[AWS Black Belt Online Seminar]
AWS Network Firewall 入門

Network Specialist SA
Yosuke Okumura

AWS Black Belt Online Seminar とは

「サービス別」「ソリューション別」「業種別」のそれぞれのテーマに分け、アマゾン　ウェブ　サービス　ジャパン株式会社が主催するオンラインセミナーシリーズです。

- AWSの技術担当者が、AWSの各サービスについてテーマごとに動画を公開します
- お好きな時間、お好きな場所でご受講いただけるオンデマンド形式です
- 動画を一時停止・スキップすることで、興味がある分野・項目だけの聴講も可能、スキマ時間の学習にもお役立ていただけます

内容についての注意点

本資料では2021年06現在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）

所属：アマゾン ウェブ サービス ジャパン株式会社
技術統括本部 レディネスソリューション本部

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

この動画のゴール

- AWS Network Firewallの概要を理解する
- 他のセキュリティサービスとの違いを理解する
- どんな機能があるのか、どんなアーキテクチャで設計するのか理解する

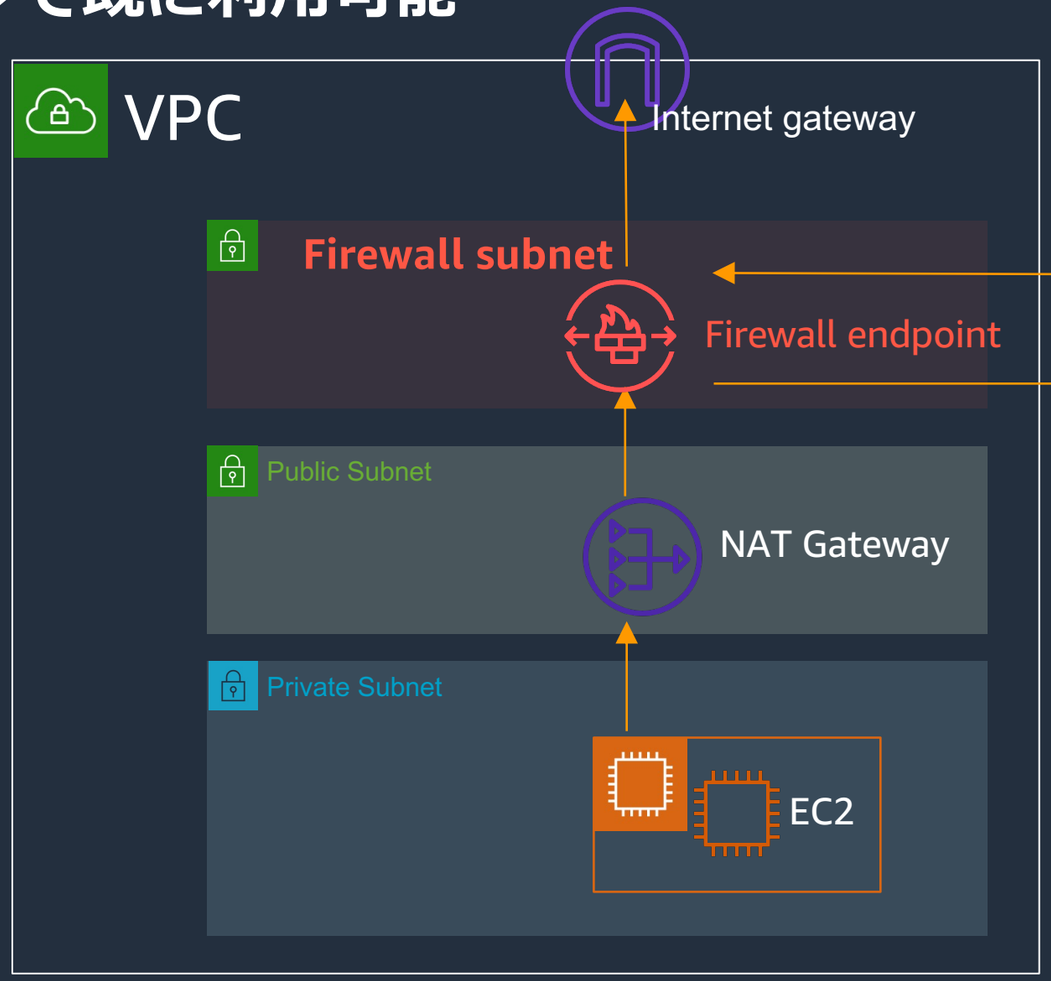
Agenda

- AWS Network Firewall 概要
- VPCのセキュリティコンポーネント
- AWS Network Firewall アーキテクチャ
- AWS Network Firewall ルール設定のポイント
- まとめ

AWS Network Firewall 概要

AWS Network Firewall 概要

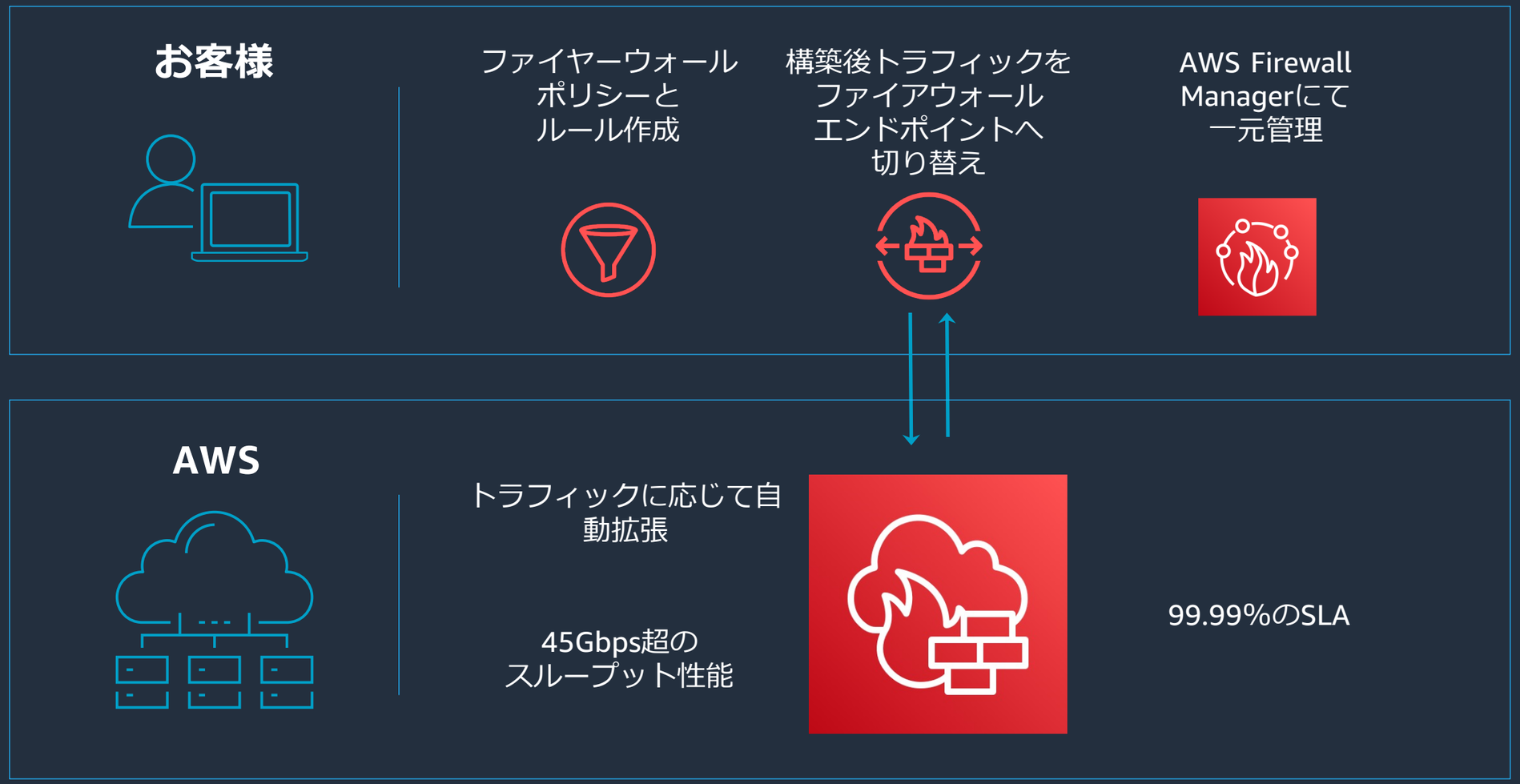
VPCのサブネットに配置するマネージドファイアウォールサービス
東京と大阪リージョンで既に利用可能



AWS Network Firewall

- スケーラブル
  - 45Gbps超
- マネージド

AWS Network Firewall 概要



AWS Network Firewall 概要

利用開始までのステップ

1. VPCにファイアウォール用のサブネットを作成
    - ファイアウォール専用にすることを推奨。このサブネットに他のリソースを配置してしまうと、そのリソースは検査できない
2. ファイアウォールの作成
    - 設置するサブネットの選択
        - 選択したサブネットにファイアウォールエンドポイントが作成される
    - ファイアウォールのルール設定
3. ルーティング設定
    - 検査対象トラフィックがファイアウォールエンドポイントを通過するようにVPCのルートテーブルの設定を行う

AWS Network Firewall 概要

機能サマリー

- ファイアウォール
  - ステートレスパケットフィルタ(5-tuple)
  - ステートフルパケットフィルタ(5-tuple)
  - ステートフルパケットフィルタ(ドメインリスト)
  - Suricata互換IPS
- 管理
  - CloudWatchルールメトリック
  - flow log、イベント、ルール別のログ
  - S3やCloudWatch Logs、Kinesis Firehoseへのログ格納
  - AWS Firewall Managerによる一元管理

AWS Network Firewall 概要

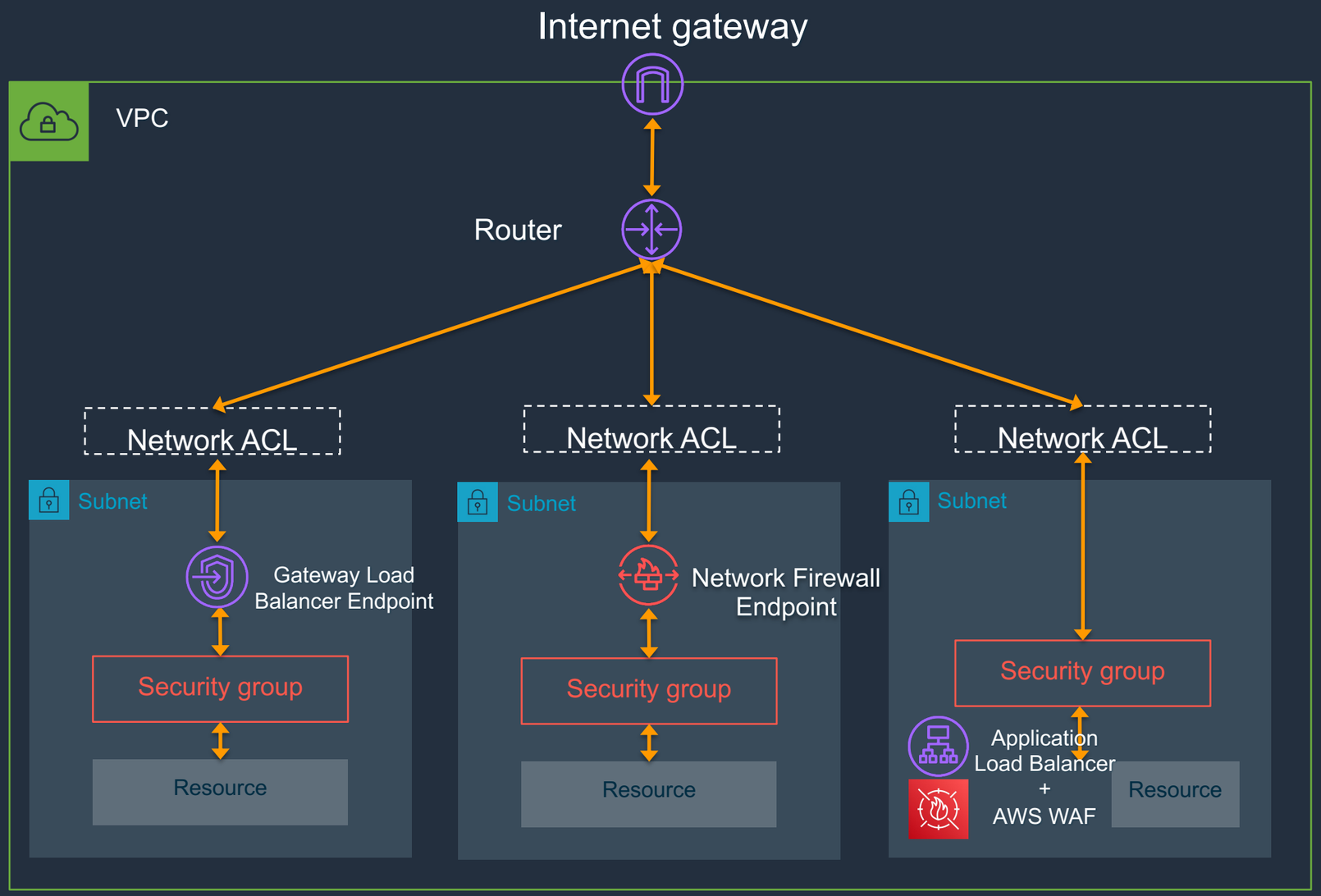
SLA、料金体系

1. SLA
    - 稼働率99.99%
    - 詳しい適用条件など https://aws.amazon.com/jp/network-firewall/sla/

2. 料金体系
    - ファイアウォールエンドポイントに対する時間課金 $0.395/hr
    - トラフィック処理量に応じた課金 $0.065/GB
    - NATゲートウェイとの併用時には免除ルールあり
    - 詳しい内容　https://aws.amazon.com/jp/network-firewall/pricing/

VPCのセキュリティコンポーネント

VPCのセキュリティコンポーネント



コンポーネント
- Network ACL
- Security Group
- AWS Gateway Load Balancer
- AWS Network Firewall
- AWS WAF

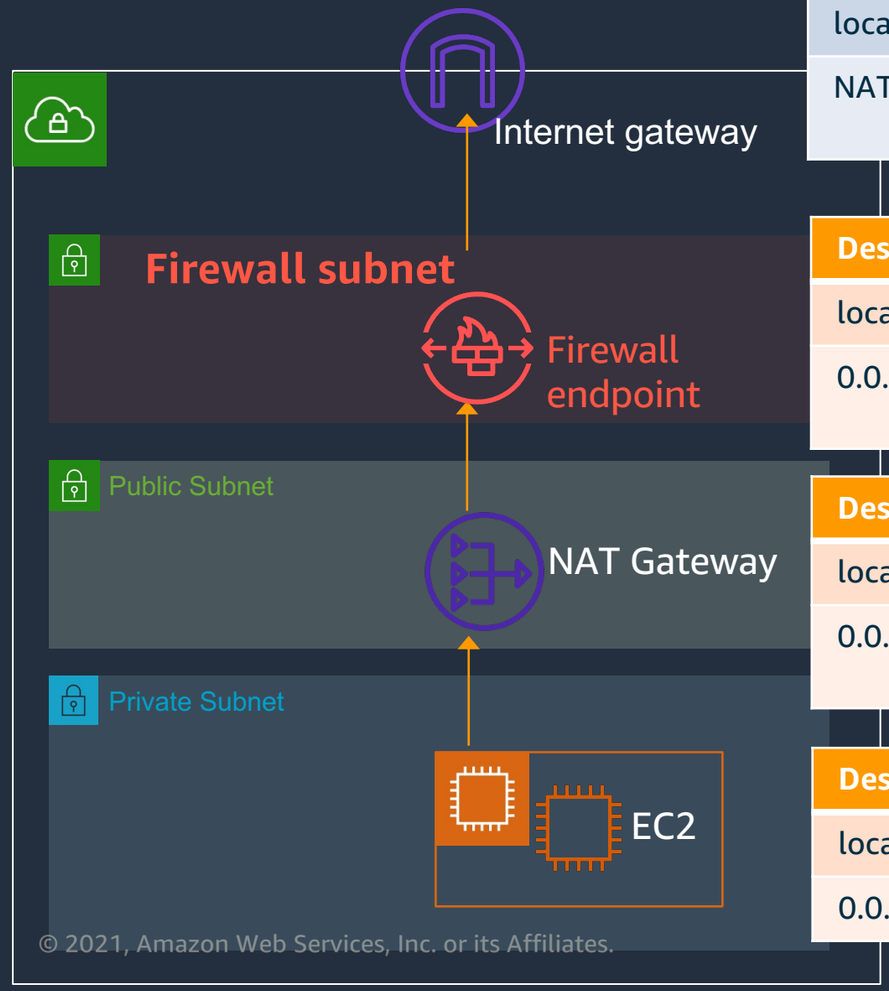
VPCのセキュリティコンポーネント

Firewall	AWS Network Firewall	AWS Gateway Load Balancer + Appliance	Security Group	Network ACL	AWS WAF
主なユースケース	トラフィック検査とフィルタリング 侵入防止	様々なセキュリティアプライアンスを冗長化	アクセス制御	アクセス制御	Webアプリ保護、ボット制御、入力検証
Firewall type	ステートフルとステートレス	アプライアンスに準ずる	ステートフル	ステートレス	ステートレス
OSIレイヤー	L3 – L7	L3 – L7	L3 – L4	L3 – L4	L7
AWS Firewall Manager	対応	未対応	対応	未対応	対応
料金	あり	あり	なし	なし	あり

AWS Network Firewall アーキテクチャ

AWS Network Firewall アーキテクチャ

同VPC内リソースのインターネット宛の通信を検査する



Destination	Target
local	-
NAT Gateway	Firewall Endpoint

Destination	Target
local	-
0.0.0.0	Internet Gateway

Destination	Target
local	-
0.0.0.0	Firewall endpoint

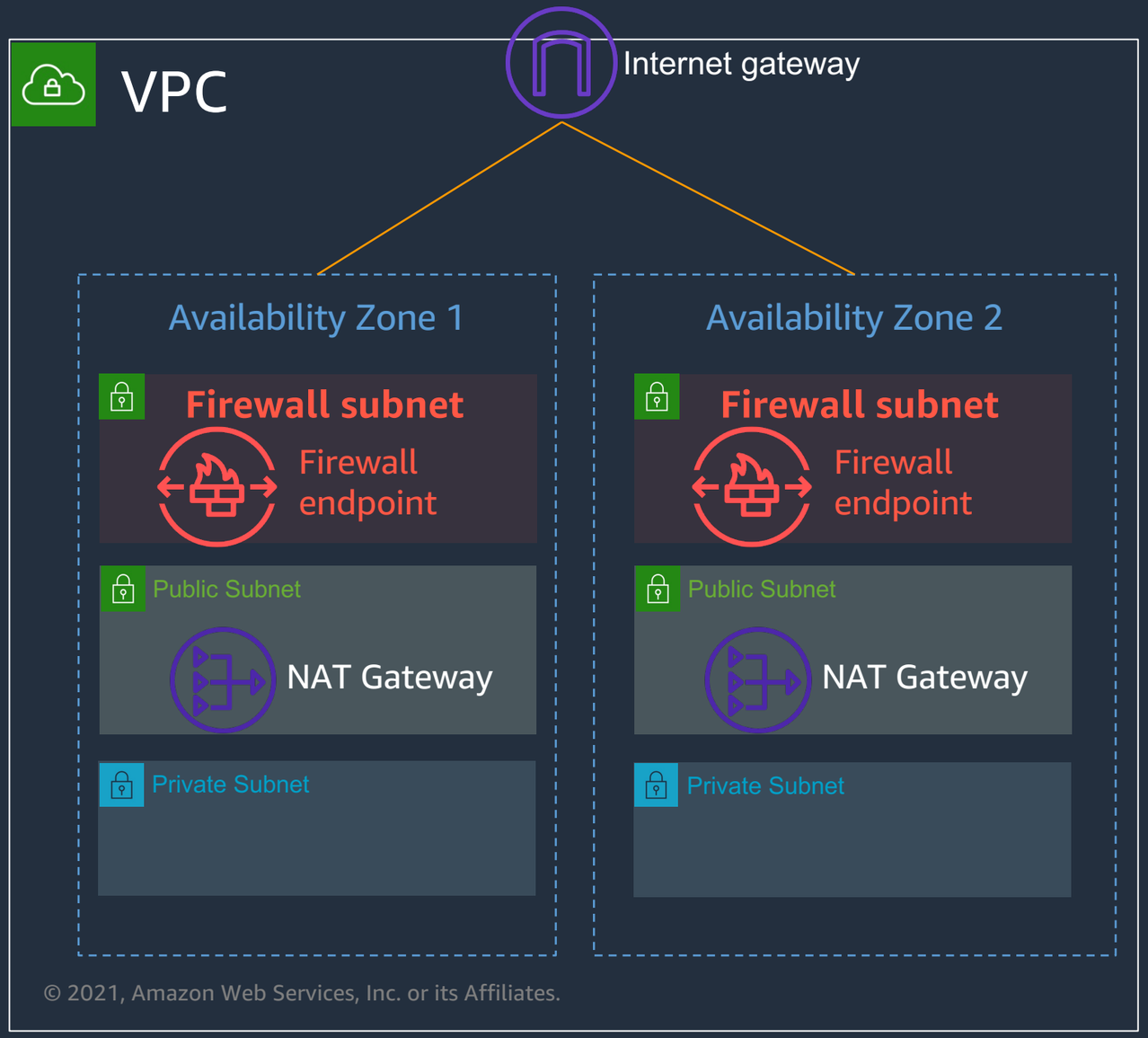
Destination	Target
local	-
0.0.0.0	NAT Gateway

Point

- 行き/戻りの通信が対称になるようにルート設定を行う
  - Ingress Routing を利用して、Internet GatewayからVPC方向の通信がFirewall endpointに戻るように設定
  - この設定を行わないと、localルートにより戻りの通信がファイアウォールを経由せず直接NATゲートウェイに戻ってしまう
- NATしてからファイアウォールに到達するため、送信元ベースのフィルタルールの設計には注意が必要

AWS Network Firewall アーキテクチャ

マルチAZ構成時のアーキテクチャ



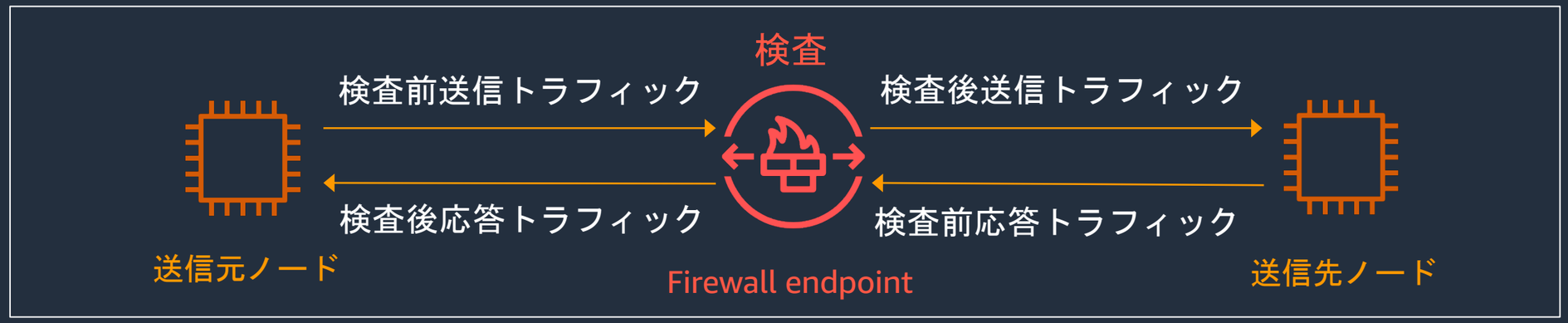
Point

- 各AZにそれぞれFirewall subnetとエンドポインを配置する
- 一つのファイアウォールで、AZごとにエンドポイントを作成可能
  - AZ1につき1エンドポイント まで
- ここでも通信の対称性については留意が必要
  - 図の構成の場合はそれぞれのAZ向けのIngress Routingを前述と同様の考え方で設定
- VPCを跨る事はできない（複数の異なるVPCで同じNetwork Firewallのエンドポイントを使うことはできない）

AWS Network Firewall ルール設定のポイント

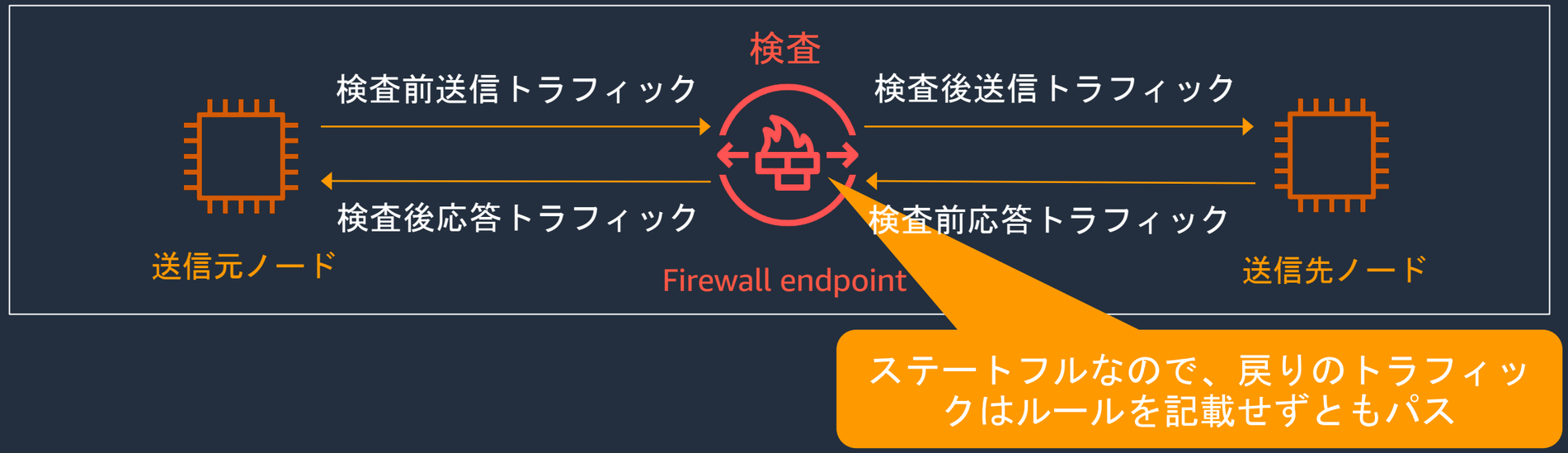
AWS Network Firewall ルール設定のポイント

- ステートレス 5-tupleフィルタ
  - どのようにトラフィックを検査するかのルールを、ACLのように優先度（評価順）つけて列挙していく
  - ルールにマッチしなかった場合のアクションを指定可能（Drop/Pass/ステートフルルールに移行）
  - ステートレスであるため、Ingress/Egress両方を設定



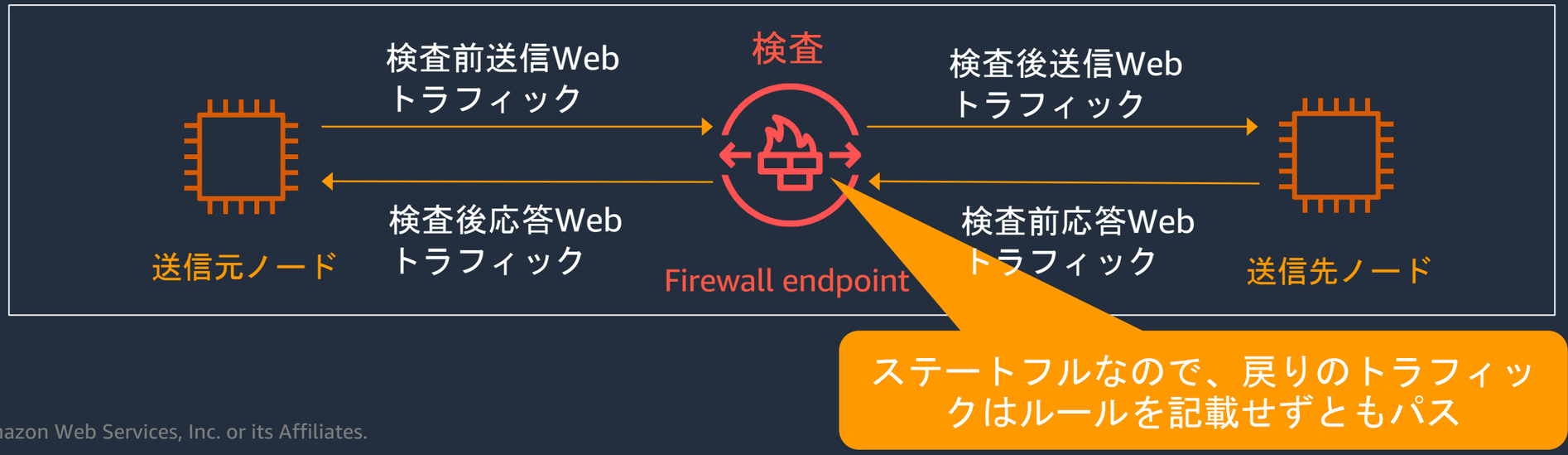
AWS Network Firewall ルール設定のポイント

- ステートフル5-tupleフィルタ
  - どのようにトラフィックを検査するかのルールを、優先度を付けずに列挙していく
  - トラフィックをパスするルールが常に優先され、マッチしなかった場合のアクションはPass固定となる
  - ステートフルなので、パスした通信に対する応答トラフィックは、自動的にパスされる



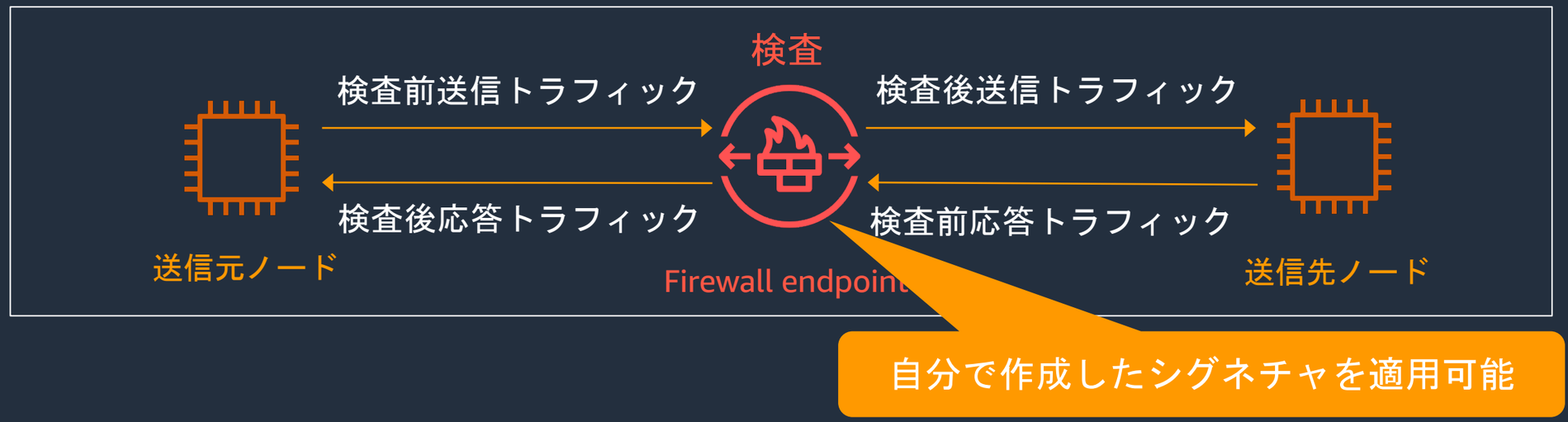
AWS Network Firewall ルール設定のポイント

- ステートフルドメインリストフィルタ
  - Web通信(HTTP/HTTPS)を宛先ドメインベースでフィルタ
  - マッチしなかったときのアクションを指定可能(Drop/Pass)
  - ワイルドカード指定可能（例: “.example.com” → example.comのすべてのサブドメインを指定)
  - SSL/TLSの場合SNIを見て検査するので、ESNIが使われている通信には適用不可
  - 送信元ノードがFirewallエンドポイントのあるVPCの外にある場合は、別途CLIで設定が必要
    - https://docs.aws.amazon.com/network-firewall/latest/developerguide/stateful-rule-groups-domain-names.html



AWS Network Firewall ルール設定のポイント

- Suricata互換IPS
  - Suricataと互換性のあるIPS機能
  - ステートフル5-tupleフィルタ、ステートフルドメインリストフィルタはこの機能でも実現可能
  - 様々なルールを組み合わせて記載する場合は、こちらに集約してしまうと運用が楽になる
  - 評価順が指定可能になるなど、柔軟な制御が可能になり、機能も豊富です
  - Suricataのシグネチャ作成の知識が必要
  - https://docs.aws.amazon.com/network-firewall/latest/developerguide/stateful-rule-groups-ips.html



まとめ

まとめ

- AWS Network Firewallの特長
  - AWSマネージドで、スケールアウトや冗長設計が不用
  - ただし、トラフィックを受け取るエンドポイントはAZ単位なので、マルチAZの設計は必要
  - 99.99%のSLA

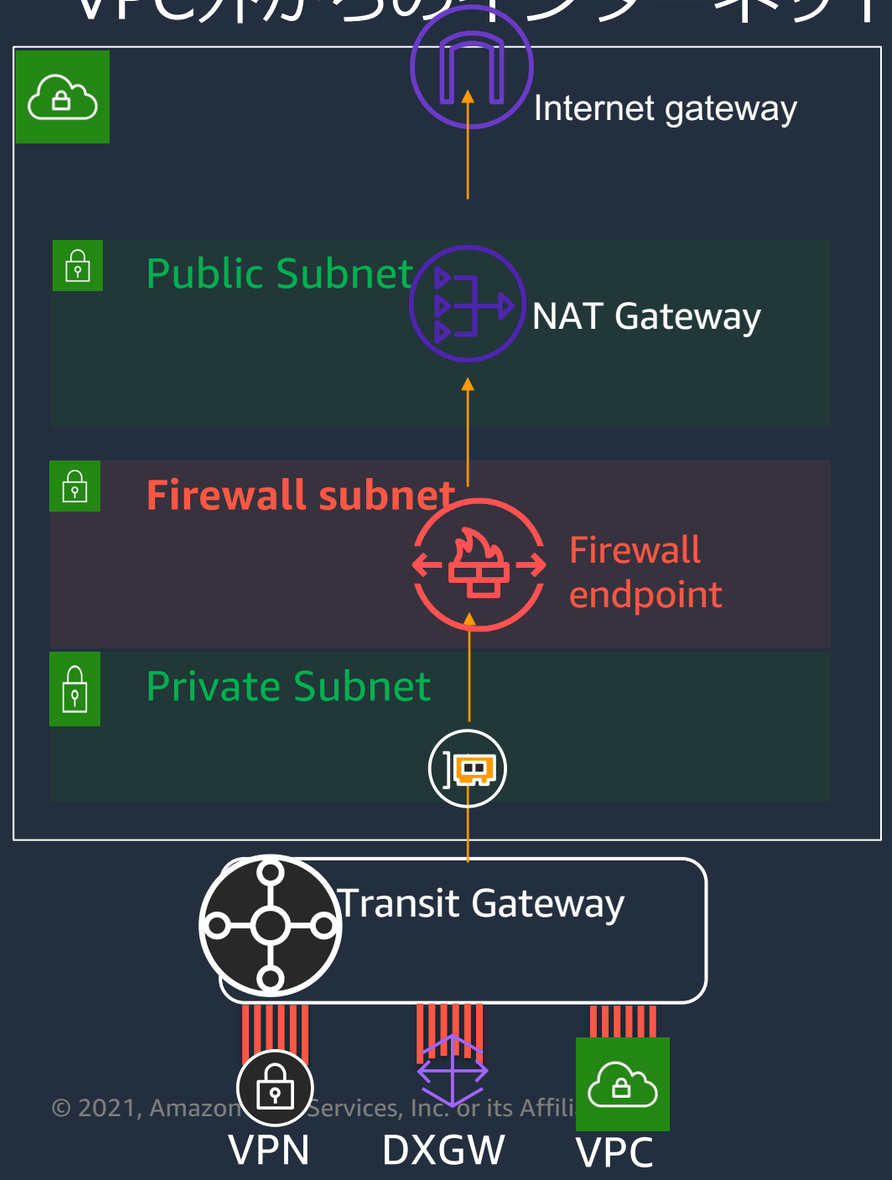
- VPCネットワークセキュリティは、様々なセキュリティ機能と合わせて考える
  - 各機能の特徴を把握して適切なサービス選択を行う

- アーキテクチャ設計
  - トラフィックをどのようにファイアウォール エンドポイントを経由させるかというルート設計が肝
  - 特に戻りの経路に注意が必要（インターネットゲートウェイがある場合はIngress Routingを利用）

- ルール設計
  - ステートレス、ステートフルの動きを理解する
  - 各機能でルールにマッチしなかった場合のアクションが異なるので注意する
  - Suricata互換IPS機能は、他のすべてのルールの機能を表現可能
  - ただし、自分でシグネチャを作成する必要がある

APPENDIX

VPC外からのインターネット通信を検査する

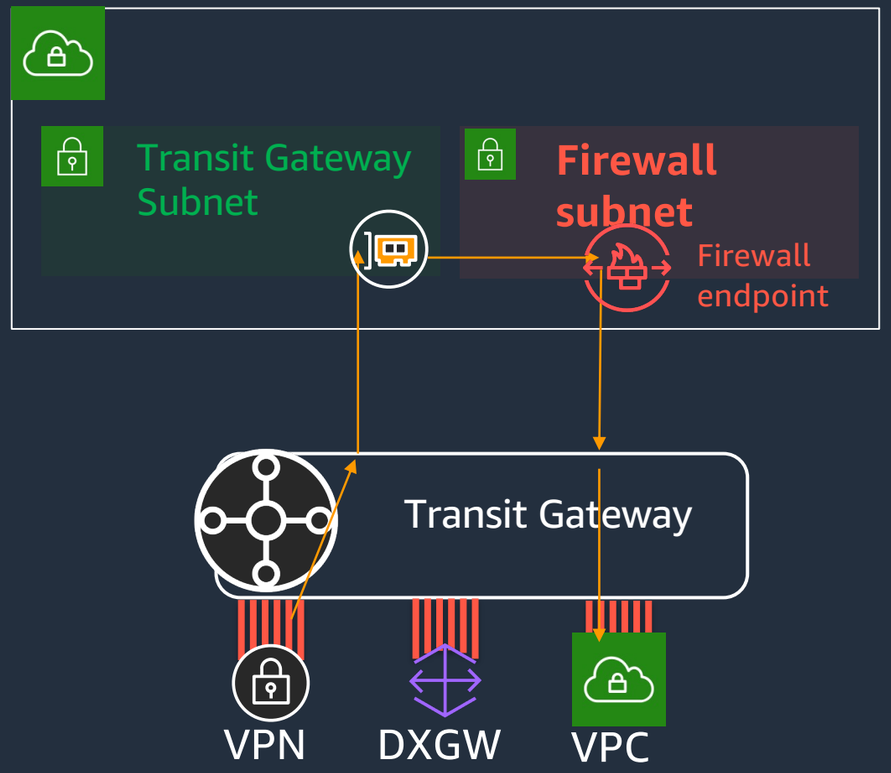


Point

- 集合型のインターネットゲートウェイを構成可能
- Transit Gatewayでトラフィックをファイアウォール用のVPCに集約
- ドメインリストフィルタは、デフォルトではFirewall subnetがあるVPC CIDRからの通信しか検査しないため、CLIでの設定が必要
  - https://docs.aws.amazon.com/network-firewall/latest/developerguide/stateful-rule-groups-domain-names.html
- VPCピアリングやVGW経由の利用は非対応

APPENDIX：

トラフィック検査用のミドルボックスVPCを構成する



Point

- Transt Gatewayのリファレンスアーキテクチャでは接続されたリソース同士の通信をミドルボックスVPCでインスペクションする構成が紹介されている。AWS Network Firewallは、そのミドルボックスとして機能させることができる
  - Transit Gatewayに接続されているリソース間の通信を検査する
  - VPC同士やオンプレミスからの通信など

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

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

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

過去資料
https://amzn.to/JPArchive