AWS Whitepaper

Konektivitas Hybrid

Konektivitas Hybrid: AWS Whitepaper

Table of Contents

Konektivitas Hybrid

Tanggal publikasi: 6 Juli 2023 () Revisi dokumen

Banyak organisasi perlu menghubungkan pusat data lokal mereka, situs jarak jauh, dan cloud. Jaringan hybrid menghubungkan lingkungan yang berbeda ini. Whitepaper ini menjelaskan blok bangunan AWS dan persyaratan utama yang perlu dipertimbangkan saat memutuskan model konektivitas hybrid mana yang tepat untuk Anda. Untuk membantu Anda menentukan solusi terbaik untuk bisnis dan persyaratan teknis Anda, kami menyediakan pohon keputusan untuk memandu Anda melalui proses seleksi logis.

Pengantar

Organisasi modern menggunakan beragam sumber daya TI. Di masa lalu, adalah umum untuk meng-host sumber daya ini di pusat data lokal atau fasilitas kolokasi. Dengan meningkatnya adopsi komputasi awan, organisasi memberikan dan mengkonsumsi sumber daya TI dari penyedia layanan cloud melalui koneksi jaringan. Organizations dapat memilih untuk memigrasikan sebagian, atau semua, sumber daya TI yang ada ke cloud. Dalam kedua kasus tersebut, jaringan umum diperlukan untuk menghubungkan sumber daya lokal dan cloud. Koeksistensi sumber daya lokal dan cloud disebut cloud hybrid, dan jaringan umum yang menghubungkannya disebut sebagai jaringan hybrid. Bahkan jika organisasi Anda menyimpan semua sumber daya TI-nya di cloud, mungkin masih memerlukan konektivitas hybrid ke situs jarak jauh.

Ada beberapa model konektivitas untuk dipilih. Meskipun memiliki opsi menambah fleksibilitas, memilih opsi yang optimal memerlukan analisis persyaratan bisnis dan teknis, dan penghapusan opsi yang tidak sesuai. Anda dapat mengelompokkan persyaratan bersama-sama di seluruh pertimbangan seperti keamanan, waktu untuk menerapkan, kinerja, keandalan, model komunikasi, skalabilitas, dan banyak lagi. Setelah mereka mengumpulkan, menganalisis, dan mempertimbangkan persyaratan dengan cermat, arsitek jaringan dan cloud dapat mengidentifikasi blok dan solusi bangunan jaringan AWS hybrid yang berlaku. Untuk mengidentifikasi dan memilih model atau model yang optimal, arsitek harus memahami kelebihan dan kekurangan masing-masing model. Ada juga batasan teknis yang dapat menyebabkan model yang cocok dikecualikan.

Untuk menyederhanakan proses seleksi, whitepaper ini memandu Anda melalui setiap pertimbangan utama dalam urutan logis. Di bawah setiap pertimbangan, ada pertanyaan yang digunakan untuk mengumpulkan persyaratan. Setiap dampak keputusan desain diidentifikasi, bersama dengan solusi potensial. Whitepaper menyajikan pohon keputusan untuk beberapa pertimbangan sebagai metode

untuk membantu proses pengambilan keputusan, menghilangkan opsi, dan memahami konsekuensi dari setiap keputusan. Ini diakhiri dengan skenario yang mencakup kasus penggunaan hibrida, menerapkan pemilihan dan desain model end-to-end konektivitas. Anda dapat menggunakan contoh ini untuk melihat bagaimana menjalankan proses yang ditata dalam whitepaper ini dalam contoh praktis.

Whitepaper ini dimaksudkan untuk membantu Anda memilih dan merancang model konektivitas hybrid yang optimal. Whitepaper ini disusun sebagai berikut:

- Blok bangunan konektivitas hibrida — Gambaran umum AWS layanan yang digunakan untuk konektivitas hybrid.
- Pemilihan konektivitas dan pertimbangan desain — Definisi setiap model konektivitas, bagaimana masing-masing mempengaruhi keputusan desain, pertanyaan identifikasi persyaratan, solusi, dan pohon keputusan.
- Kasus penggunaan pelanggan - Contoh bagaimana menerapkan pertimbangan dan pohon keputusan dalam praktik.

Apakah Anda Well-Architected?

AWSWell-Architected Framework membantu Anda memahami pro dan kontra dari keputusan yang Anda buat saat membangun sistem di cloud. Enam pilar Kerangka memungkinkan Anda mempelajari praktik terbaik arsitektur 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 ahli dan praktik terbaik lainnya untuk arsitektur cloud Anda—penerapan arsitektur referensi, diagram, dan whitepaperer—lihat Pusat Arsitektur. AWS

AWSblok bangunan konektivitas hibrida

Ada tiga blok bangunan arsitektur konektivitas jaringan hybrid:

- Koneksi jaringan hibrid: Jenis koneksi antara layanan AWS konektivitas dan perangkat gateway pelanggan lokal.
- AWSHybrid Connectivity AWS Services: Layanan yang menyediakan konektivitas dan routing antara infrastruktur pelanggan danAWS.
- Perangkat gateway pelanggan lokal: Perangkat di dalam jaringan pelanggan yang ada yang merupakan titik akhir lokal untuk koneksi jaringan hibrid. Kemianan jenis memiliki persyaratan teknis untuk perangkat ini, yang dibahas di bagian berikut.

Koneksi jaringan hibrida

Ada beberapa cara untuk menghubungkan antara peralatan di tempat Anda danAWS. Whitepaper ini difokuskan pada bagaimana cara-cara yang berbeda ini dapat digabungkan ke dalam arsitektur keseluruhan, namun, ikhtisar singkat tentang opsi yang berbeda (, Site-to-Site Virtual Private NetworkAWS Direct Connect, dan Transit Gateway Connect) disediakan.

AWS Direct Connect

AWS Direct Connectadalah layanan yang membuat koneksi jaringan khusus dari tempat Anda keAWS. Lihat AWS Direct Connect untuk detail.

Kemianan ada dua jenis AWS Direct Connect koneksi: dedicated dan host. Sambungan khusus adalah tautan langsung antara AWS perangkat dan perangkat lokal Anda, sedangkan koneksi yang dihosting didukung oleh AWS Mitra yang dapat menangani detail koneksi untuk Anda. Lihat AWS Direct Connectkoneksi untuk informasi lebih lanjut.

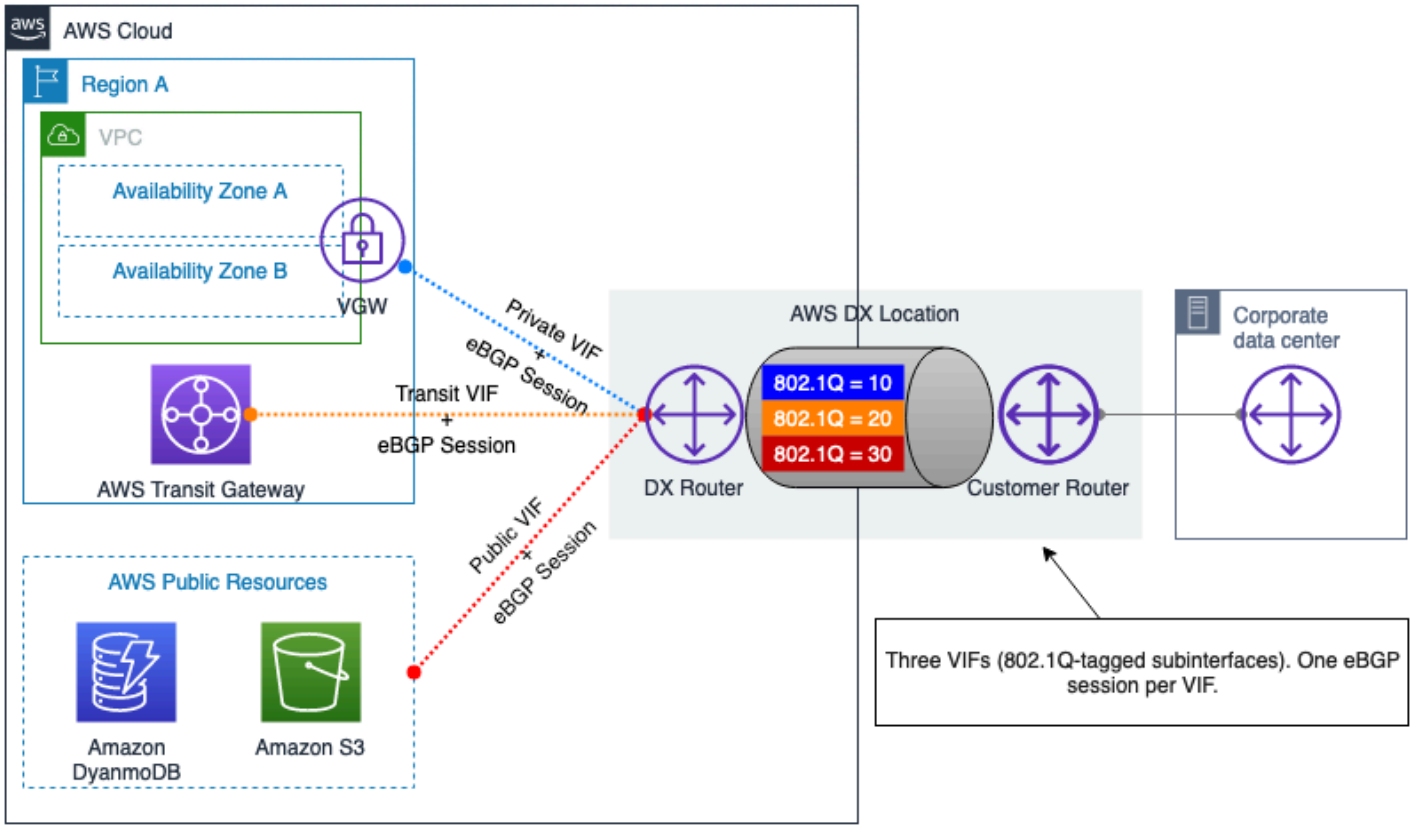
Koneksi Direct Connect menggunakan Virtual Interfaces (VIF) untuk mengisolasi arus lalu lintas yang berbeda. Beberapa VIF dapat menggunakan tautan Direct Connect yang sama, dipisahkan oleh tag VLAN (802.1q). Ada tiga jenis VIF yang menyediakan konektivitas ke AWS jaringan. Lihat antarmuka AWS Direct Connect virtual untuk detail selengkapnya. Ketiga jenis tersebut adalah:

- VIF Pribadi: VIF pribadi adalah koneksi pribadi antara perangkat Anda dan sumber daya Anda di dalamnya. AWS Ini berakhir di dalam baik AWS pada Virtual Private Gateway (VGW) secara

langsung (yang mendukung satu VPC) atau melalui Direct Connect Gateway yang kemudian terhubung ke beberapa VGW.

- VIF Publik: VIF publik memungkinkan konektivitas ke AWS sumber daya publik apa pun, seperti S3, DynamoDB, dan rentang IP EC2 publik. Meskipun VIF publik tidak memiliki akses langsung ke internet, sumber daya publik Amazon apa pun dapat mencapainya (termasuk instans EC2 publik pelanggan lain), yang harus dipertimbangkan pelanggan selama perencanaan keamanan.
- Transit VIF: VIF transit adalah koneksi pribadi antara perangkat Anda danAWS Transit Gateway, melalui Direct Connect Gateway. Transit VIF sekarang didukung pada tautan dengan kecepatan kurang dari 1 Gbps - lihat pengumuman peluncuran untuk detailnya.

> **Note**
>
> Hosted Virtual Interface (Hosted VIF) adalah jenis VIF Pribadi di mana VIF ditugaskan ke yang berbeda Akun AWS dari Akun AWS yang memiliki AWS Direct Connect koneksi (yang dapat mencakup mitra). AWS Direct Connect AWStidak lagi memungkinkan mitra baru untuk menawarkan model ini. Untuk informasi selengkapnya, lihat Membuat antarmuka virtual yang dihosting.



Gambar 1 — AWS Direct Connect VIF Pribadi dan Publik

Kemianan Jaringan Pribadi Virtual (VPN)

site-to-site VPN memungkinkan dua jaringan untuk berkomunikasi dengan aman dan dapat digunakan melalui transportasi yang tidak tepercaya, seperti internet. Pelanggan dapat membuat koneksi VPN antara situs lokal dan Amazon Virtual Private Clouds (Amazon VPC) melalui dua opsi:

- AWSVPN Site-to-Site Terkelola AWS (VPN S2S): Ini adalah layanan VPN yang dikelola sepenuhnya dan sangat tersedia, menggunakan IPSec. Lihat Apa itu AWS Site-to-Site VPN untuk informasi lebih lanjut. Anda dapat mengaktifkan akselerasi secara opsional untuk koneksi Site-to-Site VPN Anda. Lihat Koneksi VPN Site-to-Site untuk informasi selengkapnya. S2S VPN juga dapat menggunakan VIF transit Direct Connect untuk menghindari lalu lintas melintasi internet, menurunkan biaya dan memungkinkan penggunaan alamat IP pribadi. Untuk detailnya, lihat Private IP VPN dengan AWS Direct Connect.
- Perangkat Lunak Site-to-Site VPN (VPN yang dikelola pelanggan): Dengan opsi konektivitas VPN ini, Anda bertanggung jawab untuk menyediakan dan mengelola seluruh solusi VPN, biasanya

dengan menjalankan perangkat lunak VPN pada instans EC2. Untuk informasi selengkapnya, lihat Perangkat Lunak Site-to-Site VPN.

Kedua opsi tersebut memerlukan dukungan pada perangkat gateway pelanggan untuk menghentikan ujung terowongan VPN lokal. Kemianan perangkat ini bisa berupa perangkat fisik atau perangkat lunak. Untuk informasi selengkapnya tentang perangkat jaringan yang diuji olehAWS, lihat daftar perangkat gateway pelanggan yang diuji.

Transit Gateway Connect (TGW Connect)

Transit Gateway Connect menggunakan terowongan GRE antara perangkat gateway AWS Transit Gateway dan lokal. BGP digunakan di atas TGW Connect untuk mengaktifkan perutean dinamis. Perhatikan bahwa TGW Connect tidak dienkripsi. Untuk informasi selengkapnya, lihat Transit Gateway Connect.

AWSlayanan konektivitas hybrid

AWSlayanan konektivitas hybrid menyediakan komponen jaringan yang sangat skalabel dan sangat tersedia. Mereka memainkan peran penting dalam membangun solusi jaringan hybrid. Pada saat penulisan whitepaper ini, ada tiga titik akhir layanan utama:

- AWSVirtual Private Gateway (VGW) adalah layanan regional yang sangat redundan yang menyediakan perutean dan penerusan IP di tingkat VPC, bertindak sebagai gateway bagi VPC untuk berkomunikasi dengan perangkat gateway pelanggan Anda. VGW dapat menghentikan koneksi VPN AWS S2S dan VIF Pribadi. AWS Direct Connect
- AWS Transit Gateway(TGW) adalah layanan regional, sangat tersedia, dan skalabel yang memungkinkan Anda menghubungkan beberapa VPC satu sama lain, serta jaringan lokal Anda melalui Site-to-Site VPN dan/atau Direct Connect menggunakan satu gateway terpusat. Secara konseptual, sebuah AWS Transit Gateway bertindak sebagai router cloud virtual yang sangat tersedia dan berlebihan. AWS Transit Gatewaymendukung perutean multi-jalur (ECMP) biaya yang sama melalui beberapa koneksi Direct Connect, terowongan VPN, atau rekan TGW Connect. Transit Gateway dapat saling mengintip, baik di wilayah dan lintas wilayah yang sama, memungkinkan sumber daya mereka yang terhubung untuk berkomunikasi melalui tautan pengintip. Untuk detail selengkapnya, lihat AWS Transit Gatewayskenario.
- AWS CloudWAN menyediakan dasbor pusat untuk membuat koneksi antara kantor cabang, pusat data, dan Amazon VPC Anda—membangun jaringan global hanya dengan beberapa klik.

Anda menggunakan kebijakan jaringan untuk mengotomatiskan manajemen jaringan dan tugas keamanan di satu lokasi. Untuk detail selengkapnya, lihat dokumentasi AWS Cloud WAN.

- Direct Connect Gateway (DXGW) adalah layanan yang tersedia secara global yang mendistribusikan informasi routing di seluruh koneksinya, berperilaku mirip dengan reflektor rute BGP dalam jaringan tradisional. Data tidak melewati DXGW — hanya menangani informasi routing. Anda dapat membuat DXGW di bagian mana saja Wilayah AWS dan mengaksesnya dari yang lain. Wilayah AWS Anda dapat menghubungkan Direct Connect VIF ke DXGW, lalu mengaitkan DXGW dengan VGW (menggunakan VIF pribadi) atau (menggunakan VIF transit). AWS Transit Gateway Lihat gateway Direct Connect untuk informasi selengkapnya. Anda tidak perlu membuat beberapa DXGW untuk redundansi karena ini adalah layanan ketersediaan global. Namun, Anda dapat memilih untuk menggunakan beberapa DXGW untuk memisahkan domain perutean, misalnya, produksi dan jaringan pengujian yang ingin Anda pertahankan sepenuhnya terisolasi.

Jenis konektivitas hibrida dan pertimbangan desain

Bagian whitepaper ini mencakup pertimbangan yang memengaruhi pilihan Anda saat memilih jaringan hybrid untuk menghubungkan lingkungan lokal Anda. AWS Ini mengikuti proses pemikiran logis untuk mendukung Anda memilih solusi konektivitas hybrid yang optimal. Pertimbangan yang memengaruhi desain Anda dikategorikan ke dalam pertimbangan yang memengaruhi jenis konektivitas Anda, dan pertimbangan yang memengaruhi desain konektivitas Anda. Pertimbangan jenis konektivitas akan mendukung Anda memutuskan antara menggunakan VPN berbasis internet atau Direct Connect. Pertimbangan desain konektivitas akan mendukung Anda memutuskan cara mengatur koneksi.

Pertimbangan berikut yang memengaruhi jenis konektivitas Anda tercakup: waktu untuk menerapkan, keamanan, SLA, kinerja, dan biaya. Setelah meninjau pertimbangan tersebut, dan bagaimana pengaruhnya terhadap pilihan desain Anda, Anda akan dapat memutuskan apakah menggunakan koneksi berbasis internet atau Direct Connect direkomendasikan untuk memenuhi kebutuhan Anda.

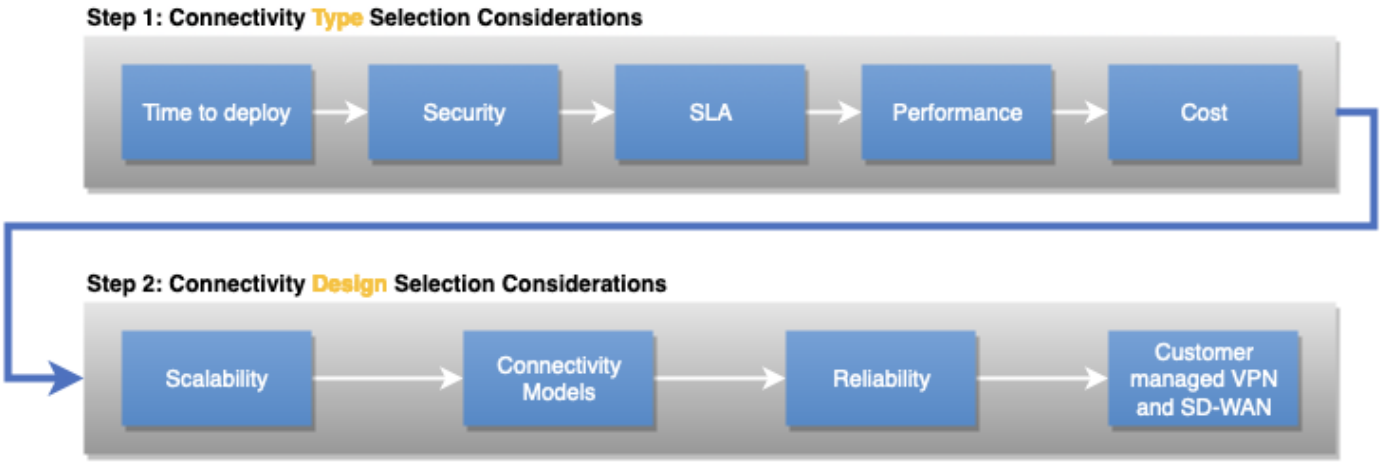
Pertimbangan berikut yang memengaruhi desain konektivitas Anda tercakup: skalabilitas, model komunikasi, keandalan, dan integrasi SD-WAN pihak ketiga. Setelah meninjau pertimbangan tersebut, dan bagaimana pengaruhnya terhadap pilihan desain Anda, Anda akan dapat memutuskan desain logis optimal yang direkomendasikan untuk memenuhi kebutuhan Anda.

Struktur berikut digunakan untuk mendiskusikan dan menganalisis setiap pertimbangan pemilihan dan desain:

- Definisi - Definisi singkat tentang apa yang menjadi pertimbangan.
- Pertanyaan kunci - Menyediakan serangkaian pertanyaan untuk memungkinkan Anda mengumpulkan persyaratan yang terkait dengan pertimbangan.
- Kemampuan untuk dipertimbangkan - Solusi untuk mengatasi persyaratan yang terkait dengan pertimbangan.
- Pohon keputusan - Untuk beberapa pertimbangan atau sekelompok pertimbangan, pohon keputusan disediakan untuk membantu Anda memilih solusi jaringan hibrida yang optimal.

Pertimbangan yang mempengaruhi desain jaringan hybrid Anda tercakup dalam urutan di mana output dari satu pertimbangan adalah bagian dari input untuk pertimbangan berikutnya. Seperti yang diilustrasikan pada Gambar 2, langkah pertama adalah memutuskan jenis konektivitas, diikuti dengan menyempurnakannya dengan pertimbangan pemilihan desain.

Gambar 2 menunjukkan dua kategori pertimbangan, pertimbangan individu, dan urutan logis di mana pertimbangan tercakup dalam sub-bagian berikutnya. Itu adalah pertimbangan penting ketika membuat keputusan desain jaringan hybrid. Jika desain yang ditargetkan tidak memerlukan semua pertimbangan ini, Anda dapat fokus pada pertimbangan yang berlaku untuk kebutuhan Anda.



Gambar 2 — Kategori pertimbangan, pertimbangan individu, dan urutan logis di antara mereka

Pemilihan tipe konektivitas

Bagian ini mencakup pertimbangan yang memengaruhi jenis konektivitas yang Anda pilih untuk beban kerja Anda. Ini termasuk waktu untuk menyebarkan, keamanan, SLA, kinerja, dan biaya.

Pertimbangan-pertimbangan

- Saatnya untuk mengirimi
- Keamanan
- Perjanjian tingkat layanan (SLA)
- Performa
- Biaya

Saatnya untuk mengirimi

Definisi

Waktu untuk menyebarkan dapat menjadi faktor penting dalam memilih jenis konektivitas yang sesuai untuk beban kerja. Bergantung pada jenis konektivitas dan lokasi lokal, konektivitas dapat dibuat

dalam beberapa jam, namun, mungkin diperlukan waktu berminggu-minggu atau berbulan-bulan jika sirkuit tambahan harus dipasang. Ini akan memengaruhi keputusan Anda untuk menggunakan koneksi berbasis internet, koneksi khusus pribadi, atau koneksi host pribadi yang disediakan sebagai layanan terkelola oleh Mitra. AWS Direct Connect

Pertanyaan kunci

- Apa timeline yang diperlukan untuk penyebaran - jam, hari, minggu, atau bulan?
- Berapa lama koneksi akan dibutuhkan — apakah itu akan menjadi proyek berumur pendek atau infrastruktur permanen?

Kemampuan untuk dipertimbangkan

Ketika Anda memerlukan AWS konektivitas dalam beberapa jam atau hari, kemungkinan besar Anda perlu menggunakan koneksi jaringan yang ada. Ini sering berarti membuat koneksi VPN AWS melalui internet publik. Jika mitra AWS DX yang ada menyediakan AWS konektivitas pribadi kepada Anda, koneksi host baru dapat disediakan dalam beberapa jam.

Ketika Anda memiliki hari hingga berminggu-minggu, Anda dapat bekerja dengan AWS Direct Connect Mitra untuk membangun konektivitas pribadiAWS. AWS Direct Connect Mitra membantu Anda membangun koneksi jaringan antara AWS Direct Connect lokasi dan lingkungan data, kantor, atau lokasi bersama Anda. AWS Direct ConnectMitra tertentu disetujui untuk menawarkan Koneksi Dihosting Direct Connect. Hosted Connections seringkali dapat disediakan lebih cepat daripada Dedicated Connections. AWS Direct Connect Mitra akan menyediakan setiap Koneksi yang Dihosting menggunakan infrastruktur yang ada yang terhubung ke AWS tulang punggung.

Ketika Anda memiliki beberapa minggu hingga berbulan-bulan, Anda dapat menyelidiki membangun koneksi pribadi khusus denganAWS. Penyedia layanan dan AWS Direct Connect Mitra memfasilitasi Koneksi AWS Direct Connect Khusus. Adalah umum bagi penyedia layanan untuk memasang peralatan jaringan di tempat pelanggan untuk memfasilitasi Koneksi Khusus Direct Connect. Bergantung pada penyedia layanan, lokasi situs Anda, dan faktor fisik lainnya, pemasangan Koneksi Khusus Direct Connect dapat berlangsung dari beberapa minggu hingga beberapa bulan.

Jika Anda sudah memasang peralatan jaringan di fasilitas colocation yang sama di mana AWS Direct Connect lokasinya ada, maka Anda dapat dengan cepat membuat Sambungan AWS Direct Connect Khusus melalui koneksi silang di situs co-location. Setelah Anda meminta koneksi, AWS membuat Letter of Authorization and Connecting Facility Assignment (LOA-CFA) tersedia bagi Anda untuk diunduh, atau mengirimi Anda email dengan permintaan untuk informasi selengkapnya. LOA-

CFA adalah otorisasi untuk terhubung ke AWS, dan diperlukan oleh penyedia jaringan Anda untuk memesan koneksi silang untuk Anda.

Tabel 1 — Perbandingan efektivitas biaya

	Konektivitas berbasis internet	DX Dedicated Connection (peralatan yang ada di lokasi DX)	Koneksi Khusus DX (net-new)	DX Hosted Connection (port yang ada dengan DX Partner)	Koneksi yang Dihosting DX (net-new)
Waktu penyediaan	Jam hingga berhari-hari	Hari	Beberapa minggu hingga berbulan-bulan	Jam hingga berhari-hari	Beberapa hari hingga berminggu-minggu hingga berbulan-bulan

> **Note**
>
> Pedoman waktu penyediaan yang disediakan didasarkan pada pengamatan dunia nyata dan hanya berfungsi sebagai ilustrasi. Saat mempertimbangkan lokasi situs Anda, kedekatan dengan lokasi koneksi langsung, dan infrastruktur yang sudah ada sebelumnya, dan semuanya akan memengaruhi waktu penyediaan. AWS Direct ConnectMitra Anda akan memberi tahu Anda tentang waktu penyediaan yang tepat.

Keamanan

Definisi

Persyaratan keamanan akan memengaruhi jenis konektivitas hybrid Anda. Pertimbangan ini meliputi:

- Jenis transportasi — koneksi internet atau jaringan pribadi
- Persyaratan enkripsi

Pertanyaan kunci

- Apakah persyaratan dan kebijakan keamanan Anda memungkinkan penggunaan koneksi terenkripsi melalui internet untuk terhubungAWS, atau apakah mereka mengamanatkan penggunaan koneksi jaringan pribadi?
- Saat memanfaatkan koneksi jaringan pribadi, apakah lapisan jaringan harus menyediakan enkripsi saat transit?

Solusi teknis

Persyaratan dan kebijakan keamanan Anda mungkin mengizinkan penggunaan internet atau memerlukan penggunaan koneksi jaringan pribadi antara AWS dan jaringan perusahaan Anda. Mereka juga mempengaruhi keputusan apakah jaringan harus menyediakan enkripsi dalam perjalanan, atau jika melakukan enkripsi pada lapisan aplikasi dapat diterima.

Jika Anda dapat memanfaatkan internet, maka AWS Site-to-Site VPN dapat digunakan untuk membuat terowongan terenkripsi antara jaringan Anda dan VPC Amazon Anda atau AWS Transit Gateway s melalui internet. Memperluas solusi SD-WAN Anda ke AWS internet juga merupakan pilihan jika Anda memanfaatkan koneksi berbasis internet. Bagian VPN yang dikelola pelanggan dan SD-WAN nanti di whitepaper ini mencakup pertimbangan khusus untuk SD-WAN.

Jika Anda memerlukan koneksi jaringan pribadi antara AWS dan jaringan perusahaan Anda, maka AWS rekomendasikan AWS Direct Connect untuk menggunakan Koneksi Khusus atau Koneksi yang Dihosting. Jika enkripsi dalam perjalanan diperlukan melalui koneksi jaringan pribadi, maka Anda harus membuat VPN melalui Direct Connect (baik melalui VIF publik atau VIF transit), atau pertimbangkan untuk menggunakan MacSec pada koneksi Khusus 10Gbps atau 100Gbps.

Tabel 2 — Contoh persyaratan jenis konektivitas Automotive Corp

	Site-to-Site VPN	Direct Connect
Transportasi	Internet	Koneksi jaringan pribadi
Enkripsi dalam transit	Ya	Memerlukan S2S VPN melalui DX, S2S VPN melalui VIF transit, atau MacSec pada Koneksi Khusus 10Gbps atau 100Gbps

Perjanjian tingkat layanan (SLA)

Definisi

Organisasi bisnis sering membutuhkan penyedia layanan untuk memenuhi SLA untuk setiap layanan yang dikonsumsi organisasi. Organisasi pada gilirannya membangun layanannya sendiri di atas dan dapat menawarkan SLA kepada konsumen mereka sendiri. SLA penting karena menggambarkan bagaimana layanan disediakan dan dioperasikan, dan sering kali mencakup karakteristik terukur tertentu, seperti ketersediaan. Jika layanan melanggar SLA yang ditentukan, penyedia layanan biasanya menawarkan kompensasi finansial yang ditentukan oleh perjanjian. SLA mendefinisikan jenis ukuran, persyaratan, dan periode pengukuran. Sebagai contoh, lihat definisi target uptime di bawah AWS Direct ConnectSLA.

Pertanyaan kunci

- Apakah koneksi konektivitas hybrid SLA dengan kredit layanan diperlukan?
- Apakah seluruh jaringan hybrid perlu mematuhi target uptime?

Kemampuan untuk dipertimbangkan

Jenis konektivitas: Konektivitas internet tidak dapat diprediksi. Meskipun AWS sangat berhati-hati dengan beberapa tautan di tempat dengan beragam ISP, administrasi internet hanya di luar AWS atau domain administratif penyedia tunggal. Ada sejumlah rekayasa rute dan pengaruh lalu lintas yang dapat dilakukan penyedia cloud setelah lalu lintas meninggalkan perbatasan jaringan mereka. Konon, ada AWS Site-to-Site VPNSLA yang menyediakan target ketersediaan untuk titik AWS Site-to-Site VPN akhir.

AWSDirect Connect menawarkan SLA formal dengan kredit layanan dihitung sebagai persentase dari total biaya AWS Direct Connect Port Hour yang dibayarkan oleh Anda untuk koneksi yang berlaku yang mengalami tidak tersedianya siklus penagihan bulanan di mana SLA tidak terpenuhi. Ini adalah transportasi yang direkomendasikan jika diperlukan SLA. AWS Direct Connectmencantumkan persyaratan konfigurasi minimal tertentu untuk setiap target uptime seperti jumlah AWS Direct Connect lokasi, koneksi, dan detail konfigurasi lainnya. Kegagalan untuk memenuhi persyaratan berarti bahwa kredit layanan tidak dapat ditawarkan jika jeda layanan menentukan SLA.

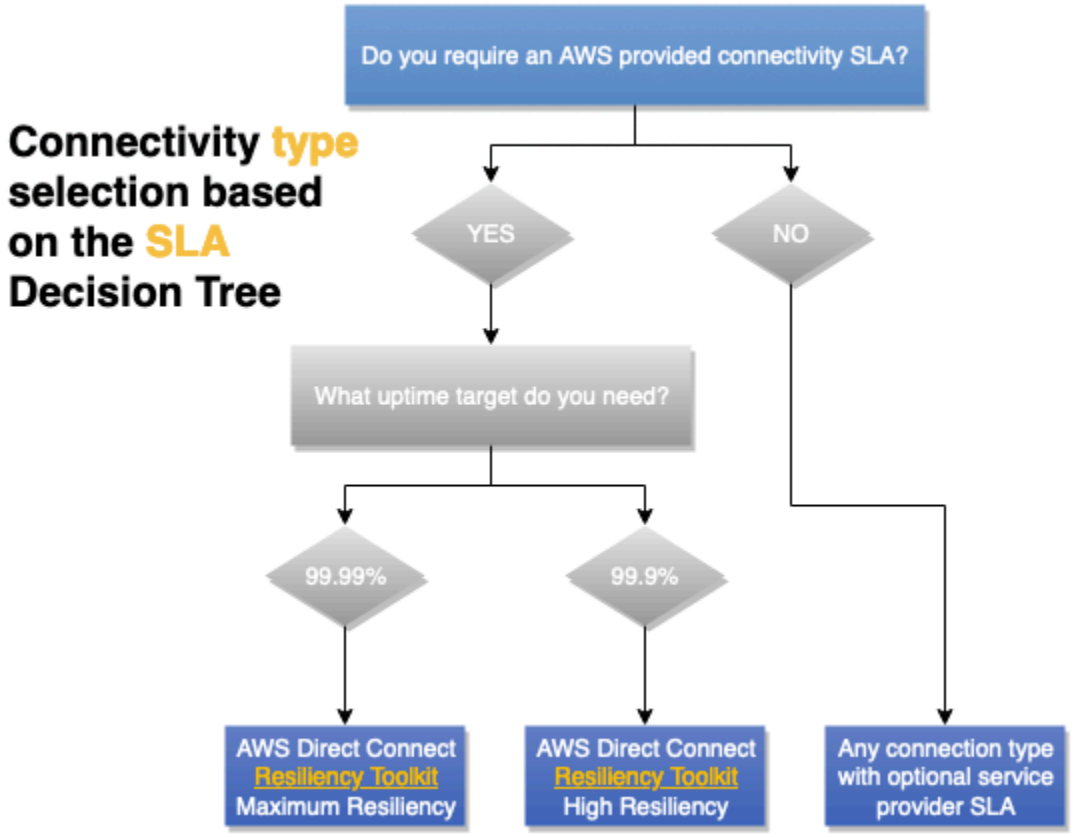
Yang penting, bahkan jika layanan yang dipilih untuk menyediakan konektivitas hybrid dikonfigurasi untuk memenuhi persyaratan SLA, sisa jaringan mungkin tidak menyediakan tingkat SLA yang sama. AWSTanggung jawab berakhir di AWS Direct Connect lokasi di AWS Direct Connect pelabuhan.

Setelah AWS menyerahkan lalu lintas ke jaringan organisasi Anda, itu bukan lagi tanggung jawabAWS. Jika Anda menggunakan penyedia layanan antara AWS dan jaringan lokal Anda, konektivitas tunduk pada SLA antara Anda dan penyedia layanan, jika berlaku. Perlu diingat bahwa seluruh jaringan hybrid sama baiknya dengan bagian terlemahnya saat merancang konektivitas hybrid.

AWS Direct Connectmitra menawarkan AWS Direct Connect konektivitas. Mitra dapat menawarkan SLA dengan kredit layanan berdasarkan penawaran produk mereka hingga titik demarkasi dengan. AWS Opsi tersebut harus dievaluasi dan diteliti lebih lanjut secara langsung dengan APN Partners. AWSmenerbitkan daftar mitra pengiriman yang divalidasi.

Desain logis: Selain jenis konektivitas, Anda juga harus mempertimbangkan blok bangunan lain sebagai bagian dari keseluruhan desain Anda. Sebagai contoh, AWS Transit Gatewaymemiliki SLA sendiri, seperti halnya AWSS2S VPN. Anda mungkin menggunakan AWS Transit Gateway untuk skala dan VPN AWS S2S untuk alasan keamanan, tetapi Anda harus merancang keduanya dengan cara yang konsisten dengan masing-masing SLA agar memenuhi syarat untuk kredit layanan dengan masing-masing layanan.

Tinjau Rekomendasi AWS Direct Connect Ketahanan dan Toolkit Ketahanan.



Gambar 3 — Pohon keputusan pertimbangan SLA

Performa

Definisi

Ada beberapa faktor yang mempengaruhi kinerja jaringan, seperti latency, packet loss, jitter, dan bandwidth. Bergantung pada persyaratan aplikasi, pentingnya masing-masing faktor ini dapat bervariasi.

Pertanyaan kunci

Berdasarkan persyaratan aplikasi Anda, Anda perlu mengidentifikasi dan memprioritaskan faktor kinerja jaringan yang memengaruhi perilaku aplikasi dan pengalaman pengguna Anda.

Bandwidth

Bandwidth mengacu pada kecepatan transfer data koneksi, dan biasanya diukur dalam bit per detik (bps). Megabit per detik (Mbps) dan gigabit per detik (Gbps) adalah penskalaan umum, dan merupakan basis 10 (1.000.000 bit per detik = 1 Mbps) sebagai lawan dari basis 2 (2 ^ 10) yang terlihat di tempat lain.

Saat mengevaluasi kebutuhan bandwidth aplikasi, perlu diingat bahwa persyaratan bandwidth dapat berubah seiring waktu. Penyebaran awal ke cloud, operasi normal, beban kerja baru, dan skenario failover semuanya dapat memiliki persyaratan bandwidth yang berbeda.

Aplikasi dapat memiliki pertimbangan bandwidth sendiri. Beberapa aplikasi mungkin memerlukan kinerja deterministik melalui koneksi bandwidth tinggi, sementara yang lain dapat memerlukan kinerja deterministik dan bandwidth tinggi. Sebuah aplikasi mungkin memerlukan konfigurasi khusus untuk menggunakan beberapa arus lalu lintas (kadang-kadang disebut sebagai aliran atau soket) secara paralel jika mencapai batas bandwidth arus lalu lintas, memungkinkannya untuk menggunakan lebih banyak bandwidth koneksi. VPN dapat membatasi throughput karena overhead tunneling, batas MTU yang lebih rendah, atau keterbatasan bandwidth perangkat keras.

Latensi

Latensi adalah waktu yang dibutuhkan untuk paket untuk pergi dari sumber ke tujuan melalui koneksi jaringan, dan biasanya diukur dalam milidetik (ms), dengan persyaratan latensi rendah kadang-kadang dinyatakan dalam mikrodetik (µs). Latensi adalah fungsi dari kecepatan cahaya, sehingga latensi meningkat dengan jarak.

Persyaratan latensi aplikasi dapat mengambil bentuk yang berbeda. Aplikasi yang sangat interaktif, seperti desktop virtual, dapat memiliki target latensi yang diukur dari saat pengguna melakukan input hingga pengguna melihat desktop virtual bereaksi terhadap input tersebut. Aplikasi Voice over IP (VoIP) dapat memiliki persyaratan serupa. Jenis beban kerja kedua yang perlu dipertimbangkan adalah beban kerja yang sangat transaksional, membutuhkan respons dari server sebelum dapat melanjutkan. Database atau bentuk penyimpanan kunci/nilai lainnya dapat sangat dipengaruhi oleh peningkatan latensi jaringan.

Jitter

Jitter mengukur seberapa konsisten latensi jaringan, dan, seperti latensi, biasanya diukur dalam milidetik (ms).

Persyaratan jitter aplikasi biasanya ditemukan dalam aplikasi streaming waktu nyata, termasuk pengiriman video dan suara. Aplikasi ini cenderung mengharuskan aliran datanya berada pada tingkat dan penundaan yang konsisten, dengan buffer kecil untuk mengoreksi sejumlah kecil jitter.

Kehilangan paket

Packet loss adalah pengukuran berapa persentase lalu lintas jaringan yang tidak terkirim. Semua jaringan memiliki beberapa tingkat kehilangan paket pada waktu karena ledakan lalu lintas yang tinggi, pengurangan kapasitas, kegagalan peralatan jaringan, dan alasan lainnya. Dengan demikian, aplikasi harus memiliki toleransi terhadap kehilangan paket, namun, seberapa banyak mereka dapat mentolerir dapat bervariasi dari aplikasi ke aplikasi.

Aplikasi yang menggunakan TCP untuk mengangkut lalu lintas mereka memiliki kemampuan untuk mengoreksi kehilangan paket melalui transmisi ulang. Aplikasi yang menggunakan UDP atau protokol mereka sendiri di atas IP perlu menerapkan cara mereka sendiri untuk menangani kehilangan paket, dan mungkin sangat sensitif terhadapnya. Aplikasi voice over IP dapat dengan mudah memasukkan keheningan ke bagian panggilan yang memiliki paket kehilangan, sebagai lawan mencoba mengirim ulang. Beberapa solusi VPN menyertakan mekanisme mereka sendiri untuk memulihkan dari kehilangan paket pada jaringan yang mereka gunakan untuk membawa lalu lintas.

Kemampuan untuk dipertimbangkan

Ketika latensi dan throughput yang dapat diprediksi diperlukan, AWS Direct Connect adalah pilihan yang disarankan, karena memberikan kinerja deterministik. Bandwidth dapat dipilih berdasarkan persyaratan throughput. AWSmerekomendasikan penggunaan AWS Direct Connect ketika Anda membutuhkan pengalaman jaringan yang lebih konsisten daripada koneksi berbasis internet dapat

menyediakan. VIF pribadi dan Transit VIF mendukung jumbo frame, yang dapat mengurangi jumlah paket melalui jaringan dan dapat meningkatkan throughput karena berkurangnya overhead. AWS Direct Connect SiteLinkmemungkinkan menggunakan AWS tulang punggung untuk menyediakan konektivitas antara lokasi Anda dan dapat diaktifkan sesuai permintaan. Bandwidth yang digunakan untuk SiteLink harus diperhitungkan untuk pemilihan bandwidth Direct Connect Anda.

Menggunakan VPN over AWS Direct Connect menambahkan enkripsi. Namun, ini mengurangi ukuran MTU yang dapat mengurangi throughput. AWSKemampuan VPN Site-to-Site (S2S) terkelola dapat ditemukan dalam dokumentasi. AWS Site-to-Site VPN Banyak lokasi Direct Connection mendukung MacSec jika enkripsi melalui koneksi Anda adalah persyaratan enkripsi utama. MACSec tidak memiliki MTU atau pertimbangan throughput potensial koneksi VPN Site-to-Site. AWS Transit Gatewaymemungkinkan pelanggan untuk menskalakan jumlah koneksi VPN secara horizontal dan meningkatkan throughput sesuai dengan Equal-cost multi-path routing (ECMP). AWSVPN Site-to-Site yang dikelola mendukung penggunaan VIF transit Direct Connect untuk konektivitas pribadi — lihat VPN IP Pribadi dengan untuk detailnya. AWS Direct Connect

Pilihan lainnya adalah menggunakan VPN Site-to-Site yang AWS dikelola melalui internet. Ini bisa menjadi pilihan yang menarik karena biaya rendah dan tersedia secara luas. Namun, perlu diingat bahwa kinerja melalui internet adalah upaya terbaik. Peristiwa cuaca internet, kemacetan, dan peningkatan periode latensi tidak dapat diprediksi. AWSmenawarkan solusi dengan AWSAccelerated S2S VPN, yang dapat mengurangi beberapa kelemahan menggunakan jalur internet. Accelerated S2S VPN menggunakan AWS Global Accelerator, yang memungkinkan lalu lintas VPN memasuki AWS jaringan sedini mungkin dan sedekat mungkin dengan perangkat gateway pelanggan. Ini mengoptimalkan jalur jaringan, menggunakan jaringan AWS global bebas kemacetan, untuk mengarahkan lalu lintas ke titik akhir yang memberikan kinerja terbaik. Anda dapat menggunakan koneksi VPN yang dipercepat untuk menghindari gangguan jaringan yang dapat terjadi ketika lalu lintas diirimi Anda untuk internet publik.

Biaya

Definisi

Di cloud, biaya konektivitas hybrid mencakup biaya sumber daya dan penggunaan yang disediakan. Biaya sumber daya yang disediakan diukur dalam satuan waktu, biasanya per jam. Penggunaannya adalah untuk transfer data dan pemrosesan biasanya diukur dalam gigabyte (GB). Biaya lainnya termasuk biaya konektivitas ke titik kehadiran AWS jaringan. Jika jaringan Anda berada dalam fasilitas colocation yang sama, mungkin sesedikit biaya koneksi silang. Jika jaringan Anda berada di lokasi yang berbeda, akan ada biaya penyedia layanan atau mitra APN Direct Connect.

Pertanyaan kunci

- Berapa banyak data yang Anda antisipasi pengiriman AWS per bulan dari fasilitas Anda dan dari internet?
- Berapa banyak data yang Anda antisipasi pengiriman dari AWS per bulan ke fasilitas Anda dan ke internet?
- Seberapa sering jumlah ini akan berubah?
- Perubahan apa dalam skenario kegagalan?

Kemampuan untuk dipertimbangkan

Jika Anda memiliki beban kerja bandwidth yang berat yang ingin Anda jalankanAWS, AWS Direct Connect dapat mengurangi biaya jaringan Anda masuk dan keluar dengan dua cara. AWS Pertama, dengan mentransfer data ke dan dari AWS langsung, Anda dapat mengurangi biaya bandwidth yang dibayarkan ke penyedia layanan internet Anda. Kedua, semua data yang ditransfer melalui koneksi khusus Anda dikenakan biaya pada kecepatan transfer AWS Direct Connect data yang dikurangi, bukan kecepatan transfer data internet — lihat halaman harga Direct Connect untuk detailnya.

AWS Direct Connectmemungkinkan penggunaan AWS Direct Connect SiteLink untuk menghubungkan situs Anda menggunakan AWS tulang punggung - lihat blog SiteLink peluncuran untuk informasi lebih lanjut. Memanfaatkan kemampuan ini menimbulkan biaya transfer data Direct Connect normal, bersama dengan biaya per jam SiteLink diaktifkan. Anda dapat mengaktifkan dan menonaktifkan SiteLink on-demand, dan ini mungkin merupakan pilihan yang baik untuk skenario kegagalan yang melibatkan internet atau konektivitas jaringan pribadi.

Jika Anda menggunakan penyedia layanan jaringan untuk konektivitas antara lokasi lokal dan lokasi Direct Connect, kemampuan Anda dan waktu yang diperlukan untuk mengubah komitmen bandwidth Anda didasarkan pada kontrak Anda dengan penyedia layanan.

AWSTulang punggung dapat mengirimkan lalu lintas Anda ke mana pun Wilayah AWS kecuali China dari titik kehadiran AWS jaringan mana pun. Kemampuan ini memiliki banyak manfaat teknis dibandingkan menggunakan internet untuk mengakses jarak jauhWilayah AWS, tetapi memiliki biaya — lihat halaman harga Transfer Data EC2 untuk detailnya. Jika ada AWS Transit Gatewaydi jalur lalu lintas, itu menambahkan biaya pemrosesan data per GB, namun jika menggunakan peering antar wilayah antara dua Gateway Transit, Anda hanya ditagih sekali untuk pemrosesan data Transit Gateway.

Desain aplikasi yang optimal menjaga pemrosesan data di dalam AWS dan meminimalkan biaya keluar data yang tidak perlu. Masuknya data ke AWS gratis.

> **Note**
>
> Sebagai bagian dari solusi konektivitas keseluruhan, selain biaya AWS koneksi, Anda juga harus mempertimbangkan biaya end-to-end konektivitas termasuk biaya penyedia layanan, sambungan silang, rak, dan peralatan di dalam lokasi DX (jika diperlukan).

Jika Anda tidak yakin apakah Anda harus menggunakan internet atau koneksi pribadi, hitung titik impas di mana AWS Direct Connect menjadi lebih murah daripada menggunakan internet. Jika volume data berarti AWS Direct Connect lebih murah, dan Anda memerlukan konektivitas permanen, AWS Direct Connect adalah pilihan konektivitas yang optimal.

Jika konektivitas bersifat sementara dan internet memenuhi persyaratan lain, bisa lebih murah untuk menggunakan AWS S2S VPN melalui internet karena elastisitas internet. Perhatikan bahwa ini mengharuskan Anda memiliki konektivitas internet yang memadai dari jaringan lokal Anda.

Jika Anda berada dalam fasilitas yang memiliki AWS Direct Connect (daftar tersedia di situs web Direct Connect), Anda dapat membuat sambungan silang keAWS. Ini berarti menggunakan koneksi khusus pada 1,10, atau 100Gbps. AWS Direct Connectmitra menawarkan lebih banyak opsi bandwidth dan kapasitas yang lebih kecil, yang dapat mengoptimalkan biaya konektivitas Anda. Misalnya, Anda dapat memulai dengan Koneksi Hosted 50 Mbps versus Koneksi Khusus 1 Gbps.

DenganAWS Transit Gateway, Anda dapat berbagi koneksi VPN dan Direct Connect dengan banyak VPC. Meskipun Anda dikenakan biaya untuk jumlah koneksi yang Anda buat AWS Transit Gateway per jam dan jumlah lalu lintas yang mengalirAWS Transit Gateway, ini menyederhanakan manajemen dan mengurangi jumlah koneksi VPN dan VIF yang diperlukan. Manfaat dan penghematan biaya overhead operasional yang lebih rendah dapat dengan mudah lebih besar daripada biaya tambahan pemrosesan data. Secara opsional, Anda dapat mempertimbangkan desain di mana AWS Transit Gateway berada di jalur lalu lintas ke sebagian besar VPC, tetapi tidak semua. Pendekatan ini menghindari biaya pemrosesan AWS Transit Gateway data untuk kasus penggunaan di mana Anda perlu mentransfer data dalam AWS jumlah besar. Lihat bagian Model Konektivitas untuk detail lebih lanjut tentang desain ini. Pendekatan lain adalah menggabungkan AWS Direct Connect sebagai jalur utama dengan AWS S2S VPN melalui internet sebagai jalur cadangan/failover. Meskipun secara teknis layak dan sangat hemat biaya, solusi ini memiliki kelemahan teknis (dibahas di bagian

Keandalan dari whitepaper ini) dan bisa lebih sulit untuk dikelola. AWStidak merekomendasikan ini untuk beban kerja yang sangat kritis atau kritis.

Pendekatan terakhir adalah VPN atau SD-WAN yang dikelola pelanggan yang digunakan di instans Amazon EC2. Ini bisa lebih murah dalam skala jika ada puluhan hingga ratusan situs jika dibandingkan dengan AWS S2S VPN. Namun, ada overhead manajemen, biaya lisensi, dan biaya sumber daya EC2 untuk setiap alat virtual untuk dipertimbangkan.

Matriks keputusan

Tabel 3 — Contoh input desain konektivitas otomotif Corp.

Kategori	VPN atau SD-WAN yang dikelola pelanggan	AWSS2S VPN	AWSVPN S2S yang dipercepat	AWS Direct ConnectKoneksi yang Dihosting	AWS Direct ConnectKoneksi Khusus
Membutuhkan koneksi internet	Ya	Ya	Ya	Tidak	Tidak
Biaya sumber daya yang disediakan	Instans EC2 dan lisensi perangkat lunak	AWSS2S VPN	AWSS2S VPN dan AWS Akselerator Global	Potongan kapasitas yang berlaku dari biaya port	Biaya port khusus
Biaya transfer data	Tarif internet	Tarif internet atau tarif Direct Connect	Internet dengan premi transfer data	Letter Connecting	Letter Connecting
Transit Gateway	Opsional	Opsional	Diperlukan	Opsional	Opsional
AWSBiaya pemrosesan data	T/A	Hanya dengan AWS Transit Gateway	Ya	Hanya dengan AWS Transit Gateway	Hanya dengan AWS Transit Gateway

Kategori	VPN atau SD-WAN yang dikelola pelanggan	AWSS2S VPN	AWSVPN S2S yang dipercepat	AWS Direct ConnectKoneksi yang Dihosting	AWS Direct ConnectKoneksi Khusus
Dapat digunakan di atasAWS Direct Connect?	Ya	Ya	Tidak	N/A	T/A

Pemilihan desain konektivitas

Bagian whitepaper ini mencakup pertimbangan yang memengaruhi pemilihan desain konektivitas Anda. Desain konektivitas mencakup aspek logis serta cara merancang dan mengoptimalkan keandalan konektivitas hybrid Anda.

Pertimbangan berikut akan dibahas: skalabilitas, model konektivitas, keandalan, dan VPN dan SD-WAN yang dikelola pelanggan.

Pertimbangan

- Skalabilitas
- Model konektivitas
- Keandalan
- VPN dan SD-WAN yang dikelola pelanggan

Skalabilitas

Definisi

Skalabilitas mengacu pada kemampuan solusi konektivitas Anda untuk tumbuh dan berkembang seiring waktu seiring dengan perubahan kebutuhan Anda.

Saat merancang solusi, Anda perlu mempertimbangkan ukuran saat ini, serta pertumbuhan yang diantisipasi. Pertumbuhan ini dapat berupa pertumbuhan organik, atau mungkin terkait dengan ekspansi yang cepat, seperti dalam skenario merger dan akuisisi.

Catatan: tergantung pada arsitektur solusi yang ditargetkan, tidak semua elemen sebelumnya mungkin perlu dipertimbangkan. Namun, mereka dapat berfungsi sebagai elemen dasar untuk mengidentifikasi persyaratan skalabilitas dari solusi jaringan hibrida yang paling umum. Whitepaper ini berfokus pada pemilihan dan desain konektivitas hybrid. Disarankan agar Anda juga mempertimbangkan skala konektivitas hybrid sehubungan dengan arsitektur jaringan VPC. Untuk informasi selengkapnya, lihat whitepaper Membangun Infrastruktur AWS Jaringan Multi-VPC yang Dapat Diskalakan dan Aman.

Pertanyaan kunci

- Berapa jumlah VPC saat ini dan yang diantisipasi yang memerlukan konektivitas ke situs atau situs lokal?
- Apakah VPC digunakan dalam satu Wilayah AWS atau beberapa Wilayah?
- Berapa banyak situs lokal yang perlu dihubungkan? AWS
- Berapa banyak perangkat gateway pelanggan (biasanya router atau firewall) yang Anda miliki per situs yang perlu terhubung? AWS
- Berapa banyak rute yang diharapkan untuk diiklankan ke VPC Amazon dan berapa jumlah rute yang diharapkan akan diterima dari samping? AWS
- Apakah ada persyaratan untuk meningkatkan bandwidth AWS seiring waktu?

Kemampuan untuk dipertimbangkan

Skala merupakan faktor penting dalam desain konektivitas hybrid. Untuk itu, bagian selanjutnya akan memasukkan skala sebagai bagian dari desain model konektivitas yang ditargetkan.

Berikut ini adalah praktik terbaik yang direkomendasikan untuk meminimalkan kompleksitas skala desain konektivitas jaringan hybrid:

- Ringkasan rute harus digunakan untuk mengurangi jumlah rute yang diiklankan dan diterima. AWS Dengan demikian, skema pengalamatan IP perlu dirancang untuk memaksimalkan penggunaan ringkasan rute. Rekayasa lalu lintas adalah pertimbangan utama secara keseluruhan. Untuk informasi lebih lanjut tentang teknik lalu lintas, lihat subbagian teknik lalu lintas di bagian Keandalan.
- Minimalkan jumlah sesi peering BGP Anda dengan menggunakan DXGW dengan VGW atau AWS Transit Gateway, di mana satu sesi BGP dapat menyediakan konektivitas ke beberapa VPC.

- Pertimbangkan Cloud WAN ketika beberapa situs Wilayah AWS dan lokal perlu dihubungkan bersama.

Model konektivitas

Definisi

Model konektivitas mengacu pada pola komunikasi antara jaringan lokal dan sumber daya cloud di AWS. Anda dapat menerapkan sumber daya cloud dalam VPC Amazon dalam Wilayah AWS satu atau beberapa VPC di beberapa Wilayah, AWS serta layanan yang memiliki titik akhir publik dalam satu atau Wilayah AWS beberapa, seperti Amazon S3 dan DynamoDB.

Pertanyaan kunci

- Apakah ada persyaratan untuk komunikasi antar-VPC dalam suatu Wilayah dan lintas Wilayah?
- Apakah ada persyaratan untuk mengakses titik akhir AWS publik langsung dari lokal?
- Apakah ada persyaratan untuk mengakses AWS layanan menggunakan titik akhir VPC dari lokal?

Kemampuan untuk dipertimbangkan

Berikut ini adalah beberapa skenario model konektivitas yang paling umum. Setiap model konektivitas mencakup persyaratan, atribut, dan pertimbangan.

Catatan: seperti yang disorot sebelumnya, whitepaper ini difokuskan pada konektivitas hibrid antara jaringan lokal dan. AWS Untuk detail lebih lanjut tentang desain untuk menghubungkan VPC, lihat whitepaper Building a Scalable and Secure AWS Multi-VPC Network Infrastructure.

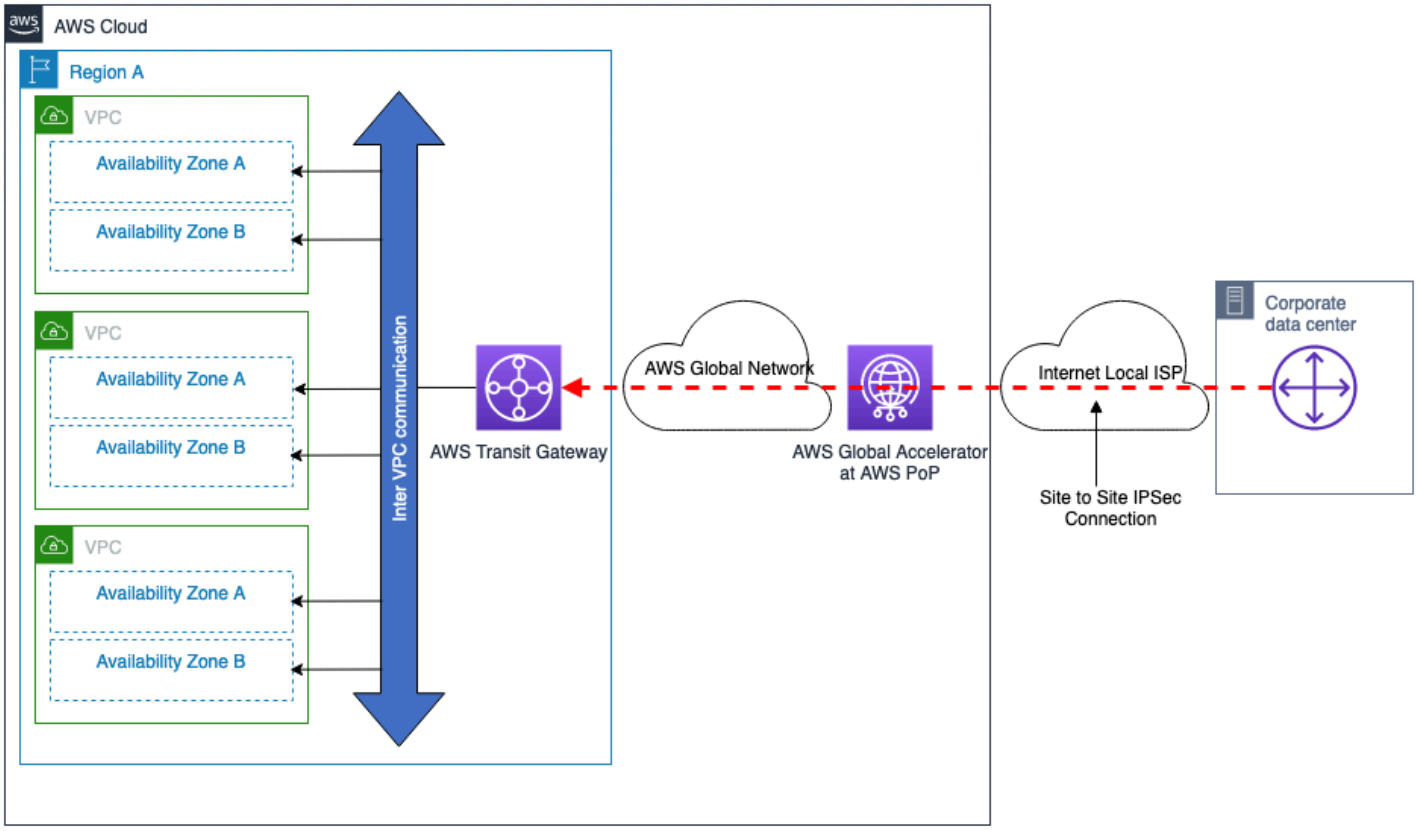
Model

- AWS VPN Site-to-Site yang Dipercepat —, Tunggal AWS Transit GatewayWilayah AWS
- AWS DX - DXGW dengan VGW, Wilayah Tunggal
- AWS DX - DXGW dengan VGW, Multi-Wilayah, dan Peering Publik AWS
- AWS DX - DXGW dengan, Multi-Wilayah AWS Transit Gateway, dan Peering Publik AWS
- AWS DX - DXGW dengan AWS Transit Gateway, Multi-Wilayah (lebih dari 3)

AWS VPN Site-to-Site yang Dipercepat —, Tunggal AWS Transit GatewayWilayah AWS

Model ini dibangun dari:

- Tunggal Wilayah AWS.
- AWS Koneksi VPN Site-to-Site yang dikelola dengan. AWS Transit Gateway
- VPN yang dipercepat diaktifkan.



Gambar 4 — VPN AWS Terkelola — AWS Transit Gateway, Tunggal Wilayah AWS

Atribut model konektivitas:

- Menyediakan kemampuan untuk membuat koneksi VPN yang dioptimalkan melalui internet publik dengan menggunakan koneksi VPN Site-to-Site yang AWS Dipercepat.
- Berikan kemampuan untuk mencapai bandwidth koneksi VPN yang lebih tinggi dengan mengonfigurasi beberapa terowongan VPN dengan ECMP.
- Dapat digunakan untuk koneksi dari beberapa situs terpencil.

- Menawarkan failover otomatis dengan perutean dinamis (BGP).
- Dengan AWS Transit Gateway terhubung ke VPC, semua VPC yang terhubung dapat menggunakan koneksi VPN yang sama. Anda juga dapat mengontrol model komunikasi yang diinginkan di antara VPC, untuk informasi lebih lanjut lihat Cara Kerja Transit Gateways.
- Menawarkan opsi desain yang fleksibel untuk mengintegrasikan keamanan pihak ketiga dan peralatan virtual SD-WAN. AWS Transit Gateway Lihat Keamanan jaringan terpusat untuk lalu lintas VPC-ke-VPC dan lokal ke VPC.

Pertimbangan skala:

- Bandwidth hingga 50 Gbps dengan beberapa terowongan IPsec dan ECMP dikonfigurasi (setiap arus lalu lintas akan dibatasi pada bandwidth maksimum per terowongan VPN).
- Ribuan VPC dapat dihubungkan per. AWS Transit Gateway
- Lihat kuota VPN Site-to-Site untuk batas skala lainnya, seperti jumlah rute.

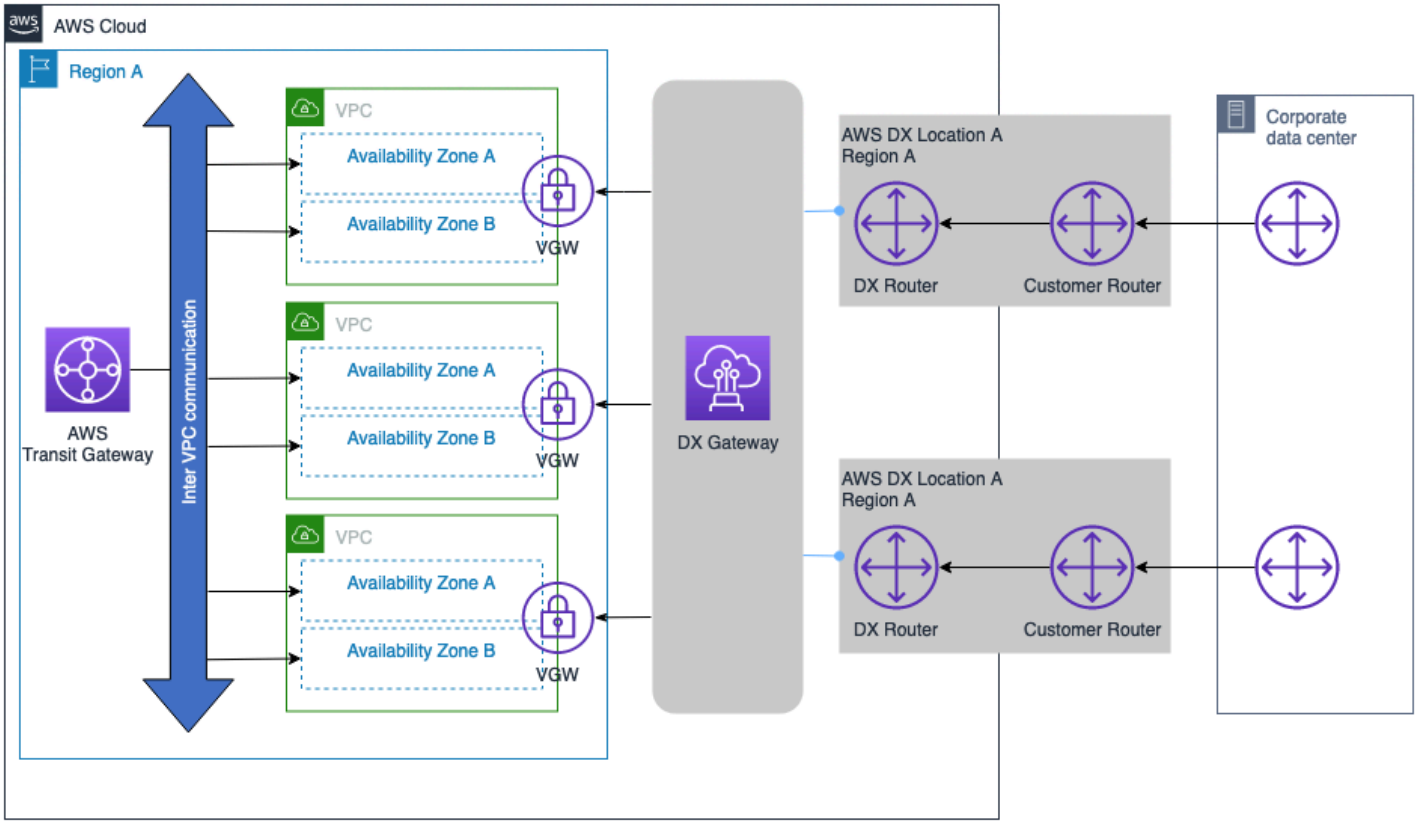
Pertimbangan lain:

- Biaya AWS Transit Gateway pemrosesan tambahan untuk transfer data antara pusat data lokal dan AWS.
- Grup keamanan dari VPC jarak jauh tidak dapat direferensikan AWS Transit Gateway - ini didukung oleh peering VPC, namun.

AWS DX - DXGW dengan VGW, Wilayah Tunggal

Model ini dibangun dari:

- Tunggal Wilayah AWS.
- AWS Direct Connect Koneksi Ganda ke lokasi DX independen.
- AWS DXGW langsung terpasang ke VPC menggunakan VGW.
- Penggunaan opsional AWS Transit Gateway untuk komunikasi antar-VPC.



Gambar 5 — AWS DX — DXGW dengan VGW, Tunggal Wilayah AWS

Atribut model konektivitas:

- Menyediakan kemampuan untuk terhubung ke VPC dan koneksi DX di Wilayah lain di masa depan.
- Menawarkan failover otomatis dengan perutean dinamis (BGP).
- Dengan AWS Transit Gateway Anda dapat mengontrol model komunikasi yang diinginkan di antara VPC. Untuk informasi lebih lanjut, lihat Cara kerja gateway transit.

Pertimbangan skala:

AWS Direct Connect Kuota referensi untuk informasi lebih lanjut tentang batas skala lainnya, seperti jumlah awalan yang didukung, jumlah VIF per jenis koneksi DX (Khusus, dihosting). Beberapa pertimbangan utama:

- Sesi BGP untuk VIF pribadi dapat mengiklankan hingga 100 rute masing-masing untuk IPv4 dan IPv6.

- Hingga 20 VPC dapat dihubungkan per DXGW melalui satu sesi BGP. Jika diperlukan lebih dari 20 VPC, DXGW tambahan dapat ditambahkan untuk memfasilitasi konektivitas dalam skala besar, atau pertimbangkan untuk menggunakan integrasi Transit Gateway.
- Tambahan AWS Direct Connect s dapat ditambahkan sesuai keinginan.

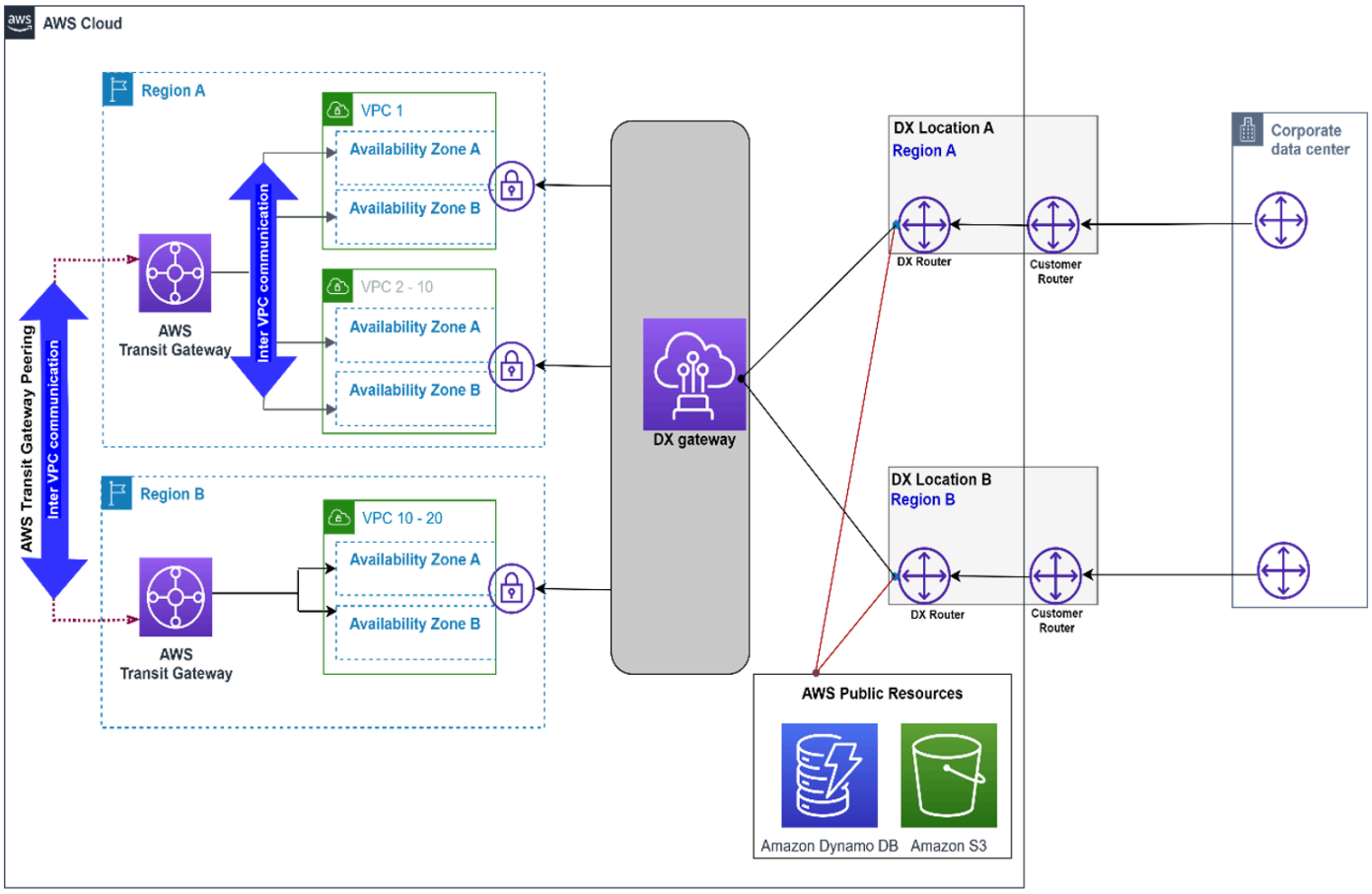
Pertimbangan lain:

- Tidak dikenakan biaya pemrosesan AWS Transit Gateway terkait untuk transfer data antara AWS dan jaringan lokal.
- Grup keamanan VPC jarak jauh tidak dapat direferensikan (AWS Transit Gateway perlu mengintip VPC).
- Pengintipan VPC dapat digunakan sebagai pengganti AWS Transit Gateway untuk memfasilitasi komunikasi antara VPC, namun, ini menambah kompleksitas operasional untuk membangun dan mengelola pengintipan VPC dalam jumlah besar. point-to-point
- Jika komunikasi antar-VPC tidak diperlukan, baik pengintipan VPC maupun AWS Transit Gateway VPC tidak diperlukan dalam model konektivitas ini.

AWS DX - DXGW dengan VGW, Multi-Wilayah, dan Peering Publik AWS

Model ini dibangun dari:

- Beberapa pusat data lokal dengan koneksi ganda ke AWS.
- AWS Direct Connect Koneksi Ganda ke lokasi DX independen.
- AWS DXGW langsung terpasang ke lebih dari 10 VPC menggunakan VGW, hingga 20 VPC menggunakan VGW.
- Penggunaan opsional AWS Transit Gateway untuk komunikasi antar-VPC dan Antar-Wilayah.



Gambar 6 - AWS DX - DXGW dengan VGW, Multi-Wilayah, dan VIF Publik

Atribut model konektivitas:

- AWS DXGW langsung terpasang ke lebih dari 10 VPC menggunakan VGW hingga 20 VPC menggunakan VGW.
- AWS VIF publik DX digunakan untuk mengakses layanan AWS publik, seperti Amazon S3, langsung melalui AWS koneksi DX.
- Menyediakan kemampuan untuk terhubung ke VPC dan koneksi DX di Wilayah lain di masa depan.
- Komunikasi antar VPC dan VPC Antar Wilayah difasilitasi oleh dan mengintip Transit Gateway. AWS Transit Gateway

Pertimbangan skala:

AWS Direct Connect Kuota referensi untuk informasi lebih lanjut tentang batas skala lainnya, seperti jumlah awalan yang didukung, jumlah VIF per jenis koneksi DX (khusus, dihosting). Beberapa pertimbangan utama:

- Sesi BGP untuk VIF pribadi dapat mengiklankan hingga 100 rute masing-masing untuk IPv4 dan IPv6.
- Hingga 20 VPC dapat dihubungkan per DXGW melalui satu sesi BGP pada setiap VIF pribadi, hingga 30 VIF pribadi per DXGW.
- Tambahan AWS Direct Connect s dapat ditambahkan sesuai keinginan.

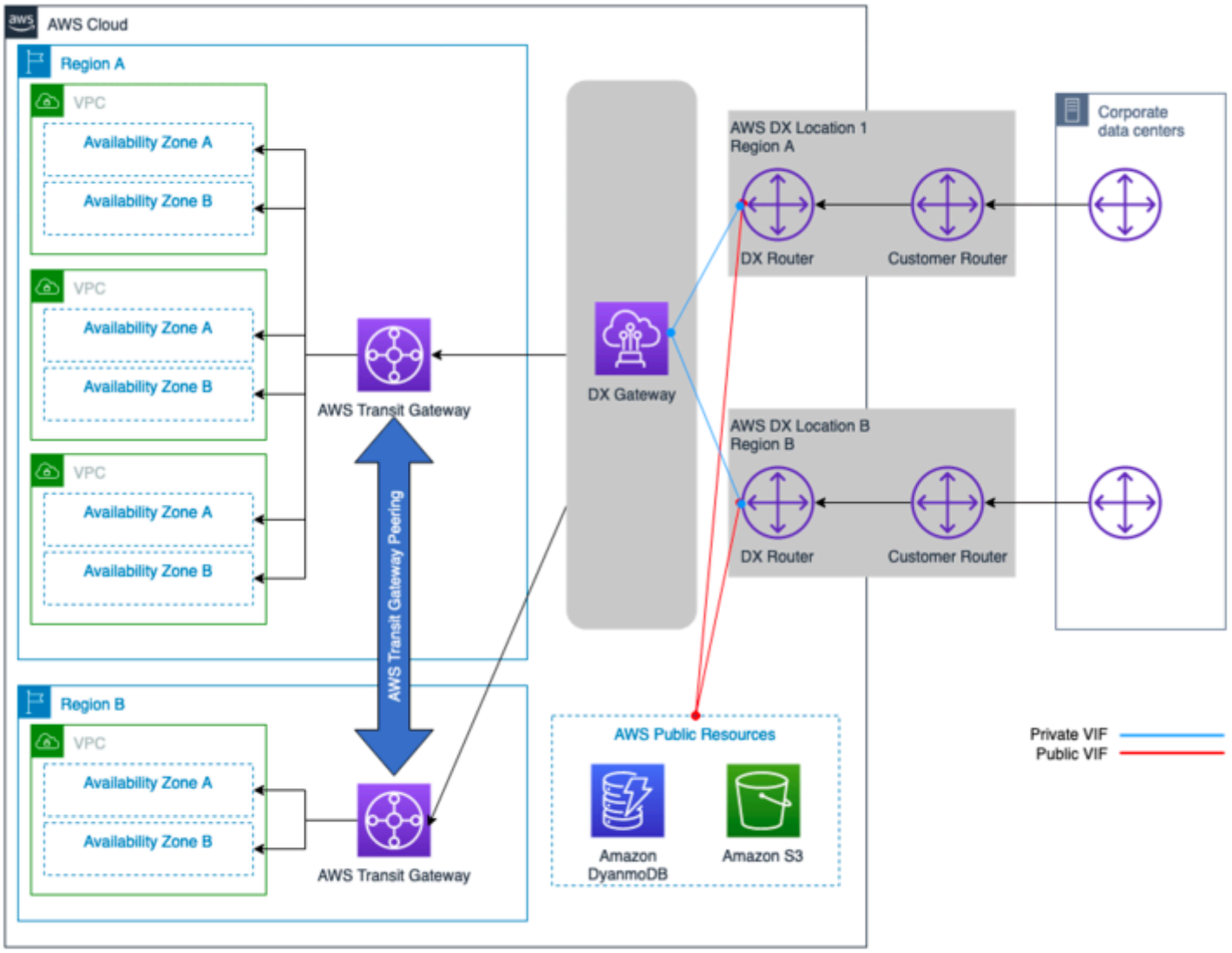
Pertimbangan lain:

- Tidak dikenakan biaya pemrosesan AWS Transit Gateway terkait untuk transfer data antara AWS dan jaringan lokal.
- Grup keamanan VPC jarak jauh tidak dapat direferensikan oleh (AWS Transit Gateway perlu mengintip VPC).
- Pengintipan VPC dapat digunakan alih-alih AWS Transit Gateway untuk memfasilitasi komunikasi antara VPC, namun, ini akan menambah kompleksitas operasional untuk membangun dan mengelola pengintipan VPC dalam skala besar. point-to-point
- Jika komunikasi antar-VPC tidak diperlukan, baik pengintipan VPC maupun AWS Transit Gateway VPC tidak diperlukan dalam model konektivitas ini.

AWS DX - DXGW dengan, Multi-Wilayah AWS Transit Gateway, dan Peering Publik AWS

Model ini dibangun dari:

- Berganda Wilayah AWS.
- AWS Direct Connect Koneksi Ganda ke lokasi DX independen.
- Pusat data lokal tunggal dengan koneksi ganda ke AWS.
- AWS DXGW dengan. AWS Transit Gateway
- Skala tinggi VPC per Wilayah.



Gambar 7 - AWS DX - DXGW dengan, Multi-Wilayah AWS Transit Gateway, dan VIF Publik AWS

Atribut model konektivitas:

- AWS VIF publik DX digunakan untuk mengakses sumber daya AWS publik seperti S3 langsung melalui koneksi DX. AWS
- Menyediakan kemampuan untuk terhubung ke VPC dan/atau koneksi DX di Wilayah lain di masa mendatang.
- Dengan AWS Transit Gateway terhubung ke VPC, konektivitas mesh penuh atau sebagian dapat dicapai antara VPC.
- Komunikasi antar VPC dan VPC Antar Wilayah difasilitasi dengan mengintip. AWS Transit Gateway

- Menawarkan opsi desain yang fleksibel untuk mengintegrasikan keamanan pihak ketiga dan peralatan virtual SDWAN dengan AWS Transit Gateway. Lihat: Keamanan jaringan terpusat untuk lalu lintas VPC-ke-VPC dan lokal ke VPC.

Pertimbangan skala:

- Jumlah rute ke dan dari AWS Transit Gateway terbatas pada jumlah rute maksimum yang didukung melalui Transit VIF (nomor masuk dan keluar bervariasi). Lihat AWS Direct Connect kuota untuk informasi lebih lanjut tentang batas skala dan jumlah rute dan VIF yang didukung.
- Skala hingga ribuan VPC per satu AWS Transit Gateway sesi BGP.
- Transit Tunggal VIF per AWS DX.
- Koneksi AWS DX tambahan dapat ditambahkan sesuai keinginan.

Pertimbangan lain:

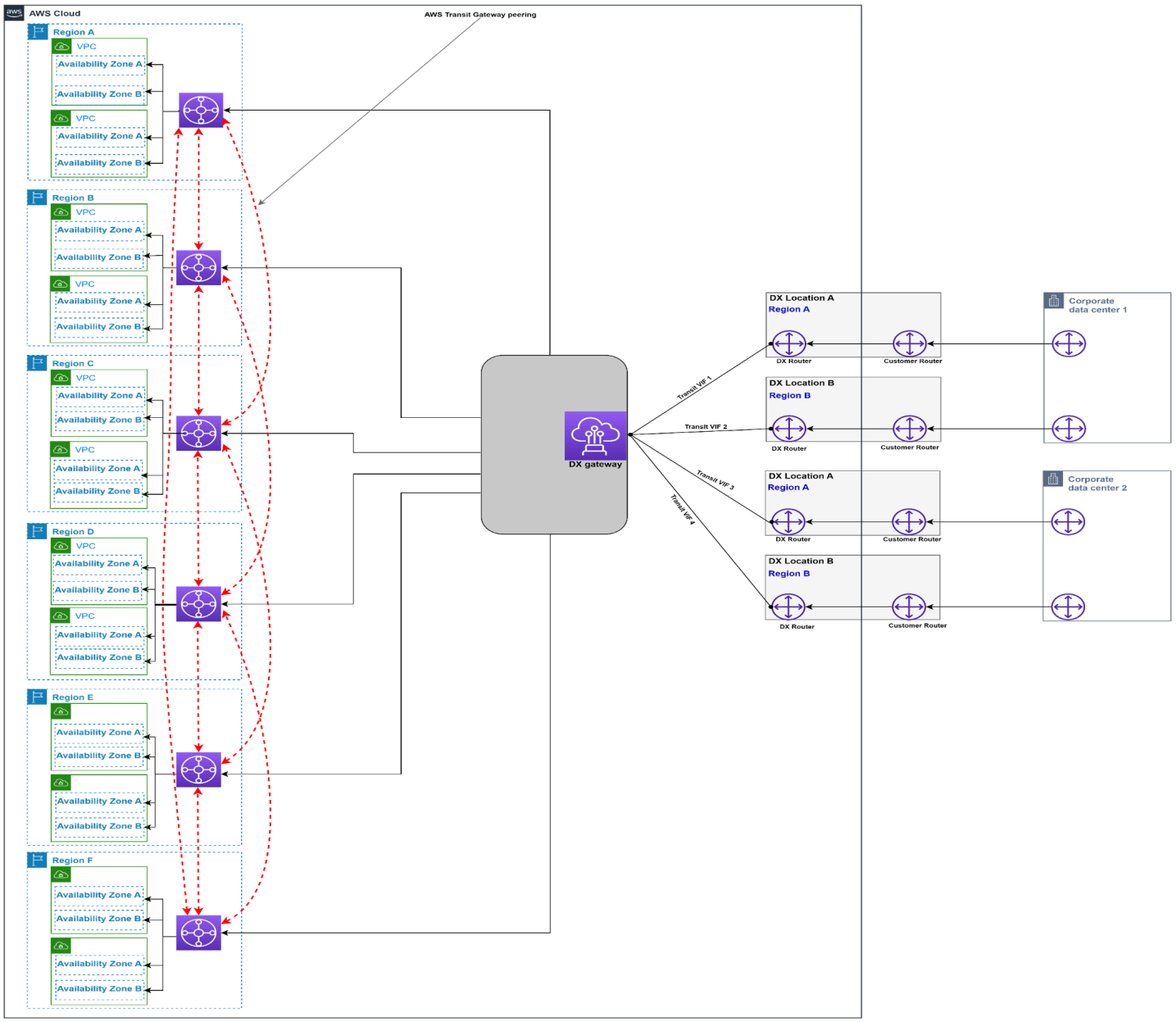
- Menimbulkan biaya AWS Transit Gateway pemrosesan tambahan untuk transfer data antara AWS dan situs lokal.
- Grup keamanan VPC jarak jauh tidak dapat direferensikan oleh (AWS Transit Gateway perlu mengintip VPC).
- Pengintipan VPC dapat digunakan alih-alih AWS Transit Gateway untuk memfasilitasi komunikasi antara VPC, namun, ini akan menambah kompleksitas operasional untuk membangun dan mengelola pengintipan VPC dalam skala besar. point-to-point
- Jika diperlukan lebih dari tiga AWS Transit Gateway detik, DXGW tambahan dapat ditambahkan - lihat mode konektivitas berikut.

AWS DX - DXGW dengan AWS Transit Gateway, Multi-Wilayah (lebih dari 3)

Model ini dibangun dari:

- Beberapa Wilayah AWS (lebih dari 3).
- Pusat data lokal ganda.
- AWS Direct Connect Koneksi Ganda melintasi lokasi DX independen per Wilayah.
- AWS DXGW dengan. AWS Transit Gateway
- Skala tinggi VPC per Wilayah.

- Jaring penuh mengintip antara AWS Transit Gateway s.



Gambar 8 — AWS DX — DXGW dengan AWS Transit Gateway, Multi-Regions (lebih dari tiga)

Atribut model konektivitas:

- Overhead operasional terendah.
- AWS VIF publik DX digunakan untuk mengakses sumber daya AWS publik, seperti S3, langsung melalui koneksi DX. AWS

- Menyediakan kemampuan untuk terhubung ke VPC dan koneksi DX di Wilayah lain di masa depan.
- Dengan AWS Transit Gateway terhubung ke VPC, konektivitas mesh penuh atau sebagian dapat dicapai antara VPC.
- Komunikasi VPC Antar Wilayah difasilitasi dengan mengintip. AWS Transit Gateway
- Menawarkan opsi desain yang fleksibel untuk mengintegrasikan keamanan pihak ketiga dan peralatan virtual SDWAN dengan AWS Transit Gateway. Lihat: Keamanan jaringan terpusat untuk lalu lintas VPC-ke-VPC dan lokal ke VPC.

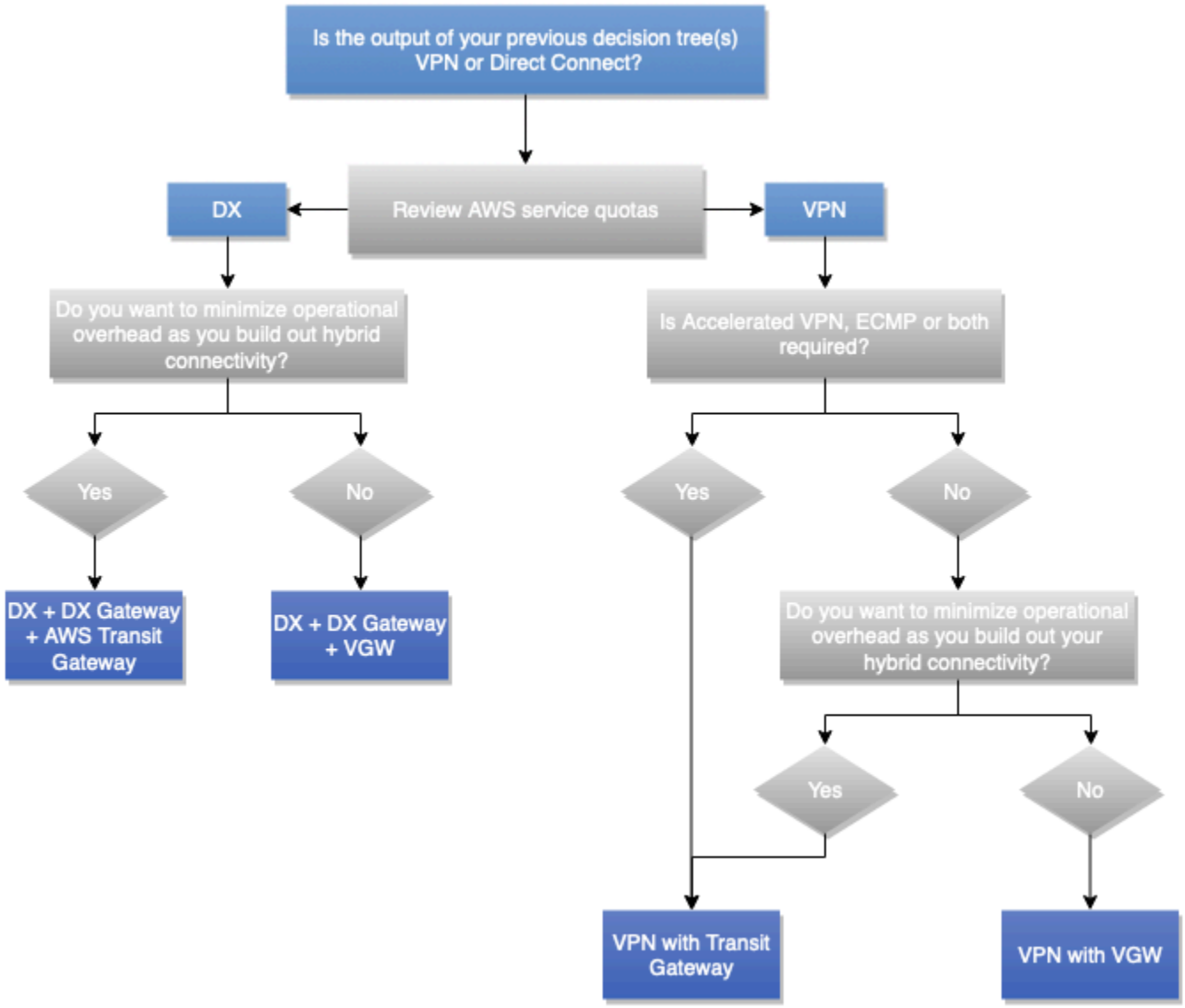
Pertimbangan skala:

- Jumlah rute ke dan dari AWS Transit Gateway terbatas pada jumlah rute maksimum yang didukung melalui Transit VIF (nomor masuk dan keluar bervariasi). Lihat AWS Direct Connect kuota untuk informasi lebih lanjut tentang batas skala. Pertimbangkan ringkasan rute jika diperlukan untuk mengurangi jumlah rute.
- Skala hingga ribuan VPC per satu sesi BGP per DXGW (dengan asumsi kinerja yang disediakan oleh koneksi DX yang disediakan AWS Transit Gateway sudah cukup). AWS
- Hingga enam AWS Transit Gateway detik dapat dihubungkan per DXGW.
- Jika lebih dari tiga Wilayah perlu dihubungkan menggunakan AWS Transit Gateway, maka DXGW tambahan diperlukan.
- Transit Tunggal VIF per AWS DX.
- Koneksi AWS DX tambahan dapat ditambahkan sesuai keinginan.

Pertimbangan lain:

- Menimbulkan biaya AWS Transit Gateway pemrosesan tambahan untuk transfer data antara situs lokal dan. AWS
- Grup keamanan VPC jarak jauh tidak dapat direferensikan oleh (AWS Transit Gateway perlu mengintip VPC).
- Pengintipan VPC dapat digunakan sebagai pengganti AWS Transit Gateway untuk memfasilitasi komunikasi antara VPC, namun, ini akan menambah kompleksitas operasional untuk membangun dan mengelola pengintipan VPC dalam skala besar. point-to-point

Pohon keputusan berikut mencakup pertimbangan skalabilitas dan model komunikasi:



Gambar 9 — Pohon keputusan model skalabilitas dan komunikasi

> **Note**
>
> Jika jenis koneksi yang dipilih adalah VPN, biasanya pada pertimbangan kinerja, keputusan harus dibuat apakah titik penghentian VPN adalah koneksi VPN AWS VGW atau AWS Transit Gateway AWS S2S. Jika belum dibuat, maka Anda dapat mempertimbangkan model komunikasi yang diperlukan antara VPC bersama dengan jumlah VPC yang diperlukan untuk dihubungkan ke koneksi VPN untuk membantu Anda membuat keputusan.

Keandalan

Definisi

Keandalan mengacu pada kemampuan layanan atau sistem untuk melakukan fungsi yang diharapkan bila diperlukan. Keandalan suatu sistem dapat diukur dengan tingkat kualitas operasionalnya dalam jangka waktu tertentu. Bandingkan ini dengan ketahanan, yang mengacu pada kemampuan sistem untuk pulih dari gangguan infrastruktur atau layanan, secara dinamis dan andal.

Untuk detail lebih lanjut tentang bagaimana ketersediaan dan ketahanan digunakan untuk mengukur keandalan, lihat Pilar Keandalan Kerangka Well-Architected AWS .

Pertanyaan kunci

Ketersediaan

Ketersediaan adalah persentase waktu beban kerja tersedia untuk digunakan. Target umum termasuk 99% (3.65 hari downtime diperbolehkan per tahun), 99,9% (8,77 jam), dan 99,99% (52,6 menit), dengan singkatan dari jumlah sembilan dalam persentase (“dua sembilan” untuk 99%, “tiga sembilan” untuk 99,9%, dan seterusnya). Ketersediaan solusi jaringan antara AWS dan pusat data lokal mungkin berbeda dari solusi keseluruhan atau ketersediaan aplikasi.

Pertanyaan kunci untuk ketersediaan solusi jaringan meliputi:

- Dapatkah AWS sumber daya saya terus beroperasi jika sumber daya tidak dapat berkomunikasi dengan sumber daya lokal saya? Begitu juga sebaliknya?
- Haruskah saya mempertimbangkan waktu henti terjadwal untuk pemeliharaan terencana sebagai disertakan atau dikecualikan dari metrik ketersediaan?
- Bagaimana saya mengukur ketersediaan lapisan jaringan, terpisah dari kesehatan aplikasi secara keseluruhan?

Bagian Ketersediaan dari Pilar Keandalan Kerangka Well-Architected memiliki saran dan rumus untuk ketersediaan perhitungan.

Ketahanan

Ketahanan adalah kemampuan beban kerja untuk pulih dari gangguan infrastruktur atau layanan, memperoleh sumber daya komputasi secara dinamis untuk memenuhi permintaan, dan mengurangi gangguan, seperti kesalahan konfigurasi atau masalah jaringan sementara. Jika komponen jaringan yang berlebihan (tautan, perangkat jaringan, dan sebagainya) tidak memiliki ketersediaan yang

cukup untuk menyediakan fungsi yang diharapkan sendiri, maka ia memiliki ketahanan yang rendah terhadap kegagalan. Konsekuensinya adalah pengalaman pengguna yang buruk dan terdegradasi.

Pertanyaan kunci untuk ketahanan solusi jaringan meliputi:

- Berapa banyak kegagalan simultan dan diskrit yang harus saya izinkan?
- Bagaimana saya bisa mengurangi satu titik kegagalan dengan solusi konektivitas dan jaringan internal saya?
- Apa kerentanan saya terhadap peristiwa penolakan layanan terdistribusi (DDoS)?

Solusi teknis

Pertama, penting untuk dicatat bahwa tidak setiap solusi konektivitas jaringan hybrid memerlukan tingkat keandalan yang tinggi, dan bahwa peningkatan tingkat keandalan memiliki peningkatan biaya yang sesuai. Dalam beberapa skenario, situs utama mungkin memerlukan koneksi yang andal (berlebihan dan tangguh) karena downtime memiliki dampak yang lebih tinggi pada bisnis, sementara situs regional, mungkin tidak memerlukan tingkat keandalan yang sama karena dampak yang lebih rendah pada bisnis jika terjadi peristiwa kegagalan. Disarankan untuk merujuk pada Rekomendasi AWS Direct Connect Ketahanan karena menjelaskan praktik AWS terbaik untuk memastikan ketahanan tinggi dengan desain. AWS Direct Connect

Untuk mencapai solusi konektivitas jaringan hybrid yang andal dalam konteks ketahanan, desain perlu mempertimbangkan aspek-aspek berikut:

- Redundansi: Bertujuan untuk menghilangkan satu titik kegagalan dalam jalur konektivitas jaringan hybrid, termasuk namun tidak terbatas pada koneksi jaringan, perangkat jaringan tepi, redundansi di seluruh Availability Zones, dan lokasi DX Wilayah AWS, dan sumber daya perangkat, jalur serat, dan sistem operasi. Untuk tujuan dan ruang lingkup whitepaper ini, redundansi berfokus pada koneksi jaringan, perangkat tepi (misalnya, perangkat gateway pelanggan), lokasi AWS DX, dan Wilayah AWS (untuk arsitektur Multi-wilayah).
- Komponen failover yang andal: Dalam beberapa skenario, sistem mungkin berfungsi, tetapi tidak menjalankan fungsinya pada tingkat yang diperlukan. Situasi seperti itu biasa terjadi selama peristiwa kegagalan tunggal di mana ditemukan bahwa komponen redundan yang direncanakan beroperasi secara non-redundan - beban jaringan mereka tidak memiliki tempat lain untuk dituju karena penggunaan, yang mengakibatkan kapasitas yang tidak mencukupi untuk seluruh solusi.
- Failover time: Failover time adalah waktu yang dibutuhkan komponen sekunder untuk sepenuhnya mengambil alih peran komponen utama. Failover time memiliki beberapa faktor — berapa lama

waktu yang dibutuhkan untuk mendeteksi kegagalan, berapa lama untuk mengaktifkan konektivitas sekunder, dan berapa lama untuk memberi tahu sisa jaringan tentang perubahan. Deteksi kegagalan dapat ditingkatkan menggunakan Dead Peer Detection (DPD) untuk tautan VPN, dan Deteksi Penerusan Dua Arah (BFD) untuk tautan. AWS Direct Connect Waktu untuk mengaktifkan konektivitas sekunder bisa sangat rendah (jika koneksi ini selalu aktif), mungkin jendela waktu yang singkat (jika koneksi VPN pra-konfigurasi perlu diaktifkan), atau lebih lama (jika sumber daya fisik perlu dipindahkan atau sumber daya baru dikonfigurasi). Memberitahu sisa jaringan biasanya terjadi melalui protokol routing di dalam jaringan pelanggan, yang masing-masing memiliki waktu konvergensi yang berbeda dan pilihan untuk konfigurasi — konfigurasi ini berada di luar lingkup whitepaper ini.

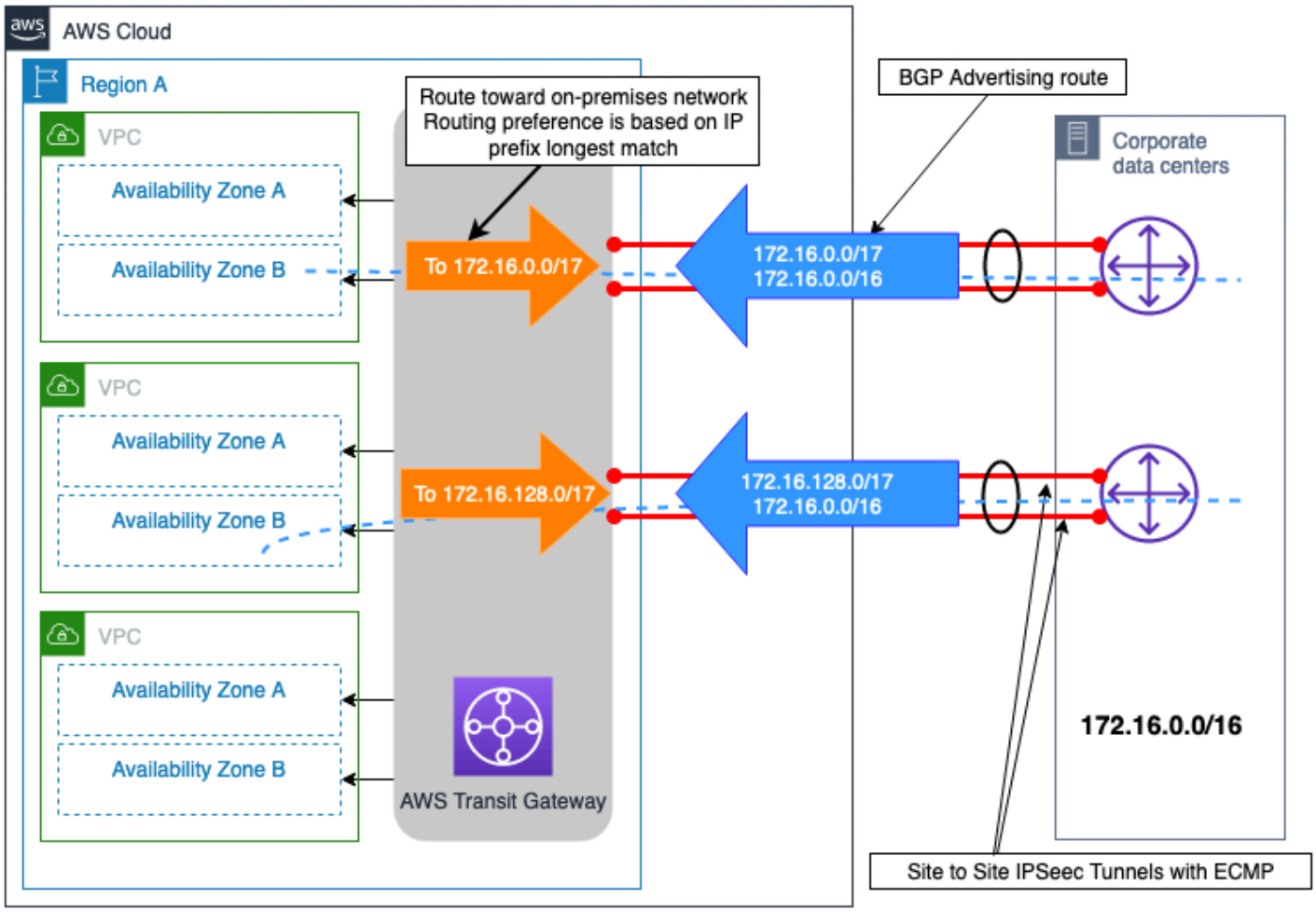
- Rekayasa Lalu Lintas: Rekayasa lalu lintas dalam konteks desain konektivitas jaringan hibrida yang tangguh bertujuan untuk mengatasi bagaimana lalu lintas harus mengalir melalui beberapa koneksi yang tersedia dalam skenario normal dan kegagalan. Disarankan untuk mengikuti konsep desain untuk kegagalan, di mana Anda perlu melihat bagaimana solusi akan beroperasi dalam skenario kegagalan yang berbeda dan apakah itu akan dapat diterima oleh bisnis atau tidak. Bagian ini membahas beberapa kasus penggunaan teknik lalu lintas umum yang bertujuan untuk meningkatkan tingkat ketahanan keseluruhan dari solusi konektivitas jaringan hibrida. AWS Direct Connect Bagian tentang routing dan BGP berbicara tentang beberapa opsi rekayasa lalu lintas untuk mempengaruhi arus lalu lintas (komunitas, preferensi lokal BGP, AS Path length). Untuk merancang solusi rekayasa lalu lintas yang efektif, Anda harus memiliki pemahaman yang baik tentang bagaimana masing-masing komponen AWS jaringan menangani perutean IP dalam hal evaluasi dan pemilihan rute, serta mekanisme yang mungkin untuk mempengaruhi pemilihan rute. Rinciannya berada di luar cakupan dokumen ini. Untuk informasi selengkapnya, lihat Urutan Evaluasi Rute Transit Gateway, Prioritas Rute VPN Site-to-Site, dan dokumentasi Routing Direct Connect dan BGP sesuai kebutuhan.

> **Note**
>
> Di tabel rute VPC, Anda dapat mereferensikan daftar awalan yang memiliki aturan pemilihan rute tambahan. Untuk informasi selengkapnya tentang kasus penggunaan ini, lihat prioritas rute untuk daftar awalan. AWS Transit Gateway tabel rute juga mendukung daftar awalan, tetapi setelah diterapkan mereka diperluas ke entri rute tertentu.

Koneksi VPN Site-to-Site ganda dengan contoh rute yang lebih spesifik

Skenario ini didasarkan pada situs lokal kecil yang terhubung ke satu Wilayah AWS melalui koneksi VPN redundan melalui internet. AWS Transit Gateway Desain teknik lalu lintas yang digambarkan pada Gambar 10 menunjukkan bahwa dengan rekayasa lalu lintas Anda dapat memengaruhi pemilihan jalur yang meningkatkan keandalan solusi konektivitas hibrida dengan:

- Konektivitas hybrid tangguh: Koneksi VPN redundan masing-masing memberikan kapasitas kinerja yang sama, mendukung failover otomatis dengan menggunakan protokol perutean dinamis (BGP), dan mempercepat deteksi kegagalan koneksi dengan menggunakan deteksi rekan mati VPN.
- Efisiensi kinerja: Mengkonfigurasi ECMP di kedua koneksi VPN untuk AWS Transit Gateway membantu memaksimalkan bandwidth koneksi VPN secara keseluruhan. Atau, dengan mengiklankan rute yang berbeda, lebih spesifik, bersama dengan rute ringkasan situs, pemuatan dapat dikelola secara independen di dua koneksi VPN



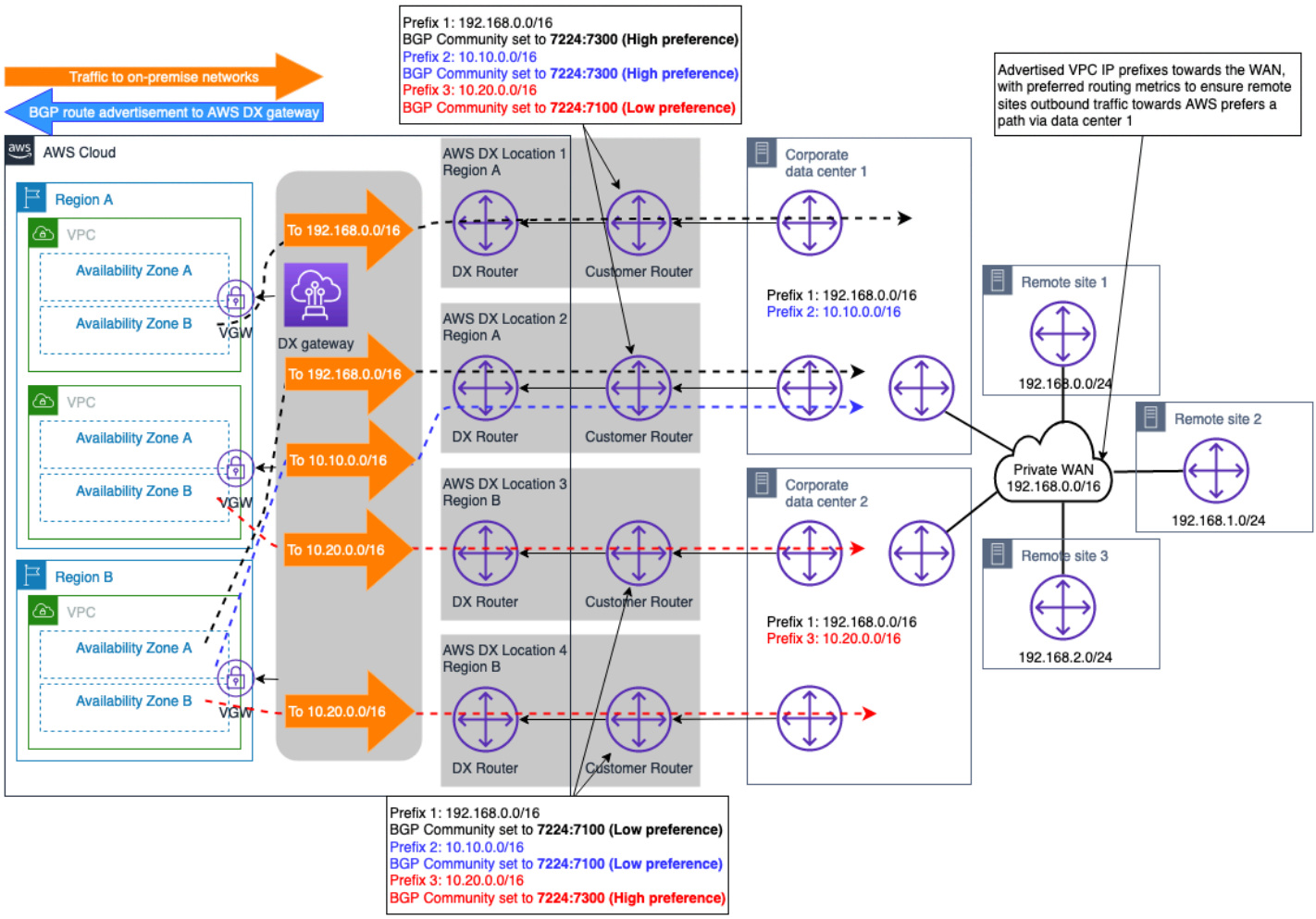
Gambar 10 — Koneksi VPN Site-to-Site Ganda dengan contoh rute yang lebih spesifik

Situs lokal ganda dengan beberapa contoh koneksi DX

Skenario yang diilustrasikan pada Gambar 11 menunjukkan dua situs pusat data lokal yang terletak di Wilayah geografis yang berbeda, dan terhubung AWS menggunakan model konektivitas Ketahanan Maksimum (dijelaskan dalam Rekomendasi Ketahanan) menggunakan dengan DXGW dan AWS Direct Connect VGW. AWS Direct Connect Kedua situs lokal ini saling berhubungan satu sama lain melalui tautan interkoneksi pusat data (DCI). Awalan IP lokal (192.168.0.0/16) milik situs cabang jarak jauh diiklankan dari kedua situs pusat data lokal. Jalur utama untuk awalan ini harus pusat data 1. Lalu lintas ke dan dari situs cabang jarak jauh akan gagal ke pusat data 2 jika terjadi kegagalan pusat data 1 atau kedua lokasi DX. Juga, ada awalan IP khusus situs untuk setiap pusat data. Awalan ini perlu dicapai secara langsung, dan melalui situs pusat data lainnya jika terjadi kegagalan kedua lokasi DX.

Dengan mengaitkan atribut Komunitas BGP dengan rute yang diiklankan ke AWS DXGW, Anda dapat memengaruhi pemilihan jalur keluar dari sisi DXGW. AWS Atribut komunitas ini mengontrol atribut AWS Preferensi Lokal BGP yang ditetapkan ke rute yang diiklankan. Untuk informasi lebih lanjut, lihat kebijakan AWS DX Routing dan komunitas BGP.

Untuk memaksimalkan keandalan konektivitas pada Wilayah AWS tingkat tersebut, setiap pasangan koneksi AWS DX mengkonfigurasi ECMP sehingga keduanya dapat digunakan pada saat yang sama untuk transfer data antara setiap situs lokal dan. AWS



Gambar 11 — Situs lokal ganda dengan beberapa contoh koneksi DX

Dengan desain ini, arus lalu lintas yang ditujukan ke jaringan lokal (dengan panjang awalan yang diiklankan dan komunitas BGP yang sama) akan didistribusikan di seluruh koneksi DX ganda per situs menggunakan ECMP. Namun, jika ECMP tidak diperlukan di seluruh koneksi DX, konsep yang sama dibahas sebelumnya dan dijelaskan dalam kebijakan Routing dan dokumentasi komunitas BGP dapat digunakan untuk merekayasa lebih lanjut pemilihan jalur pada tingkat koneksi DX.

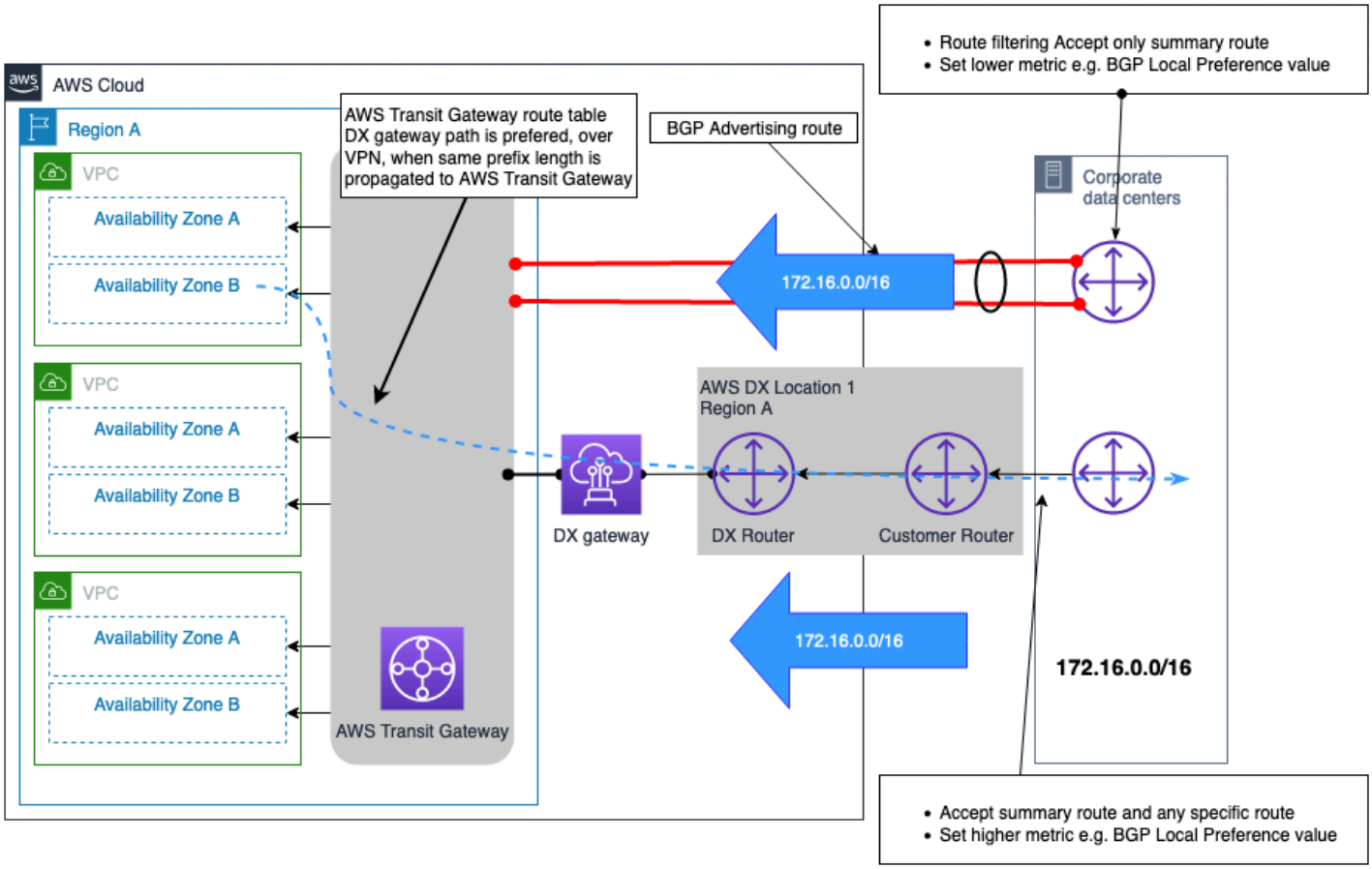
Catatan: Jika ada perangkat keamanan di jalur dalam pusat data lokal, perangkat ini perlu dikonfigurasi untuk memungkinkan arus lalu lintas meninggalkan satu tautan DX dan berasal dari tautan DX lainnya (kedua tautan digunakan dengan ECMP) dalam situs pusat data yang sama.

Koneksi VPN sebagai cadangan ke contoh koneksi AWS DX

VPN dapat dipilih untuk menyediakan koneksi jaringan cadangan ke AWS Direct Connect koneksi. Biasanya, model konektivitas jenis ini didorong oleh biaya, karena memberikan tingkat keandalan yang lebih rendah untuk solusi konektivitas hybrid secara keseluruhan karena kinerja indeterministik melalui internet, dan tidak ada SLA yang dapat diperoleh untuk koneksi melalui internet publik. Ini adalah model konektivitas yang valid dan hemat biaya, dan harus digunakan ketika biaya adalah pertimbangan prioritas utama dan ada anggaran terbatas, atau mungkin sebagai solusi sementara sampai DX sekunder dapat disediakan. Gambar 12 mengilustrasikan desain model konektivitas ini. Salah satu pertimbangan utama dengan desain ini, di mana koneksi VPN dan DX berakhir di AWS Transit Gateway, adalah bahwa koneksi VPN dapat mengiklankan jumlah rute yang lebih tinggi dibandingkan dengan yang dapat diiklankan melalui koneksi DX yang terhubung ke. AWS Transit Gateway Hal ini dapat menyebabkan situasi routing suboptimal. Opsi untuk mengatasi masalah ini adalah mengonfigurasi pemfilteran rute di perangkat gateway pelanggan (CGW) untuk rute yang diterima dari koneksi VPN, yang memungkinkan hanya rute ringkasan yang akan diterima.

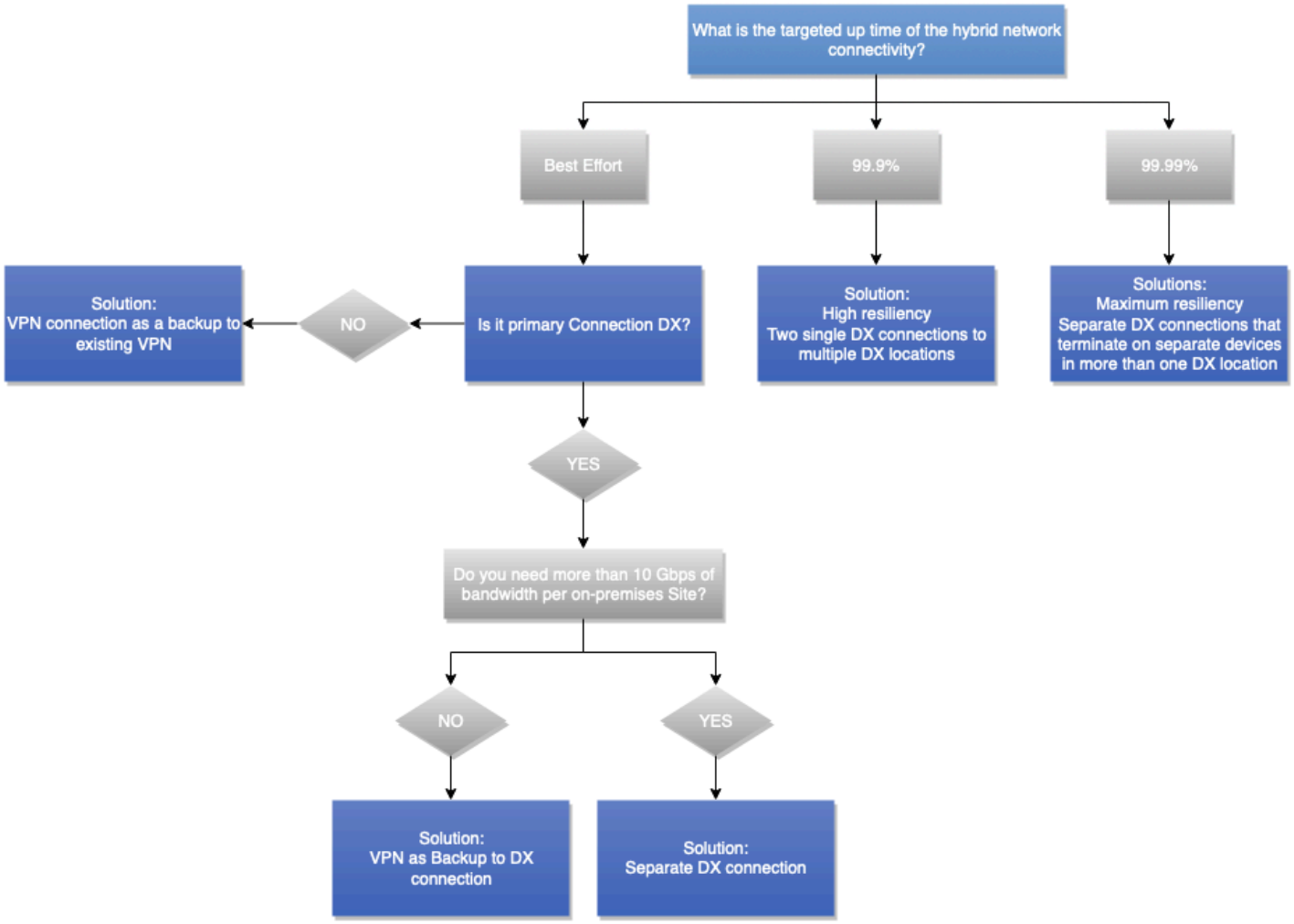
Catatan: Untuk membuat rute ringkasan pada AWS Transit Gateway, Anda perlu menentukan rute statis ke lampiran arbitrer dalam tabel AWS Transit Gateway rute sehingga ringkasan dikirim sepanjang rute yang lebih spesifik.

Dari sudut pandang tabel AWS Transit Gateway perutean, rute untuk awalan lokal diterima baik dari koneksi AWS DX (melalui DXGW) maupun dari VPN, dengan panjang awalan yang sama. Mengikuti logika prioritas AWS Transit Gateway, rute yang diterima melalui Direct Connect memiliki preferensi yang lebih tinggi daripada yang diterima melalui Site-to-Site VPN, dan dengan demikian jalur di AWS Direct Connect atas akan lebih disukai untuk menjangkau jaringan lokal.



Gambar 12 — Koneksi VPN sebagai cadangan ke contoh koneksi AWS DX

Pohon keputusan berikut memandu Anda membuat keputusan yang diinginkan untuk mencapai konektivitas jaringan hybrid yang tangguh (yang akan menghasilkan konektivitas jaringan hybrid yang andal). Untuk informasi lebih lanjut, lihat AWS Direct Connect Resiliency Toolkit.



Gambar 13 — Pohon keputusan keandalan

VPN dan SD-WAN yang dikelola pelanggan

Definisi

Konektivitas ke internet merupakan komoditas dan bandwidth yang tersedia terus meningkat setiap tahunnya. Beberapa pelanggan memilih untuk membangun WAN virtual di atas internet daripada membangun dan mengoperasikan WAN pribadi. Jaringan area luas yang ditentukan perangkat lunak (SD-WAN) memungkinkan perusahaan untuk dengan cepat menyediakan dan mengelola WAN virtual ini secara terpusat melalui penggunaan perangkat lunak yang cerdas. Pelanggan lain memilih untuk mengadopsi situs yang dikelola sendiri tradisional ke situs VPN.

Dampak pada keputusan desain

SD-WAN dan VPN yang dikelola pelanggan dapat berjalan melalui internet atau. AWS Direct Connect SD-WAN (atau hamparan VPN perangkat lunak apa pun) dapat diandalkan seperti transportasi jaringan yang mendasarinya. Oleh karena itu, pertimbangan keandalan dan SLA yang dibahas sebelumnya dalam whitepaper ini berlaku di sini. Misalnya, membangun overlay SD-WAN melalui internet tidak akan menawarkan keandalan yang sama dibandingkan jika itu dibangun di atas. AWS Direct Connect

Definisi persyaratan

- Apakah Anda menggunakan SD-WAN di jaringan lokal Anda?
- Apakah ada fitur khusus yang Anda perlukan yang hanya tersedia pada peralatan virtual tertentu yang digunakan untuk penghentian VPN?

Solusi teknis

AWS merekomendasikan mengintegrasikan SD-WAN dengan AWS Transit Gateway, dan menerbitkan daftar vendor yang mendukung integrasi. AWS Transit Gateway AWS dapat bertindak sebagai hub untuk situs SD-WAN atau sebagai situs bicara. AWS Tulang punggung dapat digunakan untuk menghubungkan berbagai hub SD-WAN yang digunakan AWS dengan jaringan yang sangat andal dan berkinerja. Solusi SD-WAN mendukung failover otomatis melalui jalur yang tersedia, pemantauan tambahan, dan kemampuan observabilitas dalam satu panel manajemen. Penggunaan konfigurasi dan otomatisasi otomatis yang ekstensif memungkinkan penyediaan dan visibilitas yang cepat dibandingkan dengan WAN tradisional. Namun, penggunaan overhead tunneling dan enkripsi tidak sebanding dengan tautan serat khusus berkecepatan tinggi yang digunakan dalam konektivitas pribadi.

Dalam beberapa kasus, Anda dapat memilih untuk menggunakan alat virtual dengan kemampuan VPN. Alasan memilih alat virtual yang dikelola sendiri mencakup fitur teknis dan kompatibilitas dengan jaringan Anda yang lain. Ketika Anda memilih VPN yang dikelola sendiri atau solusi SD-WAN yang menggunakan alat virtual yang digunakan dalam instans EC2, Anda bertanggung jawab atas pengelolaan alat tersebut. Anda juga bertanggung jawab atas ketersediaan tinggi dan kegagalan antara peralatan virtual. Desain seperti itu meningkatkan tanggung jawab operasional Anda; Namun, itu bisa memberi Anda lebih banyak fleksibilitas. Fitur dan kemampuan solusi tergantung pada alat virtual yang Anda pilih.

AWS Marketplace berisi banyak peralatan virtual VPN yang dapat digunakan pelanggan di Amazon EC2. AWS merekomendasikan memulai dengan VPN S2S AWS terkelola dan lihat opsi lain jika tidak memenuhi persyaratan Anda. Overhead manajemen peralatan virtual adalah tanggung jawab pelanggan.

Contoh kasus penggunaan otomotif Corp

Bagian whitepaper ini menunjukkan bagaimana pertimbangan, pertanyaan definisi persyaratan, dan pohon keputusan digunakan untuk membantu Anda memutuskan desain jaringan hibrida yang optimal. Mengidentifikasi dan menangkap persyaratan penting karena digunakan sebagai masukan ke pohon keputusan. Menangkap persyaratan di muka menghindari iterasi desain lebih lanjut. Menghentikan proyek sama sekali jika desain harus ditinjau kembali dan memiliki sumber daya berharga yang ditunda dapat diminimalkan dan idealnya dihindari ketika persyaratan dipahami di muka.

Contoh Corp Automotive akan digunakan di seluruh bagian ini sebagai pelanggan ilustratif. Mereka mencari untuk awalnya menyebarkan proyek analitik pertama mereka diAWS. Proyek analitik difokuskan pada analisis data dari mobil yang diproduksi oleh perusahaan dan kumpulan data lain yang sudah ada di pusat data perusahaan. Awalnya, grup arsitektur perusahaan berpikir mereka akan membutuhkan, VPC AmazonAkun AWS, dan beberapa subnet untuk menjadi tuan rumah lingkungan produksi dan pengembangan. Tim proyek sangat ingin memulai, dan mereka meminta akses lingkungan pengembangan sesegera mungkin. Mereka bertujuan untuk masuk produksi tiga bulan dari sekarang.

Contoh Corp Automotive juga berencana untuk digunakan AWS untuk beberapa proyek tambahan, seperti memigrasikan sistem ERP mereka, Virtual Desktop Infrastructure (VDI), dan 20 aplikasi lainnya dari lokal hingga AWS selama 6 bulan ke depan. Beberapa persyaratan untuk proyek tambahan masih ditentukan, tetapi jelas bahwa AWS Cloud penggunaannya akan tumbuh.

Tim arsitektur memutuskan untuk memanfaatkan pendekatan yang diuraikan dalam whitepaper ini. Mereka menggunakan pertanyaan definisi persyaratan yang diuraikan di bawah setiap pertimbangan untuk menangkap masukan untuk membuat keputusan desain mereka.

Mereka mulai dengan persyaratan yang terkait dengan jenis konektivitas yang dirangkum dalam tabel berikut.

Tabel 4 — Contoh input keandalan Automotive Corp

Pertimbangan pemilihan tipe konektivitas	Pertanyaan definisi persyaratan	Jawaban
Saatnya Menyebarkan	Apa timeline yang diperlukan untuk penerapan? Jam, hari, minggu, atau bulan?	• Dev/Test: 1 bulan • Produksi: 3 bulan
Keamanan	Apakah persyaratan dan kebijakan keamanan Anda memungkinkan penggunaan koneksi terenkripsi melalui internet untuk terhubung AWS atau mengamanatkan penggunaan koneksi jaringan pribadi?	• Dev/Test: Site-to-Site VPN dapat diterima • Produksi: Diperlukan jaringan pribadi
	Saat memanfaatkan koneksi jaringan pribadi, apakah lapisan jaringan harus menyediakan enkripsi saat transit?	Tidak, enkripsi lapisan aplikasi akan digunakan.
SLA	Apakah konektivitas hybrid SLA dengan kredit layanan diperlukan?	• Dev/Test: Tidak • Produksi: Ya
	Apa target uptime?	• Dev/Uji: N/A • Produksi: 99,99%
	Apakah seluruh jaringan hybrid mematuhi target uptime?	• Dev/Uji: N/A • Produksi: Ya
Kinerja	Apa throughput yang dibutuhkan?	• Dev/Uji: 100 Mbps • Produksi: 500 Mbps tumbuh menjadi 2 Gbps

Pertimbangan pemilihan tipe konektivitas	Pertanyaan definisi persyaratan	Jawaban
	Berapa latensi maksimum yang dapat diterima antara AWS dan jaringan lokal?	• Dev/Test: Tidak ada persyaratan sulit • Produksi: Kurang dari 30 ms
	Apa jitter jaringan maksimum yang dapat diterima?	• Dev/Test: Tidak ada persyaratan sulit • Produksi: Diperlukan jitter minimum
Biaya	Berapa banyak data yang akan Anda kirim AWS per bulan?	• Dev/Tes: 2 TB • Produksi: 20 TB tumbuh hingga 50 TB
	Berapa banyak data yang akan Anda kirim AWS per bulan?	• Dev/Tes: 1 TB • Produksi: 10 TB tumbuh hingga 25 TB
	Apakah konektivitas ini permanen?	Ya

Berdasarkan persyaratan yang diterima, tim arsitektur mengikuti pohon keputusan tipe konektivitas dari Gambar 9. Ini memungkinkan tim arsitektur untuk memutuskan jenis konektivitas untuk pengembangan dan pengujian dan lingkungan produksi. Untuk lingkungan produksi, mereka mempertimbangkan persyaratan langsung serta yang akan datang. Untuk pengembangan dan pengujian Contoh Corp Automotive akan membuat site-to-site VPN melalui internet. Untuk produksi, mereka akan bekerja dengan penyedia layanan untuk menghubungkan jaringan perusahaan merekaAWS Direct Connect. Contoh Corp Automotive awalnya mempertimbangkan untuk menggunakan Direct Connect Hosted Connect, namun karena persyaratan untuk SLA yang AWS disediakan, mereka memilih Direct Connect Dedicated Connections.

Setelah memutuskan jenis konektivitas, langkah selanjutnya adalah menangkap persyaratan yang memengaruhi pemilihan desain konektivitas. Ini terkait dengan desain logis, seperti bagaimana

koneksi dikonfigurasi dan AWS layanan mana yang digunakan untuk mendukung persyaratan bisnis dan teknis.

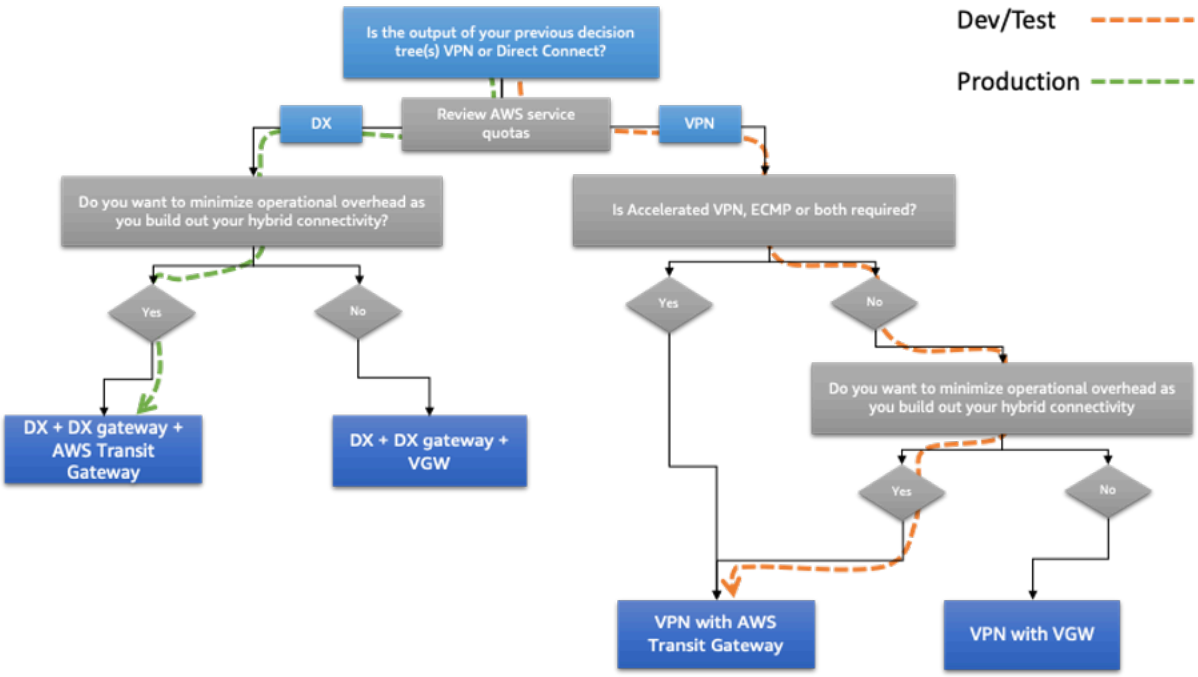
Untuk menangkap persyaratan skalabilitas dan model komunikasi, tim arsitektur menggunakan pertanyaan definisi persyaratan dari bagian terkait dari whitepaper ini. Persyaratan yang terkait dengan kedua pertimbangan tersebut dirangkum dalam tabel berikut.

Tabel 5 - Pertanyaan definisi persyaratan

Pertimbangan pemilihan desain konektivitas	Pertanyaan definisi persyaratan	Jawaban
Skalabilitas	Berapa jumlah VPC saat ini atau yang diantisipasi yang memerlukan konektivitas ke situs lokal?	2 awalnya, tumbuh menjadi 30 dalam 6 bulan
	Apakah VPC ini digunakan dalam satu Wilayah AWS atau beberapa Wilayah?	Wilayah Tunggal
	Berapa banyak situs lokal yang perlu dihubungkan? AWS	2 pusat data
	Berapa banyak perangkat gateway pelanggan yang Anda miliki, per situs, yang perlu terhubungAWS?	2 router per pusat data
	Berapa banyak rute yang diharapkan akan diiklankan ke AWS VPC serta jumlah rute yang diharapkan akan diterima dari samping? AWS	• Rute yang akan diiklankan ke AWS: 20 rute • Rute yang akan diterima dari AWS: 1 /16 rute
	Apakah ada rencana untuk mempertimbangkan peningkat	• Dev/Uji: 100 Mbps • Produksi: 500Mbps tumbuh menjadi 2Gbps.

Pertimbangan pemilihan desain konektivitas	Pertanyaan definisi persyaratan	Jawaban
	an bandwidth koneksi ke AWS dalam waktu dekat?	
Model desain konektivitas	Apakah ada persyaratan agar komunikasi antar-VPC diaktifkan (dalam Wilayah dan/atau lintas Wilayah)?	Ya, dalam Wilayah AWS
	Apakah ada persyaratan untuk mengakses layanan titik akhir AWS publik langsung dari lokal?	Ya
	Apakah ada persyaratan untuk mengakses AWS layanan menggunakan titik akhir VPC dari tempat?	Tidak

Berdasarkan masukan, tim arsitektur mengikuti pohon keputusan dari bagian Desain Konektivitas. Setelah mengantisipasi bahwa jumlah VPC akan tumbuh dari 2 menjadi 30 dalam 6 bulan ke depan, tim arsitektur memutuskan untuk menggunakan AWS Transit Gateway sebagai gateway terminasi untuk koneksi dan untuk perutean antar-VPC. Independent AWS Transit Gateway s akan menghentikan koneksi VPN yang digunakan untuk pengembangan dan pengujian, dan untuk konektivitas produksi denganAWS Direct Connect. Penggunaan AWS Transit Gateway s terpisah membuat manajemen perubahan lebih sederhana dan memberikan demarkasi yang jelas antara dev/test dan lingkungan produksi. Untuk produksi, AWS Direct Connect gateway diperlukan karenaAWS Transit Gateway. VIF publik akan digunakan untuk akses ke layanan endpoint AWS publik. Gambar 14 mengilustrasikan jalur yang diambil pada pohon keputusan berdasarkan persyaratan yang dikumpulkan.



Gambar 14 — Contoh pohon keputusan desain koneksi otomotif Corp.

Setelah memutuskan solusi untuk memenuhi persyaratan model skalabilitas dan komunikasi, langkah selanjutnya adalah menangkap persyaratan yang terkait dengan keandalan. Ini terkait dengan tingkat ketersediaan dan ketahanan yang diperlukan.

Untuk menangkap persyaratan keandalan, tim arsitektur menggunakan pertanyaan definisi persyaratan dari bagian terkait dari whitepaper ini. Persyaratan dirangkum dalam tabel berikut.

Tabel 6 - Pertanyaan persyaratan keandalan

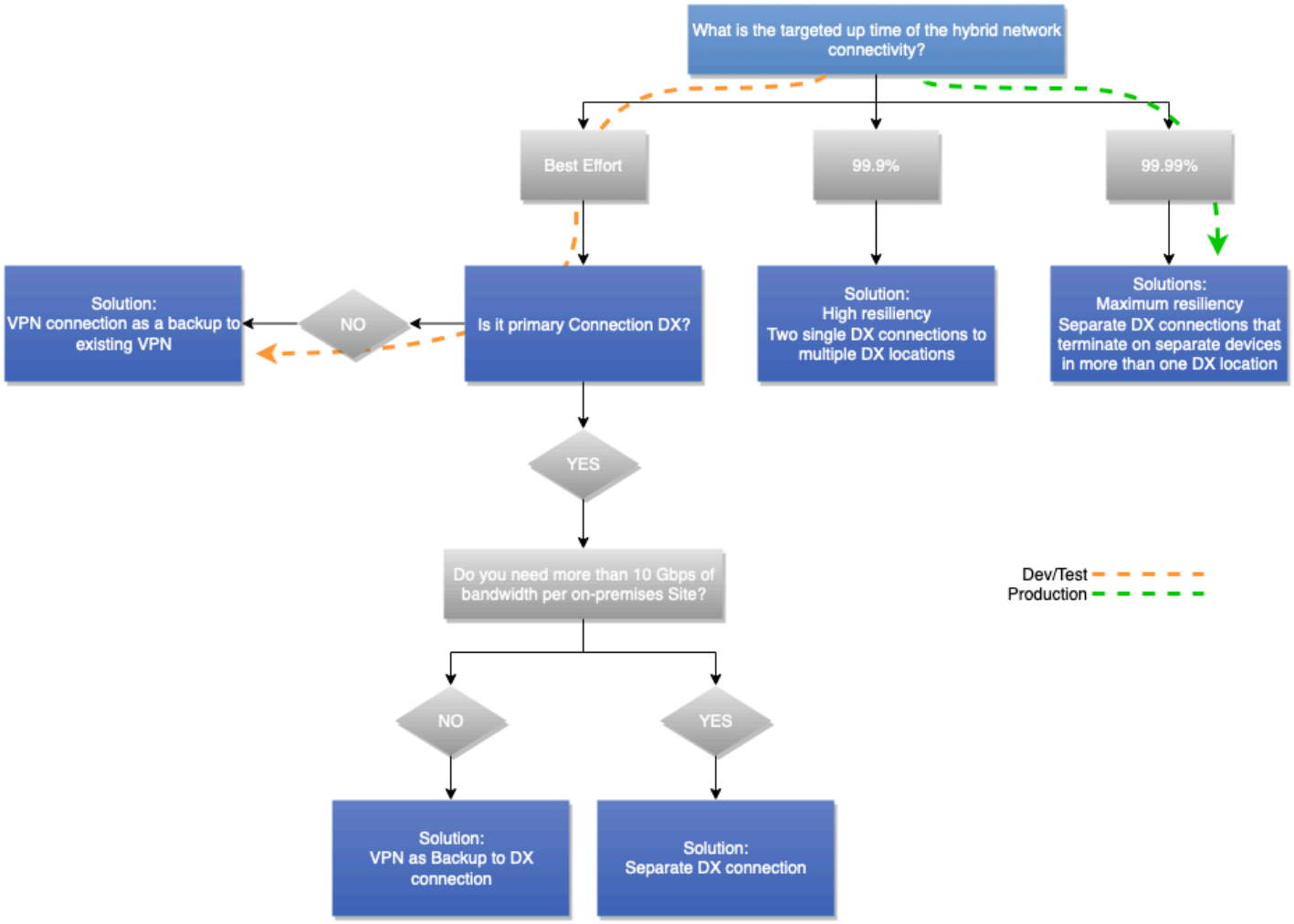
Pertimbangan pemilihan desain konektivitas	Pertanyaan definisi persyaratan	Jawaban
Keandalan	Berapa besarnya dampak pada bisnis jika terjadi kegagalan konektivitasAWS?	• Dev/Test: Rendah • Produksi: Tinggi
	Dari sudut pandang bisnis, apakah biaya mengikuti kegagalan konektivitas AWS lebih besar daripada biaya	• Dev/Test: Tidak • Produksi: Ya

Pertimbangan pemilihan desain konektivitas	Pertanyaan definisi persyaratan	Jawaban
	penerapan model konektivitas yang sangat andal? AWS	

Berdasarkan masukan yang diterima, tim arsitektur mengikuti pohon keputusan dari bagian pertimbangan keandalan yang dibahas sebelumnya pada whitepaper ini. Setelah mempertimbangkan target uptime 99,99% untuk konektivitas produksi dan dampak bisnis yang tinggi jika terjadi gangguan layanan, tim arsitektur memutuskan untuk menggunakan 2 lokasi Direct Connect dan memiliki 2 tautan dari setiap pusat data lokal ke setiap lokasi Direct Connect (total 4 tautan). Konektivitas VPN yang digunakan untuk pengembangan dan pengujian juga akan menggunakan dua koneksi VPN untuk redundansi tambahan. Menggunakan teknik rekayasa rute yang dibahas di bagian keandalan, konektivitas akan dikonfigurasi sebagai berikut:

- Untuk pengembangan dan pengujian, lalu lintas akan diseimbangkan beban menggunakan ECMP melalui 2 terowongan menuju pusat data utama. Ini memungkinkan throughput yang lebih tinggi. Terowongan yang menuju ke pusat data sekunder akan digunakan jika terjadi kegagalan terowongan utama.
- Untuk produksi, latensi antara lokal dan AWS di salah satu lokasi Direct Connect sangat mirip. Dalam hal ini, telah diputuskan untuk memuat keseimbangan lalu lintas antara AWS dan lokal melalui dua koneksi yang menuju ke pusat data utama untuk sistem lokal yang digunakan di pusat data utama. Demikian pula, untuk sistem lokal yang berjalan di pusat data sekunder, lalu lintas akan menjadi beban seimbang antara dua koneksi ke pusat data sekunder. Jika terjadi kegagalan koneksi, BGP akan memfasilitasi failover otomatis.

Gambar 15 mengilustrasikan jalur yang diambil pada pohon keputusan berdasarkan persyaratan yang dikumpulkan.



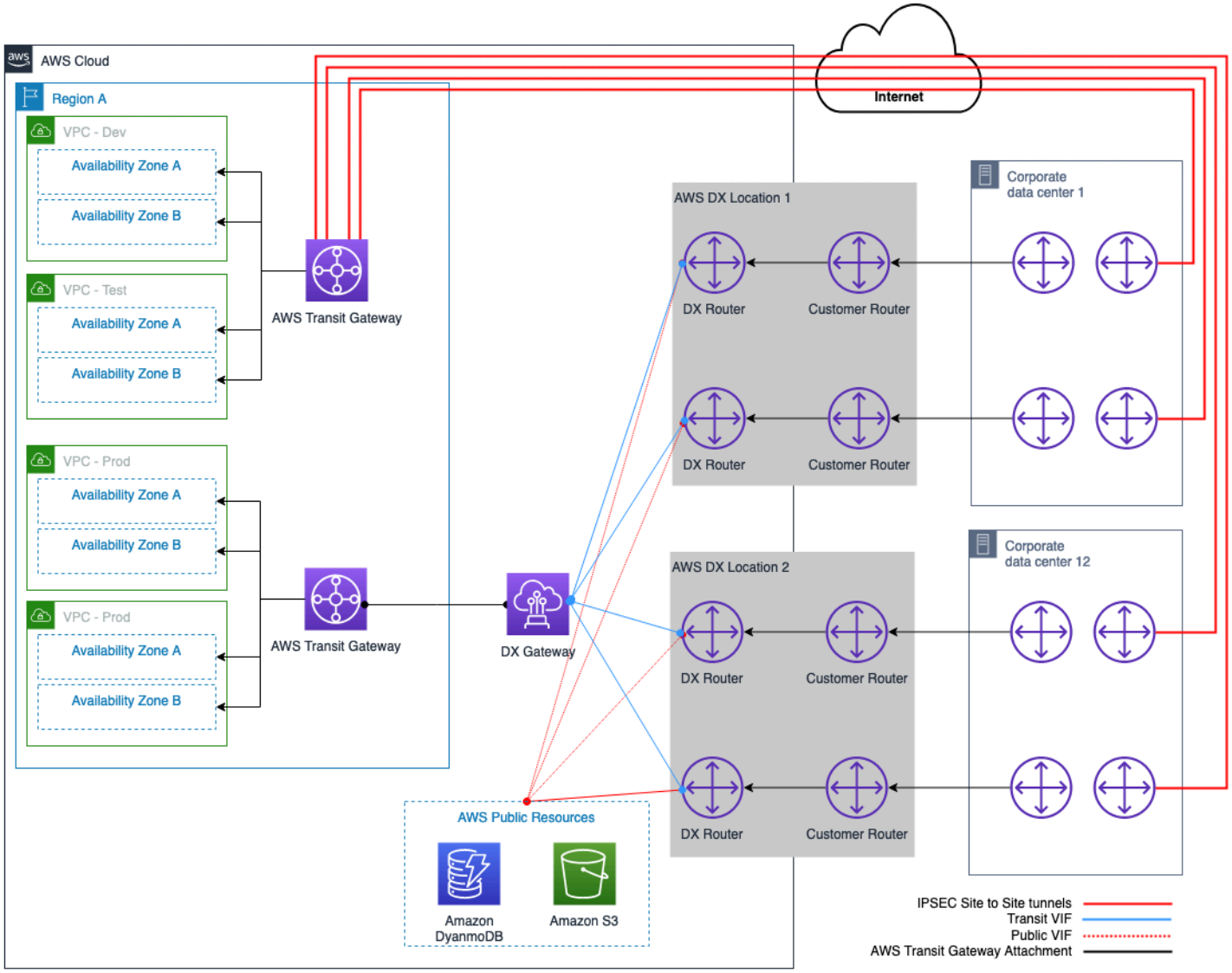
Gambar 15 — Contoh pohon keputusan keandalan otomotif Corp.

Arsitektur dipilih oleh Example Corp. Automotive

Diagram berikut menggambarkan arsitektur yang dipilih oleh Example Corp Automotive setelah mengumpulkan persyaratan dan menavigasi pohon keputusan yang tercakup dalam bagian sebelumnya dari whitepaper ini.

Ini menggunakan VPN AWS S2S melalui internet yang berakhir AWS Transit Gateway untuk pengembangan dan pengujian. Kemudian digunakan AWS Direct Connect dengan gateway Direct Connect dan yang kedua AWS Transit Gateway untuk lalu lintas produksi. AWS Transit Gatewaydigunakan untuk perutean antar-VPC. Dari perspektif jalur data, terowongan VPN untuk pusat data primer digunakan sebagai jalur utama untuk pengembangan dan pengujian, dengan terowongan ke pusat data sekunder digunakan sebagai jalur failover. Untuk lalu lintas produksi,

semua koneksi digunakan secara bersamaan. Lalu lintas dari AWS lebih memilih koneksi jaringan yang paling opsional berdasarkan pusat data di mana sistem lokal berada. Contoh Corp Automotive menggunakan teknik rekayasa rute serupa untuk memilih jalur yang sesuai ketika lalu lintas dikirim untuk AWS memastikan jalur lalu lintas simetris digunakan untuk meminimalkan penggunaan jaringan perusahaan antara pusat data primer dan sekunder lokal.



Gambar 16 — Contoh Corp. Otomotif memilih model konektivitas hibrida

Kesimpulan

Model konektivitas hybrid adalah salah satu titik awal mendasar untuk adopsi komputasi awan. Jaringan hybrid dapat dibangun dengan arsitektur optimal mengikuti proses pemilihan model konektivitas yang diuraikan dalam whitepaper ini.

Prosesnya terdiri dari pertimbangan yang diatur dalam urutan logis. Urutan ini sangat mirip dengan model mental yang diikuti oleh jaringan berpengalaman dan arsitek awan. Dalam setiap kelompok pertimbangan, pohon keputusan memungkinkan pemilihan model konektivitas yang cepat, bahkan dengan persyaratan input yang terbatas. Anda mungkin menemukan bahwa beberapa pertimbangan dan dampak yang sesuai menunjukkan solusi yang berbeda. Dalam kasus tersebut, sebagai pengambil keputusan, Anda mungkin perlu berkompromi pada beberapa persyaratan dan memilih solusi paling optimal yang memenuhi persyaratan bisnis dan teknis Anda.

Kontributor

Kontributor dokumen ini meliputi:

- James Devine, Arsitek Solusi Utama, Amazon Web Services
- Andrew Gray, Arsitek Solusi Utama - Jaringan, Amazon Web Services
- Maks Khomutskyi, Arsitek Solusi Senior, Amazon Web Services
- Marwan Al Shawi, Arsitek Solusi, Amazon Web Services
- Santiago Freitas, Kepala Teknologi, Amazon Web Services
- Evgeny Vaganov, Arsitek Solusi Spesialis - Jaringan, Amazon Web Services
- Tom Adamski, Arsitek Solusi Spesialis - Jaringan, Amazon Web Services
- Armstrong Onaiwu, Arsitek Solusi, Amazon Web Services

Bacaan lebih lanjut

- Membangun Infrastruktur Jaringan AWS Multi-VPC yang dapat Diskalakan dan Aman
- Opsi DNS Cloud Hybrid untuk Amazon VPC
- Opsi Konektivitas Aman Virtual Private Cloud Amazon Virtual
- Dokumentasi Awan Pribadi Virtual Amazon Virtual
- AWS Direct ConnectDokumentasi
- Apa perbedaan antara antarmuka virtual yang dihosting (VIF) dan koneksi yang dihosting?

Revisi dokumen

Untuk pemberitahuan tentang pembaruan laporan ini, berlangganan umpan RSS.

Perubahan	Deskripsi	Tanggal
Pembaruan kecil	Diperbarui untuk mencerminkan peningkatan batas kuota DX.	Juli 10, 2023
Pembaruan besar	Diperbarui untuk menggabungkan praktik, layanan, dan kemampuan terbaik terbaru.	Juli 6, 2023
Pembaruan kecil	Diagram arsitektur referensi yang diperbarui untuk mencerminkan perubahan kuota DX.	Juni 27, 2023
Pembaruan kecil	Memperbaiki tautan yang rusak.	Maret 22, 2022
Publikasi awal	Whitepaper pertama kali diterbitkan	22 September 2020

Pemberitahuan

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

AWSGlosarium

Untuk AWS terminologi terbaru, lihat AWSglosarium di Referensi. Glosarium AWS

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