VPC

AWSのネットワークサービスの中心はAmazon Virtual Private Cloud(以下VPC)である。

VPCは、利用者ごとのプライベートなネットワークをAWS内に作成する。

VPCはインターネットゲートウェイ(IGW)と呼ばれるインターネット側の出口を付けることにより、直接インターネットに出ていくことが可能。

また、オンプレミスの各拠点を繋げるために仮想プライベートゲートウェイ(VGW)を出口として、専用線のサービスであるDirect ConnectやVPN経由で直接的にインターネットに出ることなく各拠点と接続することも可能。

なお、S3やCloudWatch、DynamoDBなど、AWSの中にあるがVPC内に入れられないサービスも多数ある。

こういったサービスとVPC内のリソースをどのように連携するかは、設計上の重大なポイントとなる。

IPアドレス

VPCには、作成者が自由なIPアドレス(CIDRブロック)をアサインすることができる。

ネットワーク基盤の管理ポリシーに合わせたアドレスをアサインすることで、自社のネットワークの一部であるかのように

接続することが出来る。CIDRブロックは/16から/28の範囲で作成できる。

サブネットマスク

サブネットは、EC2インスタンスなどを起動するための、VPC内部に作るアドレスレンジである。

VPCに設定したCIDRブロックの範囲に収まる小さなCIDRブロックをアサインすることができる。

個々のサブネットには1つの仮想のルータがあり、このルータが後述するルートテーブルとネットワークACLの設定を持っていて、

サブネット内のEC2インスタンスのデフォルトゲートウェイになっている。

サブネットとAZ

サブネット作成時のポイントは、同一の役割を持ったサブネットを複数のAZにそれぞれ作ることである。

EC2やRDSの作成時にはAZをまたいで構築することで、AZ障害に対して耐久性の高い設計にすることが出来る。

この構成はマルチAZと呼ばれ、AWSにおける設計の基本となっている。

なお、パブリックサブネット(Public Subnet)、プライベートサブネット(Private Subnet)という概念がVPC関連のドキュメントにたびたび登場する。

しかし、サブネットの設定・機能としてそういったサブネットがあるわけではなく、

のちの、インターネットゲートウェイ、ルートテーブル、ネットワークACLなどを利用して、

そのような役割を割り当てるというだけである。

ルートテーブル

アドレス設計の次は、ルーティング設定である。

AWSのルーティング要素には、ルートテーブルと各種ゲートウェイがある。これらを用いてVPC内部の通信や、

インターネット・オンプレミスネットワーク基盤など外部への通信を実装していく。

- 個々のサブネットに1つずつ設定できる。
- 1つのルートテーブルを複数のサブネットで共有することはできるが、1つのサブネットに複数のルートテーブルを適用することはできない。
- 宛先アドレスとターゲットとなるゲートウェイ(ネクストホップ)を指定する。
- VPCにはメインルートテーブルがあり、サブネット作成時に指定しない場合のデフォルトのルートテーブルになる。

セキュリティグループとネットワークACL

VPCの通信制御は、セキュリティグループとネットワークACL(NACL)を利用して行う。

セキュリティグループはEC2、ELB、RDSなど、インスタンス単位の通信制御に利用される。

インスタンスには少なくとも１つのセキュリティグループをアタッチする必要がある。

通信の制御としては、インバウンド(内向き、外部からVPCへ)とアウトバウンド(外向き、内部から外部へ)の両方の制御が可能。

制御項目としては、プロトコル(TCPやUDPなど)とポート範囲、送受信先のCIDRかセキュリティグループを指定する。

特徴的なのは、CIDRなどのIPアドレスだけでなく、セキュリティグループを指定できる点である。

なお、セキュリティグループはデフォルトでアクセスを拒否し、設定された項目のみにアクセスを許可する。

ネットワークACL(アクセスコントロールリスト)は、サブネットごとの通信範囲に利用される。

制御できる項目はセキュリティグループと同様で、インバウンド/アウトバウンドの制御が可能、

また、送受信先のCIDRとポートを指定できるが、セキュリティグループと違って送受信先にはセキュリティグループの指定はできない。

ネットワークACLはデフォルトの状態では全ての通信を許可する。

セキュリティグループとネットワークACLの違いは、状態(ステート)を保持するかどうかである。

セキュリティグループはステートフルで、応答トラフィックはるーるにかんけいルールに関係なく通信が許可される。

これに対してネットワークACLはステートレスで、応答トラフィックであろうと明示的に許可設定をしないと通信が遮断される。

そのため、エフェメラルポート(1025 ~ 65535)を許可設定にしていないと、返りの通信が遮断される。

ゲートウェイ

ゲートウェイとは、VPCの内部と外部の通信をやり取りする出入り口である。

インターネットと接続するインターネットゲートウェイ(IGW)と、

VPNやDirect Connectを経由してオンプレミスネットワーク基盤と接続する仮想プライベートゲートウェイがある。

インターネットゲートウェイ

インターネットゲートウェイ(IGW)は、VPCとインターネットを接続するためのゲートウェイである。

各VPCに1つだけアタッチする(取り付ける)ことができる。

インターネットゲートウェイ自体には設定事項は何もない。

また、論理的には1つしか見えないため、可用性の観点で単一障害点(Single Point Of Failure、SPOF)になるのでは

と懸念されることがある。

しかし、IGWはAWSによるマネージドなサービスであり、冗長化や障害時の復旧が自動的になされている。

ルートテーブルでインターネットゲートウェイをターゲットに指定すると、

その宛先アドレスとの通信はインターネットゲートウェイを通してインターネットに向けられる。

多くの場合「0.0.0.0/0」を指定することになる。

先述のパブリックサブネットの条件の一つは、ルーティングでインターネットゲートウェイを向いていることになる。

逆に言うとプライベートサブネットとは、ルーティングが直接インターネットゲートウェイに向いていないネットワークになる。

EC2インスタンスがインターネットと通信するには、パブリックIPを持っていなければならない。

あるいは、NATゲートウェイを経由してインターネットと通信をする。

NATゲートウェイは、ネットワークアドレス変換機能を有し、

プライベートIPをNATゲートウェイが持つグローバルIPに変換し、外部と通信する。

システムの信頼性が求められる場合には、NATゲートウェイの冗長性が課題となる。

NATゲートウェイはAZに依存するサービスなので、マルチAZ構成をする場合は、AZ毎に作成する必要がある。

仮想プライベートゲートウェイ

仮想プライベートゲートウェイ(VGW)は、VPCがVPNやDirect Connectと接続するためのゲートウェイである。

VGWも各VPCに１つだけアタッチすることができる。１つだけしか存在できないが、複数のVPNやDirect Connectと接続することが可能。

ルートテーブルでVGWをターゲットに指定すると、その宛先アドレスとの通信はVGWをターゲットに指定すると、

その宛先アドレスとの通信はVGWから、VPNやDirect Connectを通してオンプレミスネットワーク基盤に向けられる。

オンプレミスネットワークの宛先については、ルートテーブルに静的に記載する方法と、ルート伝播(プロパゲーション)機能で動的に反映する方法の２つがある。

VPCエンドポイント

VPC内からインターネット上のAWSサービスに接続する方法としては、インターネットゲートウェイを利用する方法と、

VPCエンドポイントと呼ばれる特殊なゲートウェイを利用する方法がある。

VPCエンドポイントには、S3やDynamoDBと接続する際に利用するゲートウェイエンドポイントと、

それ以外の大多数のサービスで利用するインターフェイスエンドポイント(AWS PrivateLink)がある。

ゲートウェイエンドポイントは、ルーティングを利用したサービスである。

エンドポイントを作成しサブネットと関連づけると、

そのサブネットからS3、DynamoDBへの通信はインターネットゲートウェイではなくエンドポイントを通じて行われる。

セキュリティの観点でVPCエンドポイントは重要になる。

経路の安全性を問われる場合は、インターネットを経由しないことを求められることが多い。

その際には、VPCエンドポイントは重要な要素となるので設計パターンを押さえる必要がある。

ピアリング接続

VPCピアリングは、２つのVPC間でプライベートな接続をするための機能である。

VPCピアリングでは、同一AWSアカウントのVPC間のみならず、AWSアカウントをまたがっての接続も可能。

VPCピアリングでの通信相手は、VPC内のEC2インスタンスなどであり、IGWやVGWなどにトランジット(接続すること)

はできない。

また、相手先のVPCがピアリングしている別のVPCに推移的に接続することもできない。

VPCフローログ

VPC内の通信の解析には、 VPCフローログ(VPC Flow Logs)を利用する。

VPCフローログはAWSでの仮想ネットワークインターフェイスカードである

ENI(Elastic Network Interface)単位で記録される。

記録される内容は、送信元・送信先アドレスとポート、プロトコル番号、データ量と許可/拒否の区別である。

Direct ConnectとDirect Connect Gateway

AWSとオフィスやデータセンターなどの物理拠点を専用線で繋げたい場合は、

AWS Direct Connect(以下 Direct Connect)を利用する。

Direct Connectを利用すると、VPNに比べて遅延やパケット損失量が低下し、スループットが向上するなど、

安定したネットワーク品質で利用することが出来る。

また、アウトバウンドトラフィック料金は、Direct Connect経由の方が安価に設定されている。

ネットワーク品質が重要になる場合や大量のデータをやり取りする場合は、Direct Connectの導入を検討する。

また最近では、複数のAWSアカウントやVPCを利用することが一般的になっている。

Direct Connect Gatewayを利用すると、1つのDirect Connect接続で

拠点と複数のAWSアカウントやVPCに接続することができる。(Direct Connect導入時にセットで検討)

さらには、複数のVPCとオンプレミスネットワークを中心ハブを介して接続するAWS Transit Gatewayという

サービスもある。