VPC

IPアドレスの基礎

IPアドレス

ネットワーク機器　WEBサイトなどの場所特定に使うもの

ICANNという非営利組織が管理

重複×

32ビット　0.0.0.0～255.255.255.255

IPアドレスはネットワークインタフェースカード（NIC）

に割り当てられホストにアタッチされる

IPv4不足してきている

ｖ４　＝　バージョン４

IPv6形式のＩＰアドレスへ移行してきている

種別

グローバルＩＰアドレス

世界で一意

ＩＣＡＮＮ管理

プライベートＩＰアドレス

限定的

エリア内重複不可　エリア外ＯＫ

サブネットマスクとサブネット

プライベートネットワークをどのように作る？

ネットワーク範囲を定義することが必要

ネットワークの範囲＝利用範囲

10.0.0.0/16　　/16・・・サブネットマスク

ＩＰアドレス+サブネットマスク＝ＩＰの範囲

ＶＰＣのなかでネットワークを分割していく

ＣＩＤＲ

　　/24　は24ビットまでが固定されますよっていう宣言

それ以降がＩＰアドレスとして指定できる

サブネットによるグループ化

ＶＰＣ概要

仮想ネットワークを作成するサービス

自分専用のＡＷＳクラウドを作成

バーチャルプライベートクラウド

単一のＶＰＣ　＝　単一のＡＺ

複数のＡＺにサブネットを配置できる

冗長化

ウィザード利用しない場合

ＶＰＣ作成

サブネット作成

ＧａｔｅＷａｙ設定

トラフィック許可をネットワークＡＣＬで設定

設定できないホストアドレス（AWSが利用している）

.0 ネットワークアドレス

.1 VPCルータ

.2 Amazonが提供するDNSサービス

.255 ブロードキャストアドレス

パブリック サブネット インターネットからアクセスできる

プライベートサブネット インターネットからアクセスできない

パブリックorプライベートサブネット

インターネットゲートウェイがあるかないかで決まる

ルートテーブルのターゲットにigw(インターネットゲートウェイ)を設定することで

パブリックにできる

推奨　ＶＰＣ/16　　サブネット/24

プライベートサブネットがインターネットに接続するには

パブリックサブネット側でＮＡＴを設定する

外部接続

・パブリックのＡＷＳネットワーク

・エンドポイント

ポイント

将来性を見据える

社内のオフィスなどと被らない設計

ＩＰアドレスは適当に決めないように！！

全体を見てＶＰＣの割り当てを考える

冗長化させる

トラフィックを適切に制御する

モニタリングする（ＶＰＣフローログ）

ＮＡＴ

　グローバルＩＰとプライベートＩＰの変換機能

ＩＰマスカレード

複数の端末をひとつのＩＰアドレスを関連させることが出来る技術

ＤＨＣＰ

プライベートのＩＰアドレスを配布

踏み台サーバ

パブリックサブネットに配置してこの踏み台サーバを介してプライベート

サブネットのリソースにアクセス

インターネットにプライベートサブネットからの

返信トラフィックにはＮＡＴゲートウェイを介して情報を渡す

ＮＡＴゲートウェイは有料

パブリックサブネットのルートテーブルのターゲットはＩＧＷ

プライベートサブネットのルートテーブルのターゲットはＮＡＴ　ＧＷ

めちゃ大事！！

メールを送信したい

ブラウザみたい

全て通信のルールがある

プロトコルでの送受信をするためのＩＰアドレスを設定する

メール用のプロトコル

ブラウザのプロトコルetc・・・

この通信プロトコルのルールを７つの層に分けて規格としてルール化している

ＯＳＩ参照モデル！！！

アプリケーション層 Outlook　chrome

データリンク層 MACアドレスによるノード間の通信

アプリケーション層 WEBアプリケーションの通信サービスを実現のための もの

プレゼンテーション層 文字の送り方を決めている

言語の設定など

セッション層 アプリケーション間でのセッションの確立

ログインが継続＝セッションのイメージ

セッションの確立　維持　終了がルール化

トランスポート層 信頼確立

ポート番号の割り当て

TCPで到着順序や確認を実施

ネットワーク層 ノードの起点から終点までの通信を規定

IPアドレスの割り当て

ルータの宛先までの最適なパスを選択

データリンク層 MACアドレスを使った通信

LANではイーサネットによる通信を行う！ここ！

物理層　 機器同士の物理的な接続

0と１のビット列を電気信号に変換して送ることの規格

TCP/IPモデル

アプリケーション層 HTTP　SSH　DNS　SMTP　FTPなど

トランスポート層 ＴＣＰ　ＵＤＰなど

ネットワーク層 ＩＰ　ＩＣＭＰ　ＡＲＰ　ＢＧＰなど

物理層 Ethernet　PPPなど

リクエストとレスポンスの確認

HTTPプロトコルで送信　 アプリケーション層

コネクション確立 トランスポート層

送信先にパケットを送付 ネットワーク層

物理機器間の電信 物理層

ポート番号

オペレーティングシステムがデータ通信を行うためのエンドポイント（OS）

複数のソフトウェアのどれと通信するのか選択

HTTP 80

HTTPS 443

LINE 5000/5528

SSH 22

SMTP 25

POP 110　143

セキュリティグループ

トラフィックの制御

デフォルトはすべてのアクセスを拒否している

0.0.0.0　と設定することで誰でもアクセスOKになる

一つのEC2インスタンスに対して一つずつセキュリティグループをy使う

共有も可能

ネットワークACL

サブネットに対してトラフィック制御

特徴

セキュリティグループ

サーバ単位で適用

ステートフル

インバウンドの設定すればアウトバウンドも許可される

許可のみをIn/Outで指定

デフォルトでは同じセキュリティグループ内通信のみ許可

全てのルールを適用

ネットワークACL

VPC/サブネット単位で適用

ステートレス

許可拒否をIn/Outで設定

デフォルトではすべての通信を許可

番号の順序通りに適用

重要

セキュリティグループはインスタンスのトラフィックを制御するファイアウォールを提供

ネットワークACLはサブネットのトラフィックを制御するファイアウォールを提供

注意

エファメルポートをアウトバウンドルールに割り当てておく

これしないと自分のPCからリソースにアクセスできない

YUMのコマンドたたくとエラーになる可能性考慮して

　　インバウンドルールにも同じように割り当てる

エファメルポート・・・動的に割り当てられるポート番号

NATゲートウェイハンズオンでやること

パブリックサブネットとプライベートサブネットに一つずつインスタンス配置

パブリックサブネットのEC2インスタンスからプライベートサブネットのEC2インスタンスに接続してyum updateコマンド実行

パブリックサブネットにNATゲートウェイ配置してプライベートサブネットのルートテーブルにNATゲートウェイへのルートを設定する

再度yum update実行

補足

NATゲートウェイ作成時にプライベート版が利用できるようになった

→オンプレミス環境とプライベート接続するときに使う

VPCとの接続

オンプレとの接続

VPN　と　DirectConnect

DirectConnect

　　AWSサービス

　　データセンターやオフィスを専用線などを介してAWSへぷらおべーとにアクセスするサービス

DirectConnect　ＧａｔｅＷａｙ

リージョン間でのネットワーク接続が出来る

特徴

VPN

コスト

安価なベストエフォート回線が利用可能

リードタイム

クラウド上で設定可能なため即時

帯域幅

暗号化のオーバーヘッドにより制限がある

品質

インターネット経由の為ネットワークの状態の影響を受ける

障害切り分け

インターネットベースの為自社で保持している範囲以外の確認が難

VPCエンドポイント

グローバルIPを持つAWSサービスに対してVPC内から直接アクセスするための出口

パブリックサブネット

10.0.0.0/24　　　　　　　10.0.0.100

EC2　　　→　VPCエンドポイント　→　S3

VPCE-9j9kh9

接続種類

Gateway型特徴

サブネットに特殊なルーティングを設定し、VPC内部から

直接、外のサービスと通信する

ルートテーブルを介して行う

アクセス制御 ：エンドポリシーを設定

料金 ：無料

冗長性 ：AWS側が対応

PrivateLink型特徴

サブネットにエンドポイント用のプライベートＩＰアドレスを生成

ＤＮＳが名前解決でルーティングする

アクセス制御 ： セキュリティグループを設定

料金 ： 有料

冗長性 ： マルチＡＺ設計

NATゲートウェイ

プライベートサブネットが外の通信と可能になる

VPC　Flow　Logs

ネットワークトラフィックを取得しCloud Watchでモニタリングできる

VPC設定上限

リージョンあたりのＶＰＣの上限 ：5

ＶＰＣあたりのサブネット ：200

ＡＷＳアカウントあたりのElasticIP : 5

ルートテーブルあたりのルート上限：100

ＶＰＣあたりのセキュリティグループの上限数：　500

セキュリティグループあたりのルールの上限数：50

VPC分割ケース

アプリケーションによる分割

監査のスコープによる分割

リスクレベルによる分割

本番/検証/開発フェーズによる分割

部署による分割 共通サービスの切り出し

VPC　peering

２つのVPC間でのトラフィックルートを確立する

基本的には1：1

3つの場合

VPC1　―　VPC2　―　VPC3

更にVPC1とVPC3をPeering接続する