AWS Network Firewall 応用編1

新機能：MSRの活用/トラフィックを集約して監査する

AWS Black Belt Online Seminar

Yosuke Okumura
Network Solutions Architect

2021/10

AWS 公式 Webinar
https://amzn.to/JPWebinar

過去資料
https://amzn.to/JPArchive

内容についての注意点

- 本資料では2021年10月時点のサービス内容および価格についてご説明しています。
  最新の情報はAWS公式ウェブサイト(http://aws.amazon.com)にてご確認ください。
- 資料作成には十分注意しておりますが、資料内の価格とAWS公式ウェブサイト記載の価格に相違があった場合、AWS公式ウェブサイトの価格を優先とさせていただきます。
- 価格は税抜表記となっています。
  日本居住者のお客様には別途消費税をご請求させていただきます。

- AWS does not offer binding price quotes. AWS pricing is publicly available and is subject to change in accordance with the AWS Customer Agreement available at http://aws.amazon.com/agreement/. Any pricing information included in this document is provided only as an estimate of usage charges for AWS services based on certain information that you have provided. Monthly charges will be based on your actual use of AWS services, and may vary from the estimates provided.

自己紹介

名前：　奥村 洋介（おくむら ようすけ）

ポジション：ネットワークソリューションアーキテクト

経歴：　国内のISP、通信キャリアで10年ほどネットワークエンジニア
　　を経験後、AWSに入社

好きなAWSサービス：

AWS Transit Gateway, AWS Network Firewall

今回のゴール

- Amazon VPCの新機能、More specific routing （MSR）で新しく可能になった構成を理解する
- 様々なトラフィックをAWS Transit GatewayをAWS Network Firewallに集約して、まとめて監査する設計と構築ができるようになる

なお、Network Firewallについての基礎は、「AWS Network Firewall入門」をご参照ください。

Agenda

- VPCの新機能、More specific routing （MSR）
- 様々な通信をNetwork Firewallに集約して監査する
  - この構成のメリット
  - トラフィックフロー
  - 設計ポイントはルート設定にあり
  - 応用：公開サーバ宛の通信を集約する
- マルチAZの際の注意事項
- まとめ

Amazon VPCの新機能、More specific routing（MSR）

Amazon VPCの新機能 More specific routing(MSR)

✓VPC CIDRで作られるlocalルートのTargetを変更できるようになった

✓VPC のサブネット宛のルートを設定できるようになった

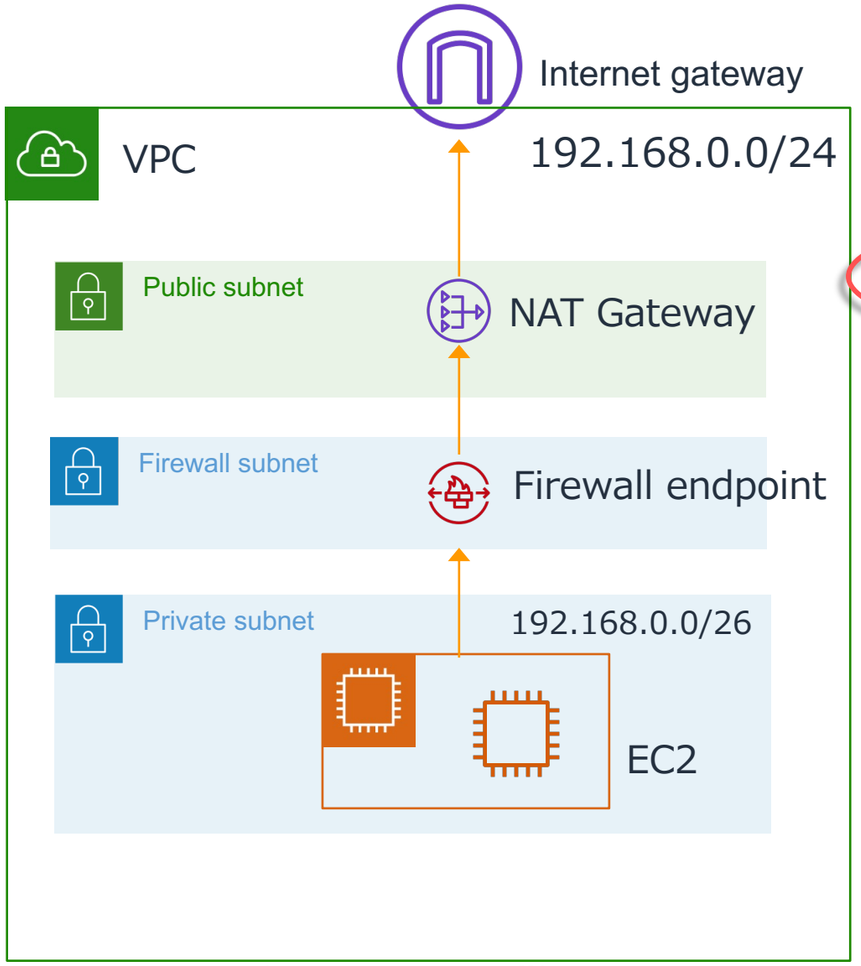
注意事項

・VPCの外へ向かうようなTarget設定(Transit Gatewayなど)は不可

・VPCにサブネットとして存在しない宛先の設定は不可

Amazon VPCの新機能 More specific routing(MSR)

✓Network Firewallでの活用例



Destination	Target
192.168.0.0/24	**local**
192.168.0.0/26 (Private subnet)	**Firewall endpoint**
0.0.0.0/0	Internet Gateway

Destination	Target
192.168.0.0/24	local
0.0.0.0/0	NAT Gateway

Destination	Target
192.168.0.0/24	local
0.0.0.0/0	Fireawll endpoint

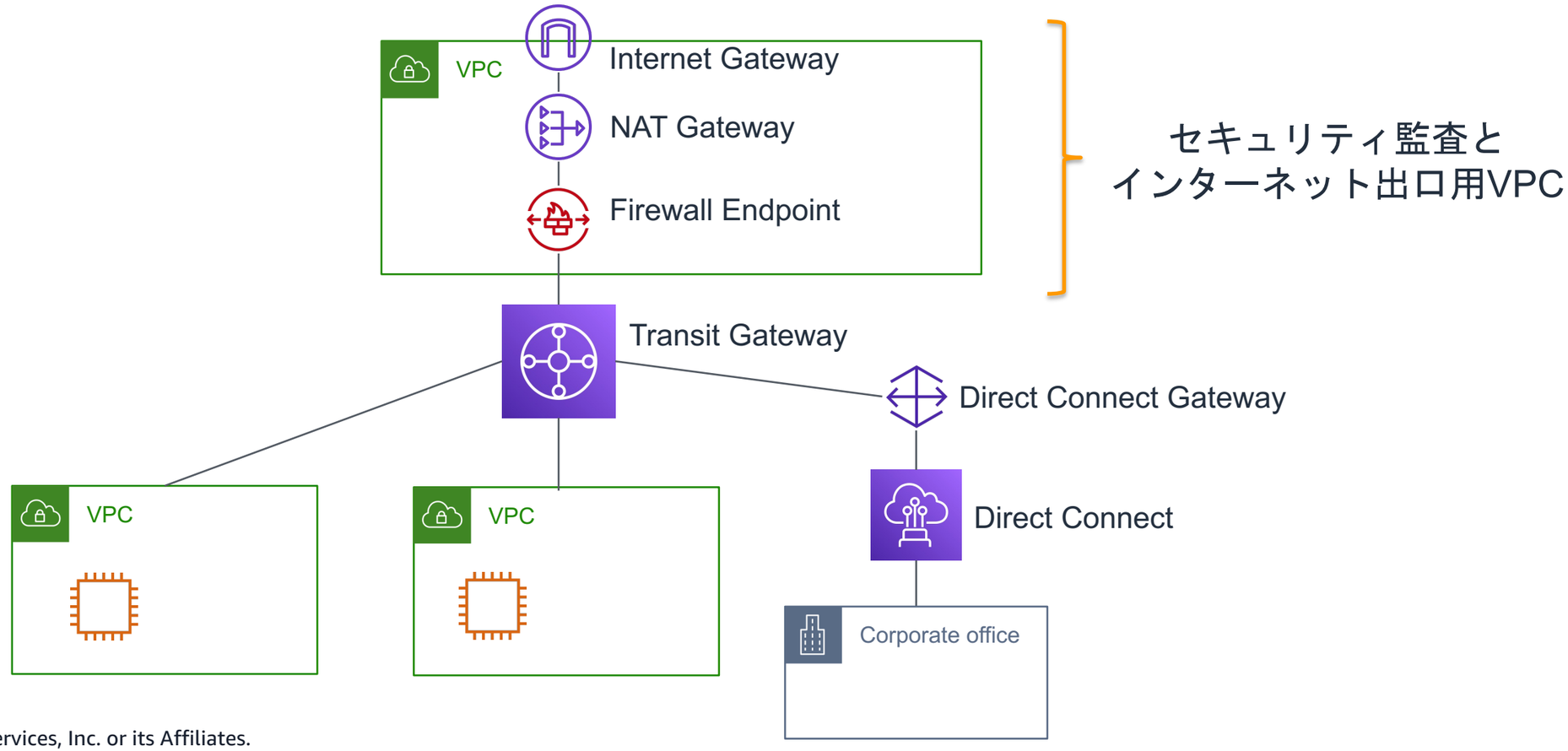
MSRを使ってlocalルートに含まれる戻りの経路のTargetをFirewall endpointに指定することにより、VPCが一つの場合でも、NAT Gatewayを外側に配置できるようになりました。

これにより、Network Firewallから見て、送信元がNAT GatewayのIPアドレスに集約されてしまう状態を改善することができます。

様々な通信をNetwork Firewallに集約して監査する

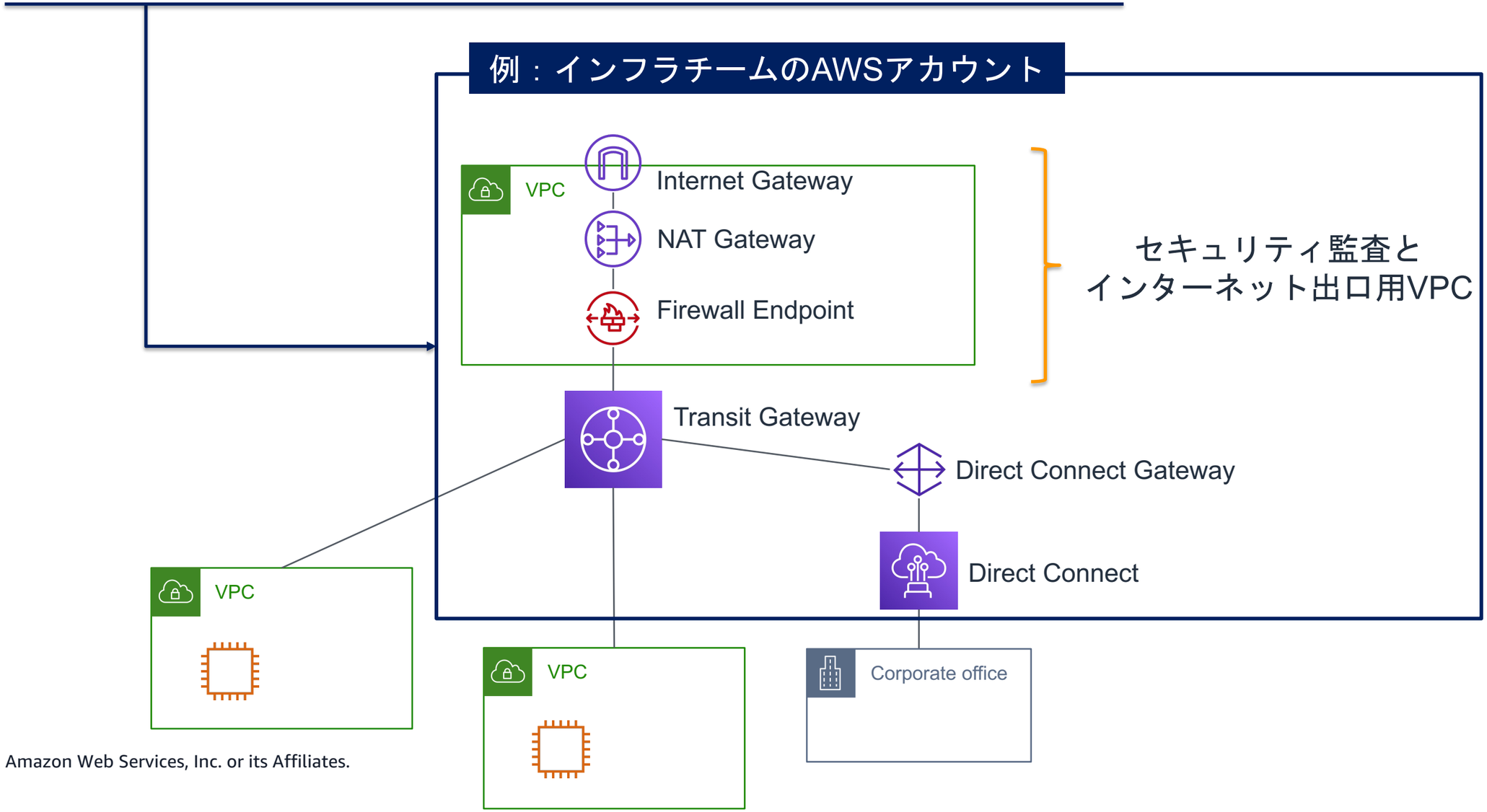
様々な通信をNetwork Firewallに集約して監査する

これらの通信を強制的にNetwork Firewall経由にします。
1. VPC同士の通信
2. オンプレミス(Direct Connect/VPN) とVPCへの通信
3. VPCやオンプレミス(Direct Connect/VPN)からインターネットへの通信



この構成のメリット

1.すべての通信をNetwork Firewall経由にすることにより、一元的に管理できる
2.マルチアカウント構成の際にネットワークセキュリティ機能を取り扱いやすい



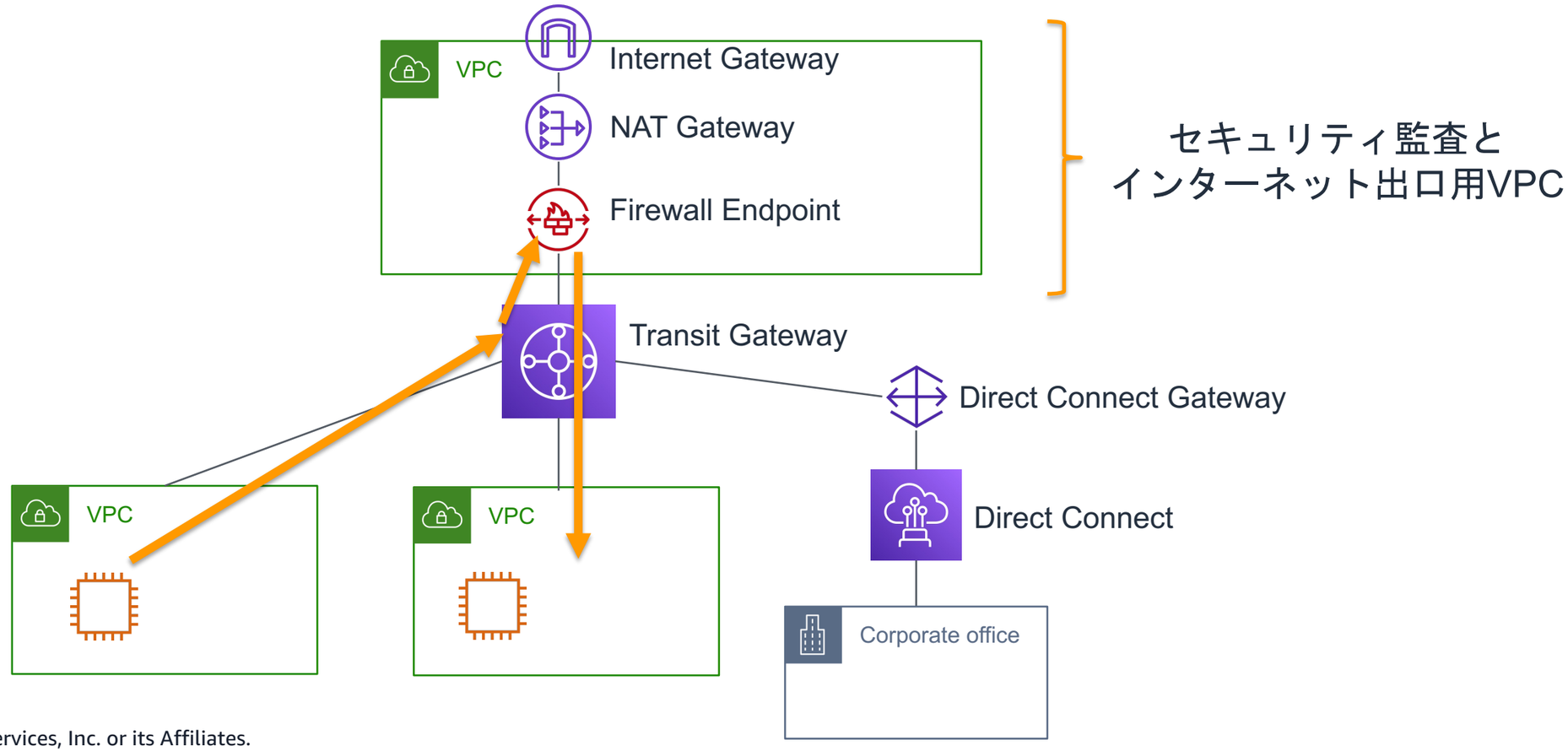
トラフィックフロー

これらの通信を強制的にNetwork Firewall経由にする。

1. VPC同士の通信

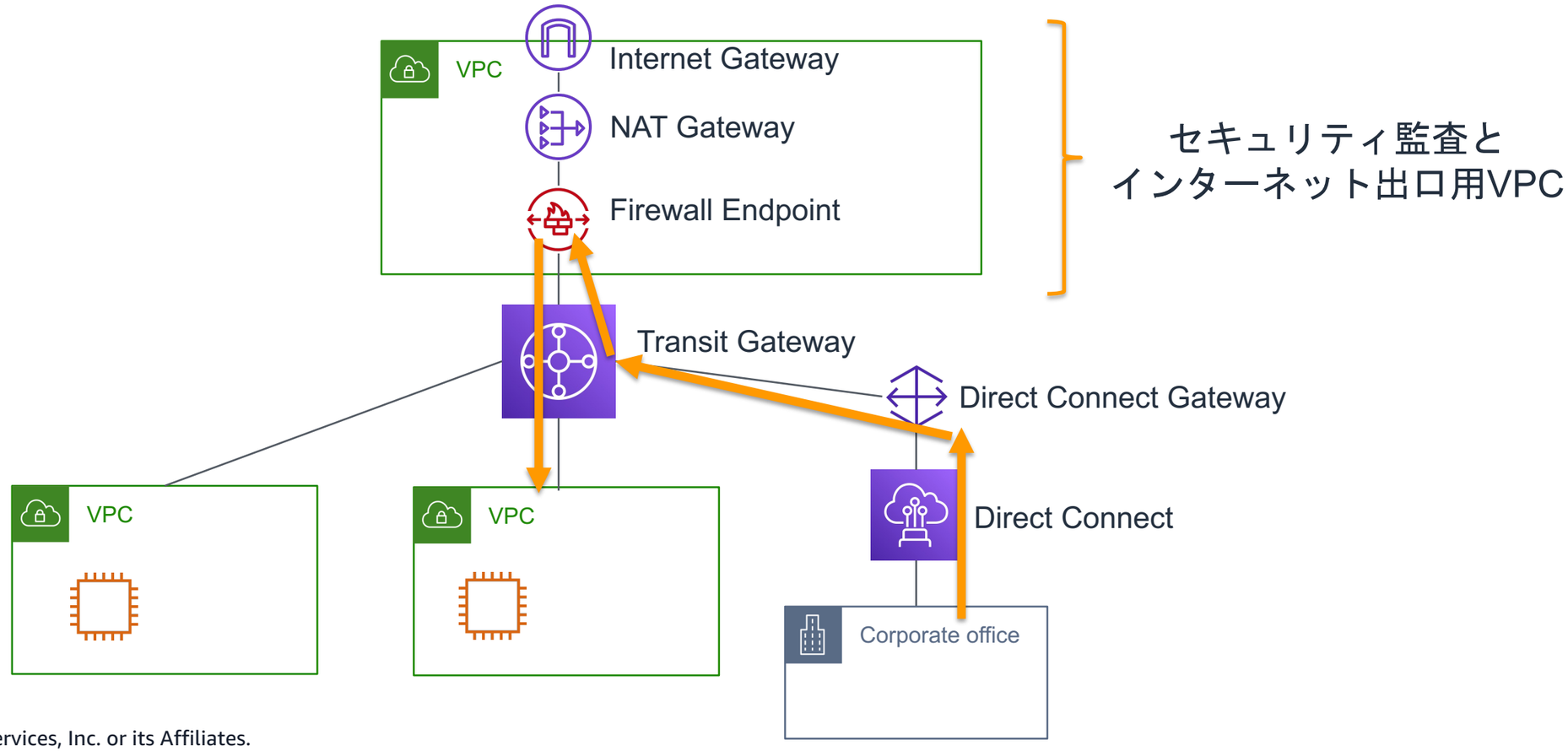
2. オンプレミス(Direct Connect/VPN) とVPCへの通信

3. VPCやオンプレミス(Direct Connect/VPN)からインターネットへの通信



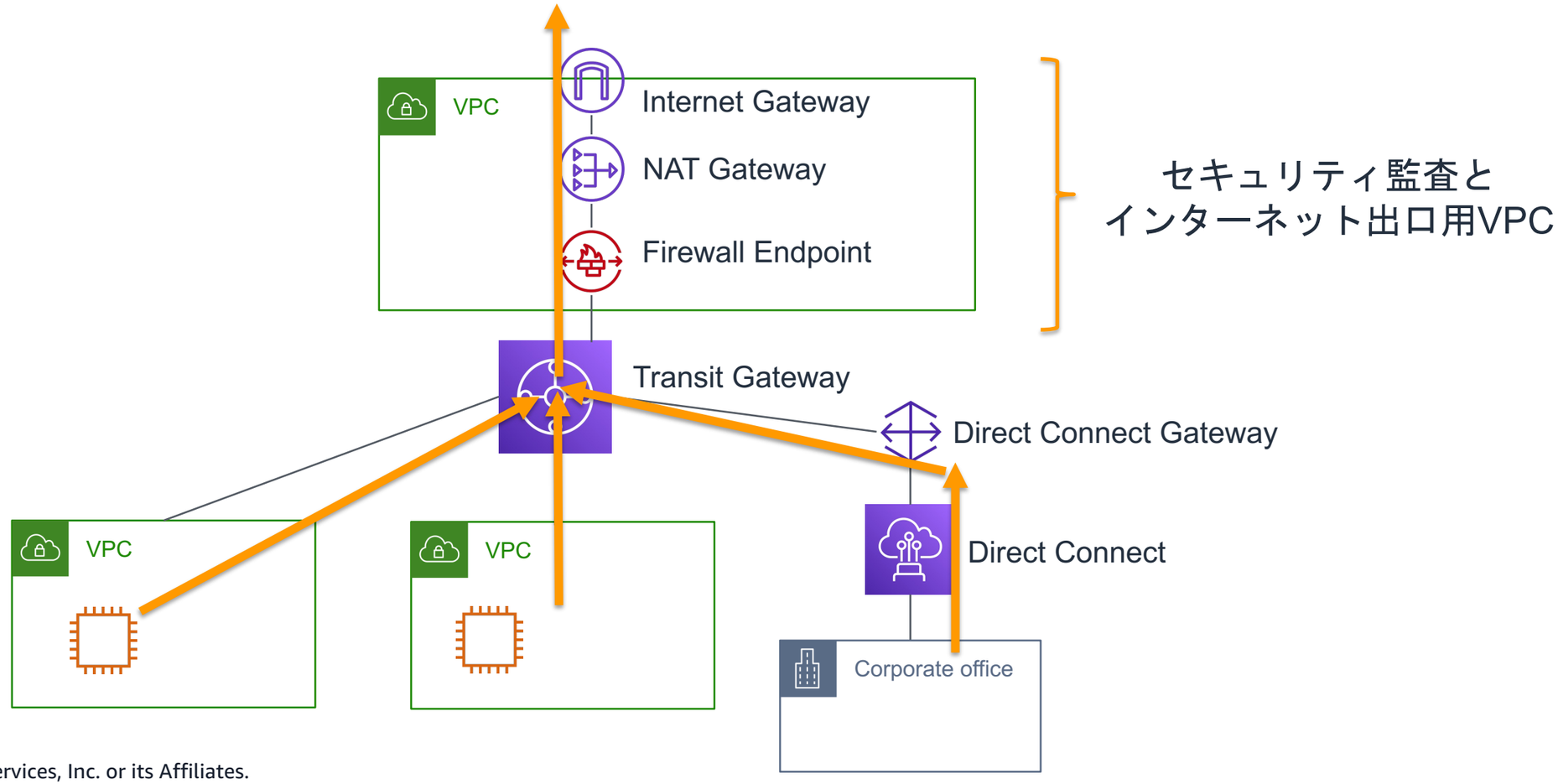
トラフィックフロー

これらの通信を強制的にNetwork Firewall経由にする。
1. VPC同士の通信
2. オンプレミス(Direct Connect/VPN) とVPCへの通信
3. VPCやオンプレミス(Direct Connect/VPN)からインターネットへの通信



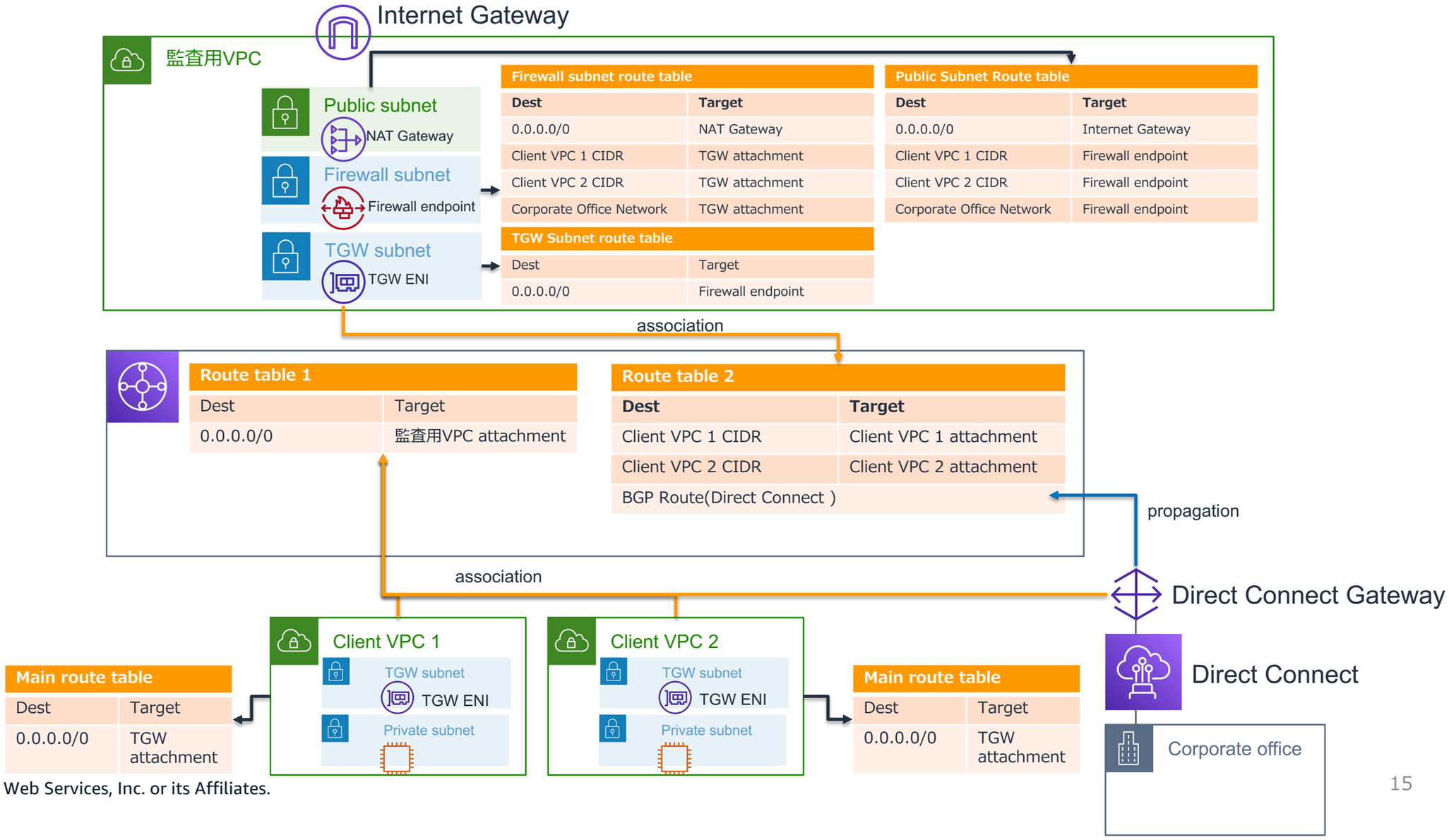
トラフィックフロー

これらの通信を強制的にNetwork Firewall経由にする。
1. VPC同士の通信
2. オンプレミス(Direct Connect/VPN) とVPCへの通信
3. **VPCやオンプレミス(Direct Connect/VPN)からインターネットへの通信**



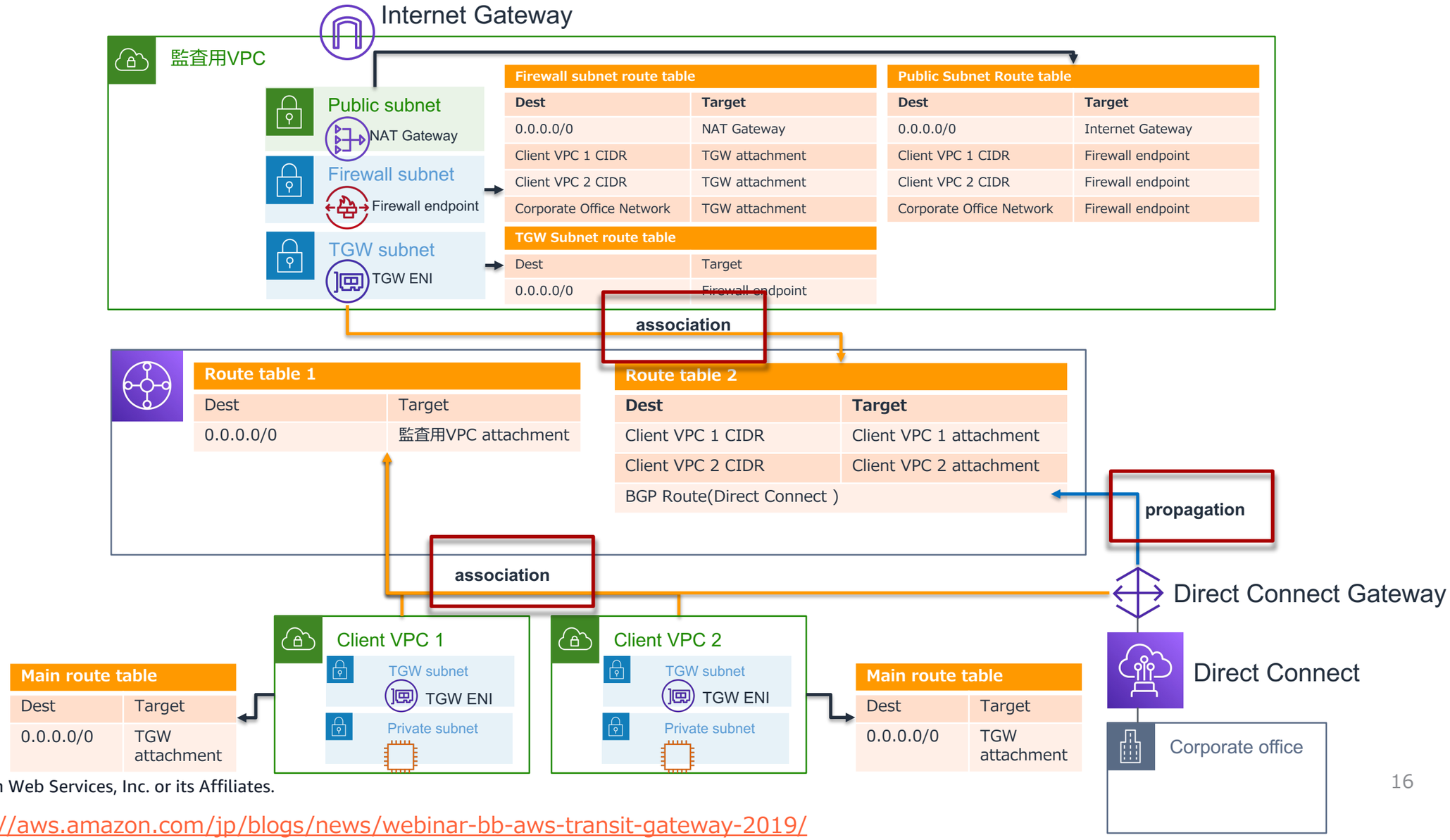
設計ポイントはルート設定にあり

✓Transit Gatewayのルートテーブルを複数作成し、必ず監査用VPCを通るように制御する



設計ポイントはルート設定にあり

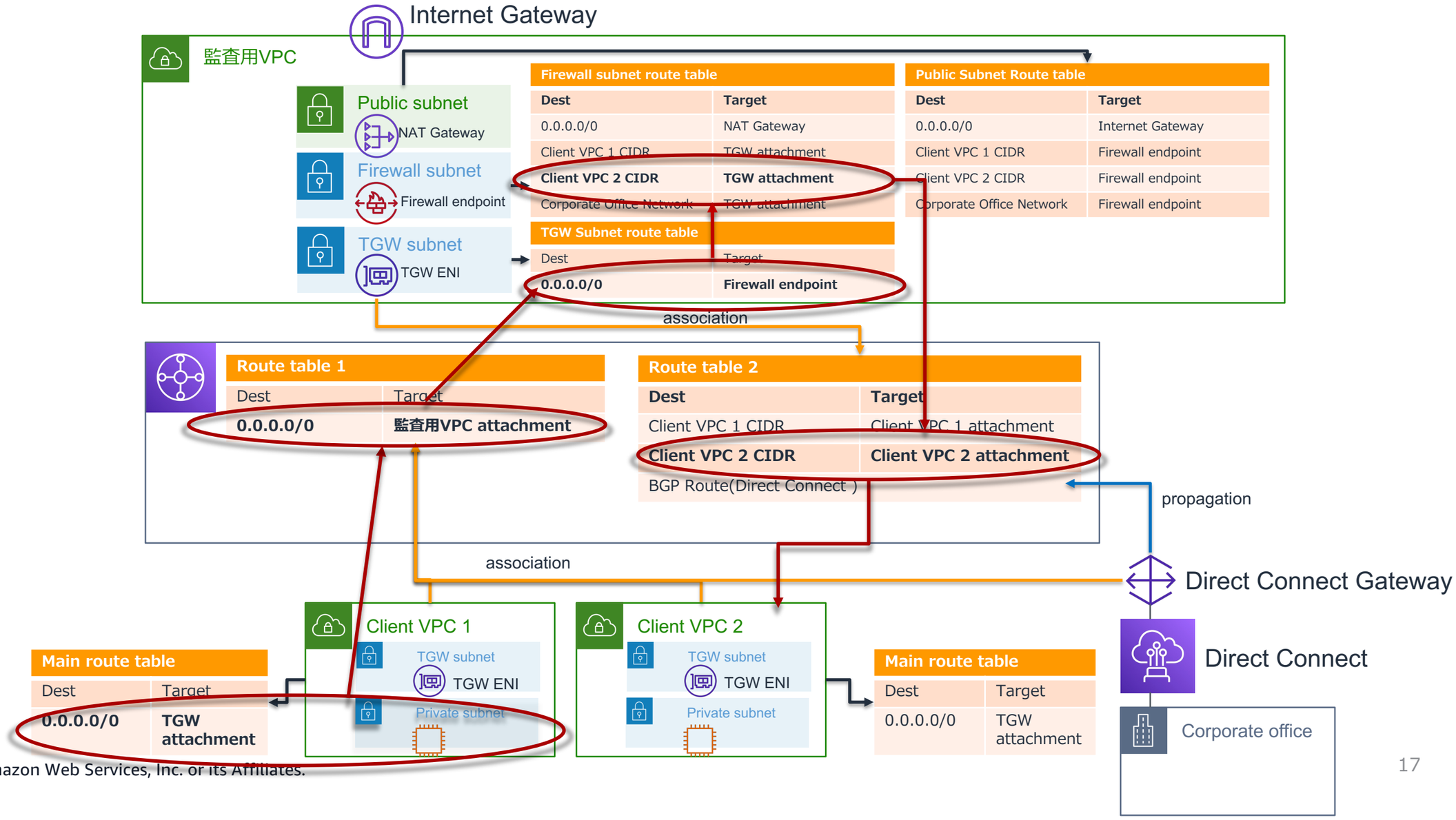
✓association,propagationとは？



参考：https://aws.amazon.com/jp/blogs/news/webinar-bb-aws-transit-gateway-2019/

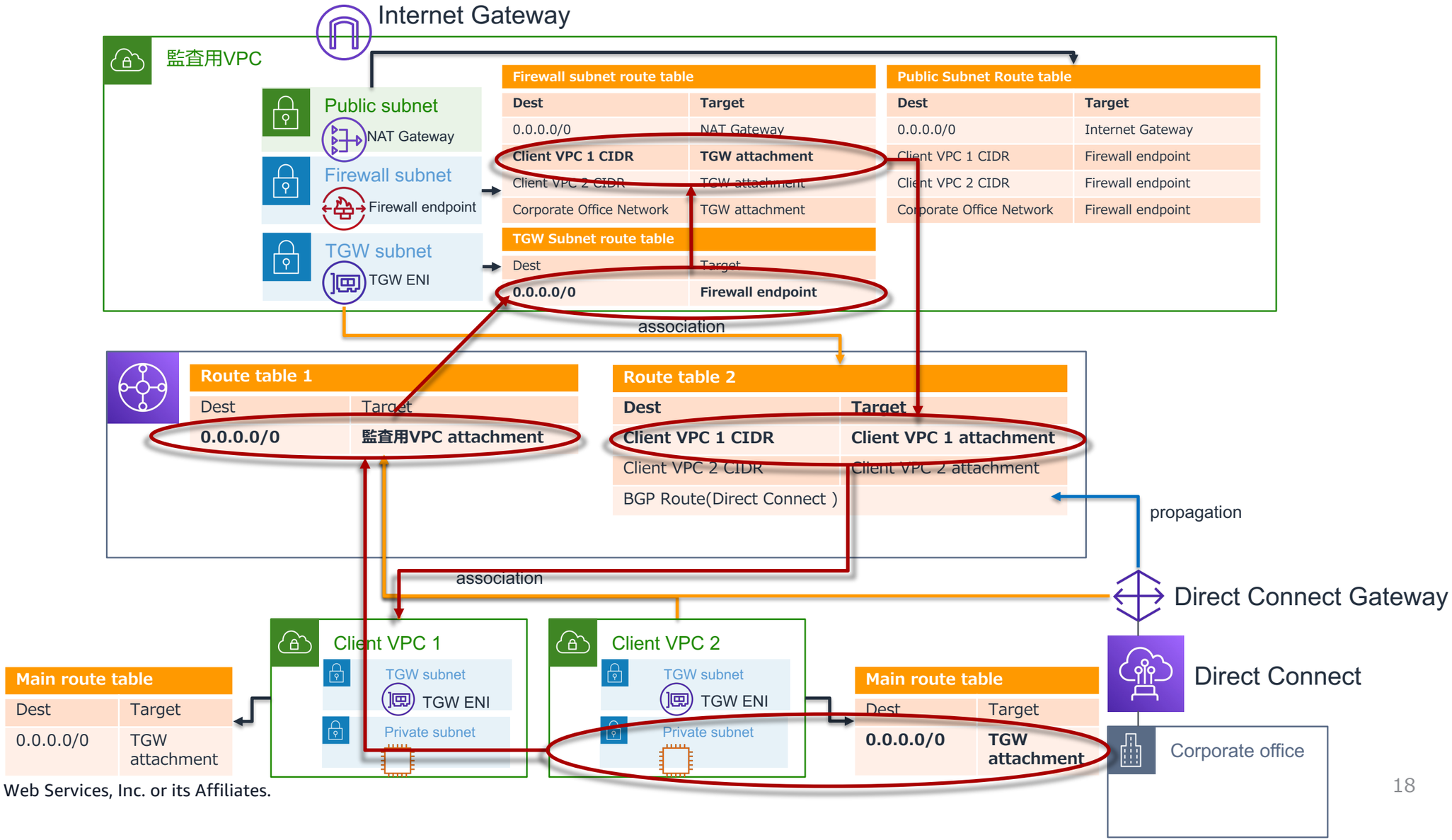
設計ポイントはルート設定にあり

✓ VPC同士の通信（行き）



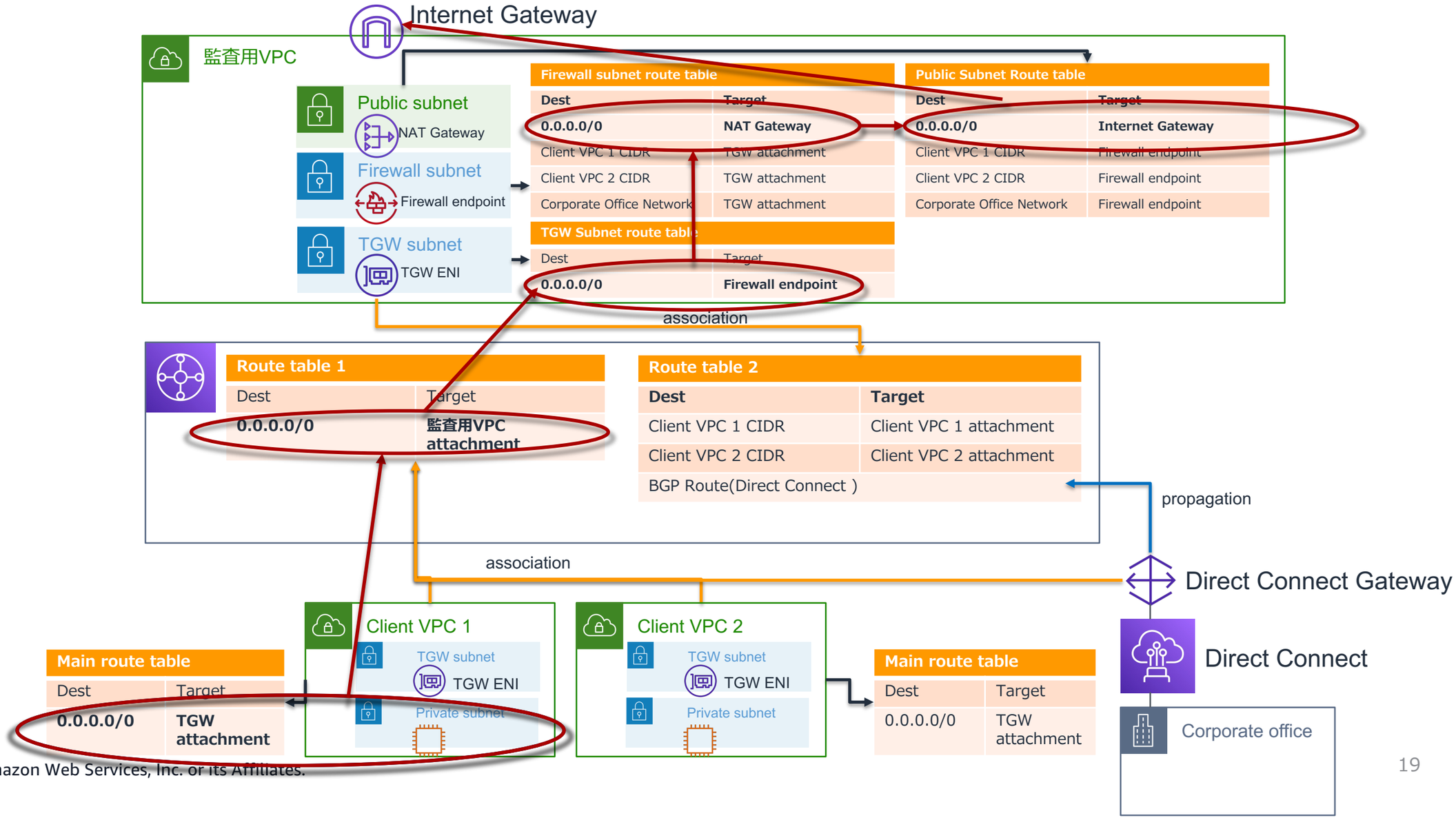
設計ポイントはルート設定にあり

✓ VPC同士の通信（戻り）



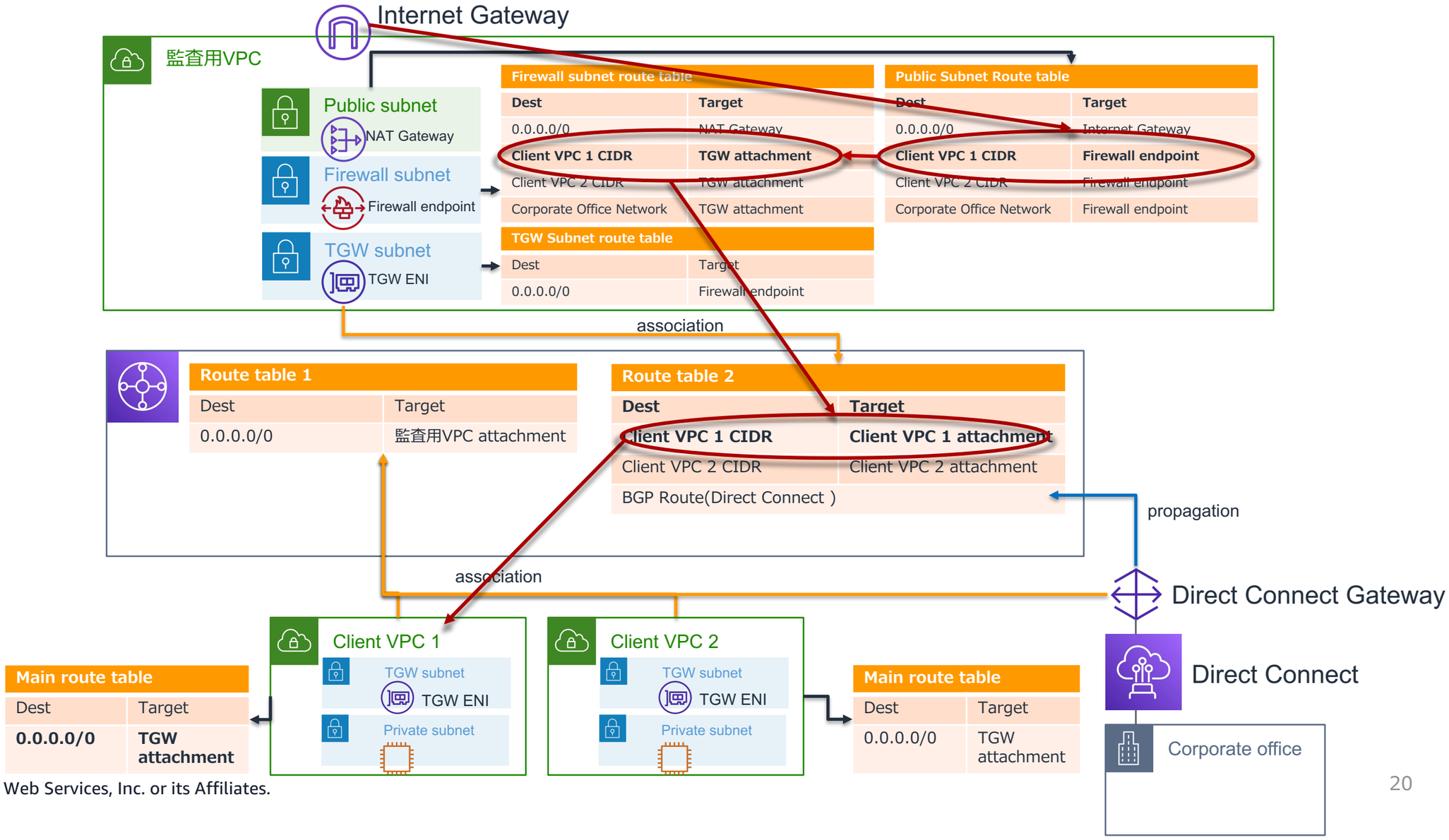
設計ポイントはルート設定にあり

✓インターネット宛の通信（行き）



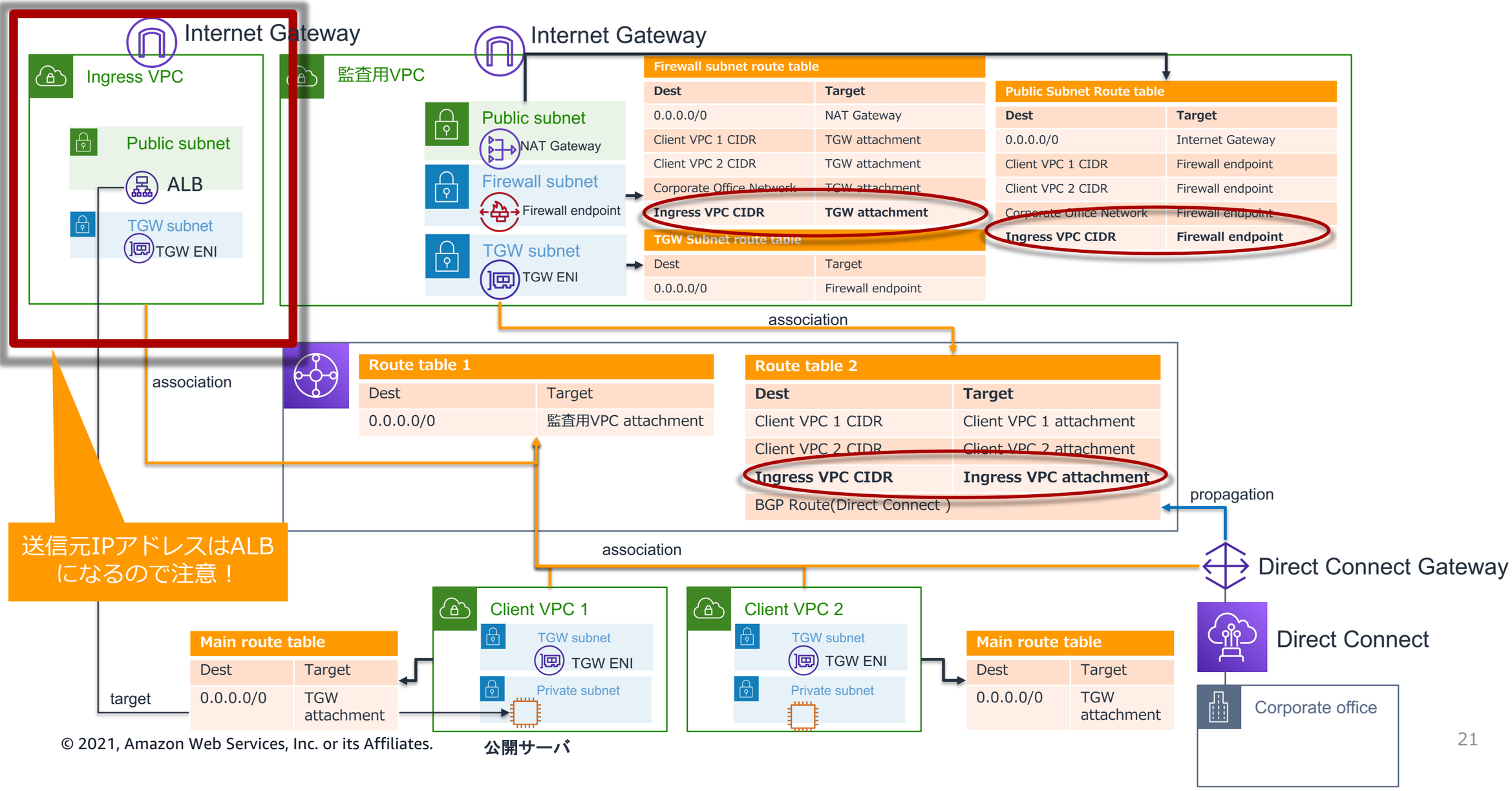
設計ポイントはルート設定にあり

✓インターネット宛の通信（戻り）



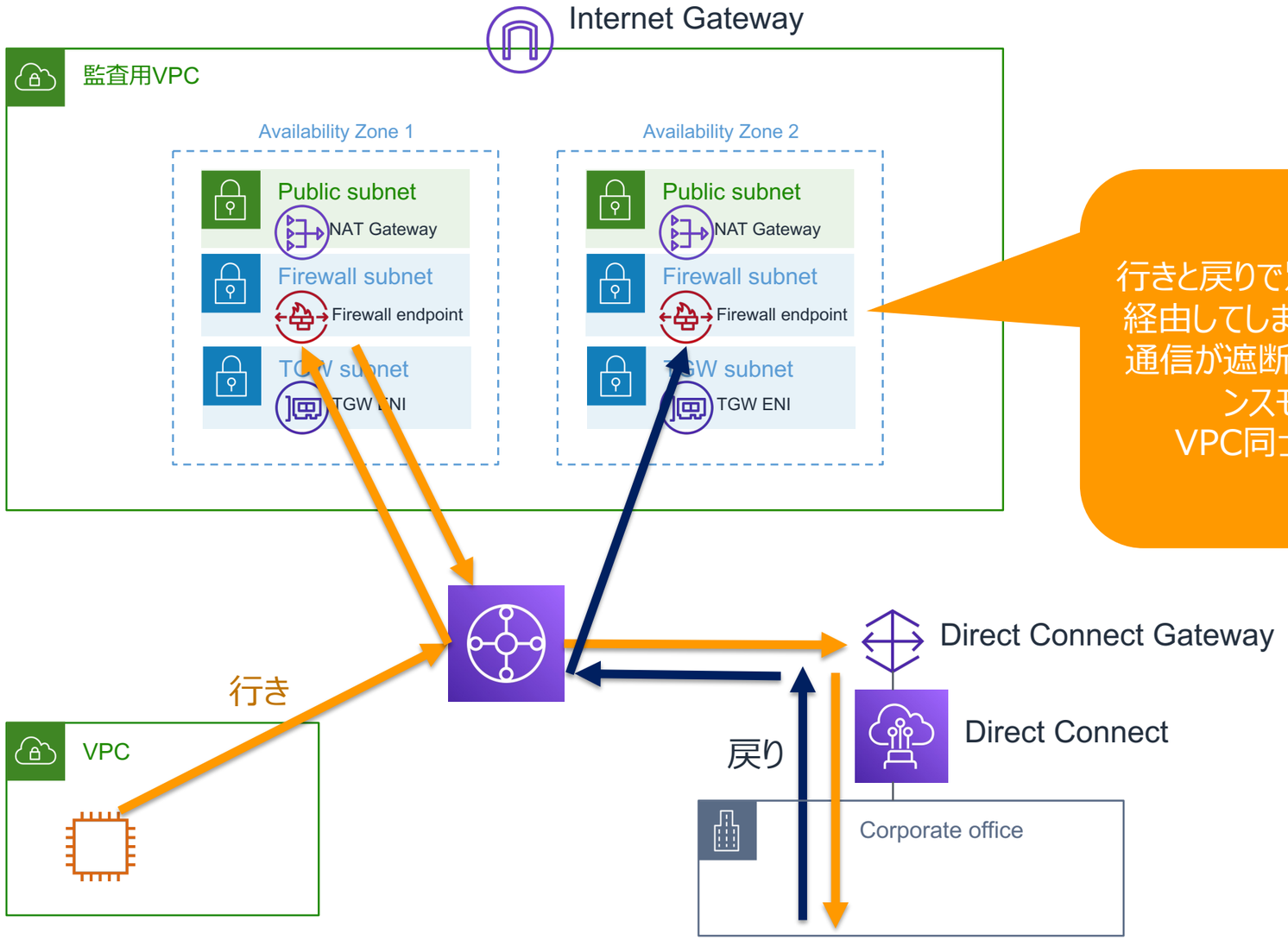
応用：公開サーバ宛の通信を集約する

✓ALBまたはNLBを使ってインターネットからの通信をまとめて検査する



マルチAZの際の注意事項

✓監査用のVPCをマルチAZ構成にする際には、Transit Gatewayのアプライアンスモード有効に！



参考：https://docs.aws.amazon.com/vpc/latest/tgw/transit-gateway-appliance-scenario.html

まとめ

- More specific routing により、VPC一つで完結する構成の幅が増えた
  - NAT GatewayをInternet Gateway側に配置できるようになり、Network Firewallから見て、source addrがNAT Gatewayになってしまう状態を解消できる
- Transit Gatewayを使って、Network FirewallがあるVPCに通信を集約することにより、一元的な監査が可能となる
  - Transit Gatewayに接続されているリソース同士の通信を必ずFirewall経由にする
- マルチAZ構成の場合は、Transit Gatewayのプライアンスモードを有効にする
  - そうしないと、行きと戻りで通信が非対称となり、正常に検査できない

本資料に関するお問い合わせ・ご感想

- 技術的な内容に関しましては、有料のAWSサポート窓口へ
  お問い合わせください
  - https://aws.amazon.com/jp/premiumsupport/
- 料金面でのお問い合わせに関しましては、カスタマーサポート窓口へ
  お問い合わせください（マネジメントコンソールへのログインが必要です）
  - https://console.aws.amazon.com/support/home#/case/create?issueType=customer-service
- 具体的な案件に対する構成相談は、後述する個別技術相談会をご活用ください

ご感想はTwitterへ！ハッシュタグは以下をご利用ください
#awsblackbelt

AWSの日本語資料の場所「AWS 資料」で検索

https://amzn.to/JPArchive

AWSのハンズオン資料の場所「AWS ハンズオン」で検索

AWS 初心者向けハンズオン

AWS 初心者向けに「AWS Hands-on for Beginners」と題し、初めて AWS を利用する方や、初めて対象のサービスを触る方向けに、操作手順の解説動画を見ながら自分のペースで進められるハンズオンをテーマごとにご用意しています。

https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-hands-on/

AWS Well-Architected個別技術相談会

- 毎週「W-A個別技術相談会」を実施中
  - AWSのソリューションアーキテクト（SA）に対策などを相談することも可能
- 申込みはイベント告知サイトから
  - https://aws.amazon.com/jp/about-aws/events/

AWS イベント で[検索]

ご視聴ありがとうございました