NAT pribadi. Sekarang lalu lintas dapat diarahkan ke alamat IP routable yang ditetapkan ke Application Load Balancer (ALB) di VPC B `10.0.2.10` (), yang memiliki target. `100.64.0.10` Lalu lintas dialihkan melalui Transit Gateway. Lalu lintas pengembalian diproses oleh gateway NAT pribadi kembali ke instans Amazon EC2 asli yang meminta koneksi.

Gateway NAT pribadi juga dapat digunakan ketika jaringan lokal Anda membatasi akses ke IP yang disetujui. Jaringan lokal dari beberapa pelanggan diwajibkan oleh kepatuhan untuk berkomunikasi hanya dengan jaringan pribadi (tanpa IGW) hanya melalui blok terbatas IP yang disetujui yang dimiliki oleh pelanggan. Alih-alih mengalokasikan setiap instance IP terpisah dari blok, Anda dapat menjalankan beban kerja besar pada AWS VPC di belakang setiap IP yang terdaftar yang diizinkan menggunakan gateway NAT pribadi. Untuk detailnya, lihat [Cara mengatasi kelelahan IP Pribadi dengan Posting blog Solusi NAT Pribadi](#).



Contoh penyiapan - Cara menggunakan gateway NAT pribadi untuk menyediakan IP yang disetujui untuk jaringan lokal

AWS Awan WAN

AWS Cloud WAN adalah cara baru untuk menghubungkan jaringan bersama yang sebelumnya dapat kami lakukan dengan Transit Gateways, VPC Peering, dan terowongan VPN IPSEC. Sebelumnya Anda akan mengonfigurasi satu atau lebih VPC, menghubungkannya bersama dengan salah satu metode sebelumnya, dan menggunakan IPSEC VPN atau AWS Direct Connect untuk terhubung ke jaringan lokal. Anda akan memiliki konstruksi postur jaringan dan keamanan yang ditentukan di satu tempat, dan jaringan Anda di tempat lain. Cloud WAN memungkinkan Anda untuk memusatkan semua konstruksi ini di satu tempat. Berdasarkan kebijakan, Anda dapat mengelompokkan jaringan Anda untuk menentukan siapa yang dapat berbicara dengan siapa, dan mengisolasi lalu lintas produksi melalui segmen ini dari beban kerja pengembangan atau pengujian, atau jaringan di tempat Anda.

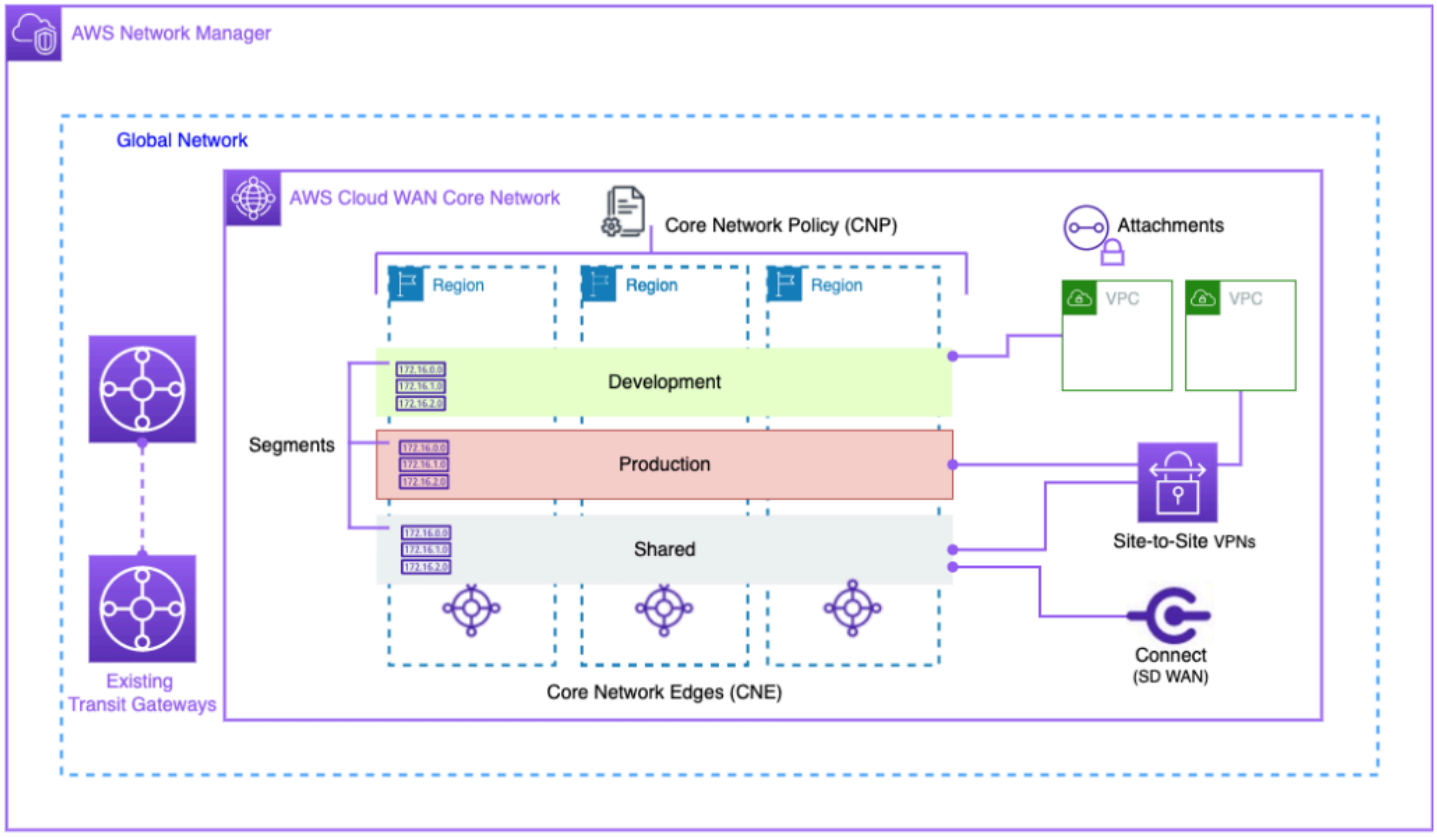


Diagram Blok WAN Awan

Kelola jaringan global Anda melalui antarmuka pengguna AWS Network Manager dan API. Jaringan global adalah wadah tingkat root untuk semua objek jaringan Anda; jaringan inti adalah bagian

dari jaringan global Anda yang dikelola oleh AWS. Kebijakan jaringan inti (CNP) adalah dokumen kebijakan berversi tunggal yang mendefinisikan semua aspek jaringan inti Anda. Lampiran adalah koneksi atau sumber daya apa pun yang ingin Anda tambahkan ke jaringan inti Anda. Core Network Edge (CNE) adalah titik koneksi lokal untuk lampiran yang mematuhi kebijakan. Segmen jaringan adalah domain routing yang, secara default, memungkinkan komunikasi hanya dalam segmen.

Untuk menggunakan CloudWAN:

1. Di AWS Network Manager, buat jaringan global dan jaringan inti terkait.
2. Buat CNP yang mendefinisikan segmen, rentang ASN, Wilayah AWS dan tag yang akan digunakan untuk melampirkan ke segmen.
3. Terapkan kebijakan jaringan.
4. Bagikan jaringan inti dengan pengguna, akun, atau organisasi Anda menggunakan pengelola akses sumber daya.
5. Buat dan tag lampiran.
6. Perbarui rute di VPC terlampir Anda untuk menyertakan jaringan inti.

Cloud WAN dirancang untuk menyederhanakan proses menghubungkan infrastruktur AWS Anda secara global. Ini memungkinkan Anda untuk menyegmentasikan lalu lintas dengan kebijakan izin terpusat dan menggunakan infrastruktur yang ada di lokasi perusahaan Anda. Cloud WAN juga menghubungkan VPC, SD-WAN, VPN Klien, firewall, VPN, dan sumber daya pusat data Anda untuk terhubung ke Cloud WAN. Untuk informasi selengkapnya, lihat postingan blog AWS Cloud WAN.

AWS Cloud WAN memungkinkan jaringan terpadu yang menghubungkan cloud dan lingkungan lokal. Organizations menggunakan Next-Gen Firewall (NGFWs) dan Intrusion Prevention Systems (IPS) untuk keamanan. Posting blog pola migrasi dan interoperabilitas AWS Cloud WAN dan Transit Gateway menjelaskan pola arsitektur untuk mengelola dan memeriksa lalu lintas jaringan keluar secara terpusat di jaringan Cloud WAN, termasuk jaringan Single-region dan Multi-region, dan mengonfigurasi tabel rute. Arsitektur ini memastikan data dan aplikasi tetap aman sambil mempertahankan lingkungan cloud yang aman.

Untuk informasi selengkapnya tentang Cloud WAN, lihat arsitektur inspeksi keluar terpusat di postingan blog AWS Cloud WAN.

Kisi VPC Amazon

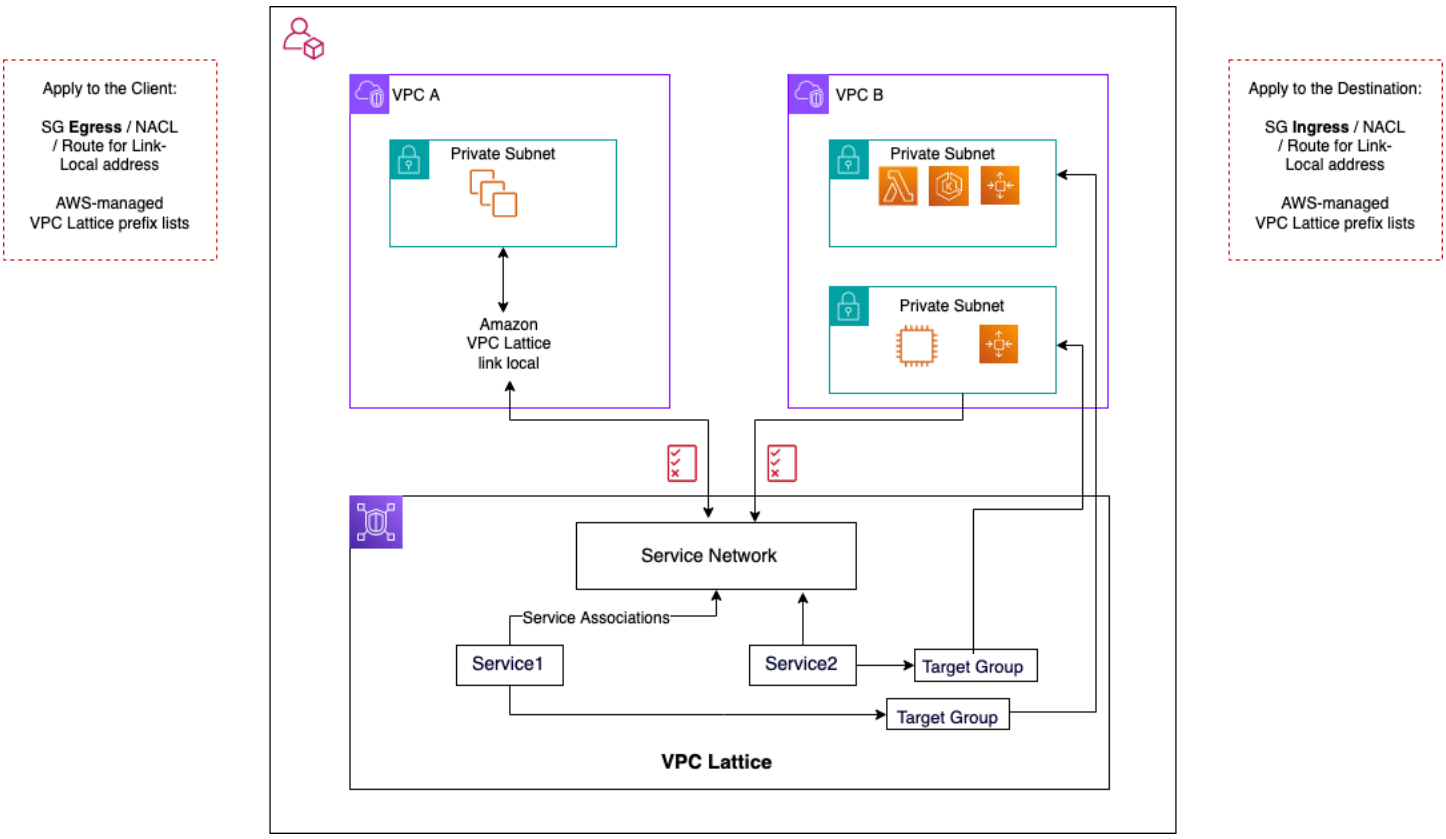
Amazon VPC Lattice adalah layanan jaringan aplikasi yang dikelola sepenuhnya yang digunakan untuk menghubungkan, memantau, dan mengamankan layanan di berbagai akun dan cloud pribadi virtual. VPC Lattice membantu menghubungkan layanan dalam batas logis, sehingga Anda dapat mengelola dan menemukannya secara efisien.

Komponen VPC Lattice terdiri dari:

- Layanan - Ini adalah unit aplikasi yang berjalan pada instance, wadah, atau fungsi Lambda dan terdiri dari pendengar, aturan, dan kelompok target.
- Jaringan layanan - Ini adalah batas logis yang digunakan untuk secara otomatis mengimplementasikan penemuan layanan dan konektivitas dan menerapkan kebijakan akses dan observabilitas umum ke kumpulan layanan.
- Kebijakan autentikasi - Kebijakan sumber daya IAM yang dapat dikaitkan dengan jaringan layanan atau layanan individual untuk mendukung otentikasi tingkat permintaan dan otorisasi khusus konteks.
- Direktori Layanan - Tampilan terpusat dari layanan yang Anda miliki atau yang telah dibagikan kepada Anda melalui AWS Resource Access Manager.

Langkah-langkah penggunaan VPC Lattice:

1. Buat jaringan layanan. Jaringan layanan biasanya berada di akun jaringan di mana administrator jaringan memiliki akses penuh. Jaringan layanan dapat dibagi di beberapa akun dalam suatu organisasi. Berbagi dapat dilakukan pada layanan individu atau seluruh akun layanan.
2. Lampirkan VPC ke jaringan layanan untuk mengaktifkan jaringan aplikasi untuk setiap VPC, sehingga layanan yang berbeda dapat mulai mengkonsumsi layanan lain yang terdaftar dalam jaringan. Kelompok keamanan diterapkan untuk mengontrol lalu lintas.
3. Pengembang mendefinisikan layanan, yang diisi dalam direktori layanan dan terdaftar ke jaringan layanan. VPC Lattice berisi buku alamat semua layanan yang dikonfigurasi. Pengembang juga dapat menentukan kebijakan perutean untuk menggunakan penerapan biru/hijau. Keamanan dikelola pada tingkat jaringan layanan di mana kebijakan otentikasi dan otorisasi didefinisikan dan pada tingkat layanan di mana kebijakan akses dengan IAM diterapkan.



Aliran komunikasi VPC Lattice

Rincian lebih lanjut dapat ditemukan di panduan pengguna VPC Lattice.

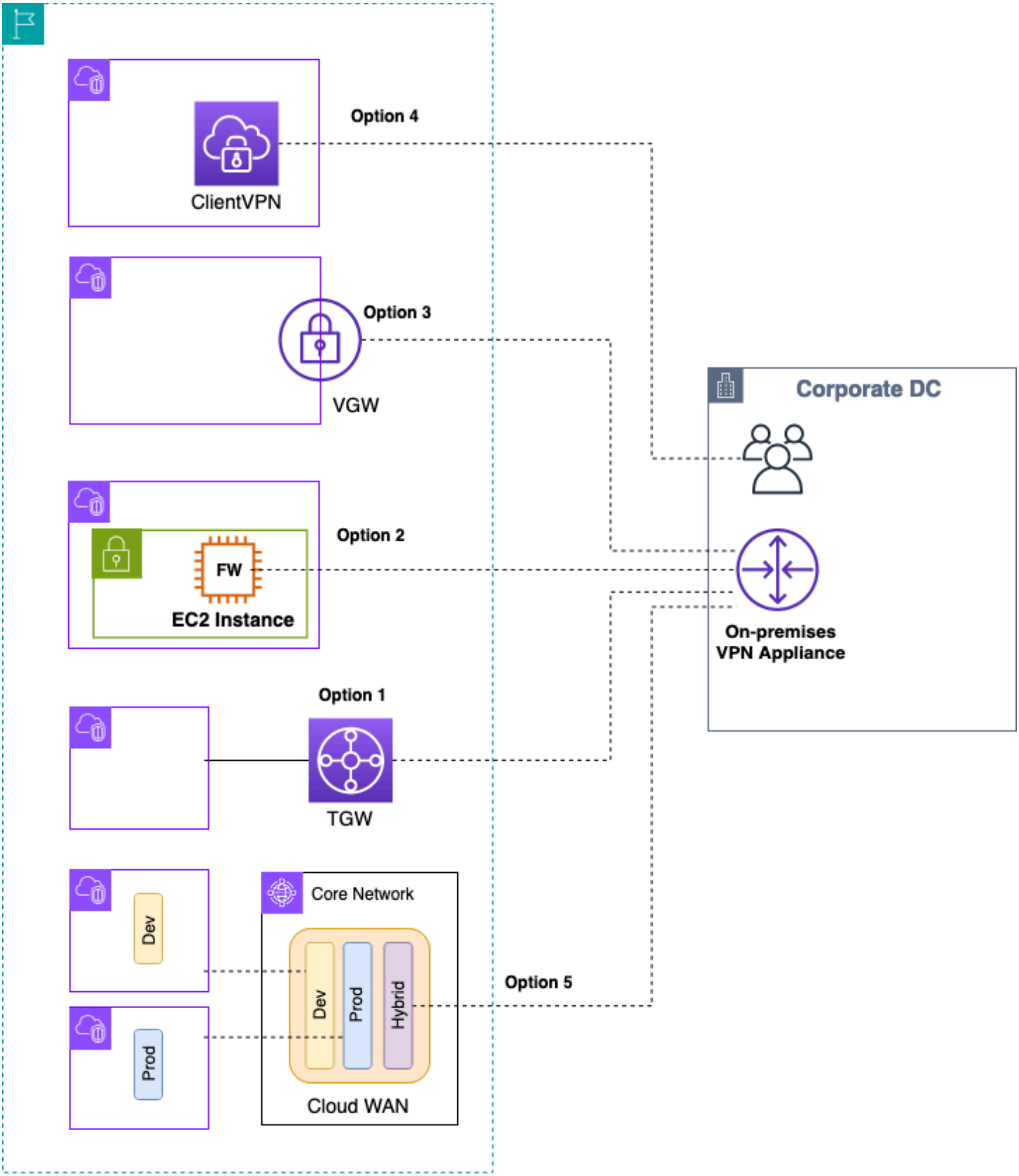
Konektivitas hibrida

Bagian ini berfokus untuk menghubungkan sumber daya cloud Anda secara aman dengan pusat data lokal. Ada tiga pendekatan untuk mengaktifkan konektivitas hybrid:

- ne-to-one Konektivitas O — Dalam pengaturan ini, koneksi VPN dan/atau VIF pribadi Direct Connect dibuat untuk setiap VPC. Hal ini dilakukan dengan menggunakan virtual private gateway (VGW). Opsi ini sangat bagus untuk sejumlah kecil VPC, tetapi ketika pelanggan menskalakan VPC mereka, mengelola konektivitas hybrid per VPC bisa menjadi sulit.
- Konsolidasi tepi — Dalam pengaturan ini, pelanggan mengkonsolidasikan konektivitas TI hybrid untuk beberapa VPC pada satu titik akhir. Semua VPC berbagi koneksi hybrid ini. Hal ini dilakukan dengan menggunakan AWS Transit Gateway dan AWS Direct Connect gateway.
- Konsolidasi hybrid mesh penuh - Dalam pengaturan ini, pelanggan mengkonsolidasikan konektivitas untuk beberapa VPC pada satu titik akhir menggunakan CloudWAN, bawaan. AWS Transit Gateway Ini adalah pendekatan berbasis kebijakan lengkap untuk jaringan di satu atau lebih akun AWS, yang direpresentasikan dalam kode. Pada saat ini, penggunaan AWS Direct Connect untuk konektivitas edge memerlukan peering Transit Gateway ke CloudWAN.

VPN

Ada berbagai cara untuk mengatur VPN ke AWS:



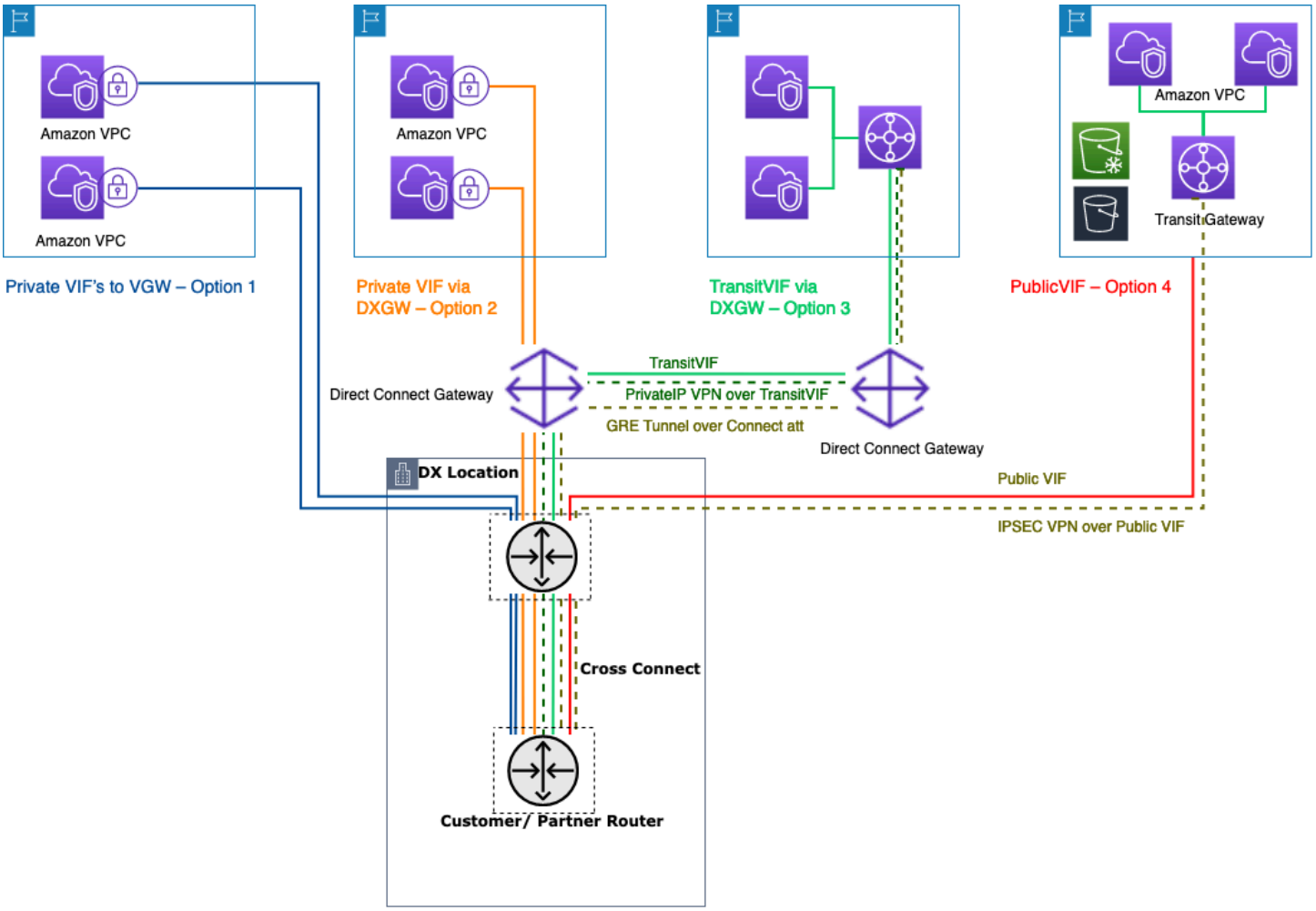
AWS VPN pilihan

- Opsi 1: Konsolidasikan konektivitas VPN di Transit Gateway — Opsi ini memanfaatkan lampiran Transit Gateway VPN di Transit Gateway. Transit Gateway mendukung penghentian IPsec untuk site-to-site VPN. Pelanggan dapat membuat terowongan VPN ke Transit Gateway, dan dapat mengakses VPC yang terpasang padanya. Transit Gateway mendukung koneksi Dynamic VPN berbasis Statis dan BGP. Transit Gateway juga mendukung Equal-Cost Multi-Path (ECMP) pada lampiran VPN. Setiap koneksi VPN memiliki throughput maksimum 1,25-Gbps per terowongan. Mengaktifkan ECMP memungkinkan Anda untuk mengumpulkan throughput di seluruh koneksi VPN, memungkinkan skala melampaui batas maksimum default 1,25 Gbps. Dalam opsi ini, Anda membayar harga Transit Gateway serta AWS VPN harga. AWS merekomendasikan penggunaan opsi ini untuk konektivitas VPN. Untuk informasi selengkapnya, lihat throughput Scaling VPN menggunakan postingan blog AWS Transit Gateway.
- Opsi 2: Hentikan VPN di instans Amazon EC2 — Opsi ini dimanfaatkan oleh pelanggan dalam kasus tepi ketika mereka menginginkan set fitur perangkat lunak vendor tertentu (seperti Cisco DMVPN atau Generic Routing Encapsulation (GRE)), atau mereka menginginkan konsistensi operasional di berbagai penerapan VPN. Anda dapat menggunakan desain VPC transit untuk konsolidasi tepi, tetapi penting untuk diingat bahwa semua pertimbangan utama dari bagian untuk VPC transit Konektivitas VPC ke VPC berlaku untuk konektivitas VPN hybrid. Anda bertanggung jawab untuk mengelola ketersediaan tinggi, dan Anda membayar instans EC2 serta biaya lisensi dan dukungan perangkat lunak vendor.
- Opsi 3: Hentikan VPN pada gateway pribadi virtual (VGW) — Opsi layanan AWS Site-to-Site VPN ini memungkinkan one-to-one desain konektivitas tempat Anda membuat satu koneksi VPN (terdiri dari sepasang terowongan VPN redundan) per VPC. Ini adalah cara yang bagus untuk memulai konektivitas VPN ke AWS, tetapi saat Anda meningkatkan jumlah VPC, mengelola semakin banyak koneksi VPN dapat menjadi tantangan. Oleh karena itu, desain konsolidasi tepi yang memanfaatkan Transit Gateway pada akhirnya akan menjadi pilihan yang lebih baik. Throughput VPN ke VGW dibatasi hingga 1,25 Gbps per terowongan dan penyeimbangan beban ECMP tidak didukung. Dari perspektif harga, Anda hanya membayar harga AWS VPN, tidak ada biaya untuk menjalankan VGW. Untuk informasi lebih lanjut, lihat AWS VPN Harga dan AWS VPN gateway pribadi virtual.
- Opsi 4: Hentikan koneksi VPN pada titik akhir VPN klien — AWS Client VPN adalah layanan VPN berbasis klien terkelola yang memungkinkan Anda mengakses sumber daya dan sumber daya AWS dengan aman di jaringan lokal Anda. Dengan Client VPN, Anda dapat mengakses sumber daya Anda dari lokasi mana pun menggunakan klien VPN yang disediakan OpenVPN atau AWS. Dengan menyiapkan titik akhir Client VPN, klien dan pengguna dapat terhubung untuk membuat koneksi VPN Transport Layer Security (TLS). Untuk informasi selengkapnya, lihat dokumentasi AWS Client VPN.

- Opsi 5: Konsolidasikan koneksi VPN di AWS Cloud WAN — Opsi ini mirip dengan opsi pertama dalam daftar ini, tetapi menggunakan kain CloudWAN untuk mengonfigurasi koneksi VPN secara terprogram melalui dokumen kebijakan jaringan.

AWS Direct Connect

Meskipun VPN melalui internet adalah pilihan yang bagus untuk memulai, konektivitas internet mungkin tidak dapat diandalkan untuk lalu lintas produksi. Karena tidak dapat diandalkan ini, banyak pelanggan memilih AWS Direct Connect. AWS Direct Connect adalah layanan jaringan yang menyediakan alternatif untuk menggunakan internet untuk terhubung ke AWS. Menggunakan AWS Direct Connect, data yang sebelumnya akan diangkut melalui internet dikirimkan melalui koneksi jaringan pribadi antara fasilitas Anda dan AWS. Dalam banyak keadaan, koneksi jaringan pribadi dapat mengurangi biaya, meningkatkan bandwidth, dan memberikan pengalaman jaringan yang lebih konsisten daripada koneksi berbasis internet. Ada beberapa cara yang dapat digunakan AWS Direct Connect untuk terhubung ke VPC:



Cara menghubungkan pusat data lokal Anda menggunakan AWS Direct Connect

- Opsi 1: Buat antarmuka virtual pribadi (VIF) ke VGW yang terpasang ke VPC - Anda dapat membuat 50 VIF per koneksi Direct Connect, memungkinkan Anda untuk terhubung ke maksimum 50 VPC (satu VIF menyediakan konektivitas ke satu VPC). Ada satu BGP peering per VPC. Konektivitas dalam pengaturan ini dibatasi untuk Wilayah AWS tempat lokasi Direct Connect berada. one-to-one Pemetaan VIF ke VPC (dan kurangnya akses global) menjadikan ini cara yang paling tidak disukai untuk mengakses VPC di Zona Pendaratan.
- Opsi 2: Buat VIF pribadi ke gateway Direct Connect yang terkait dengan beberapa VGW (setiap VGW dilampirkan ke VPC) - Gateway Direct Connect adalah sumber daya yang tersedia secara global. Anda dapat membuat gateway Direct Connect di Wilayah mana pun dan mengaksesnya dari semua Wilayah lain, termasuk GovCloud (tidak termasuk China). Direct Connect Gateway dapat terhubung hingga 20 VPC (melalui VGW) secara global di akun AWS apa pun melalui satu VIF pribadi. Ini adalah pilihan yang bagus jika Zona Pendaratan terdiri dari sejumlah kecil VPC (sepuluh atau lebih sedikit VPC) dan/atau Anda memerlukan akses global. Ada satu sesi peering BGP per Direct Connect Gateway per koneksi Direct Connect. Direct Connect gateway hanya untuk arus lalu lintas utara/selatan dan tidak mengizinkan konektivitas VPC-ke-VPC. Lihat asosiasi gateway pribadi virtual dalam AWS Direct Connect dokumentasi untuk detail selengkapnya. Dengan opsi ini, konektivitas tidak terbatas pada Wilayah AWS tempat lokasi Direct Connect berada. AWS Direct Connect gateway hanya untuk aliran utara/selatan dan tidak mengizinkan konektivitas VPC-ke-VPC. Pengecualian untuk aturan ini adalah ketika supernet diiklankan di dua atau lebih VPC yang memiliki VGW terlampir yang terkait dengan AWS Direct Connect gateway yang sama dan pada antarmuka virtual yang sama. Dalam hal ini, VPC dapat berkomunikasi satu sama lain melalui titik AWS Direct Connect akhir. Lihat dokumentasi AWS Direct Connect gateway untuk detail selengkapnya.
- Opsi 3: Buat VIF transit ke gateway Direct Connect yang terkait dengan Transit Gateway — Anda dapat mengaitkan instance Transit Gateway ke gateway Direct Connect dengan menggunakan Transit VIF. AWS Direct Connect sekarang mendukung koneksi ke Transit Gateway untuk semua kecepatan port, memberikan pilihan yang lebih hemat biaya bagi pengguna Transit Gateway ketika koneksi berkecepatan tinggi (lebih besar dari 1Gbps) tidak diperlukan. Ini memungkinkan Anda untuk menggunakan Direct Connect pada kecepatan 50, 100, 200, 300, 400, dan 500 Mbps yang terhubung ke Transit Gateway. Transit VIF memungkinkan Anda menghubungkan pusat data lokal Anda ke hingga enam instans Transit Gateway per AWS Direct Connect gateway (yang dapat terhubung ke ribuan VPC) di berbagai Wilayah AWS dan akun AWS melalui peering VIF dan BGP transit tunggal. Ini adalah pengaturan paling sederhana di antara opsi untuk menghubungkan beberapa VPC dalam skala besar, tetapi Anda harus memperhatikan kuota Transit Gateway. Satu

batasan utama yang perlu diperhatikan adalah Anda hanya dapat mengiklankan 200 awalan dari Transit Gateway ke router lokal melalui VIF transit. Dengan opsi sebelumnya, Anda membayar harga Direct Connect. Untuk opsi ini, Anda juga membayar biaya lampiran Transit Gateway dan pemrosesan data. Untuk informasi selengkapnya, lihat dokumentasi Asosiasi Transit Gateway di Direct Connect.

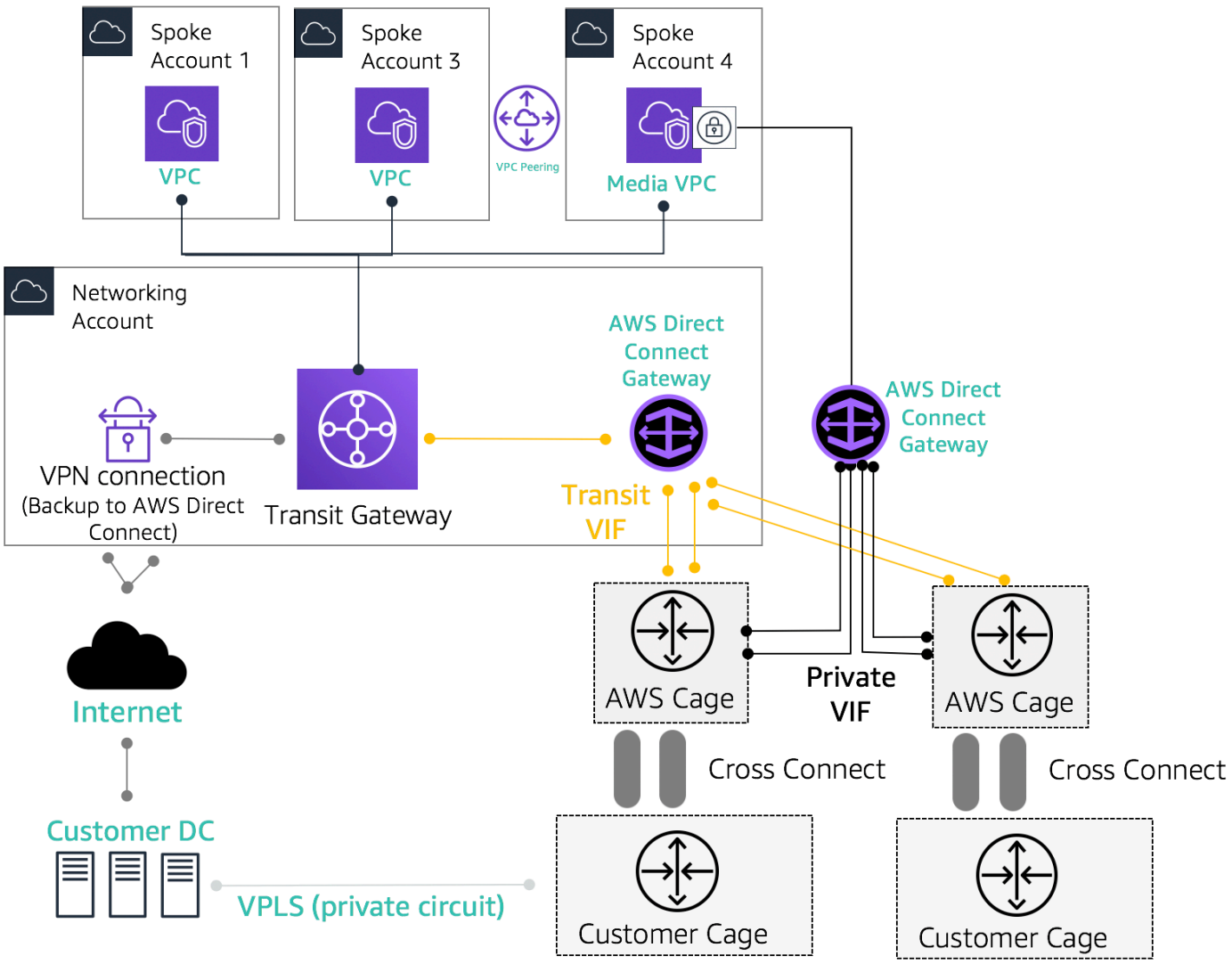
- Opsi 4: Buat koneksi VPN ke Transit Gateway melalui VIF publik Direct Connect — VIF publik memungkinkan Anda mengakses semua layanan publik AWS dan titik akhir menggunakan alamat IP publik. Saat Anda membuat lampiran VPN di Transit Gateway, Anda mendapatkan dua alamat IP publik untuk titik akhir VPN di sisi AWS. IP publik ini dapat dijangkau melalui VIF publik. Anda dapat membuat koneksi VPN sebanyak mungkin ke instans Transit Gateway sebanyak yang Anda inginkan melalui VIF Publik. Saat Anda membuat BGP mengintip VIF publik, AWS mengiklankan seluruh rentang IP publik AWS ke router Anda. Untuk memastikan bahwa Anda hanya mengizinkan lalu lintas tertentu (misalnya, mengizinkan lalu lintas hanya ke titik akhir penghentian VPN), Anda disarankan untuk menggunakan fasilitas lokal firewall. Opsi ini dapat digunakan untuk mengenkripsi Direct Connect Anda di lapisan jaringan.
- Opsi 5: Buat koneksi VPN ke Transit Gateway melalui AWS Direct Connect menggunakan Private IP VPN — Private IP VPN adalah fitur yang memberi pelanggan kemampuan untuk menerapkan koneksi AWS Site-to-Site VPN melalui Direct Connect menggunakan alamat IP pribadi. Dengan fitur ini, Anda dapat mengenkripsi lalu lintas antara jaringan lokal dan AWS melalui koneksi Direct Connect tanpa memerlukan alamat IP publik, sehingga meningkatkan keamanan dan privasi jaringan secara bersamaan. Private IP VPN digunakan di atas Transit VIF, sehingga memungkinkan Anda menggunakan Transit Gateway untuk pengelolaan terpusat VPC pelanggan dan koneksi ke jaringan lokal dengan cara yang lebih aman, pribadi, dan skalabel.
- Opsi 6: Buat terowongan GRE ke Transit Gateway melalui VIF transit — Jenis lampiran Transit Gateway Connect mendukung GRE. Dengan Transit Gateway Connect, infrastruktur SD-WAN dapat terhubung secara native ke AWS tanpa harus menyiapkan VPN IPsec antara peralatan virtual jaringan SD-WAN dan Transit Gateway. Terowongan GRE dapat dibuat melalui VIF transit, memiliki Transit Gateway Connect sebagai tipe lampiran, memberikan kinerja bandwidth yang lebih tinggi dibandingkan dengan koneksi VPN. Untuk informasi lebih lanjut, lihat Simplify SD-WAN konektivitas dengan posting blog AWS Transit Gateway Connect.

Opsi “transit VIF ke Direct Connect gateway” mungkin tampak sebagai pilihan terbaik karena memungkinkan Anda mengkonsolidasikan semua konektivitas lokal Anda untuk diberikan Wilayah AWS pada satu titik (Transit Gateway) menggunakan satu sesi BGP per koneksi Direct Connect; namun, beberapa batasan dan pertimbangan seputar opsi ini dapat mengarahkan Anda untuk

menggunakan VIF pribadi dan transit bersamaan untuk persyaratan konektivitas Zona Pendaratan Anda.

Gambar berikut mengilustrasikan pengaturan sampel di mana Transit VIF digunakan sebagai metode default untuk menghubungkan ke VPC dan VIF pribadi digunakan untuk kasus penggunaan tepi di mana sejumlah besar data harus ditransfer dari Pusat Data lokal ke VPC media. VIF pribadi digunakan untuk menghindari biaya pemrosesan data Transit Gateway. Sebagai praktik terbaik, Anda harus memiliki setidaknya dua koneksi di dua lokasi Direct Connect yang berbeda untuk redundansi maksimum — total empat koneksi. Anda membuat satu VIF per koneksi untuk total empat VIF pribadi dan empat VIF transit. Anda juga dapat membuat VPN sebagai konektivitas cadangan ke AWS Direct Connect koneksi.

Dengan opsi “Buat terowongan GRE ke Transit Gateway melalui VIF transit”, Anda mendapatkan kemampuan untuk menghubungkan infrastruktur SD-WAN Anda secara native dengan AWS. Ini menghilangkan kebutuhan untuk mengatur VPN IPsec antara peralatan virtual jaringan SD-WAN dan Transit Gateway.



Contoh arsitektur referensi untuk konektivitas hybrid

Gunakan akun Network Services untuk membuat sumber daya Direct Connect yang memungkinkan demarkasi batas administratif jaringan. Koneksi Direct Connect, gateway Direct Connect, dan Transit Gateway semuanya dapat berada di akun Layanan Jaringan. Untuk berbagi AWS Direct Connect konektivitas dengan Zona Pendaratan Anda, cukup bagikan Transit Gateway melalui AWS RAM akun lain.

Keamanan MACSec pada koneksi Direct Connect

Pelanggan dapat menggunakan enkripsi MAC Security Standard (MacSec) (IEEE 802.1AE) dengan koneksi Direct Connect mereka untuk koneksi khusus 10 Gbps dan 100 Gbps di lokasi tertentu. Dengan kemampuan ini, pelanggan dapat mengamankan data mereka di tingkat lapisan 2, dan

Direct Connect memberikan point-to-point enkripsi. Untuk mengaktifkan fitur Direct Connect MacSec, pastikan bahwa prasyarat MacSec terpenuhi. Karena MacSec melindungi tautan hop-by-hop secara dasar, perangkat Anda harus memiliki kedekatan lapisan 2 langsung dengan perangkat Direct Connect kami. Penyedia last-mile Anda dapat membantu Anda memverifikasi bahwa koneksi Anda akan berfungsi dengan MacSec. Untuk informasi selengkapnya, lihat Menambahkan keamanan MacSec ke koneksi AWS Direct Connect.

AWS Direct Connect rekomendasi ketahanan

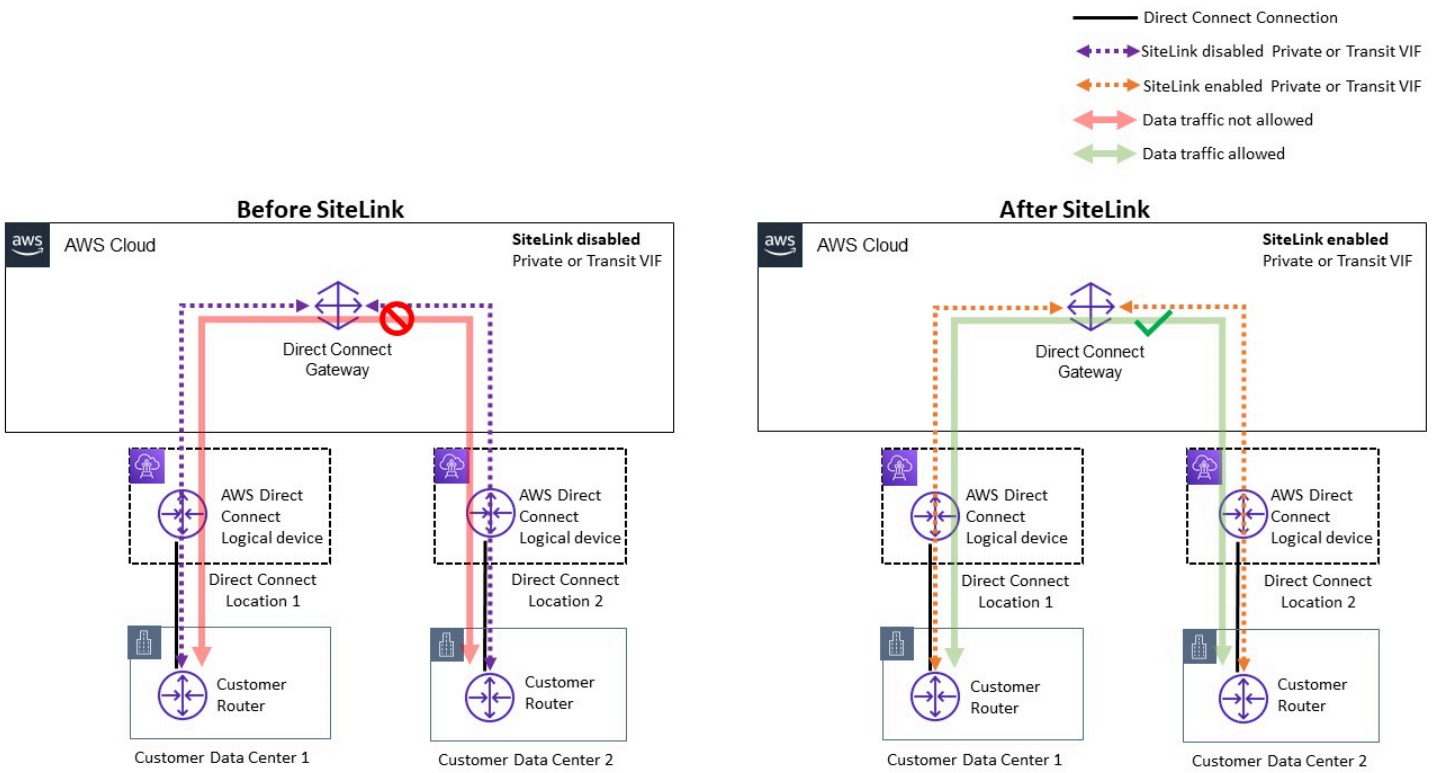
Dengan AWS Direct Connect, pelanggan dapat mencapai konektivitas yang sangat tangguh ke VPC Amazon dan sumber daya AWS mereka dari jaringan lokal mereka. Ini adalah praktik terbaik bahwa pelanggan terhubung dari beberapa pusat data untuk menghilangkan kegagalan lokasi fisik titik tunggal. Juga disarankan bahwa, tergantung pada jenis beban kerja, pelanggan menggunakan lebih dari satu koneksi Direct Connect untuk redundansi.

AWS juga menawarkan AWS Direct Connect Resiliency Toolkit, yang menyediakan wizard koneksi dengan beberapa model redundansi kepada pelanggan; untuk membantu mereka menentukan model mana yang paling sesuai dengan persyaratan perjanjian tingkat layanan (SLA) mereka dan merancang konektivitas hybrid mereka menggunakan koneksi Direct Connect yang sesuai. Untuk informasi lebih lanjut, lihat Rekomendasi AWS Direct Connect Ketahanan.

AWS Direct Connect SiteLink

Sebelumnya, mengonfigurasi site-to-site tautan untuk jaringan lokal Anda hanya dimungkinkan dengan menggunakan pengembangan sirkuit langsung melalui serat gelap atau teknologi lain, VPN IPSEC, atau dengan menggunakan penyedia sirkuit pihak ketiga dengan teknologi seperti MPLS,, atau sirkuit T1 lama. MetroEthernet Dengan munculnya SiteLink, pelanggan sekarang dapat mengaktifkan site-to-site konektivitas langsung untuk lokasi lokal mereka yang berakhir di suatu lokasi. AWS Direct Connect Gunakan sirkuit Direct Connect Anda untuk menyediakan site-to-site konektivitas tanpa harus merutekan lalu lintas melalui VPC Anda, melewati wilayah AWS sepenuhnya.

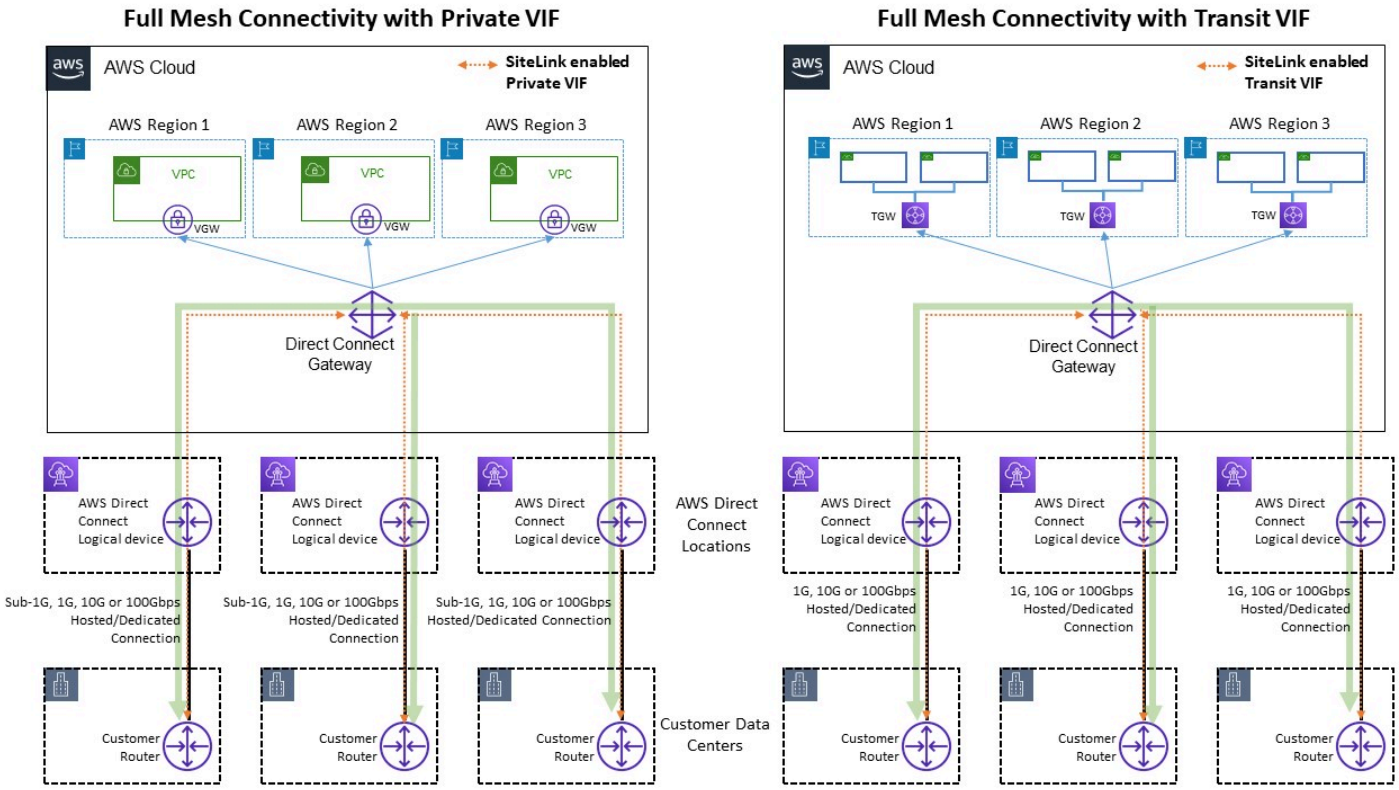
Sekarang, Anda dapat membuat pay-as-you-go koneksi global, andal, dan antara kantor dan pusat data di jaringan global Anda dengan mengirimkan data melalui jalur tercepat antar AWS Direct Connect lokasi.



Contoh arsitektur referensi untuk AWS Direct Connect SiteLink

Saat menggunakan SiteLink, pertama-tama Anda menghubungkan jaringan lokal Anda ke AWS di lebih dari 100 AWS Direct Connect lokasi di seluruh dunia. Kemudian, Anda membuat antarmuka virtual (VIF) pada koneksi tersebut dan mengaktifkan. SiteLink Setelah semua VIF dilampirkan ke AWS Direct Connect gateway yang sama (DXGW), Anda dapat mulai mengirim data di antara mereka. Data Anda mengikuti jalur terpendek antar AWS Direct Connect lokasi ke tujuannya, menggunakan jaringan global AWS yang cepat, aman, dan andal. Anda tidak perlu memiliki sumber daya apa pun Wilayah AWS untuk digunakan SiteLink.

Dengan SiteLink, DXGW mempelajari awalan IPv4/IPv6 dari router Anda melalui VIF yang SiteLink diaktifkan, menjalankan algoritma jalur terbaik BGP, memperbarui atribut seperti dan AS_Path, NextHop dan mengiklankan kembali awalan BGP ini ke sisa VIF Anda yang diaktifkan yang terkait dengan DXGW itu. SiteLink Jika Anda menonaktifkan SiteLink pada VIF, DXGW tidak akan mengiklankan awalan lokal yang dipelajari melalui VIF ini ke VIF berkemampuan lainnya. SiteLink Awalan lokal dari VIF yang SiteLink dinonaktifkan hanya diiklankan ke asosiasi Gateway DXGW, seperti instans AWS Virtual Private Gateways (VGW) atau Transit Gateway (TGW) yang terkait dengan DXGW.



Sitelink memungkinkan contoh arus lalu lintas

SiteLink memungkinkan pelanggan untuk menggunakan jaringan global AWS untuk berfungsi sebagai koneksi primer atau sekunder/cadangan antara lokasi jarak jauh mereka, dengan bandwidth tinggi dan latensi rendah, dengan perutean dinamis untuk mengontrol lokasi mana yang dapat berkomunikasi satu sama lain dan dengan sumber daya regional AWS Anda.

Untuk informasi lebih lanjut, lihat Memperkenalkan AWS Direct Connect SiteLink.

Jalan keluar terpusat ke internet

Saat Anda menyebarkan aplikasi di lingkungan multi-akun Anda, banyak aplikasi akan memerlukan akses internet outbound saja (misalnya, mengunduh pustaka, tambalan, atau pembaruan OS). Ini dapat dicapai untuk keduanya IPv4 dan IPv6 lalu lintas. UntukIPv4, ini dapat dicapai melalui terjemahan alamat jaringan (NAT) dalam bentuk NAT gateway (disarankan), atau sebagai alternatif, NAT instance yang dikelola sendiri yang berjalan pada EC2 instance Amazon, sebagai sarana untuk semua akses internet jalan keluar. Aplikasi internal berada di subnet pribadi, sementara instance NAT Gateways dan EC2 NAT Amazon berada di subnet publik.

AWSmerekomendasikan agar Anda menggunakan NAT gateway karena mereka menyediakan ketersediaan dan bandwidth yang lebih baik dan membutuhkan lebih sedikit kemudahan di pihak Anda untuk mengelola. Untuk informasi selengkapnya, lihat Bandingkan NAT gateway dan NAT instance.

Untuk IPv6 lalu lintas, lalu lintas keluar dapat dikonfigurasi untuk meninggalkan masing-masing VPC melalui gateway internet jalan keluar saja dengan cara yang terdesentralisasi atau dapat dikonfigurasi untuk dikirim ke terpusat VPC menggunakan instance atau instance proxy. NAT IPv6Pola-pola tersebut dibahas dalamJalan keluar terpusat untuk IPv6.

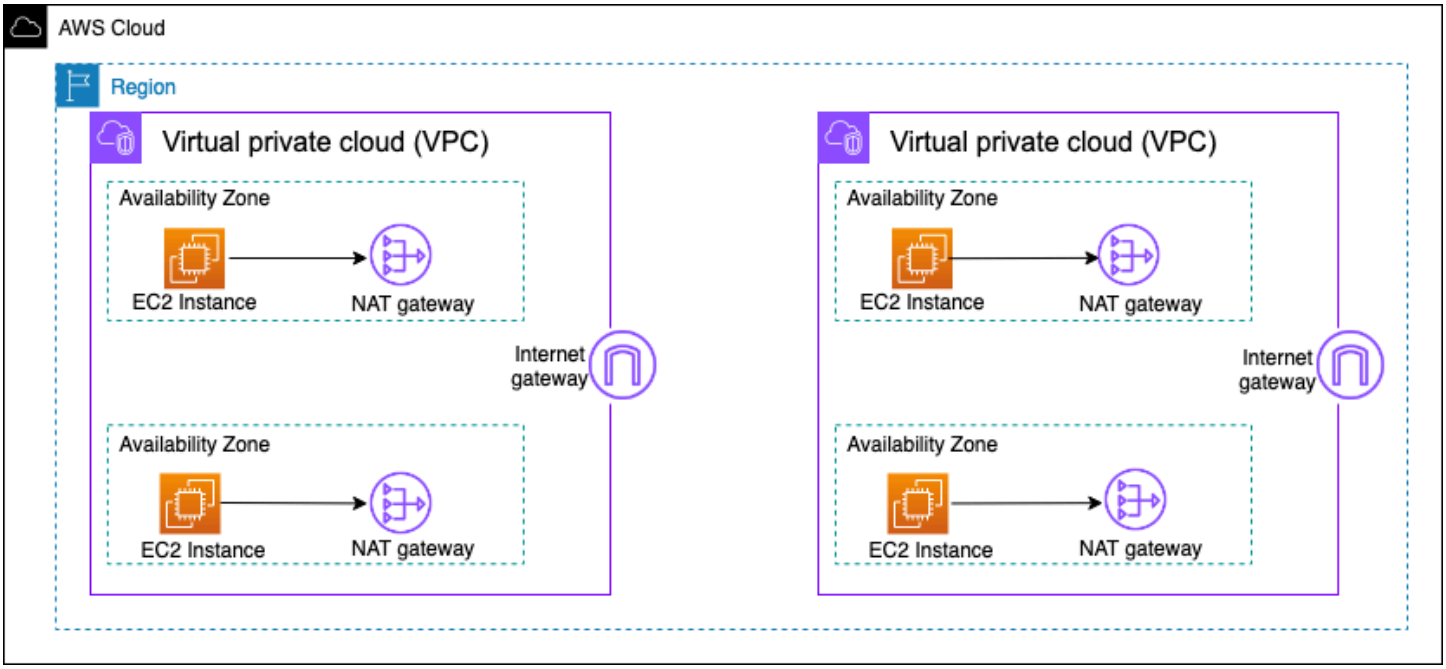
Topik

- Menggunakan NAT gateway untuk jalan keluar terpusat IPv4
- Menggunakan NAT gateway dengan jalan AWS Network Firewall keluar terpusat IPv4
- Menggunakan NAT gateway dan Load Balancer Gateway dengan EC2 instans Amazon untuk jalan keluar terpusat IPv4
- Jalan keluar terpusat untuk IPv6

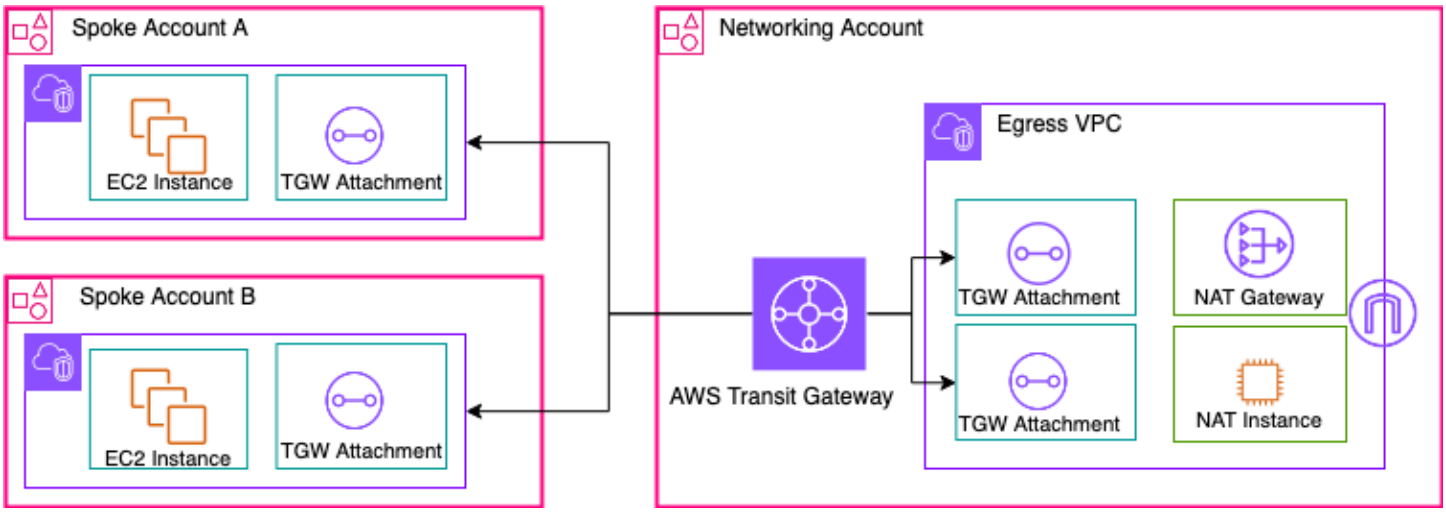
Menggunakan NAT gateway untuk jalan keluar terpusat IPv4

NATgateway adalah layanan terjemahan alamat jaringan terkelola. Menyebarkan NAT gateway di setiap spoke VPC bisa menjadi penghalang biaya karena Anda membayar biaya per jam untuk setiap NAT gateway yang Anda gunakan (lihat harga Amazon). VPC NATGateway sentralisasi dapat menjadi pilihan yang layak untuk mengurangi biaya. Untuk memusatkan, Anda membuat jalan keluar terpisah VPC di akun layanan jaringan, menyebarkan NAT gateway di jalan keluarVPC, dan merutekan semua lalu lintas keluar dari spoke ke gateway yang berada di jalan keluar menggunakan Transit VPCs Gateway atau Cloud, seperti yang NAT ditunjukkan pada gambar berikut. VPC WAN

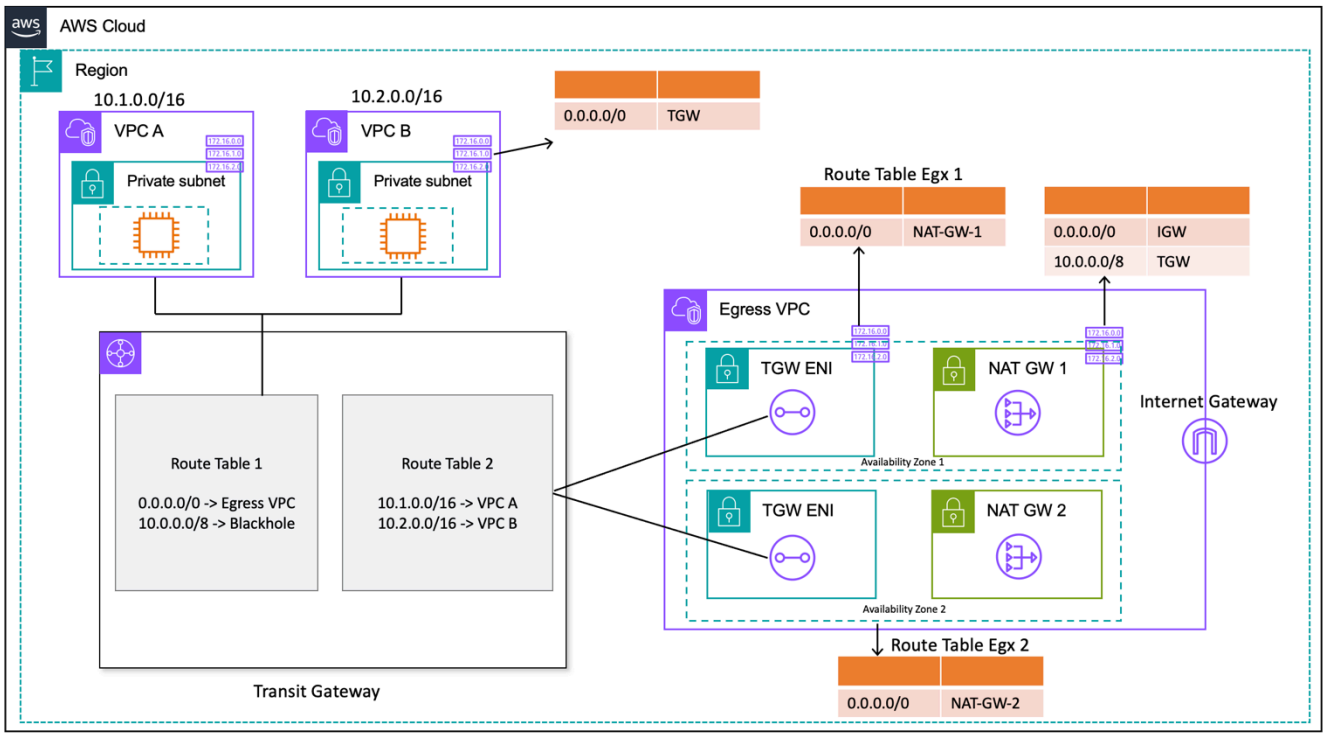
> **Note**
>
> Saat Anda memusatkan NAT gateway menggunakan Transit Gateway, Anda membayar biaya pemrosesan data Gateway Transit tambahan — dibandingkan dengan pendekatan desentralisasi dalam menjalankan NAT gateway di setiap gerbang. VPC Dalam beberapa kasus tepi ketika Anda mengirim data dalam jumlah besar melalui NAT gateway dari aVPC, menjaga NAT lokal VPC untuk menghindari biaya pemrosesan data Gateway Transit mungkin merupakan opsi yang lebih hemat biaya.



Arsitektur gateway ketersediaan NAT tinggi yang terdesentralisasi



NATGateway terpusat menggunakan Transit Gateway (ikhtisar)



NATGateway terpusat menggunakan Transit Gateway (desain tabel rute)

Dalam pengaturan ini, VPC lampiran spoke dikaitkan dengan Route Tabel 1 (RT1) dan disebarkan ke Route Tabel 2 (RT2). Ada rute Blackhole untuk VPCs melarang keduanya berkomunikasi satu sama lain. Jika Anda ingin mengizinkan antar VPC komunikasi, Anda dapat menghapus entri `10.0.0.0/8 -> Blackhole` rute dariRT1. Hal ini memungkinkan mereka untuk berkomunikasi melalui gateway transit. Anda juga dapat menyebarkan VPC lampiran spoke ke RT1 (atau sebagai alternatif, Anda dapat menggunakan satu tabel rute dan mengaitkan/menyebarkan semuanya ke sana), memungkinkan arus lalu lintas langsung antara menggunakan Transit Gateway. VPCs

Anda menambahkan rute statis dalam RT1 mengarahkan semua lalu lintas ke jalan keluar. VPC Karena rute statis ini, Transit Gateway mengirimkan semua lalu lintas internet melalui jalan keluarVPC. ENIs Setelah di jalan keluarVPC, lalu lintas mengikuti rute yang ditentukan dalam tabel rute subnet tempat Gateway Transit ini berada. ENIs Anda menambahkan rute dalam tabel rute subnet yang mengarahkan semua lalu lintas ke NAT gateway masing-masing di Availability Zone yang sama untuk meminimalkan lalu lintas Cross-availability Zone (AZ). Tabel rute subnet NAT gateway memiliki internet gateway (IGW) sebagai lompatan berikutnya. Agar lalu lintas kembali mengalir kembali, Anda harus menambahkan entri tabel rute statis di tabel rute subnet NAT gateway yang menunjuk semua lalu lintas yang VPC terikat bicara ke Transit Gateway sebagai lompatan berikutnya.

Ketersediaan tinggi

Untuk ketersediaan tinggi, Anda harus menggunakan lebih dari satu NAT gateway (satu di setiap Availability Zone). Jika NAT gateway tidak tersedia, lalu lintas mungkin dijatuhkan di Availability Zone yang melintasi gateway yang terpengaruh. NAT Jika satu Availability Zone tidak tersedia, titik akhir Transit Gateway bersama dengan NAT gateway di Availability Zone tersebut akan gagal, dan semua lalu lintas akan mengalir melalui Gateway Transit dan titik akhir NAT gateway di Availability Zone lainnya.

Keamanan

Anda dapat mengandalkan grup keamanan pada instance sumber, rute blackhole di tabel rute Transit Gateway, dan jaringan ACL subnet tempat NAT gateway berada. Misalnya, pelanggan dapat menggunakan ACLs subnet publik NAT Gateway untuk mengizinkan atau memblokir alamat IP sumber atau tujuan. Atau, Anda dapat menggunakan NAT Gateway with AWS Network Firewall untuk jalan keluar terpusat yang dijelaskan di bagian berikutnya untuk memenuhi persyaratan ini.

Skalabilitas

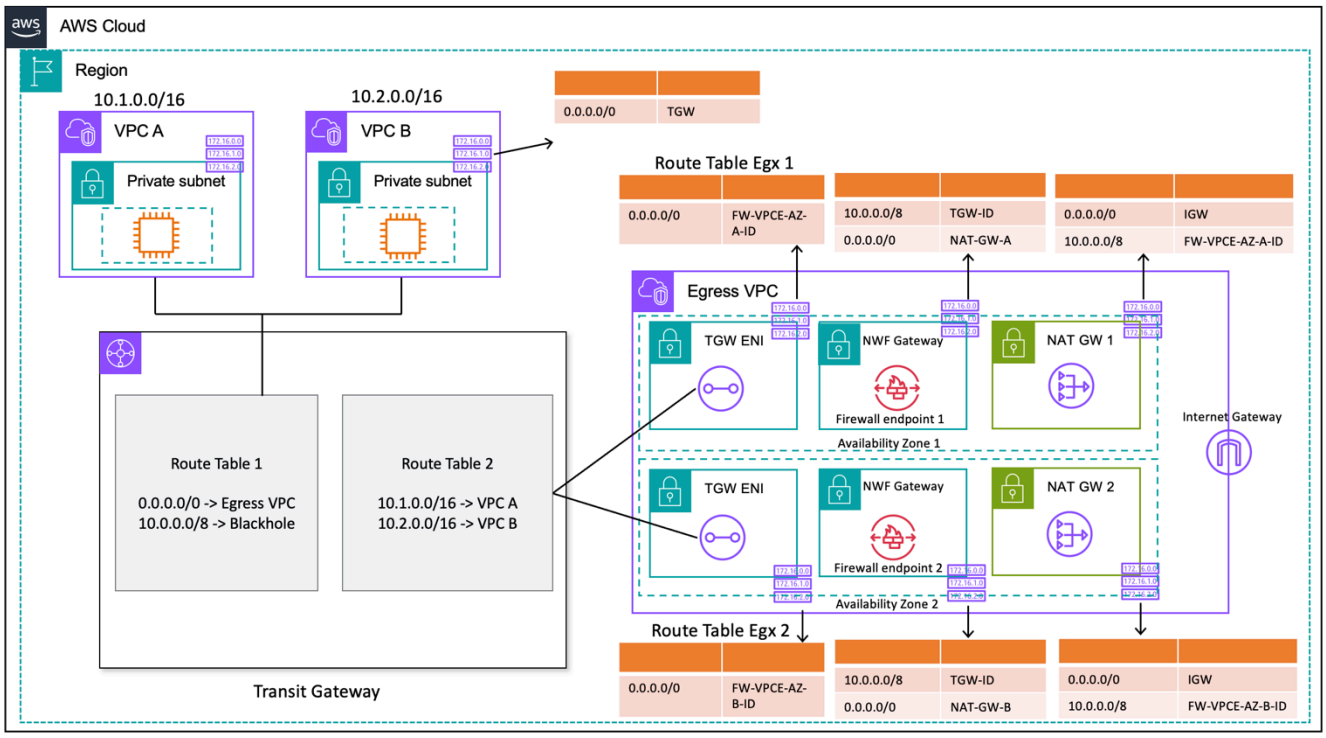
Sebuah NAT gateway tunggal dapat mendukung hingga 55.000 koneksi simultan per alamat IP yang ditetapkan ke setiap tujuan unik. Anda dapat meminta penyesuaian kuota untuk memungkinkan hingga delapan alamat IP yang ditetapkan, memungkinkan 440.000 koneksi simultan ke IP dan port tujuan tunggal. NATgateway menyediakan bandwidth 5 Gbps dan secara otomatis menskalakan hingga 100 Gbps. Transit Gateway umumnya tidak bertindak sebagai penyeimbang beban dan tidak akan mendistribusikan lalu lintas Anda secara merata di seluruh NAT gateway di beberapa Availability Zone. Lalu lintas melintasi Transit Gateway akan tetap berada dalam Availability Zone, jika memungkinkan. Jika EC2 instans Amazon yang memulai lalu lintas berada di Availability Zone 1, lalu lintas akan keluar dari Transit Gateway elastic network interface di Availability Zone 1 yang sama di jalan keluar VPC dan akan mengalir ke lompatan berikutnya berdasarkan tabel rute subnet tempat elastic network interface berada. Untuk daftar lengkap aturan, lihat NATgateway di dokumentasi Amazon Virtual Private Cloud.

Untuk informasi selengkapnya, lihat Membuat titik keluar internet tunggal dari beberapa posting blog VPCs Menggunakan AWS Transit Gateway.

Menggunakan NAT gateway dengan jalan AWS Network Firewall keluar terpusat IPv4

Jika Anda ingin memeriksa dan memfilter lalu lintas keluar Anda, Anda dapat menggabungkan AWS Network Firewall dengan NAT gateway dalam arsitektur jalan keluar terpusat Anda. AWS Network Firewall adalah layanan terkelola yang memudahkan untuk menerapkan perlindungan jaringan penting untuk semua Anda. VPCs Ini memberikan kontrol dan visibilitas ke lalu lintas jaringan Layer 3-7 untuk keseluruhan Anda. VPC Anda dapat URL melakukan/nama domain, alamat IP, dan pemfilteran lalu lintas keluar berbasis konten untuk menghentikan kemungkinan kehilangan data, membantu memenuhi persyaratan kepatuhan, dan memblokir komunikasi malware yang diketahui. AWS Network Firewall mendukung ribuan aturan yang dapat menyaring lalu lintas jaringan yang ditujukan untuk alamat IP buruk yang diketahui atau nama domain yang buruk. Anda juga dapat menggunakan IPS aturan Suricata sebagai bagian dari AWS Network Firewall layanan dengan mengimpor kumpulan aturan sumber terbuka atau membuat aturan Intrusion Prevention System () Anda sendiri menggunakan sintaks aturan Suricata. IPS AWS Network Firewall juga memungkinkan Anda untuk mengimpor aturan kompatibel yang bersumber dari AWS mitra.

Dalam arsitektur jalan keluar terpusat dengan inspeksi, AWS Network Firewall titik akhir adalah target tabel rute default dalam tabel rute subnet lampiran gateway transit untuk jalan keluar. VPC Lalu lintas antara spoke VPCs dan internet diperiksa menggunakan AWS Network Firewall seperti yang ditunjukkan pada diagram berikut.



Jalan keluar terpusat dengan AWS Network Firewall dan NAT gateway (desain tabel rute)

Untuk model penerapan terpusat dengan Transit Gateway, AWS rekomendasikan untuk menerapkan AWS Network Firewall titik akhir di beberapa Availability Zone. Harus ada satu titik akhir firewall di setiap Availability Zone tempat pelanggan menjalankan beban kerja, seperti yang ditunjukkan pada diagram sebelumnya. Sebagai praktik terbaik, subnet firewall tidak boleh berisi lalu lintas lain karena AWS Network Firewall tidak dapat memeriksa lalu lintas dari sumber atau tujuan dalam subnet firewall.

Mirip dengan pengaturan sebelumnya, VPC lampiran spoke dikaitkan dengan Route Table 1 (RT1) dan disebarkan ke Route Table 2 (RT2). Rute Blackhole ditambahkan secara eksplisit untuk VPCs melarang keduanya berkomunikasi satu sama lain.

Terus gunakan rute default dalam RT1 mengarahkan semua lalu lintas ke jalan keluar. VPC Transit Gateway akan meneruskan semua arus lalu lintas ke salah satu dari dua zona ketersediaan di jalan keluar. VPC Setelah lalu lintas mencapai salah satu Transit Gateway ENIs di jalan keluarVPC, Anda mencapai rute default yang akan meneruskan lalu lintas ke salah satu AWS Network Firewall titik akhir di zona ketersediaan masing-masing. AWS Network Firewall kemudian akan memeriksa lalu lintas berdasarkan aturan yang Anda tetapkan sebelum meneruskan lalu lintas ke NAT gateway menggunakan rute default.

Kasus ini tidak memerlukan mode alat Transit Gateway, karena Anda tidak mengirim lalu lintas antar lampiran.

> **Note**
>
> AWS Network Firewall tidak melakukan terjemahan alamat jaringan untuk Anda, fungsi ini akan ditangani oleh NAT gateway setelah inspeksi lalu lintas melalui. AWS Network Firewall Ingress routing tidak diperlukan dalam kasus ini karena lalu lintas kembali akan diteruskan ke default. NATGW IPs

Karena Anda menggunakan Transit Gateway, di sini kita dapat menempatkan firewall sebelum NAT gateway. Dalam model ini, firewall dapat melihat IP sumber di belakang Transit Gateway.

Jika Anda melakukan ini dalam satuVPC, kita dapat menggunakan peningkatan VPC routing yang memungkinkan Anda untuk memeriksa lalu lintas antara subnet dalam hal yang sama. VPC Untuk detailnya, lihat model Deployment untuk AWS Network Firewall dengan peningkatan VPC perutean posting blog.

Skalabilitas

AWS Network Firewall dapat secara otomatis meningkatkan atau menurunkan kapasitas firewall berdasarkan beban lalu lintas untuk mempertahankan kinerja yang stabil dan dapat diprediksi untuk meminimalkan biaya. AWS Network Firewall dirancang untuk mendukung puluhan ribu aturan firewall dan dapat meningkatkan throughput hingga 100 Gbps per Availability Zone.

Pertimbangan utama

- Setiap titik akhir firewall dapat menangani sekitar 100 Gbps lalu lintas, jika Anda memerlukan burst yang lebih tinggi atau throughput berkelanjutan, hubungi dukungan. AWS
- Jika Anda memilih untuk membuat NAT gateway di AWS akun Anda bersama dengan Network Firewall, pemrosesan NAT gateway standar dan biaya penggunaan per jam dibebaskan one-to-one berdasarkan pemrosesan per GB dan jam penggunaan yang dikenakan untuk firewall Anda.
- Anda juga dapat mempertimbangkan titik akhir firewall terdistribusi melalui AWS Firewall Manager tanpa Transit Gateway.
- Uji aturan firewall sebelum memindahkannya ke produksi, mirip dengan daftar kontrol akses jaringan, karena urutannya penting.
- Aturan Suricata tingkat lanjut diperlukan untuk pemeriksaan lebih dalam. Firewall jaringan mendukung inspeksi lalu lintas terenkripsi untuk masuknya serta lalu lintas keluar.
- Variabel grup `HOME_NET` aturan mendefinisikan rentang IP sumber yang memenuhi syarat untuk diproses di mesin Stateful. Menggunakan pendekatan terpusat, Anda harus menambahkan semua tambahan yang VPC CIDRs dilampirkan ke Transit Gateway agar memenuhi syarat untuk diproses. Lihat dokumentasi Network Firewall untuk detail selengkapnya tentang variabel grup `HOME_NET` aturan.
- Pertimbangkan untuk menggunakan Transit Gateway dan jalan keluar VPC di akun Layanan Jaringan terpisah untuk memisahkan akses berdasarkan pendelegasian tugas; misalnya, hanya administrator jaringan yang dapat mengakses akun Layanan Jaringan.
- Untuk menyederhanakan penyebaran dan manajemen AWS Network Firewall dalam model ini, AWS Firewall Manager dapat digunakan. Firewall Manager memungkinkan Anda mengelola firewall yang berbeda secara terpusat dengan secara otomatis menerapkan perlindungan yang Anda buat di lokasi terpusat ke beberapa akun. Firewall Manager mendukung model penyebaran terdistribusi dan terpusat untuk Network Firewall. Untuk mempelajari lebih lanjut, lihat posting blog Cara menyebarkan AWS Network Firewall dengan menggunakan AWS Firewall Manager.

Menggunakan NAT gateway dan Load Balancer Gateway dengan EC2 instans Amazon untuk jalan keluar terpusat IPv4

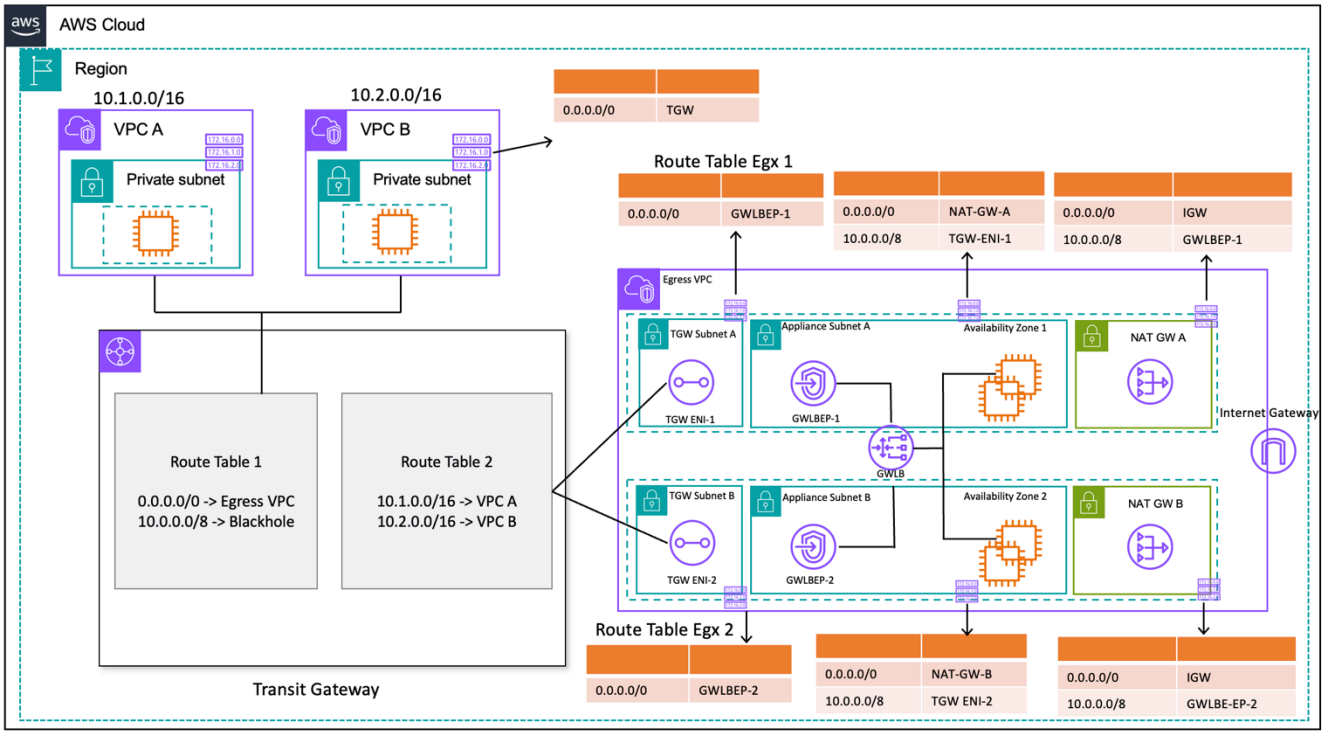
Menggunakan alat virtual berbasis perangkat lunak (di AmazonEC2) dari AWS Marketplace dan AWS Partner Network sebagai titik keluar mirip dengan pengaturan gateway. NAT Opsi ini dapat digunakan jika Anda ingin menggunakan lapisan lanjutan 7 FireWall/Intrusion Prevention/Detection System (IPS/IDS) dan kemampuan inspeksi paket mendalam dari berbagai penawaran vendor.

Pada gambar berikut, selain NAT gateway, Anda menerapkan peralatan virtual menggunakan EC2 instance di belakang Gateway Load GWLB Balancer (). Dalam pengaturan iniGWLB, Gateway Load Balancer Endpoint (GWLBE), peralatan virtual, dan NAT gateway dikerahkan di pusat yang VPC terhubung ke Transit Gateway menggunakan lampiran. VPC VPCsBicara juga terhubung ke Transit Gateway menggunakan VPC Lampiran. Karena GWLBEs merupakan target yang dapat dirutekan, Anda dapat merutekan lalu lintas yang bergerak ke dan dari Transit Gateway ke armada peralatan virtual yang dikonfigurasi sebagai target di belakang. GWLB GWLBbertindak sebagai bump-in-the-wire dan secara transparan melewati semua lalu lintas Layer 3 melalui peralatan virtual pihak ketiga, dan dengan demikian tidak terlihat oleh sumber dan tujuan lalu lintas. Oleh karena itu, arsitektur ini memungkinkan Anda untuk secara terpusat memeriksa semua lalu lintas jalan keluar Anda yang melintasi Transit Gateway.

Untuk informasi lebih lanjut tentang bagaimana lalu lintas mengalir dari aplikasi di internet dan kembali melalui pengaturan ini, lihat Arsitektur inspeksi terpusat dengan AWS Gateway Load AWS Transit Gateway Balancer dan. VPCs

Anda dapat mengaktifkan mode alat di Transit Gateway untuk menjaga simetri aliran melalui peralatan virtual. Ini berarti lalu lintas dua arah diarahkan melalui alat yang sama dan Availability Zone untuk masa pakai aliran. Pengaturan ini sangat penting untuk firewall stateful yang melakukan inspeksi paket mendalam. Mengaktifkan mode alat menghilangkan kebutuhan akan solusi yang kompleks, seperti terjemahan alamat jaringan sumber (SNAT), untuk memaksa lalu lintas kembali ke alat yang benar untuk mempertahankan simetri. Lihat Praktik terbaik untuk menerapkan Load Balancer Gateway untuk detailnya.

Dimungkinkan juga untuk menerapkan GWLB titik akhir secara terdistribusi tanpa Transit Gateway untuk mengaktifkan inspeksi jalan keluar. Pelajari lebih lanjut tentang pola arsitektur ini di Introducing AWS Gateway Load Balancer: Postingan blog pola arsitektur yang didukung.



Jalan keluar terpusat dengan Gateway Load Balancer dan EC2 instance (desain tabel rute)

Ketersediaan tinggi

AWSmerekomendasikan penerapan Gateway Load Balancer dan peralatan virtual di beberapa Availability Zone untuk ketersediaan yang lebih tinggi.

Gateway Load Balancer dapat melakukan pemeriksaan kesehatan untuk mendeteksi kegagalan alat virtual. Dalam hal alat yang tidak sehat, GWLB alihkan aliran baru ke peralatan sehat. Arus yang ada selalu menuju ke target yang sama terlepas dari status kesehatan target. Hal ini memungkinkan pengeringan koneksi dan mengakomodasi kegagalan pemeriksaan kesehatan karena CPU lonjakan pada peralatan. Untuk detail selengkapnya, lihat bagian 4: Memahami skenario kegagalan peralatan dan Availability Zone di posting blog Praktik terbaik untuk menerapkan Load Balancer Gateway. Load Balancer Gateway dapat menggunakan grup penskalaan otomatis sebagai target. Manfaat ini menghilangkan beban berat dalam mengelola ketersediaan dan skalabilitas armada alat.

Keuntungan

Gateway Load Balancer dan titik akhir Gateway Load Balancer didukung AWS PrivateLink oleh, yang memungkinkan pertukaran lalu lintas lintas VPC melintasi batas dengan aman tanpa perlu melintasi internet publik.

Gateway Load Balancer adalah layanan terkelola yang menghilangkan beban berat yang tidak terdiferensiasi dalam mengelola, menerapkan, menskalakan peralatan keamanan virtual sehingga Anda dapat fokus pada hal-hal yang penting. Load Balancer Gateway dapat mengekspos tumpukan firewall sebagai layanan endpoint bagi pelanggan untuk berlangganan menggunakan. AWS Marketplace Ini disebut Firewall as a Service (FWaaS); ini memperkenalkan penyebaran yang disederhanakan dan menghilangkan kebutuhan untuk mengandalkan BGP dan ECMP mendistribusikan lalu lintas di beberapa instans AmazonEC2.

Pertimbangan utama

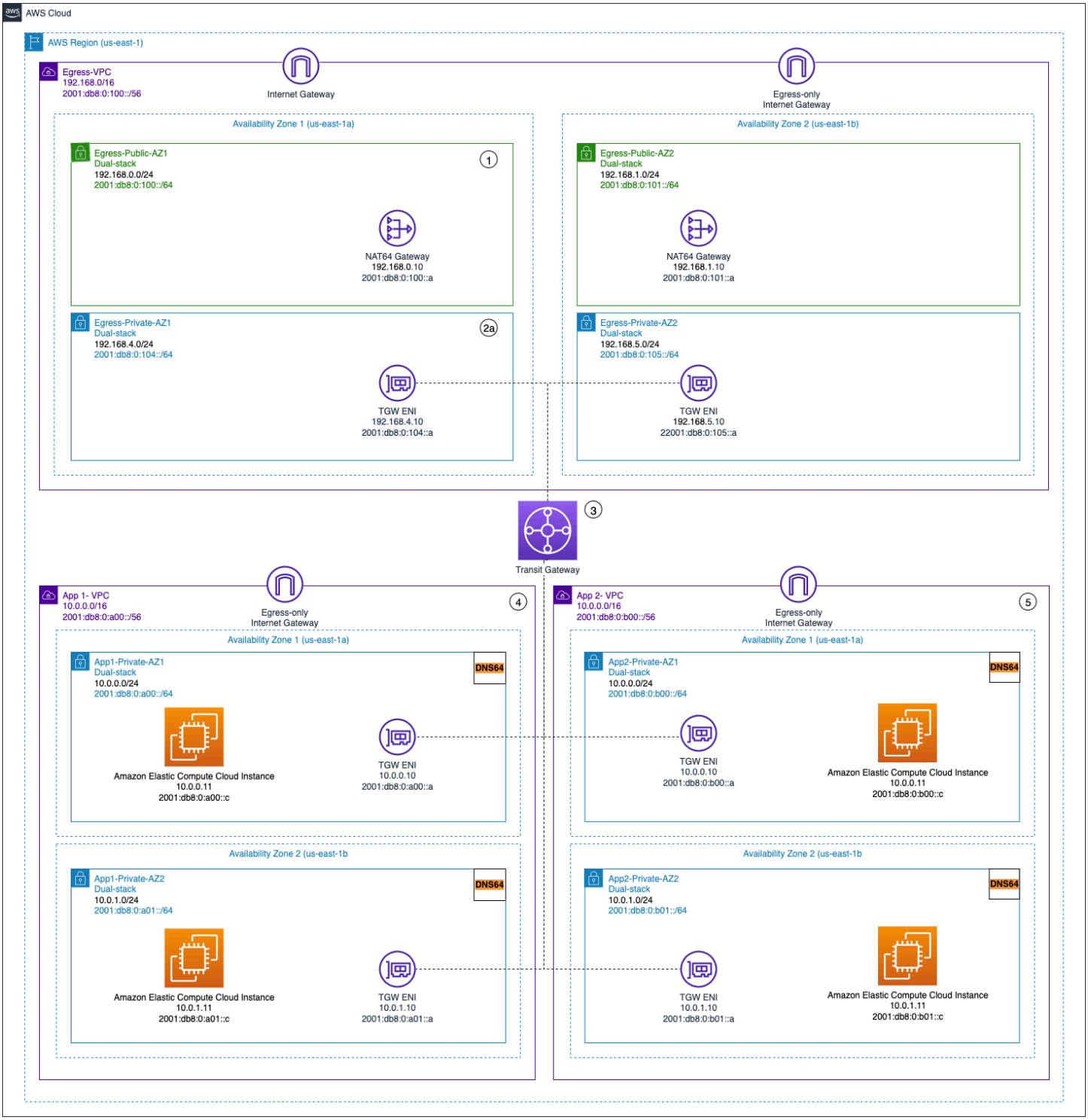
- Peralatan perlu mendukung protokol enkapsulasi Geneve untuk diintegrasikan. GWLB
- Beberapa peralatan pihak ketiga dapat mendukung SNAT dan melapisi perutean (mode dua lengan) sehingga menghilangkan kebutuhan untuk membuat NAT gateway untuk menghemat biaya. Namun, konsultasikan dengan AWS mitra pilihan Anda sebelum menggunakan mode ini karena ini tergantung pada dukungan dan implementasi vendor.
- Catat batas waktu GWLB idle. Hal ini dapat mengakibatkan batas waktu koneksi pada klien. Anda dapat menyetel batas waktu Anda di level klien, server, firewall, dan OS untuk menghindari hal ini. Lihat Bagian 1: Sesuaikan nilai TCP keep-alive atau batas waktu untuk mendukung TCP aliran jangka panjang dalam Praktik terbaik untuk menerapkan postingan blog Gateway Load Balancer untuk informasi selengkapnya.
- GWLBEdidukung oleh AWS PrivateLink, sehingga AWS PrivateLink biaya akan berlaku. Anda dapat mempelajari lebih lanjut di halaman AWS PrivateLink harga. Jika Anda menggunakan model terpusat dengan Transit Gateway, biaya pemrosesan TGW data akan berlaku.
- Pertimbangkan untuk menggunakan Transit Gateway dan jalan keluar VPC di akun Layanan Jaringan terpisah untuk memisahkan akses berdasarkan pendelegasian tugas, seperti hanya administrator jaringan yang dapat mengakses Akun Layanan Jaringan.

Jalan keluar terpusat untuk IPv6

Untuk mendukung jalan IPv6 keluar dalam penerapan tumpukan ganda yang memiliki jalan keluar terpusat, salah satu IPv4 dari dua pola harus dipilih:

- Jalan IPv4 keluar terpusat dengan jalan keluar yang terdesentralisasi IPv6
- Jalan IPv4 keluar terpusat dan jalan keluar terpusat IPv6

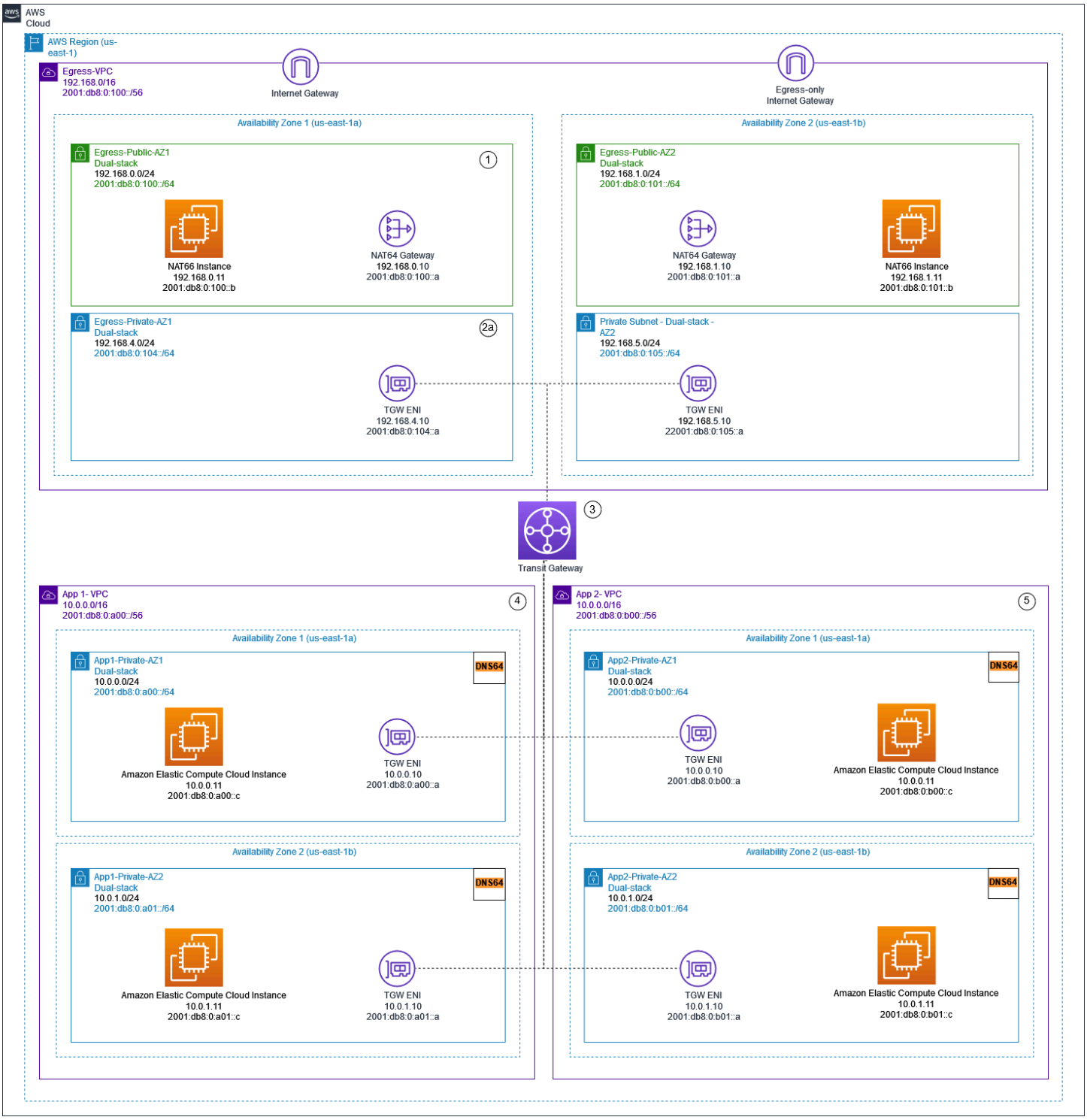
Pada pola pertama, yang ditunjukkan pada diagram berikut, gateway internet khusus egres digunakan di setiap pembicaraan. VPC Gateway internet khusus Egress adalah gateway yang diskalakan secara horizontal, redundan, dan sangat tersedia yang memungkinkan komunikasi keluar dari instans di dalam Anda. IPv6 VPC Mereka mencegah internet memulai IPv6 koneksi dengan instans Anda. Gateway internet khusus Egress tidak dikenakan biaya. Dalam model penyebaran ini, IPv6 lalu lintas mengalir keluar dari gateway internet khusus egres di masing-masing VPC dan arus IPv4 lalu lintas melalui Gateway terpusat yang digunakan. NAT



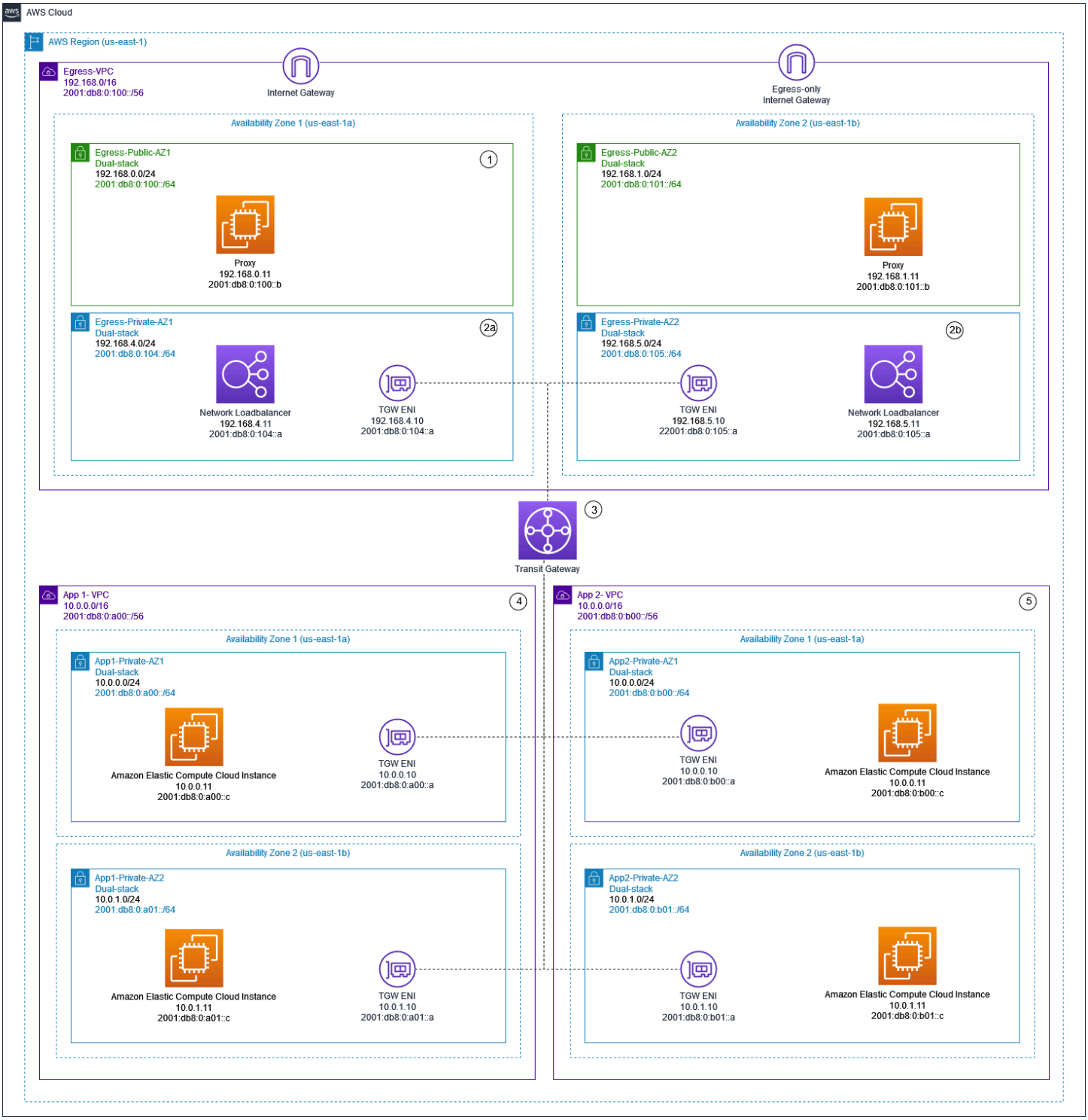
Jalan IPV4 keluar terpusat dan jalan keluar yang terdesentralisasi saja IPv6

Dalam pola kedua, yang ditunjukkan dalam diagram berikut, IPv6 lalu lintas keluar dari instance Anda dikirim ke terpusat. VPC Hal ini dapat dicapai dengan menggunakan IPv6 -to- IPv6 Network Prefix Translation (NPTv6) dengan NAT66 instance dan NAT Gateway atau dengan menggunakan Instans

Proxy dan Network Load Balancer. Pola ini berlaku jika inspeksi lalu lintas terpusat untuk lalu lintas keluar diperlukan dan tidak dapat dilakukan di setiap palang. VPC



Jalan IPv6 keluar terpusat menggunakan NAT gateway dan instance NAT66



Terpusat IPv4 dan IPv6 keluar menggunakan instance proxy dan Network Load Balancer

AWSWhitepaper IPv6 on menggambarkan pola jalan keluar terpusatIPv6. Pola jalan IPv6 keluar dibahas secara lebih rinci di blog Lalu lintas internet keluar terpusat untuk tumpukan ganda IPv4 dan IPv6 VPCs, bersama dengan pertimbangan khusus, solusi sampel, dan diagram.

Keamanan jaringan terpusat untuk lalu lintas VPC-ke-VPC dan lokal ke VPC

Mungkin ada skenario di mana pelanggan ingin mengimplementasikan lapisan 3-7 Firewall/IPS/ID dalam lingkungan multi-akun mereka untuk memeriksa arus lintas antara VPC (lalu lintas timur-barat) atau antara pusat data lokal dan VPC (lalu lintas utara-selatan). Ini dapat dicapai dengan cara yang berbeda, tergantung pada kasus penggunaan dan persyaratan. Misalnya, Anda dapat menggabungkan Load Balancer Gateway, Network Firewall, Transit VPC, atau menggunakan arsitektur terpusat dengan Transit Gateways. Skenario ini dibahas di bagian berikut.

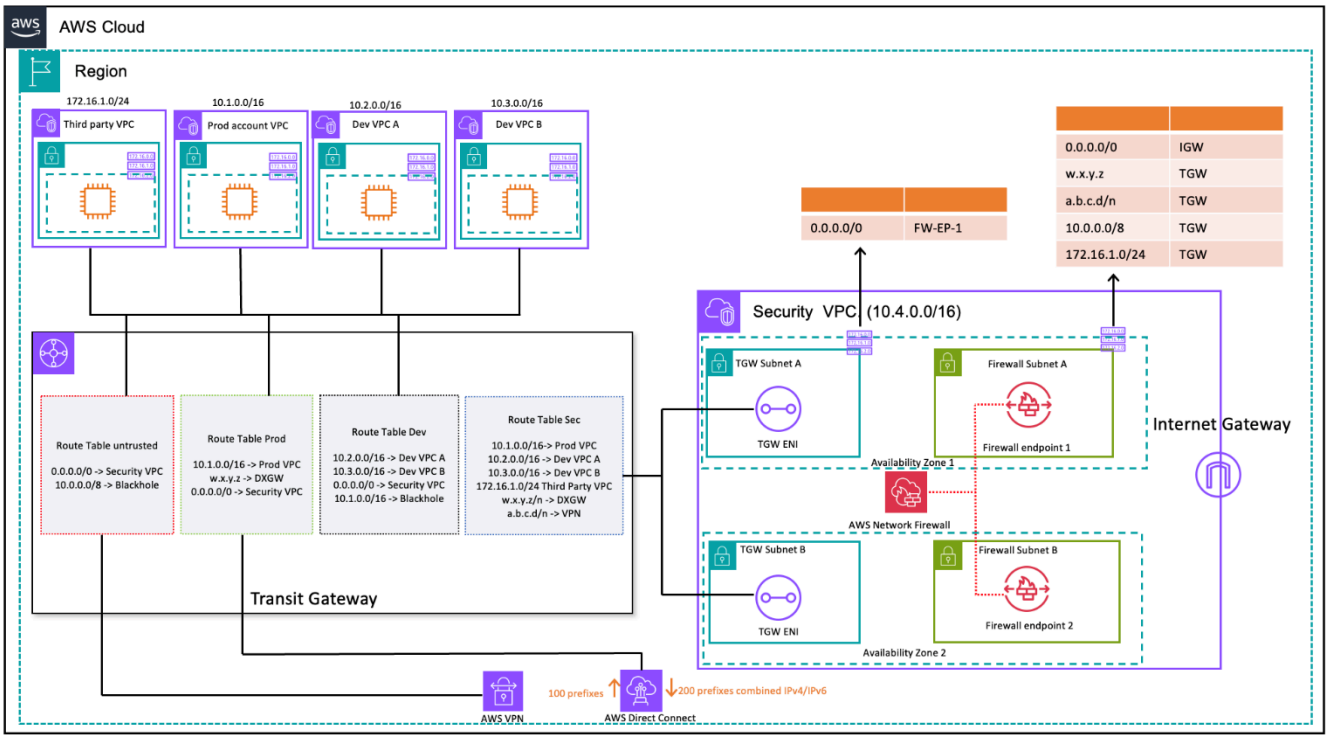
Pertimbangan menggunakan model inspeksi keamanan jaringan terpusat

Untuk mengurangi biaya, Anda harus selektif dalam lalu lintas apa yang melewati Load Balancer AWS Network Firewall atau Gateway Anda. Salah satu cara untuk melanjutkan adalah dengan menentukan zona keamanan dan memeriksa lalu lintas antara zona yang tidak tepercaya. Zona yang tidak dipercaya dapat berupa situs jarak jauh yang dikelola oleh pihak ketiga, VPC vendor yang tidak Anda kendali/percayai, atau VPC sandbox/dev, yang memiliki aturan keamanan yang lebih santai dibandingkan dengan lingkungan Anda lainnya. Ada empat zona dalam contoh ini:

- Zona Tidak Terpercaya — Ini untuk semua lalu lintas yang berasal dari 'VPN ke situs yang tidak dipercaya jauh' atau VPC vendor pihak ketiga.
- Zona Produksi (Prod) — Ini berisi lalu lintas dari VPC produksi dan DC pelanggan lokal.
- Zona Pengembangan (Dev) —Ini berisi lalu lintas dari dua VPC pengembangan.
- Zona Keamanan (Sec) - Berisi komponen firewall kami Network Firewall atau Gateway Load Balancer.

Pengaturan ini memiliki empat zona keamanan, tetapi Anda mungkin memiliki lebih banyak. Anda dapat menggunakan beberapa tabel rute dan rute lubang hitam untuk mencapai isolasi keamanan dan arus lalu lintas yang optimal. Memilih set zona yang tepat tergantung pada strategi desain Zona Pendaratan Anda secara keseluruhan (struktur akun, desain VPC). Anda dapat memiliki zona untuk mengaktifkan isolasi antara Unit Bisnis (BUS), aplikasi, lingkungan, dan sebagainya.

Jika Anda ingin memeriksa dan memfilter VPC-ke-VPC, lalu lintas antar zona, dan lalu lintas VPC di tempat, Anda dapat menggabungkan dengan Transit Gateway dalam arsitektur terpusat Anda. AWS Network Firewall Dengan memiliki hub-and-spoke model AWS Transit Gateway, model penyebaran terpusat dapat dicapai. AWS Network Firewall Ini digunakan dalam VPC keamanan terpisah. VPC keamanan terpisah menyediakan pendekatan yang disederhanakan dan sentral untuk mengelola inspeksi. Arsitektur VPC seperti itu memberikan AWS Network Firewall visibilitas IP sumber dan tujuan. IP sumber dan tujuan dipertahankan. VPC keamanan ini terdiri dari dua subnet di setiap Availability Zone; di mana satu subnet didedikasikan untuk AWS Transit Gateway attachment dan subnet lainnya didedikasikan untuk endpoint firewall. Subnet dalam VPC ini seharusnya hanya AWS Network Firewall berisi titik akhir karena Network Firewall tidak dapat memeriksa lalu lintas di subnet yang sama dengan titik akhir. Ketika Anda menggunakan Network Firewall untuk memeriksa lalu lintas secara terpusat, ia dapat melakukan inspeksi paket mendalam (DPI) pada lalu lintas masuk. Pola DPI diperluas di bagian Inspeksi Masuk Terpusat dari paper ini.



VPC-ke-VPC dan inspeksi lalu lintas lokal ke VPC menggunakan Transit Gateway dan (desain tabel rute) AWS Network Firewall

Dalam arsitektur terpusat dengan inspeksi, subnet Transit Gateway memerlukan tabel rute VPC terpisah untuk memastikan lalu lintas diteruskan ke titik akhir firewall dalam Availability Zone yang sama. Untuk lalu lintas kembali, satu tabel rute VPC yang berisi rute default menuju Gateway Transit dikonfigurasi. Lalu lintas dikembalikan ke AWS Transit Gateway dalam Availability Zone yang sama setelah diperiksa oleh AWS Network Firewall. Hal ini dimungkinkan karena fitur mode alat dari Transit

Gateway. Fitur mode alat dari Transit Gateway juga membantu AWS Network Firewall untuk memiliki kemampuan inspeksi lalu lintas stateful di dalam VPC keamanan.

Dengan mode alat diaktifkan pada gateway transit, ia memilih antarmuka jaringan tunggal menggunakan algoritme hash aliran untuk seluruh masa pakai koneksi. Gateway transit menggunakan antarmuka jaringan yang sama untuk lalu lintas kembali. Ini memastikan bahwa lalu lintas dua arah dirutekan secara simetris—itu dirutekan melalui Availability Zone yang sama di attachment VPC selama masa pakai aliran. Untuk informasi selengkapnya tentang mode alat, lihat mode peralatan dan alat stateful dalam dokumentasi VPC Amazon.

Untuk opsi penerapan VPC keamanan yang berbeda AWS Network Firewall dengan dan Transit Gateway, lihat postingan blog Model Deployment untuk AWS Network Firewall.

Menggunakan Load Balancer Gateway dengan Transit Gateway untuk keamanan jaringan terpusat

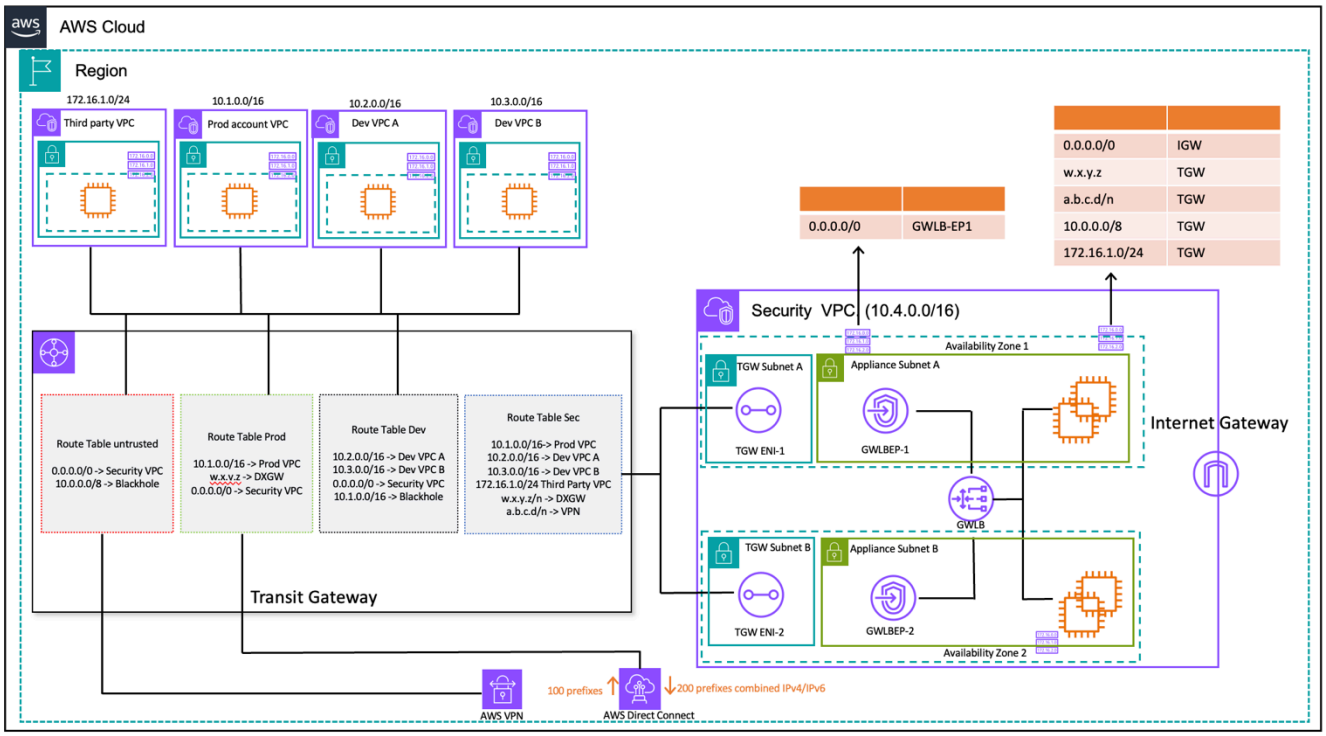
Sering kali, pelanggan ingin menggabungkan peralatan virtual untuk menangani penyaringan lalu lintas dan untuk memberikan kemampuan inspeksi keamanan. Dalam kasus penggunaan seperti itu, mereka dapat mengintegrasikan Gateway Load Balancer, peralatan virtual, dan Transit Gateway untuk menerapkan arsitektur terpusat untuk memeriksa lalu lintas VPC-ke-VPC dan VPC. to-on-premises

Load Balancer Gateway digunakan dalam VPC keamanan terpisah bersama dengan peralatan virtual. Peralatan virtual yang akan memeriksa lalu lintas dikonfigurasi sebagai target di belakang Load Balancer Gateway. Karena titik akhir Load Balancer Gateway adalah target yang dapat dirutekan, pelanggan dapat merutekan lalu lintas yang bergerak ke dan dari Transit Gateway ke armada peralatan virtual. Untuk memastikan simetri aliran, mode alat diaktifkan di Transit Gateway.

Setiap VPC spoke memiliki tabel rute yang terkait dengan Transit Gateway, yang memiliki rute default ke lampiran VPC Keamanan sebagai lompatan berikutnya.

VPC Keamanan terpusat terdiri dari subnet alat di setiap Availability Zone; yang memiliki titik akhir Gateway Load Balancer dan peralatan virtual. Ini juga memiliki subnet untuk lampiran Transit Gateway di setiap Availability Zone, seperti yang ditunjukkan pada gambar berikut.

Untuk informasi selengkapnya tentang inspeksi keamanan terpusat dengan Gateway Load Balancer dan Transit Gateway, lihat arsitektur inspeksi terpusat dengan AWS Gateway Load Balancer dan postingan blog. AWS Transit Gateway



on-premises-toPemeriksaan lalu lintas VPC-ke-VPC dan -VPC menggunakan Transit Gateway dan AWS Gateway Load Balancer (desain tabel rute)

Pertimbangan utama untuk AWS Network Firewall dan AWS Gateway Load Balancer

- Mode alat harus diaktifkan di Transit Gateway saat melakukan inspeksi timur-barat.
- Anda dapat menerapkan model yang sama untuk pemeriksaan lalu lintas ke yang lain Wilayah AWS menggunakan pengintip AWS Transit Gateway Antar Wilayah.
- Secara default, setiap Load Balancer Gateway yang digunakan di Availability Zone mendistribusikan lalu lintas di seluruh target terdaftar dalam Availability Zone yang sama saja. Ini disebut afinitas Availability Zone. Jika Anda mengaktifkan penyeimbangan beban lintas zona, Load Balancer Gateway mendistribusikan lalu lintas ke semua target yang terdaftar dan sehat di semua Availability Zone yang diaktifkan. Jika semua target di semua Availability Zone tidak sehat, Load Balancer Gateway gagal dibuka. Lihat bagian 4: Memahami skenario kegagalan peralatan dan Availability Zone dalam Praktik terbaik untuk menerapkan postingan blog Gateway Load Balancer untuk detail selengkapnya.
- Untuk penerapan Multi-wilayah, AWS sarankan Anda menyiapkan VPC inspeksi terpisah di Wilayah lokal masing-masing untuk menghindari dependensi antar wilayah dan mengurangi biaya

transfer data terkait. Anda harus memeriksa lalu lintas di Wilayah setempat alih-alih memusatkan inspeksi ke Wilayah lain.

- Biaya menjalankan pasangan ketersediaan tinggi (HA) berbasis EC2 tambahan di penerapan Multi-wilayah dapat bertambah. Untuk informasi selengkapnya, lihat Praktik terbaik untuk menerapkan postingan blog Gateway Load Balancer.

AWS Network Firewall vs. Load Balancer Gateway

Tabel 2 - AWS Network Firewall vs Gateway Load Balancer

Kriteria	AWS Network Firewall	Gateway Load Balancer
Kasus penggunaan	Firewall jaringan stateful, terkelola, dengan deteksi intrusi dan kemampuan layanan pencegahan yang kompatibel dengan Suricata.	Layanan terkelola yang memudahkan untuk menyebarkan, menskalakan, dan mengelola peralatan virtual pihak ketiga
Kompleksitas	AWS layanan terkelola. AWS menangani skalabilitas dan ketersediaan layanan.	Layanan terkelola AWS. AWS akan menangani skalabilitas dan ketersediaan layanan Load Balancer Gateway. Pelanggan bertanggung jawab untuk mengelola penskalaan dan ketersediaan peralatan virtual di belakang Gateway Load Balancer.
Skala	AWS Network Firewall endpoint didukung oleh AWS PrivateLink. Network Firewall mendukung hingga 100 Gbps lalu lintas jaringan per endpoint firewall.	Endpoint Load Balancer Gateway mendukung bandwidth maksimum hingga 100 Gbps per titik akhir

Kriteria	AWS Network Firewall	Gateway Load Balancer
Biaya	AWS Network Firewall biaya titik akhir+Biaya pemrosesan data	Gateway Load Balancer+Titik akhir Load Balancer+peralatan virtual+biaya pemrosesan data

Inspeksi masuk terpusat

Aplikasi yang menghadap ke internet, menurut sifatnya, memiliki permukaan serangan yang lebih besar dan terpapar pada kategori ancaman yang tidak harus dihadapi sebagian besar jenis aplikasi lain. Memiliki perlindungan yang diperlukan dari serangan pada jenis aplikasi ini, dan meminimalkan area permukaan dampak, adalah bagian inti dari strategi keamanan apa pun.

Saat Anda menyebarkan aplikasi di Zona Pendaratan Anda, banyak aplikasi akan diakses oleh pengguna melalui internet publik (misalnya, melalui Jaringan Pengiriman Konten (CDN), atau melalui aplikasi web yang menghadap publik) melalui penyeimbang beban yang menghadap publik, gateway API atau langsung melalui gateway internet. Anda dapat mengamankan beban kerja dan aplikasi Anda dalam hal ini dengan menggunakan AWS Web Application Firewall (AWS WAF) untuk Inspeksi Aplikasi Masuk, atau sebagai alternatif Inspeksi Masuk IDS/IPS menggunakan Gateway Load Balancer atau. AWS Network Firewall

Saat Anda terus menerapkan aplikasi di Zona Pendaratan Anda, Anda mungkin memiliki persyaratan untuk memeriksa lalu lintas internet masuk. Anda dapat mencapai ini dengan berbagai cara, baik menggunakan arsitektur inspeksi terdistribusi, terpusat, atau gabungan menggunakan Gateway Load Balancer yang menjalankan peralatan firewall pihak ketiga Anda AWS Network Firewall atau dengan kemampuan DPI dan IDS/IPS tingkat lanjut melalui penggunaan aturan Suricata open source. Bagian ini mencakup Gateway Load Balancer dan AWS Network Firewall dalam penyebaran terpusat, menggunakan AWS Transit Gateway bertindak sebagai hub pusat untuk merutekan lalu lintas.

AWS WAF dan AWS Firewall Manager untuk memeriksa lalu lintas masuk dari internet

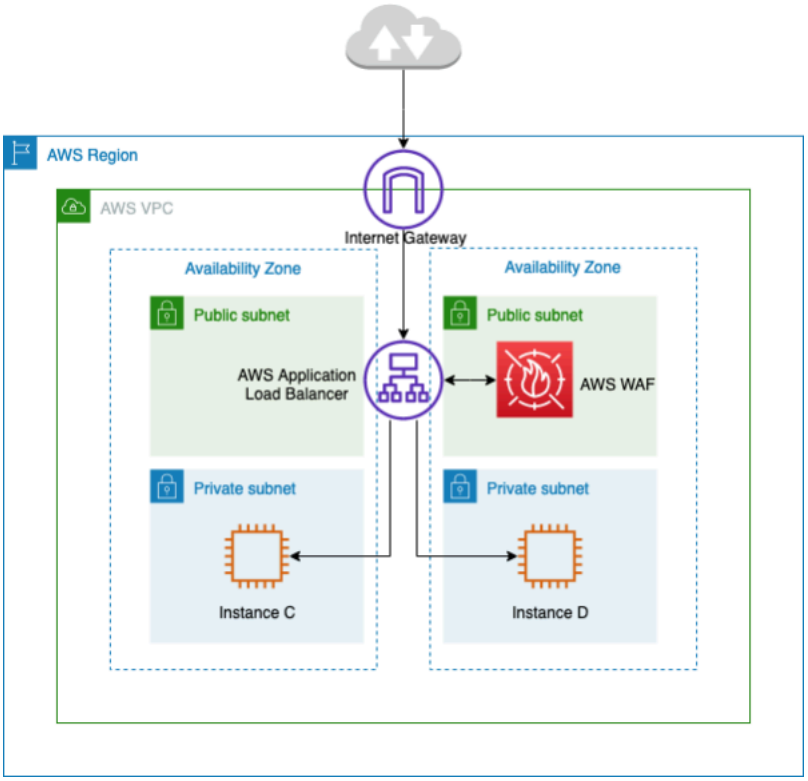
AWS WAF adalah firewall aplikasi web yang membantu melindungi aplikasi web atau API Anda terhadap eksploitasi web umum dan bot yang dapat memengaruhi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan. AWS WAF memberi Anda kontrol atas bagaimana lalu lintas mencapai aplikasi Anda dengan memungkinkan Anda membuat aturan keamanan yang mengontrol lalu lintas bot dan memblokir pola serangan umum, seperti injeksi SQL atau skrip lintas situs (XSS). Anda juga dapat menyesuaikan aturan yang menyaring pola lalu lintas tertentu.

Anda dapat menerapkan AWS WAF di Amazon CloudFront sebagai bagian dari solusi CDN Anda, Application Load Balancer yang mengedepankan server web Anda, Amazon API Gateway untuk REST API Anda, atau AWS AppSync untuk GraphQL API Anda.

Setelah Anda menerapkan AWS WAF, Anda kemudian dapat membuat aturan filter lalu lintas Anda sendiri menggunakan pembuat aturan visual, kode di JSON, aturan terkelola yang dikelola oleh AWS, atau Anda dapat berlangganan aturan pihak ketiga dari. AWS Marketplace Aturan-aturan ini dapat menyaring lalu lintas yang tidak diinginkan dengan mengevaluasi lalu lintas terhadap pola yang ditentukan. Anda dapat menggunakan Amazon lebih lanjut CloudWatch untuk memantau metrik lalu lintas masuk dan pencatatan.

Untuk manajemen terpusat di semua akun dan aplikasi Anda AWS Organizations, Anda dapat menggunakannya AWS Firewall Manager. AWS Firewall Manager adalah layanan manajemen keamanan yang memungkinkan Anda untuk mengkonfigurasi dan mengelola aturan firewall secara terpusat. Saat aplikasi baru Anda dibuat, AWS Firewall Manager membuatnya mudah untuk membawa aplikasi dan sumber daya baru ke dalam kepatuhan dengan menegakkan seperangkat aturan keamanan umum.

Dengan menggunakan AWS Firewall Manager, Anda dapat dengan mudah meluncurkan AWS WAF aturan untuk Application Load Balancers, instans API Gateway, dan distribusi Amazon. CloudFront AWS Firewall Manager terintegrasi dengan Peraturan yang Dikelola AWS for AWS WAF, yang memberi Anda cara mudah untuk menerapkan AWS WAF aturan yang telah dikonfigurasi sebelumnya dan dikuratori pada aplikasi Anda. Untuk informasi lebih lanjut tentang pengelolaan AWS WAF secara terpusat AWS Firewall Manager, lihat Kelola terpusat AWS WAF (API v2) dan sesuai skala Peraturan yang Dikelola AWS dengan. AWS Firewall Manager



Inspeksi lalu lintas masuk terpusat menggunakan AWS WAF

Dalam arsitektur sebelumnya, aplikasi berjalan di instans Amazon EC2 di beberapa zona ketersediaan di subnet pribadi. Ada Application Load Balancer (ALB) yang menghadap publik yang diterapkan di depan instans Amazon EC2, load balancing permintaan di antara target yang berbeda. AWS WAF Ini terkait dengan ALB.

Keuntungan

- Dengan AWS WAF Bot Control, Anda mendapatkan visibilitas dan kontrol atas lalu lintas bot umum dan meresap ke aplikasi Anda.
- Dengan Managed Rules for AWS WAF, Anda dapat dengan cepat memulai dan melindungi aplikasi web atau API Anda terhadap ancaman umum. Anda dapat memilih dari banyak jenis aturan, seperti yang menangani masalah seperti Open Web Application Security Project (OWASP) Top 10 risiko keamanan, ancaman khusus untuk Content Management Systems (CMS) seperti WordPress atau Joomla, atau bahkan Common Vulnerabilities and Exposures (CVE) yang muncul. Aturan terkelola diperbarui secara otomatis saat masalah baru muncul, sehingga Anda dapat menghabiskan lebih banyak waktu untuk membangun aplikasi.
- AWS WAF adalah layanan yang dikelola dan tidak diperlukan alat untuk inspeksi dalam arsitektur ini. Selain itu, ia menyediakan log hampir real-time melalui Amazon Data Firehose. AWS WAF memberikan visibilitas mendekati waktu nyata ke dalam web web Anda, yang dapat Anda gunakan untuk membuat aturan atau peringatan baru di Amazon. CloudWatch

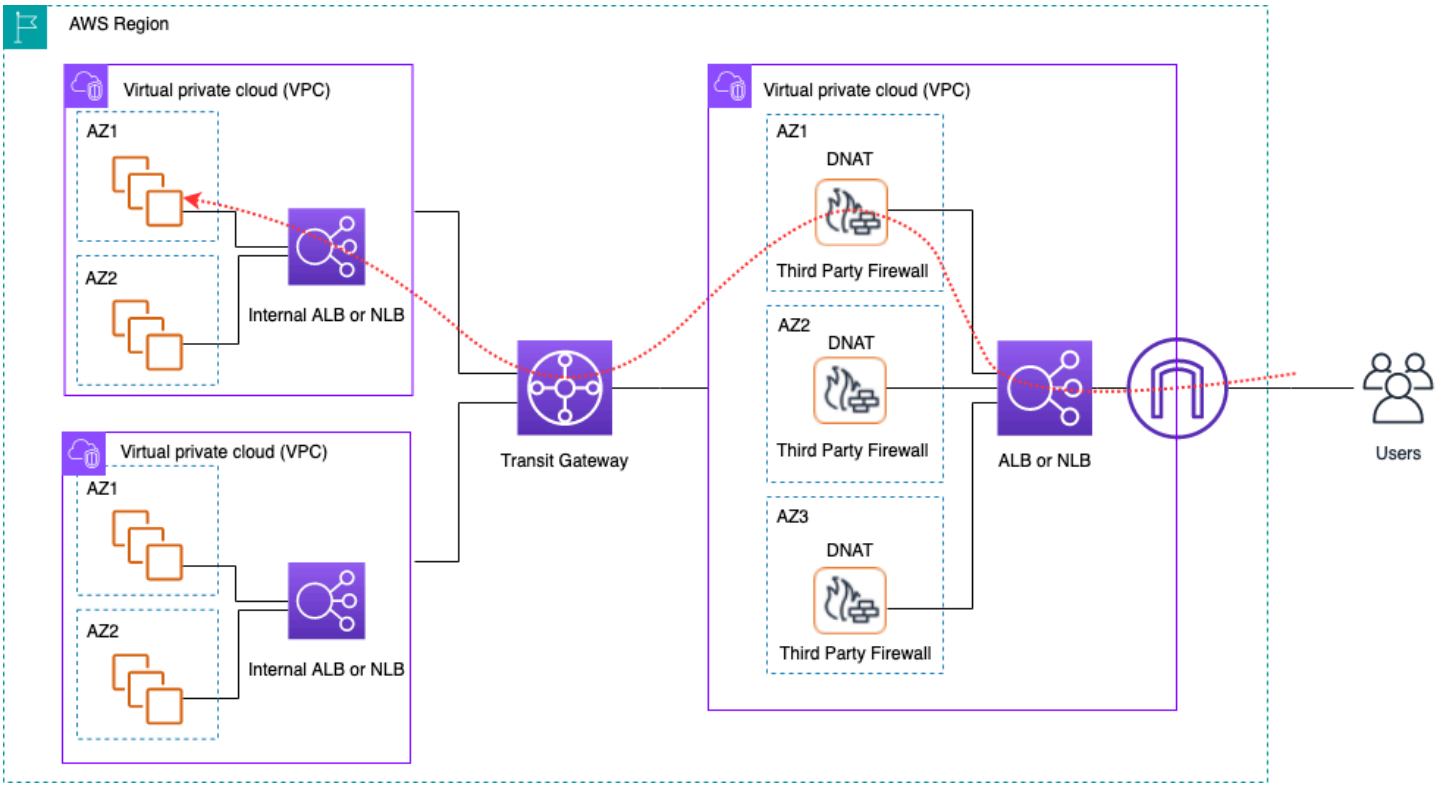
Pertimbangan utama

- Arsitektur ini paling cocok untuk inspeksi header HTTP dan inspeksi terdistribusi, karena AWS WAF terintegrasi pada per-ALB, distribusi dan CloudFront API Gateway. AWS WAF tidak mencatat badan permintaan.
- Lalu lintas ke set kedua ALB (jika ada) mungkin tidak diperiksa oleh AWS WAF contoh yang sama; karena permintaan baru akan dibuat ke set kedua ALB.

Inspeksi masuk terpusat dengan peralatan pihak ketiga

Dalam pola desain arsitektur ini, Anda menggunakan peralatan firewall pihak ketiga di Amazon EC2 di beberapa zona ketersediaan di belakang Elastic Load Balancer (ELB) seperti Aplikasi/ Penyeimbang Beban Jaringan dalam VPC Inspeksi terpisah.

VPC Inspeksi bersama dengan VPC Spoke lainnya terhubung bersama melalui Transit Gateway sebagai lampiran VPC. Aplikasi di Spoke VPC adalah frontend oleh ELB internal yang dapat berupa ALB atau NLB tergantung pada jenis aplikasi. Klien melalui internet terhubung ke DNS ELB eksternal di VPC inspeksi yang mengarahkan lalu lintas ke salah satu peralatan Firewall. Firewall memeriksa lalu lintas dan kemudian mengarahkan lalu lintas ke Spoke VPC melalui Transit Gateway menggunakan DNS ELB internal seperti yang ditunjukkan pada gambar berikut. Untuk informasi selengkapnya mengenai inspeksi keamanan masuk dengan peralatan pihak ketiga, lihat Cara mengintegrasikan peralatan firewall pihak ketiga ke dalam postingan blog lingkungan AWS.



Inspeksi lalu lintas masuk terpusat menggunakan peralatan pihak ketiga dan ELB

Keuntungan

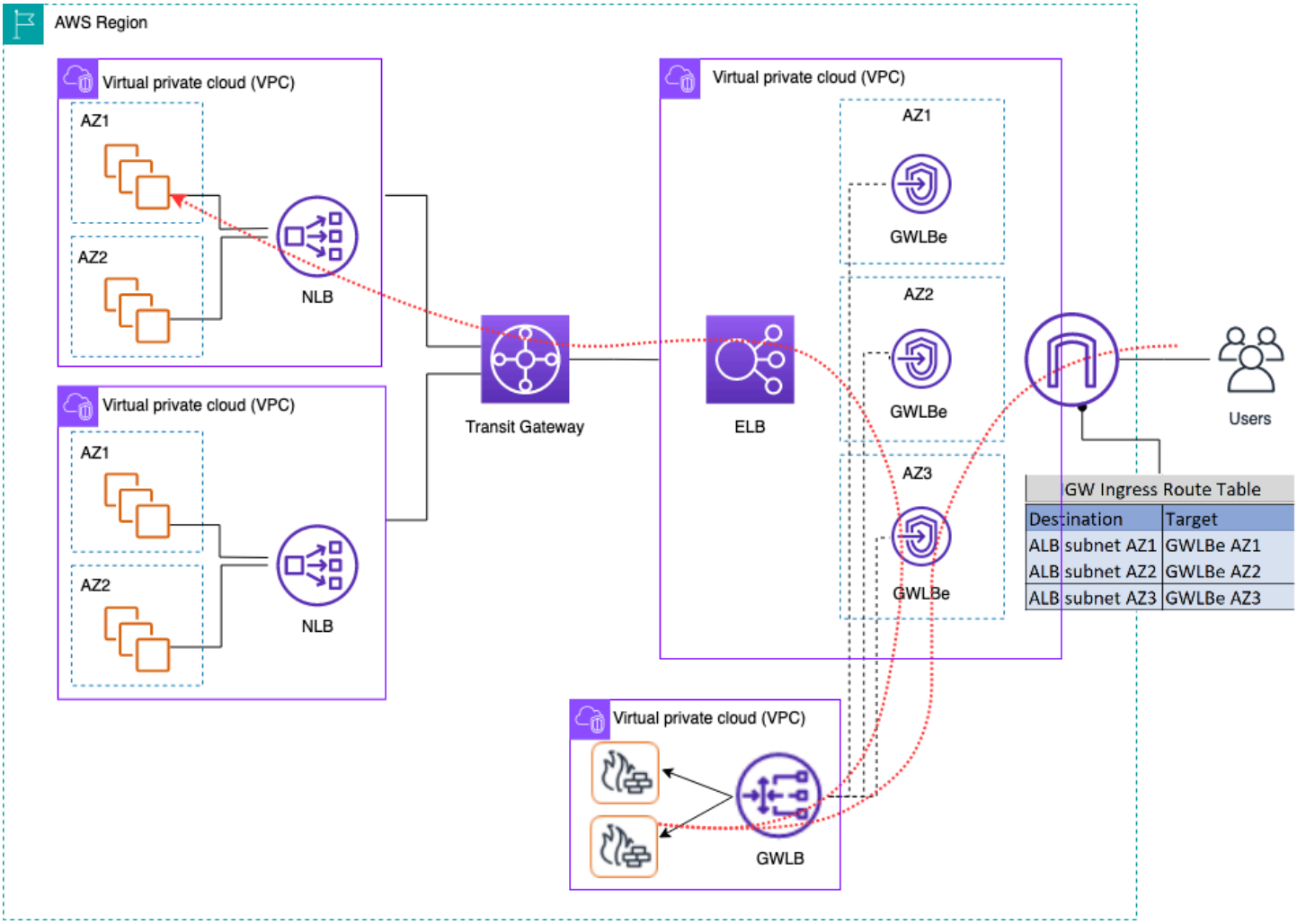
- Arsitektur ini dapat mendukung semua jenis aplikasi untuk inspeksi dan kemampuan inspeksi lanjutan yang ditawarkan melalui peralatan firewall pihak ketiga.
- Pola ini mendukung perutean berbasis DNS dari peralatan firewall ke VPC spoke, yang memungkinkan aplikasi di Spoke VPC untuk menskalakan secara independen di belakang ELB.
- Anda dapat menggunakan Auto Scaling dengan ELB untuk menskalakan peralatan firewall di VPC Inspeksi.

Pertimbangan utama

- Anda perlu menerapkan beberapa peralatan firewall di seluruh Availability Zone untuk ketersediaan tinggi.
- Firewall perlu dikonfigurasi dengan dan melakukan Source NAT untuk mempertahankan simetri aliran, yang berarti alamat IP klien tidak akan terlihat oleh aplikasi.
- Pertimbangkan untuk menggunakan Transit Gateway dan Inspeksi VPC di akun Layanan Jaringan.
- Biaya lisensi/dukungan firewall vendor pihak ketiga tambahan. Biaya Amazon EC2 tergantung pada jenis instans.

Memeriksa lalu lintas masuk dari internet menggunakan peralatan firewall dengan Gateway Load Balancer

Pelanggan menggunakan firewall generasi berikutnya (NGFW) dan sistem pencegahan intrusi (IPS) pihak ketiga sebagai bagian dari strategi pertahanan mereka secara mendalam. Secara tradisional ini sering merupakan perangkat keras atau perangkat lunak/peralatan virtual khusus. Anda dapat menggunakan Load Balancer Gateway untuk menskalakan peralatan virtual ini secara horizontal untuk memeriksa lalu lintas dari dan ke VPC Anda, seperti yang ditunjukkan pada gambar berikut.



Inspeksi lalu lintas masuk terpusat menggunakan peralatan firewall dengan Gateway Load Balancer

Dalam arsitektur sebelumnya, titik akhir Load Balancer Gateway diterapkan ke setiap Availability Zone dalam VPC edge yang terpisah. Firewall generasi berikutnya, sistem pencegahan intrusi, dll. Digunakan di belakang Load Balancer Gateway di VPC alat terpusat. VPC alat ini dapat berada di akun AWS yang sama dengan VPC spoke atau akun AWS yang berbeda. Peralatan virtual dapat dikonfigurasi untuk menggunakan grup Auto Scaling dan terdaftar secara otomatis dengan Load Balancer Gateway, memungkinkan penskalaan otomatis lapisan keamanan.

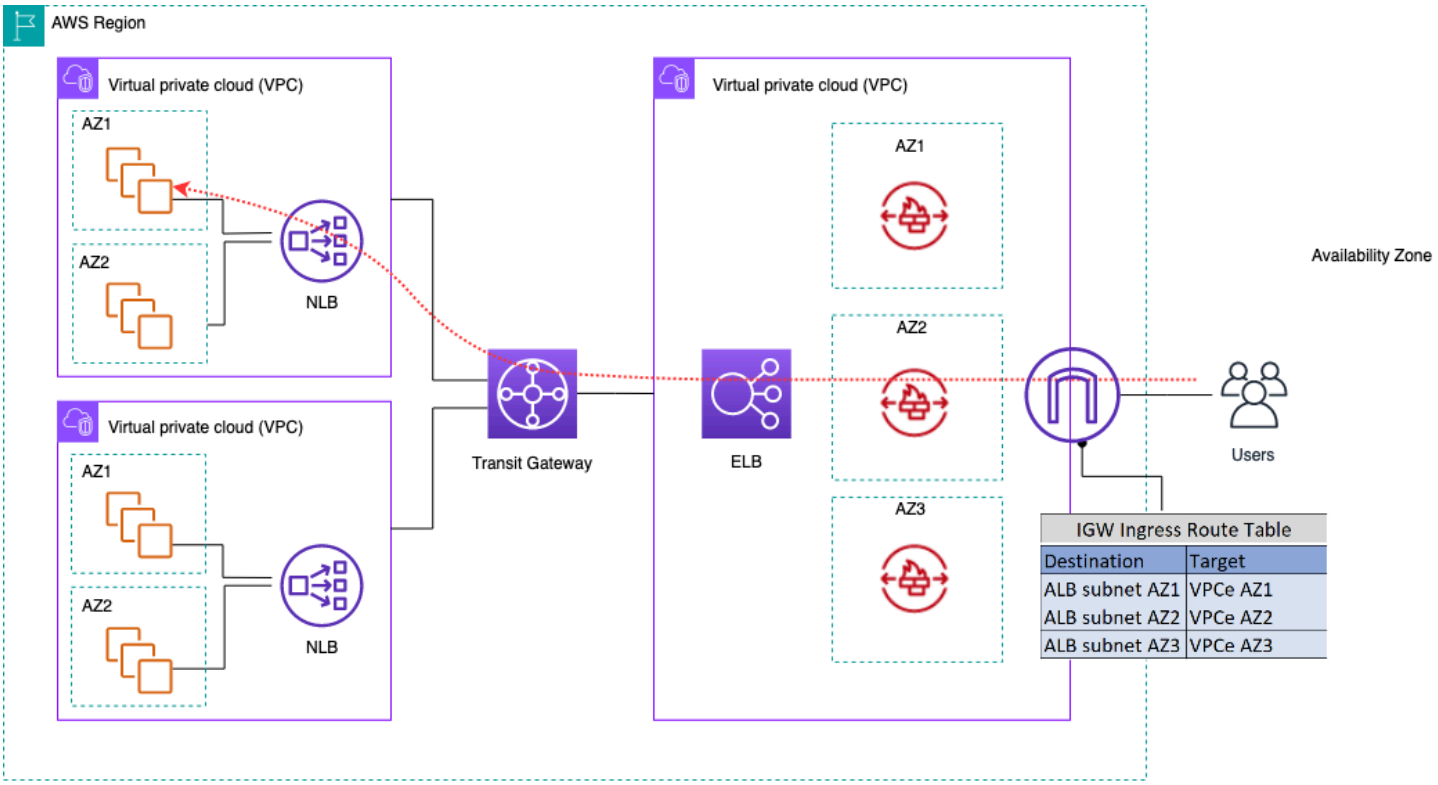
Peralatan virtual ini dapat dikelola dengan mengakses antarmuka manajemen mereka melalui Internet Gateway (IGW) atau menggunakan pengaturan host benteng di VPC alat.

Menggunakan fitur perutean masuk VPC, tabel rute tepi diperbarui untuk merutekan lalu lintas masuk dari internet ke peralatan firewall di belakang Gateway Load Balancer. Lalu lintas yang diperiksa dirutekan melalui titik akhir Load Balancer Gateway untuk menargetkan instance VPC. Lihat posting

blog Introducing AWS Gateway Load Balancer: Pola arsitektur yang didukung untuk detail tentang berbagai cara menggunakan Load Balancer Gateway.

Menggunakan AWS Network Firewall untuk masuknya terpusat

Dalam arsitektur ini, lalu lintas masuk diperiksa oleh AWS Network Firewall sebelum mencapai sisa VPC. Dalam pengaturan ini, lalu lintas dibagi di antara semua titik akhir firewall yang digunakan di VPC Edge. Anda menerapkan subnet publik antara titik akhir firewall dan subnet Transit Gateway. Anda dapat menggunakan ALB atau NLB, yang berisi target IP di VPC spoke Anda saat menangani Auto Scaling untuk target di belakangnya.

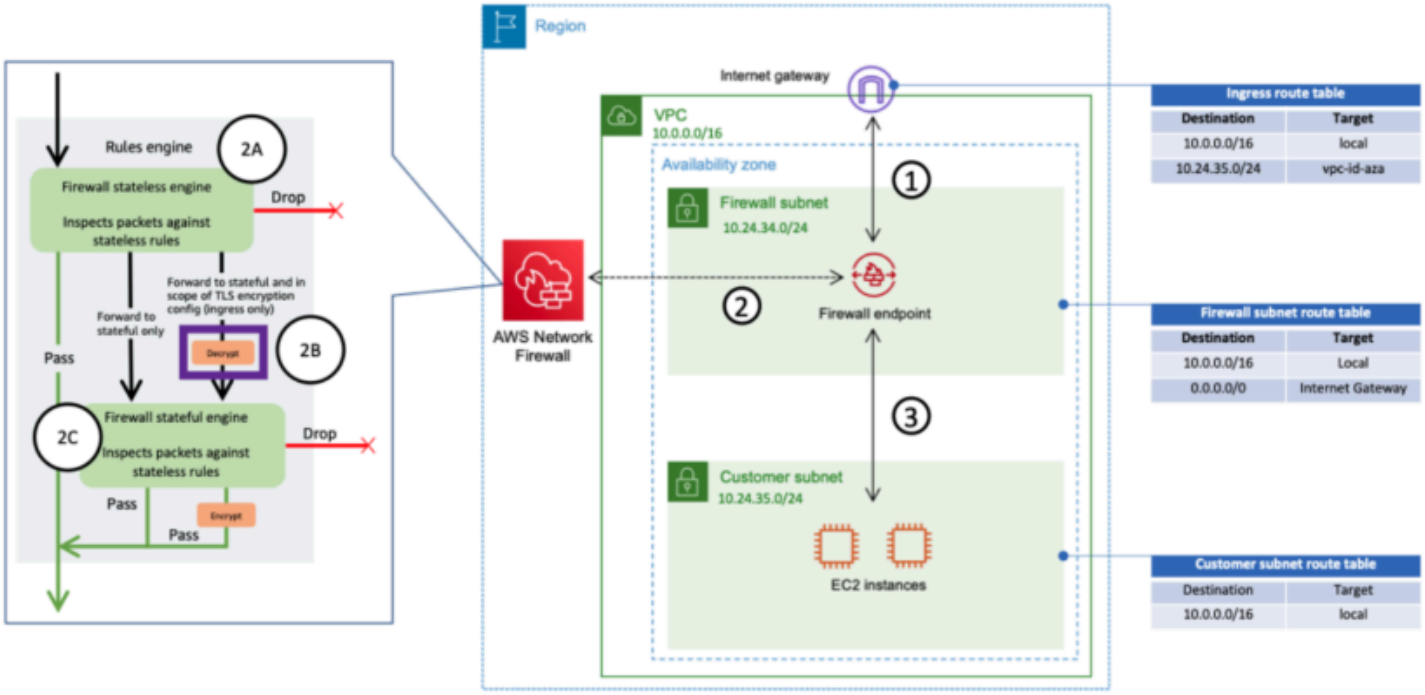


Inspeksi lalu lintas masuk menggunakan AWS Network Firewall

Untuk menyederhanakan penyebaran dan manajemen AWS Network Firewall dalam model ini, AWS Firewall Manager dapat digunakan. Firewall Manager memungkinkan Anda mengelola firewall yang berbeda secara terpusat dengan secara otomatis menerapkan perlindungan yang Anda buat di lokasi terpusat ke beberapa akun. Firewall Manager mendukung model penyebaran terdistribusi dan terpusat untuk Network Firewall. Posting blog Cara menyebarkan AWS Network Firewall dengan menggunakan AWS Firewall Manager memberikan rincian lebih lanjut tentang model.

Inspeksi Paket Dalam (DPI) dengan AWS Network Firewall

Network Firewall dapat melakukan inspeksi paket mendalam (DPI) pada lalu lintas masuk. Menggunakan sertifikat Transport Layer Security (TLS) yang disimpan di AWS Certificate Manager (ACM), Network Firewall dapat mendekripsi paket, melakukan DPI, dan mengenkripsi ulang paket. Ada beberapa pertimbangan untuk menyiapkan DPI dengan ANetwork Firewall. Pertama, sertifikat TLS tepercaya harus disimpan di ACM. Kedua, aturan Network Firewall harus dikonfigurasi untuk mengirim paket dengan benar untuk dekripsi dan enkripsi ulang. Lihat posting blog konfigurasi inspeksi TLS untuk lalu lintas terenkripsi dan AWS Network Firewall untuk lebih jelasnya.



Inspeksi lalu lintas masuk menggunakan Network Firewall dengan DPI

Pertimbangan utama untuk arsitektur AWS Network Firewall ingress terpusat

- Elastic Load Balancing di Edge VPC hanya dapat memiliki alamat IP sebagai tipe target, bukan nama host. Pada gambar sebelumnya, targetnya adalah IP pribadi Network Load Balancer di VPC spoke. Menggunakan target IP di belakang ELB di tepi VPC mengakibatkan hilangnya Auto Scaling.
- Pertimbangkan untuk menggunakan AWS Firewall Manager sebagai satu panel kaca untuk titik akhir firewall Anda.

- Model penyebaran ini menggunakan inspeksi lalu lintas tepat saat memasuki VPC edge, sehingga berpotensi mengurangi biaya keseluruhan arsitektur inspeksi Anda.

DNS

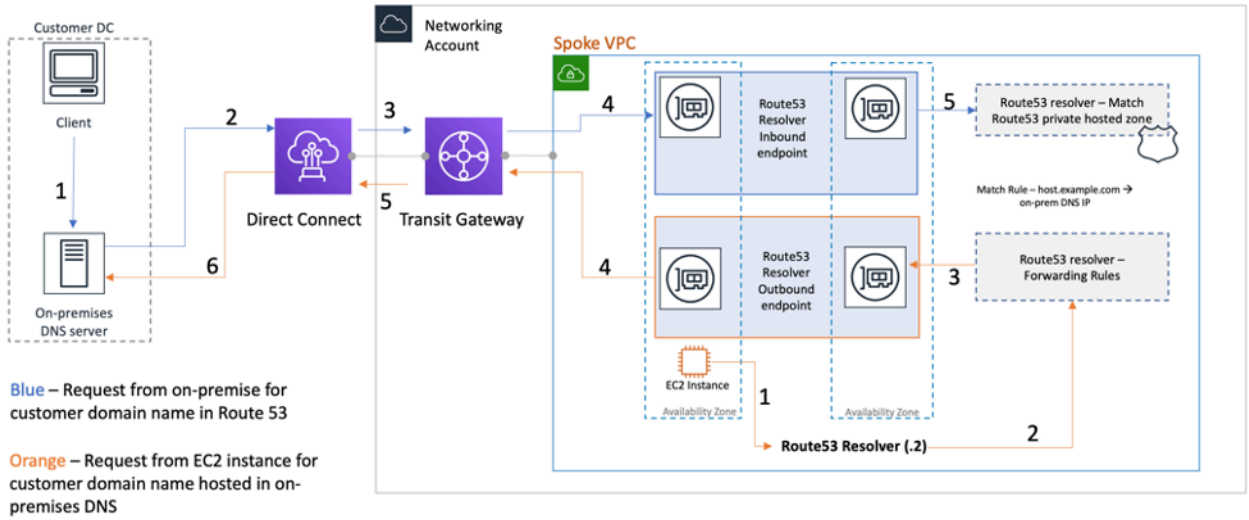
Saat Anda meluncurkan instance ke VPC, tidak termasuk VPC default, AWS menyediakan instance dengan nama host DNS pribadi (dan berpotensi nama host DNS publik) tergantung pada atribut DNS yang Anda tentukan untuk VPC dan jika instance Anda memiliki alamat IPv4 publik. Ketika `enableDnsSupport` atribut diatur `ketrue`, Anda mendapatkan resolusi DNS dalam VPC dari Route 53 Resolver (+2 IP offset ke VPC CIDR). Secara default, Route 53 Resolver menjawab kueri DNS untuk nama domain VPC seperti nama domain untuk instans EC2 atau penyeimbang beban Elastic Load Balancing. Dengan VPC peering, host dalam satu VPC dapat menyelesaikan nama host DNS publik ke alamat IP pribadi untuk instance di VPC peered, asalkan opsi untuk melakukannya diaktifkan. Hal yang sama berlaku untuk VPC yang terhubung melalui AWS Transit Gateway. Untuk informasi selengkapnya, lihat Mengaktifkan Dukungan Resolusi DNS untuk Koneksi Peering VPC.

Jika ingin memetakan instans ke nama domain khusus, Anda dapat menggunakan Amazon Route 53 untuk membuat catatan pemetaan DNS-ke-IP kustom. Zona yang dihosting Amazon Route 53 adalah wadah yang menyimpan informasi tentang bagaimana Anda ingin Amazon Route 53 merespons kueri DNS untuk domain dan subdomainnya. Public Hosted Zones berisi informasi DNS yang dapat diselesaikan melalui internet publik sementara Private Hosted Zones adalah implementasi khusus yang hanya menyajikan informasi ke VPC yang telah dilampirkan ke zona host pribadi tertentu. Dalam pengaturan Zona Pendaratan di mana Anda memiliki beberapa VPC atau akun, Anda dapat mengaitkan satu zona host pribadi dengan beberapa VPC di seluruh akun AWS dan di seluruh Wilayah (hanya dapat dilakukan dengan SDK/CLI/API). Host akhir di VPC menggunakan IP Resolver Route 53 masing-masing (+2 mengimbangi VPC CIDR) sebagai server nama untuk kueri DNS. Resolver Route 53 di VPC hanya menerima kueri DNS dari sumber daya dalam VPC.

DNS Hibrida

DNS adalah komponen penting dari infrastruktur apa pun, hybrid atau lainnya, karena menyediakan resolusi Hostname-to-IP-address yang diandalkan aplikasi. Pelanggan yang menerapkan lingkungan hybrid biasanya memiliki sistem resolusi DNS yang sudah ada, dan mereka menginginkan solusi DNS yang bekerja bersama-sama dengan sistem mereka saat ini. Native Route 53 resolver (+2 set dari VPC CIDR dasar) tidak dapat dijangkau dari jaringan lokal menggunakan VPN atau. AWS Direct Connect Oleh karena itu, ketika Anda mengintegrasikan DNS untuk VPC di Wilayah AWS dengan DNS untuk jaringan Anda, Anda memerlukan titik akhir masuk Route 53 Resolver (untuk kueri DNS yang diteruskan ke VPC) dan titik akhir keluar Route 53 Resolver (untuk kueri yang Anda teruskan dari VPC ke jaringan Anda).

Seperti yang ditunjukkan pada gambar berikut, Anda dapat mengonfigurasi titik akhir Resolver keluar untuk meneruskan kueri yang diterimanya dari instans Amazon EC2 di VPC ke server DNS di jaringan Anda. Untuk meneruskan kueri yang dipilih, dari VPC ke jaringan lokal, buat aturan Resolver Route 53 yang menentukan nama domain untuk kueri DNS yang ingin diteruskan (seperti example.com), dan alamat IP resolver DNS di jaringan tempat Anda ingin meneruskan kueri. Untuk kueri masuk dari jaringan lokal ke zona host Route 53, server DNS di jaringan Anda dapat meneruskan kueri ke titik akhir Resolver masuk dalam VPC tertentu.



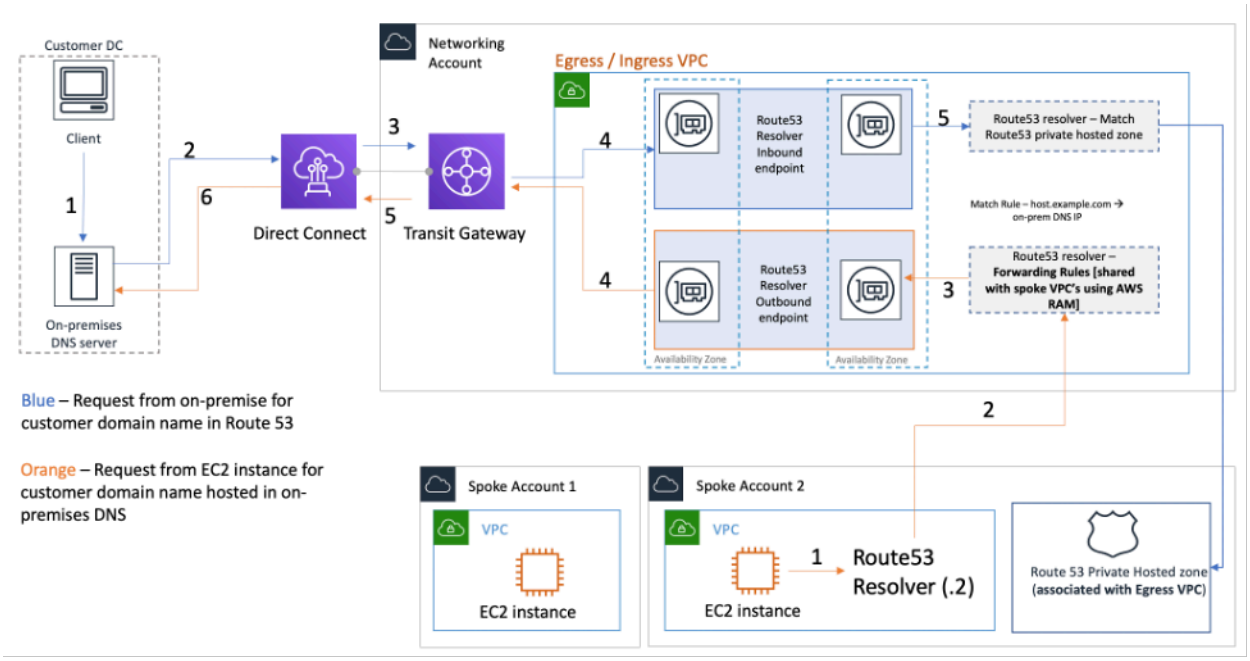
Resolusi DNS Hybrid menggunakan Resolver Route 53

Hal ini memungkinkan resolver DNS lokal Anda untuk dengan mudah menyelesaikan nama domain untuk sumber daya AWS, seperti instans atau catatan Amazon EC2 di zona host pribadi Route 53 yang terkait dengan VPC tersebut. Selain itu, titik akhir Route 53 Resolver dapat menangani hingga sekitar 10.000 kueri per detik per ENI, sehingga dapat menskalakan ke volume kueri DNS yang jauh lebih besar dengan mudah. Lihat Praktik terbaik untuk Resolver di dokumentasi Amazon Route 53 untuk detail selengkapnya.

Anda tidak disarankan untuk membuat titik akhir Route 53 Resolver di setiap VPC Zona Pendaratan. Pusatkan mereka di VPC jalan keluar pusat (di akun layanan Jaringan). Pendekatan ini memungkinkan pengelolaan yang lebih baik sambil menjaga biaya tetap rendah (Anda dikenakan biaya per jam untuk setiap titik akhir resolver inbound/outbound yang Anda buat). Anda berbagi titik akhir masuk dan keluar terpusat dengan sisa Zona Pendaratan.

- Resolusi keluar — Gunakan akun Layanan Jaringan untuk menulis aturan resolver (berdasarkan kueri DNS mana yang akan diteruskan ke server DNS lokal). Menggunakan Resource Access Manager (RAM), bagikan aturan Resolver Route 53 ini dengan beberapa akun (dan kaitkan dengan VPC di akun). Instans EC2 dalam VPC spoke dapat mengirim kueri DNS ke Route 53

Resolver dan Route 53 Resolver Service akan meneruskan kueri ini ke server DNS lokal melalui titik akhir Route 53 Resolver keluar di VPC jalan keluar. Anda tidak perlu mengintip VPC spoke ke VPC jalan keluar, atau menghubungkannya melalui Transit Gateway. Jangan gunakan IP titik akhir resolver keluar sebagai DNS utama di VPC spoke. Spoke VPC harus menggunakan Route 53 Resolver (untuk mengimbangi VPC CIDR) di VPC mereka.



Memusatkan titik akhir Rute 53 Resolver di VPC masuk/keluar

- Resolusi DNS masuk — Buat titik akhir masuk Resolver Route 53 di VPC terpusat dan kaitkan semua zona host pribadi di Zona Pendaratan Anda dengan VPC terpusat ini. Untuk informasi selengkapnya, lihat Mengaitkan Lebih Banyak VPC dengan Zona Hosting Pribadi. Beberapa Zona Dihosting Pribadi (PHZ) yang terkait dengan VPC tidak dapat tumpang tindih. Seperti yang ditunjukkan pada gambar sebelumnya, asosiasi PHZ dengan VPC terpusat ini akan memungkinkan server lokal menyelesaikan DNS untuk entri apa pun di zona host pribadi apa pun (terkait dengan VPC pusat) menggunakan titik akhir masuk di VPC terpusat. Untuk informasi lebih lanjut tentang pengaturan DNS hybrid, lihat Manajemen DNS terpusat dari cloud hybrid dengan Amazon Route 53 dan AWS Transit Gateway dan Opsi DNS Cloud Hybrid untuk Amazon VPC.

Route 53 DNS Firewall

Amazon Route 53 Resolver DNS Firewall membantu memfilter dan mengatur lalu lintas DNS keluar untuk VPC Anda. Penggunaan utama DNS Firewall adalah untuk membantu mencegah eksfiltrasi data data Anda dengan menentukan daftar izin nama domain yang memungkinkan sumber daya di VPC Anda untuk membuat permintaan DNS keluar hanya untuk situs yang dipercaya organisasi Anda. Ini juga memberi pelanggan kemampuan untuk membuat daftar blokir untuk domain yang tidak mereka inginkan sumber daya di dalam VPC untuk berkomunikasi melalui DNS. Amazon Route 53 Resolver Firewall DNS memiliki beberapa fitur berikut:

Pelanggan dapat membuat aturan untuk menentukan bagaimana kueri DNS dijawab. Tindakan yang dapat didefinisikan untuk nama domain meliputi`NODATA`, `OVERRIDE` dan`NXDOMAIN`.

Pelanggan dapat membuat peringatan untuk daftar izin dan daftar penolakan untuk memantau aktivitas aturan. Ini bisa berguna ketika pelanggan ingin menguji aturan sebelum memindahkannya ke produksi.

Untuk informasi lebih lanjut, lihat posting blog Cara Memulai dengan Amazon Route 53 Resolver DNS Firewall untuk Amazon VPC.

Akses terpusat ke titik akhir VPC pribadi

VPCEndpoint memungkinkan Anda untuk menghubungkan secara pribadi VPC ke AWS layanan yang didukung tanpa memerlukan gateway internet atau NAT perangkat, VPN koneksi, atau AWS Direct Connect koneksi. Karena itu, Anda VPC tidak terpapar internet publik. Instans di Anda VPC tidak memerlukan alamat IP publik untuk berkomunikasi dengan titik akhir AWS layanan dengan titik akhir antarmuka ini. Lalu lintas antara layanan Anda VPC dan layanan lainnya tidak meninggalkan tulang punggung AWS jaringan. VPCEndpoint adalah perangkat virtual. Mereka adalah komponen yang diskalakan secara horizontal, berlebihan, dan sangat tersedia. VPC Dua jenis titik akhir saat ini dapat disediakan: titik akhir antarmuka (didukung oleh AWS PrivateLink) dan titik akhir gateway. Titik akhir Gateway dapat digunakan untuk mengakses layanan Amazon S3 dan Amazon DynamoDB secara pribadi. Tidak dikenakan biaya tambahan untuk menggunakan titik akhir gateway. Biaya standar untuk transfer data dan penggunaan sumber daya berlaku.

Titik VPC akhir antarmuka

Endpoint antarmuka terdiri dari satu atau lebih antarmuka jaringan elastis dengan alamat IP pribadi yang berfungsi sebagai titik masuk untuk lalu lintas yang ditujukan ke layanan yang didukung. AWS Saat Anda menyediakan titik akhir antarmuka, biaya dikeluarkan untuk setiap jam titik akhir berjalan bersama dengan biaya pemrosesan data. Secara default, Anda membuat titik akhir antarmuka di setiap VPC tempat Anda ingin mengakses AWS layanan. Ini bisa menjadi penghalang biaya dan menantang untuk dikelola dalam pengaturan Zona Pendaratan di mana pelanggan ingin berinteraksi dengan AWS layanan tertentu di beberapa. VPCs Untuk menghindari hal ini, Anda dapat meng-host titik akhir antarmuka secara terpusatVPC. Semua spoke VPCs akan menggunakan titik akhir terpusat ini melalui Transit Gateway.

Saat Anda membuat VPC titik akhir ke AWS layanan, Anda dapat mengaktifkan privateDNS. Saat diaktifkan, pengaturan akan membuat zona host pribadi Route 53 AWS terkelola (PHZ), yang memungkinkan resolusi titik akhir AWS layanan publik ke IP pribadi titik akhir antarmuka. Yang dikelola PHZ hanya berfungsi di dalam VPC dengan titik akhir antarmuka. Dalam pengaturan kami, ketika kami ingin berbicara VPCs untuk dapat menyelesaikan VPC titik akhir yang DNS dihosting di terpusatVPC, yang dikelola tidak PHZ akan berfungsi. Untuk mengatasinya, nonaktifkan opsi yang secara otomatis membuat pribadi DNS saat titik akhir antarmuka dibuat. Selanjutnya, buat zona host pribadi Route 53 secara manual yang cocok dengan nama titik akhir layanan dan tambahkan catatan Alias dengan nama Layanan AWS titik akhir lengkap yang menunjuk ke titik akhir antarmuka.

1. Masuk ke AWS Management Console dan navigasikan ke Route 53.

2. Pilih zona yang dihosting pribadi dan arahkan ke Buat Rekaman.
3. Isi bidang Record Name, pilih Record Type as A, dan aktifkan Alias.

   Perhatikan bahwa beberapa layanan, seperti Docker dan titik akhir OCI klien (**`dkr.ecr`**), memerlukan alias wildcard (**`*`**) digunakan untuk Nama Rekam.
4. Di bawah Rute Lalu Lintas ke bagian, pilih layanan yang harus dikirim lalu lintas dan pilih wilayah dari daftar dropdown.
5. Pilih kebijakan perutean yang sesuai dan aktifkan opsi untuk Mengevaluasi kesehatan target.

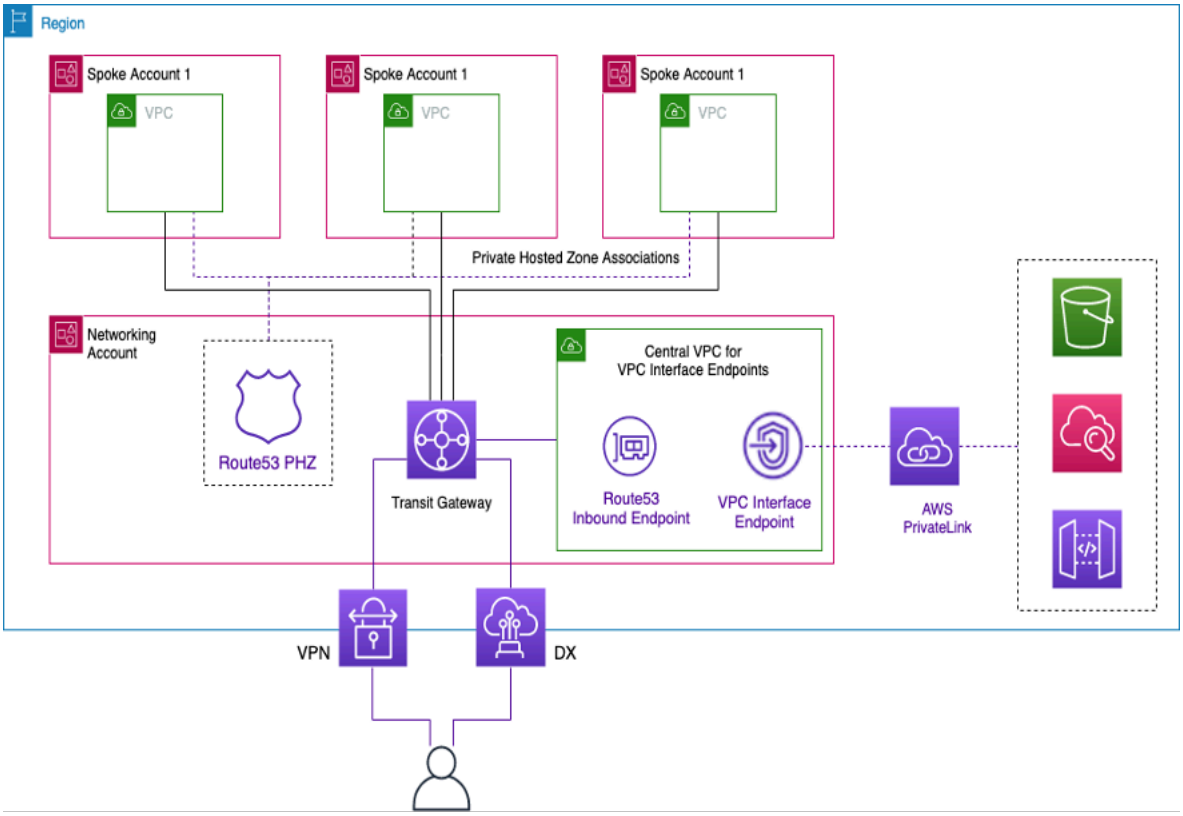
Anda mengaitkan zona host pribadi ini dengan yang lain VPCs di dalam Zona Pendaratan. Konfigurasi ini memungkinkan spoke VPCs untuk menyelesaikan nama titik akhir layanan lengkap ke titik akhir antarmuka di pusat. VPC

> **Note**
>
> Untuk mengakses zona host pribadi bersama, host di spoke VPCs harus menggunakan IP Resolver Route 53 dari mereka. VPC Endpoint antarmuka juga dapat diakses dari jaringan lokal melalui VPN dan Direct Connect. Gunakan aturan penerusan bersyarat untuk mengirim semua DNS lalu lintas untuk nama titik akhir layanan lengkap ke titik akhir masuk Route 53 Resolver, yang akan menyelesaikan permintaan sesuai dengan zona host pribadi. DNS

Pada gambar berikut, Transit Gateway memungkinkan arus lalu lintas dari spoke VPCs ke titik akhir antarmuka terpusat. Buat VPC Endpoint dan zona host pribadi untuknya di Akun Layanan Jaringan dan bagikan dengan spoke VPCs di akun spoke. Untuk detail selengkapnya tentang berbagi informasi titik akhir dengan orang lainVPCs, lihat posting blog Integrating AWS Transit Gateway with dan AWS PrivateLink Amazon Route 53 Resolver.

> **Note**
>
> Pendekatan VPC titik akhir terdistribusi yaitu, titik akhir per VPC memungkinkan Anda menerapkan kebijakan hak istimewa paling sedikit pada titik akhir. VPC Dalam pendekatan terpusat, Anda akan menerapkan dan mengelola kebijakan untuk semua VPC akses bicara pada satu titik akhir. Dengan meningkatnya jumlahVPCs, kompleksitas mempertahankan hak istimewa paling sedikit dengan satu dokumen kebijakan dapat tumbuh. Dokumen kebijakan

tunggal juga menghasilkan radius ledakan yang lebih besar. Anda juga dibatasi pada ukuran dokumen kebijakan (20.480 karakter).



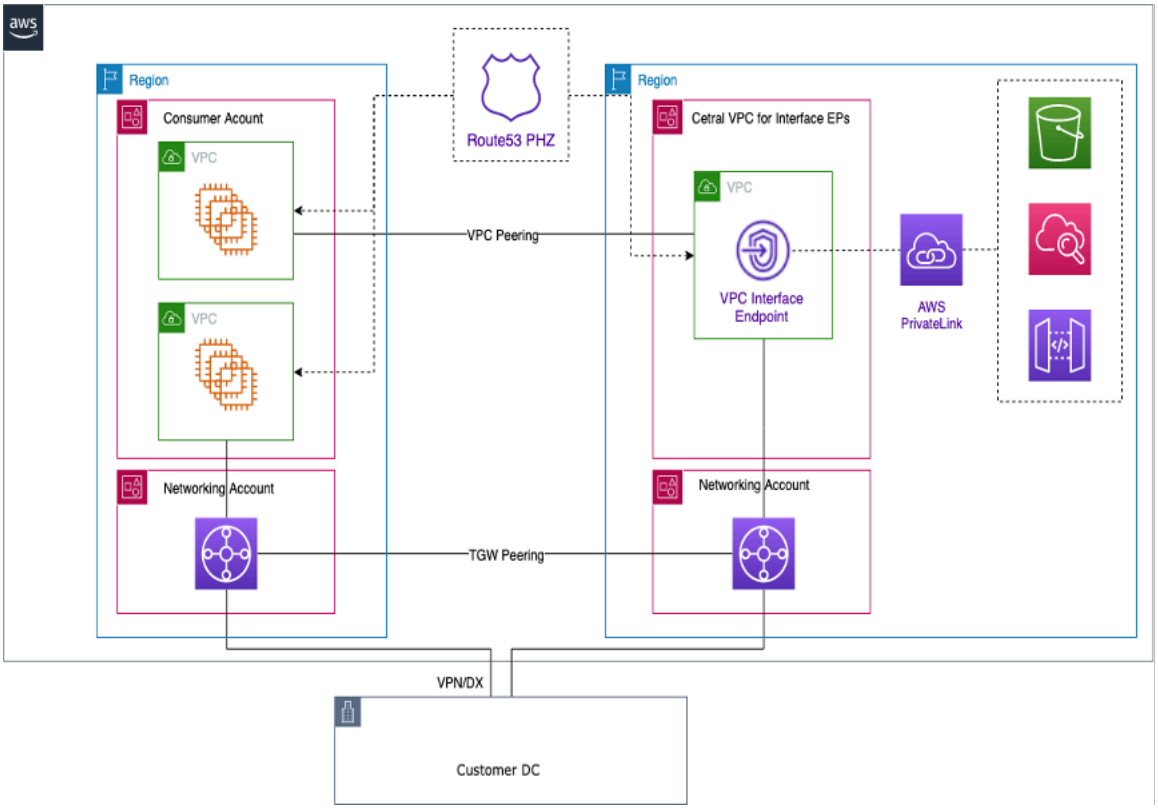
Memusatkan titik akhir antarmuka VPC

Akses titik akhir Lintas Wilayah

Bila Anda ingin beberapa VPCs pengaturan di Wilayah berbeda yang berbagi VPC titik akhir yang sama, gunakanPHZ, seperti yang diuraikan sebelumnya. Keduanya VPCs di setiap Wilayah akan dikaitkan dengan PHZ dengan alias ke titik akhir. Untuk merutekan lalu lintas antara VPCs arsitektur Multi-wilayah, Gerbang Transit di setiap Wilayah perlu diintip bersama. Untuk informasi lebih lanjut, lihat blog ini: Menggunakan Route 53 Private Hosted Zones for Cross-account Multi-Region Architectures.

VPCsdari daerah yang berbeda dapat dialihkan ke satu sama lain menggunakan Transit Gateways atau Peering. VPC Gunakan dokumentasi berikut untuk mengintip Transit Gateways: Transit gateway peering attachment.

Dalam contoh ini, EC2 instans Amazon di VPC `us-west-1` Wilayah akan menggunakan PHZ untuk mendapatkan alamat IP pribadi dari titik akhir di `us-west-2` Wilayah dan mengarahkan lalu lintas ke `us-west-2` Wilayah VPC melalui mengintip atau VPC mengintip Gateway Transit. Dengan menggunakan arsitektur ini, lalu lintas tetap berada dalam AWS jaringan, dengan aman memungkinkan EC2 instance masuk `us-west-1` untuk mengakses VPC layanan `us-west-2` tanpa melalui internet.



Titik akhir Multi-Wilayah VPC

> **Note**
>
> Biaya transfer data Antar Wilayah berlaku saat mengakses titik akhir di seluruh Wilayah.

Mengacu pada gambar sebelumnya, layanan endpoint dibuat di a VPC in the `us-west-2` Region. Layanan endpoint ini menyediakan akses ke AWS layanan di Wilayah tersebut. Agar instans Anda di Wilayah lain (sepertius-east-1) mengakses titik akhir di `us-west-2` Wilayah, Anda perlu membuat catatan alamat PHZ dengan alias ke titik akhir yang diinginkan. VPC

Pertama, pastikan bahwa VPCs di setiap Wilayah dikaitkan dengan PHZ yang Anda buat.

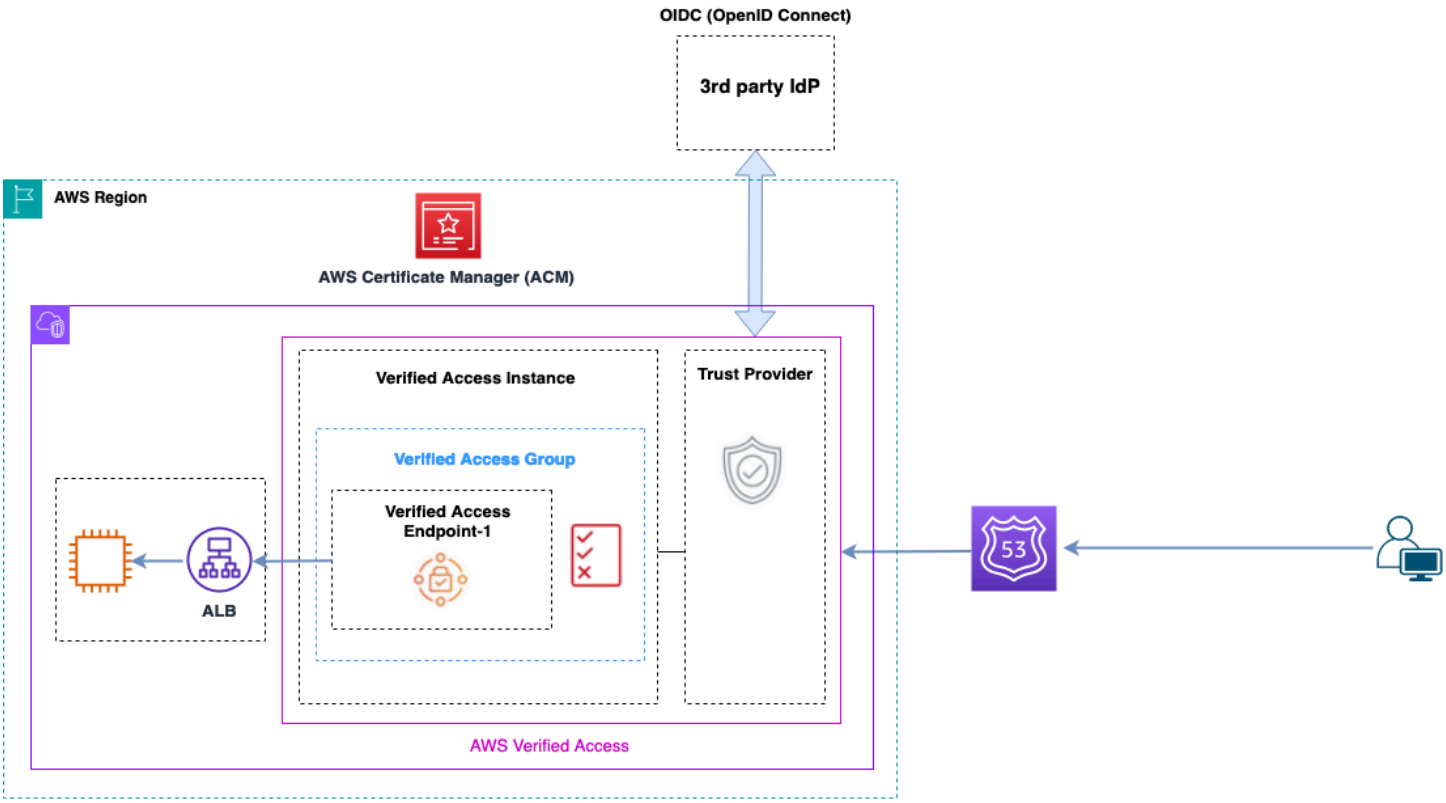
Saat menerapkan titik akhir di beberapa Availability Zone, alamat IP titik akhir yang dikembalikan dari DNS akan berasal dari salah satu subnet di Availability Zone yang dialokasikan.

Saat memanggil titik akhir, gunakan nama domain yang sepenuhnya memenuhi syarat (FQDN) yang ada di. PHZ

Akses Terverifikasi AWS

Akses Terverifikasi AWS memberikan akses aman ke aplikasi di jaringan pribadi tanpa file. VPN Ini mengevaluasi permintaan secara real time seperti identitas, perangkat, dan lokasi. Layanan ini memberikan akses berdasarkan kebijakan untuk aplikasi dan menghubungkan pengguna dengan meningkatkan keamanan organisasi. Akses Terverifikasi menyediakan akses ke aplikasi pribadi dengan bertindak sebagai proxy terbalik yang sadar identitas. Identitas pengguna dan kesehatan perangkat, jika berlaku, dilakukan sebelum merutekan lalu lintas ke aplikasi.

Diagram berikut memberikan ikhtisar tingkat tinggi Akses Terverifikasi. Pengguna mengirim permintaan untuk mengakses aplikasi. Akses Terverifikasi mengevaluasi permintaan terhadap kebijakan akses untuk grup dan kebijakan titik akhir khusus aplikasi apa pun. Jika akses diizinkan, permintaan dikirim ke aplikasi melalui titik akhir.



Ikhtisar Akses Terverifikasi

Komponen utama dalam Akses Terverifikasi AWS arsitektur adalah:

- Instans Akses Terverifikasi — Instance mengevaluasi permintaan aplikasi dan memberikan akses hanya jika persyaratan keamanan Anda terpenuhi.
- Titik akhir Akses Terverifikasi - Setiap titik akhir mewakili aplikasi. Endpoint dapat berupaNLB, ALB atau antarmuka jaringan.
- Grup Akses Terverifikasi — Kumpulan titik akhir Akses Terverifikasi. Kami menyarankan Anda mengelompokkan titik akhir untuk aplikasi dengan persyaratan keamanan serupa untuk menyederhanakan administrasi kebijakan.
- Kebijakan akses — Seperangkat aturan yang ditentukan pengguna yang menentukan apakah akan mengizinkan atau menolak akses ke aplikasi.
- Penyedia kepercayaan — Akses Terverifikasi adalah layanan yang memfasilitasi pengelolaan identitas pengguna dan status keamanan perangkat. Ini kompatibel dengan keduanya AWS dan penyedia kepercayaan pihak ketiga, yang mengharuskan setidaknya satu penyedia kepercayaan dilampirkan ke setiap instance Akses Terverifikasi. Masing-masing contoh ini dapat mencakup penyedia kepercayaan identitas tunggal serta beberapa penyedia kepercayaan perangkat.
- Data kepercayaan — Data keamanan yang dikirim oleh penyedia kepercayaan Anda ke Akses Terverifikasi, seperti alamat email pengguna atau grup tempat mereka berada, dievaluasi berdasarkan kebijakan akses Anda setiap kali permintaan aplikasi diterima.

Rincian lebih lanjut dapat ditemukan di posting blog Akses Terverifikasi.

Kesimpulan

Saat Anda menskalakan penggunaan AWS dan penerapan aplikasi di Zona AWS Pendaratan, jumlah VPC dan komponen jaringan meningkat. Whitepaper ini menjelaskan bagaimana Anda dapat mengelola infrastruktur yang berkembang ini memastikan skalabilitas, ketersediaan tinggi, dan keamanan sambil menjaga biaya tetap rendah. Membuat keputusan desain yang tepat saat menggunakan layanan seperti Transit Gateway, VPC Bersama,, titik akhir VPC, AWS Direct Connect Gateway Load Balancer, AWS Network Firewall Amazon Route 53, dan peralatan perangkat lunak pihak ketiga menjadi penting. Penting untuk memahami pertimbangan utama dari setiap pendekatan dan bekerja mundur dari kebutuhan Anda dan menganalisis opsi atau kombinasi opsi mana yang paling cocok untuk Anda.

Kontributor

Individu-individu berikut berkontribusi pada dokumen ini:

- Sohaib Tahir, Arsitek Solusi, Amazon Web Services
- Shirin Bhambhani, Arsitek Solusi, Amazon Web Services
- Kunal Pansari, Arsitek Solusi, Amazon Web Services
- Eric Vasquez, Arsitek Solusi, Amazon Web Services
- Tushar Jagdale, Arsitek Solusi, Amazon Web Services
- Ameer Shariff, Arsitek Solusi, Amazon Web Services
- Glenn Davis, Arsitek Solusi, Amazon Web Services
- Nick Kniveton, Arsitek Solusi, Amazon Web Services
- Sidhartha Chauhan, Arsitek Solusi Utama, Amazon Web Services

Riwayat dokumen

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

Perubahan	Deskripsi	Tanggal
Pembaruan besar	Pembaruan di seluruh whitepaper untuk perubahan pada CloudWAN, Amazon VPC Lattice, ENA Express, konektivitas hybrid, Sitelink, Inspeksi Paket Dalam AWS Direct Connect , dan. Akses Terverifikasi AWS	April 17, 2024
Pembaruan kecil	Diagram yang diperbarui agar lebih konsisten, opsi konektivitas DX yang diperbarui untuk menyertakan VPN IP pribadi, dan banyak perubahan kecil di seluruh.	6 Juli 2023
Pembaruan kecil	AWS Control Tower Informasi yang diperbarui, mencerminkan batas throughput baru untuk berbagai layanan, diagram gateway NAT yang diperbarui, bagian keamanan yang diperbarui untuk jalan keluar terpusat.	4 April 2023
Pembaruan kecil	Bagian yang ditambahkan: Akses titik akhir Lintas Wilayah.	19 Juli 2022

Pembaruan besar	Bagian Transit Gateway yang diperbarui dengan Transit Gateway Connect, bagian Transit VPC yang diperbarui; AWS Direct Connect bagian diperbarui dengan MacSec dan rekomendasi ketahanan; bagian yang diperbarui. AWS PrivateLink Menambahkan tabel perbandingan VPC peering vs Transit VPC vs Transit Gateway; menambahk an bagian inspeksi masuk terpusat; keamanan jaringan terpusat yang diperbarui untuk VPC-ke-VPC dan VPC-On-premise ke VPC dan jalan keluar terpusat ke internet dengan dan pola desain Load Balancer Gateway; menambahkan gateway NAT pribadi dan bagian Amazon Route 53 DNS AWS Network Firewall Firewall.	Februari 22, 2022
Pembaruan kecil	Bagian Transit Gateway vs VPC yang Diperbarui	2 April 2021
Laporan resmi diperbarui	Teks yang dikoreksi agar sesuai dengan opsi yang diilustrasikan pada Gambar 7	10 Juni 2020
Publikasi awal	Whitepaper diterbitkan.	15 November 2019

Pemberitahuan

Pelanggan bertanggung jawab untuk membuat penilaian independen mereka sendiri atas informasi dalam dokumen ini. Dokumen ini: (a) hanya disediakan sebagai informasi, (b) berisi penawaran produk dan praktik AWS saat ini, yang dapat berubah tanpa pemberitahuan, dan (c) tidak menjadi komitmen atau jaminan apa pun dari AWS dan afiliasi, pemasok, atau pemberi lisensinya. Produk atau layanan AWS disediakan “sebagaimana adanya” tanpa jaminan, representasi, atau ketentuan 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.

© 2019, Amazon Web Services, Inc. atau afiliasinya. Semua hak cipta dilindungi undang-undang.

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