AWSネットワーク周り基礎知識まとめ

AWS 初心者 セキュリティ ネットワーク

はじめに

AWSのネットワーク周りの知識があやふやなことが判明したため復習。間違ってたらご指摘お願いします。

ネットワーク

VPC

- AWS内の利用者専用の仮想プライベートネットワーク
- リージョンの中に作成する
- CIDRブロックは/16～/28の範囲で作成できる
  (例： `10.0.0.0/16`)
- 可能な限り大きなサイズ(/16)で作成する
  - アドレス不足を防ぐため

サブネット

- VPCをさらに小さなネットワークに区切った単位
- CIDRブロックは/16～/28の範囲で作成できる
  - VPCよりも小さな範囲を指定する

    (例： `10.0.1.0/24`)
- インターネットと通信するサブネット（パブリックサブネット）、通信しないサブネット（プライベートサブネット）など、役割・ルーティングによって分割する
- 同一の役割を持ったサブネット、リソース群を複数のAZに作成することで、耐障害性の向上に繋がる（マルチAZ）

ルートテーブル

- パケットが次にどこに向かうか、転送先を決める
- 通信経路（送信先とターゲット）を設定する
  - 送信先：パケットに指定された宛先IP
  - ターゲット：実際の転送先
- １つのサブネットに割り当てられるルートテーブルは１つ

- 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ができる
- ターゲットが `local` の場合はそのネットワーク内を意味する

(例)パケットの宛先IPが `10.1.0.0/16` の範囲内の場合は `local` に通信を転送する
(`10.1.0.0/16` の範囲外を指している場合、転送先が存在しないため通信は破棄される)

送信先	ターゲット
10.1.0.0/16	local

インターネットゲートウェイ

- VPCとインターネットを接続するためのゲートウェイ

(例)サブネットをインターネットと通信できるようにする（＝パブリックサブネットにする）場合は全ての通信
(`0.0.0.0/0`)をインターネットゲートウェイ(`igw-`)に向け

るようにルートテーブルを設定する

送信先	ターゲット
10.1.0.0/16	local
0.0.0.0/0	igw-[redacted]

仮想プライベートゲートウェイ

- VPCとVPN、Direct Connectを接続するためのゲートウェイ

NATゲートウェイ

- インターネットから通信されたくないインスタンスがインターネットと通信することを実現する（データベースのアップデート、サーバーをプライベートサブネットに置きたい場合など）
- インターネットからの通信は、リクエストした戻りの通信のみ許可する
- パブリックサブネットに配置し、ElasticIPを割り当てる

- リソースのプライベートIPをNATゲートウェイのパブリックIPに変換することでインターネットとの通信を実現する

セキュリティ

セキュリティグループ

- インスタンスに適用される(EC2、RDSなど)
- 一つのインスタンスに少なくとも一つのセキュリティグループを紐づける
- デフォルトではインバウンドの通信は全て拒否
- どの通信を許可するかを指定する
- ソース（＝送信元）にはIPアドレスの他に、セキュリティグループを指定することもできる
    - セキュリティグループを指定した場合、送信元のリソースがそのセキュリティグループに紐づいていたら通信を許可する
- ステートフルでセッションを見ているため戻りの通信の許可は不要

-例-

下図の場合、 `0.0.0.0/0` （全ての通信）からのHTTPおよびHTTPS通信を許可している

タイプ	プロトコル	ポート範囲	ソース
HTTP	TCP	80	0.0.0.0/0
HTTPS	TCP	443	0.0.0.0/0

下の図の場合、HTTP通信で送信元が sg- のIDのセキュリティグループと紐づいている場合に通信を許可する

タイプ	プロトコル	ポート範囲	ソース
HTTP	TCP	80	sg-[redacted]

ネットワークACL

- サブネット単位で適用される
- デフォルトでは全て許可
- ステートレスなので、戻りの通信も明示的に許可する必要がある

その他

リージョン、AZ、VPC、サブネットの関係

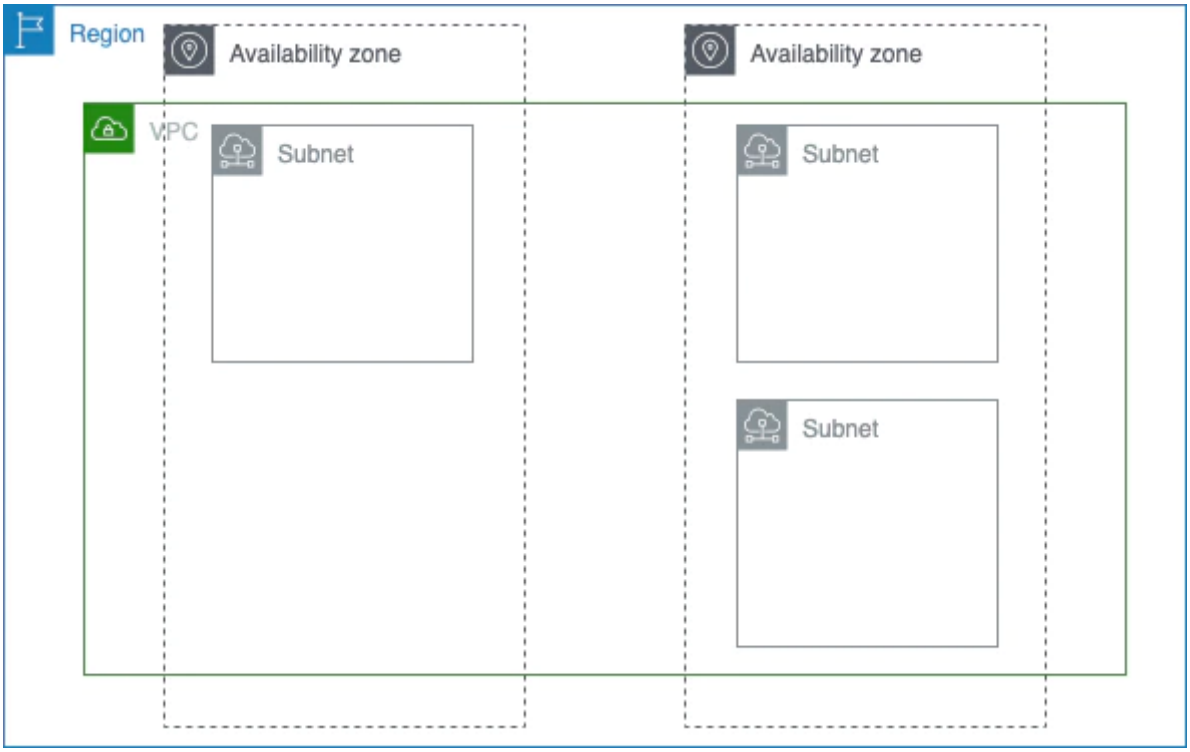
リージョンをさらに小さく区切った単位がAZ（アベイラビリティゾーン）

VPCをさらに小さく区切った単位がサブネット

VPCはリージョンの中に作成する

サブネットはAZの中に作成する（AZをまたぐことはできない）

-例-



パブリックサブネットの通信

パブリックサブネットのリソースもプライベートIPアドレスを持っている

VPC内で通信するときはプライベートIPを使っている

インターネットと通信するときはパブリックIPを使っている