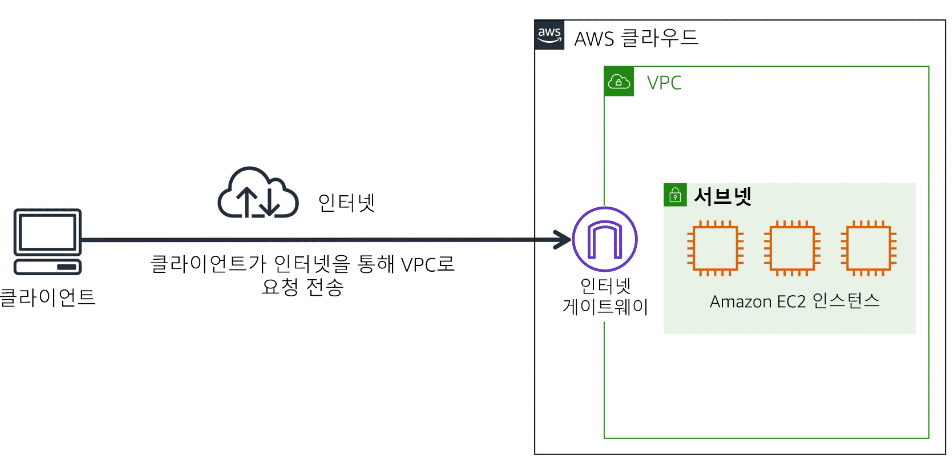
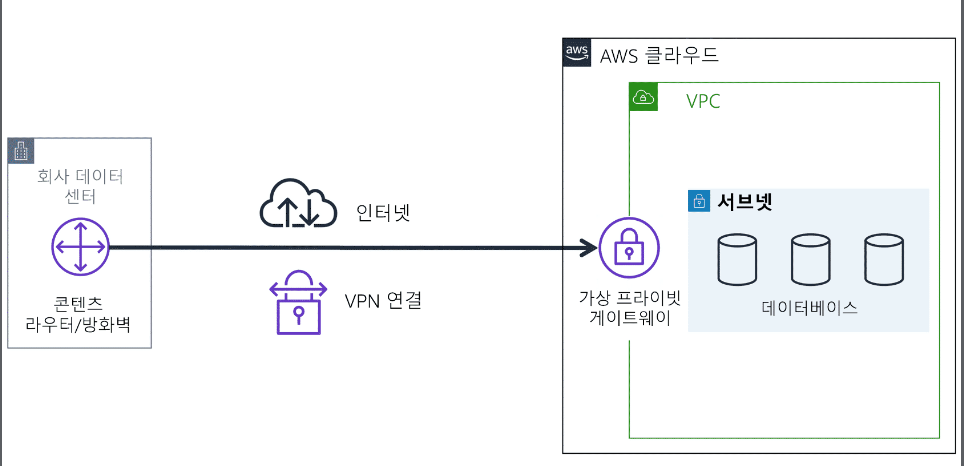
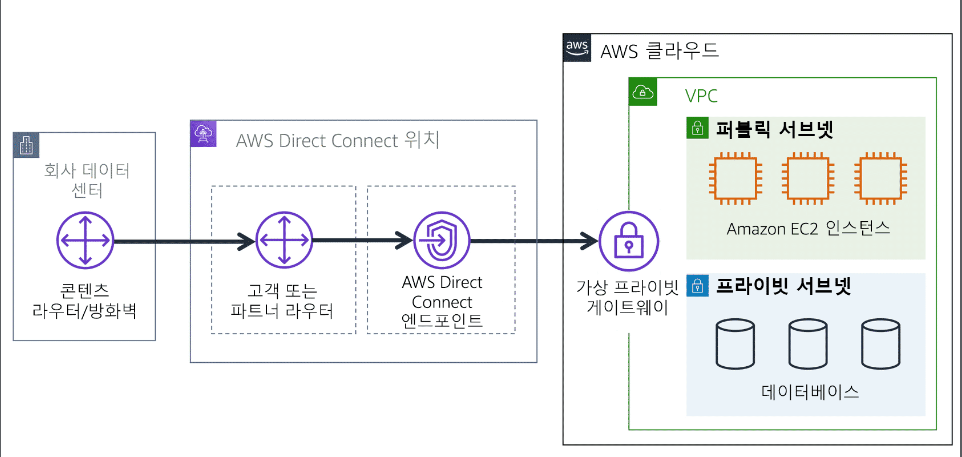
1. Amazon Virtual Private Cloud (Amazon VPC)  
 - AWSリソースに境界を設定するために使用できるネットワーキングサービス  
 VPC内で複数のサブネットでリソースを構成することができる。  
 サブネットは、リソース（例:Amazon EC2 インスタンス）を含むことができるVPC セクション  
 プライベート サブネット: 顧客の個人情報を含むデータベースを隔離  
 パブリック サブネット: 顧客向けウェブサイトをサポート



インターネットゲートウェイ:vpcとインターネット間の接続(顧客がコーヒーショップに入るための出入り口と似ている)  
 インターネットゲートウェイがなければ誰もVPC内のリソースにアクセスできない

2. 仮想 private gateway  
 : VPC内のプライベート リソースにアクセスするために使用  
 VPC とプライベートネットワーク（例:オンプレミス データセンターまたは社内ネットワーク）との間に仮想プライベートネットワーク（VPN）接続を設定することができる。  
 承認されたネットワークからのトラフィックのみVPCに入ることを許可する。

3. AWS Direct Connect  
 - オンプレミスデータセンターとVPC間の非公開専用接続を設定するサービス

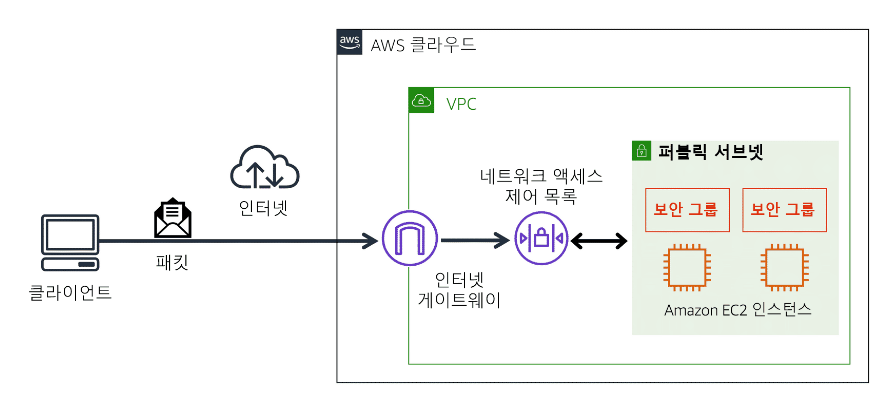


会社のデータセンターはネットワークトラフィックをAWS Direct Connect ロケーションにルーティングする。  
 ->このトラフィックは仮想プライベートゲートウェイを通じてVPCにルーティングされる、->会社のデータセンターとVPC間のすべてのネットワークトラフィックはこの非公開専用連結を通じて伝送される。  
 VPC内でサブネットは互いに通信できる。 例えば、パブリックサブネットにあるAmazon EC2 インスタンスがプライベートサブネットにあるデータベースと通信するアプリケーションがあり得る。

4. VPCのネットワークトラフィック  
 顧客がAWSクラウドでホスティングされるアプリケーションにデータを要請すると、この要請はパケットに送信される。  パケットはインターネットやネットワークを介して伝送されるデータの単位である。   
 パケットはインターネットゲートウェイを通じてVPCに入る。 パケットがサブネットに入るか、サブネットから出るには、まず権限を確認しなければならない。 このような使用権限は、パケットを送信者とパケットがサブネットのリソースと通信しようとする方法を示している。  
 サブネットのパケット権限を確認するVPC コンポーネントは、ネットワークアクセス制御リスト（ACL）である。

5. ネットワークアクセス制御リストACL  
 - サブネットレベルでインバウンドおよびアウトバウンドトラフィックを制御する仮想ファイアウォール  
 例）空港旅行者:パケット、出入国審査員:ネットワークACL  
 各AWSアカウントには基本ネットワークACLが含まれる、基本ネットワークアクセス制御リストはステートレスであり、すべてのインバウンドおよびアウトバウンドトラフィックを許可する。  
 または、ユーザ指定ネットワークACLを生成することができ、ユーザが許可するトラフィックを指定する規則を追加するまで、すべてのインバウンドおよびアウトバウンドトラフィックを拒否する。

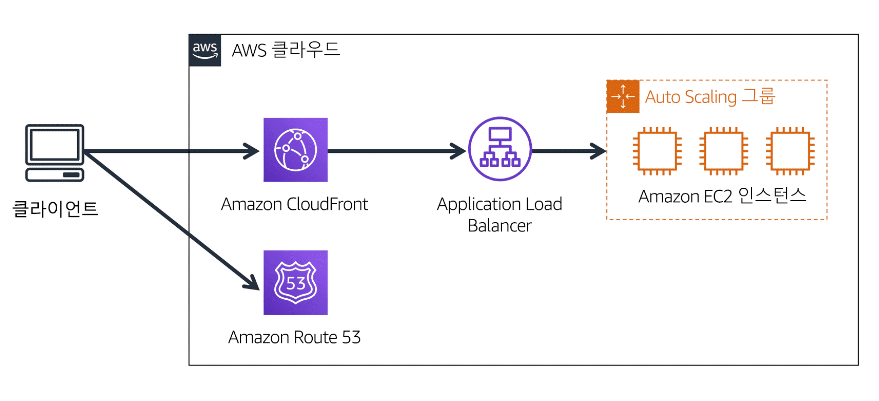
6. ステートレス·パケット·フィルタリング  
 - ネットワークACL はステートレスパケットフィルタリングを行う必要がある。  
 すなわち、何も記憶せずに各方向(インバウンドおよびアウトバウンド)でサブネット境界を通過するパケットだけを確認する。  
 その要求に対するパケット応答がサブネットに返されるとき、ネットワークACLは以前の要求を覚えていない。 ネットワークACLは、ルールリストに従ってパケット応答を確認し、許可するか拒否するかを決定する。  
 パケットがサブネットに入った後は、サブネット内のリソース（例:Amazon EC2 インスタンス）に対する権限が評価されなければならない。  
 パケットでAmazon EC2 インスタンスに対する権限を確認するVPC 構成要素はセキュリティグループである。

7. セキュリティ·グループ  
 - Amazon EC2 インスタンスに対するインバウンドおよびアウトバウンドトラフィックを制御する仮想ファイアウォール  
 デフォルトでは、セキュリティ グループはすべてのインバウンド トラフィックを拒否し、すべてのアウトバウンド トラフィックを許可する。  
 カスタム ルールを追加して許可すべきトラフィックを構成すると、残りのトラフィックは拒否される。  
 例）訪問者:パケット、警備員:セキュリティグループ  
 訪問客が入ってくる時はリストを確認するが、出る時は確認しない。  
 ステートフルパケットフィルタリング  
 - セキュリティ グループは、ステートフル パケット フィルタリングを実行する、着信パケットに対する以前の決定を記憶する。  
 Amazon EC2 インスタンスからインターネットに要請を伝送する時、該当要請に対するパケット応答がインスタンスに返還される時、セキュリティグループが以前の要請を記憶する。 セキュリティグループは、インバウンドセキュリティグループ規則に関係なく、応答が進行することを許可する。

パケットはインターネットを通じてクライアントからインターネットゲートウェイ、VPCに移動する。 ->その後、パケットはネットワークアクセス制御リストを経て二つのEC2 インスタンスがあるパブリックサブネットにアクセスする。

8. ドメイン名システム(DNS)  
 - DNS確認:ドメイン名をIPアドレスに変換するプロセス  
 ブラウザにドメイン名を入力すると、この要求が顧客のDNS確認者に送信される -> 顧客のDNS確認者は、会社のDNSサーバーにAnyCompanyウェブサイトに該当するIPアドレスを要請 ->会社のDNSサーバーは、AnyCompanyウェブサイトのIPアドレスである192.0.2.0を提供して応答する

9. Amazon Route 53  
 - DNSウェブサービス  
 ユーザーのリクエストをAWSで実行されるインフラストラクチャ（例:Amazon EC2 インスタンスおよびロード バランサー）に接続  
 また、ユーザーをAWS外部のインフラにルーティングすることができる。  
 ドメイン名のDNSレコードを管理する機能:Amazon Route 53に直接新しいドメイン名を登録することができる。 他のドメイン登録代行者が管理する既存ドメイン名のDNSレコードを伝送することもできる。 そうすれば、単一の位置ですべてのドメイン名を管理することができる。

Amazon Route 53及びAmazon Cloud Frontがコンテンツを配信する方式

顧客がAnyCompanyのウェットサイトに移動してアプリケーションからデータを要請する ->  
 Amazon Route 53はDNS確認を使用してAnyCompany.com のIPアドレスである192.0.2.0を識別し、この情報はお客様に再送信 ->お客様の要請はAmazon CloudFrontを通じて最も近いエッジロケーションで送信される -> Amazon CloudFrontは受信パケットをAmazon EC2インスタンスに送信するApplication Load Balancerに接続される