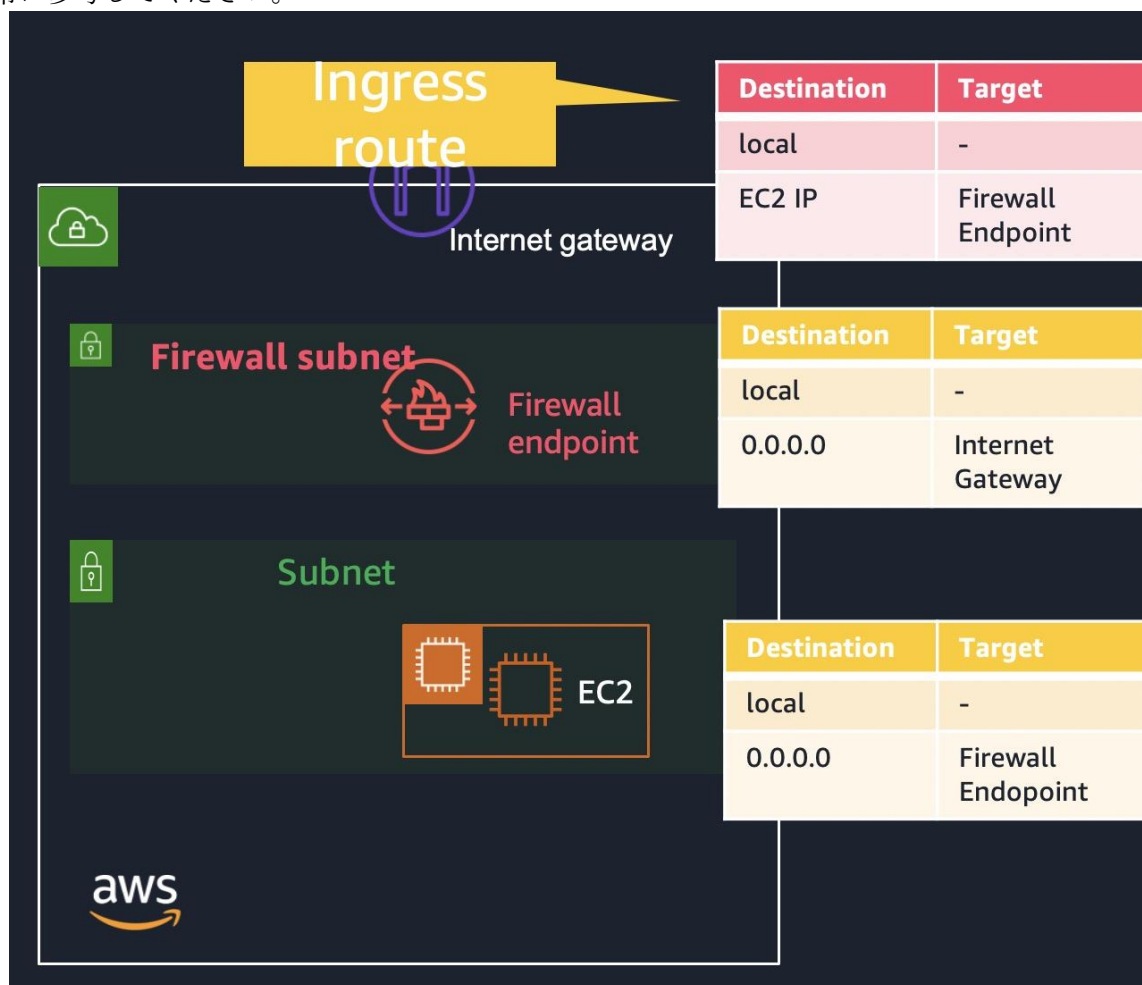


[はじめに]このハンズオンでは多くの設定パラメータを取り扱います。それらを管理する memo.txt が用意されていますので、手順の指示に従い memo.txt に設定項目を書き込んで下さい。

また VPC の少し複雑な構成を構築するため、作業途中で混乱してしまった場合は以下を常に参考してください。



## VPC と Public サブネット、EC2 の起動

1. VPC ウィザードを起動します



2. [1 個のパブリックサブネットを持つ VPC]を選びます



3. memo.txt の内容を参考にしながら値を入力し、[VPC の作成]を押します

ステップ 2: 1 個のパブリックサブネットを持つ VPC

IPv4 CIDR ブロック: 10.10.0.0/16 (65531 利用可能な IP アドレス)

IPv6 CIDR ブロック: ☒ IPv6 CIDR ブロックなし  
☐ Amazon が提供した IPv6 CIDR ブロック  
☐ IPv6 CIDR block owned by me

VPC 名: nwfwvpc

パブリックサブネットの IPv4 CIDR: 10.10.0.0/24 (251 利用可能な IP アドレス)

アベイラビリティゾーン: 指定なし

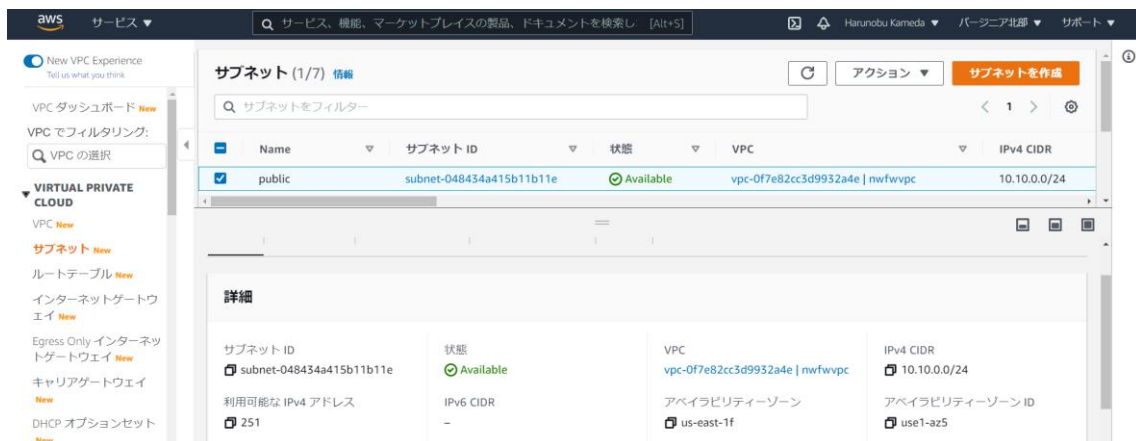
サブネット名: public

サービスエンドポイント:

DNS ホスト名を有効化: ☒ はい ☐ いいえ

ハードウェアのデナンス: デフォルト

4. 作成されたら画面左ペイン、[サブネット]を選択し、作成されている Public という名のサブネットの AZ 情報を memo.txt の[Public Subnet AZ]に記載しておきます。



- 同様にインターネットゲートウェイの ID を memo.txt の [Internet Gateway] に記載します
- EC2 の画面から [インスタンスを起動] を押します



- wordpress と検索し、[AWS Marketplace] をクリックします



- [WordPress Certified by Bitnami] を選びます。(ブラウザでアクセス可能な EC2 を起動したいだけなので何でも大丈夫です)



- 画面一番下の [Continue] を押します
- [t2.micro] を選び、[次のステップ] をおします

	ファミリー	タイプ	vCPU	メモリ (GiB)	インスタンスストレージ (GiB)	EBS 最適化利用	ネットワークパフォーマンス	IPv6 サポート
	t2	t2.nano	1	0.5	EBS のみ	-	低から中	はい
<input checked="" type="checkbox"/>	t2	t2.micro <small>無料利用枠の制限</small>	1	1	EBS のみ	-	低から中	はい
<input type="checkbox"/>	t2	t2.small	1	2	EBS のみ	-	低から中	はい
<input type="checkbox"/>	t2	t2.medium	2	4	EBS のみ	-	低から中	はい
<input type="checkbox"/>	t2	t2.large	2	8	EBS のみ	-	低から中	はい

キャンセル 戻る 確認と作成 次のステップ: インスタンスの詳細の設定

11. ネットワーク設定を先程作成したサブネットに配置するように指定します。[自動割り当てパブリック IP]を有効にしてください

ネットワーク vpc-0f7e82cc3d9932a4e | nwfwvpc 新しい VPC の作成

サブネット subnet-048434a415b11b11e | public | us-east-1f 新しいサブネットの作成  
251 個の IP アドレスが利用可能

自動割り当てパブリック IP ☒ 有効

12. その他全てデフォルトで[確認と作成]をおします。次の画面で再度[起動]をおします
13. [キーペアなしで続行]を選び[インスタンスの作成]をおします。(SSH の FW による制御などをテストされたい方は正しい鍵を設定してください。このハンズオンでは割愛します)

既存のキーペアを選択するか、新しいキーペアを作成します。

キーペアは、AWS が保存する**パブリックキー**とユーザーが保存する**プライベートキーファイル**で構成されます。組み合わせて使用することで、インスタンスに安全に接続できます。Windows AMI の場合、プライベートキーファイルは、インスタンスへのログインに使用されるパスワードを取得するために必要です。Linux AMI の場合、プライベートキーファイルを使用してインスタンスに SSH で安全に接続できます。

注: 選択したキーペアは、このインスタンスに対して権限がある一連のキーに追加されます。 [「パブリック AMI から既存のキーペアを削除する」](#) の詳細情報をご覧ください。

既存のキーペアの選択

キーペアの選択

transfertest

☐ 選択したプライベートキーファイル (transfertest.pem) へのアクセス権があり、このファイルなしではインスタンスにログインできないことを認識しています。

キャンセル

インスタンスの作成

14. EC2 が起動中で順次ステータスが以下のように変更していくので待ちます

<input type="checkbox"/>	Name	インスタンス ID	インスタンスの状態	インスタンス...	ステータスチェ...
<input type="checkbox"/>	-	i-04551d4630d4b38d0	保留中	t2.micro	-

<input type="checkbox"/>	Name	インスタンス ID	インスタンスの状態	インスタンス...	ステータスチェ...
<input type="checkbox"/>	-	i-04551d4630d4b38d0	🟢 実行中	t2.micro	🕒 初期化しています。

待っている間に、Name に[wordpress]と設定しておきます。インスタンス ID を memo.txt の[EC2 ID]にコピーしておきます  
ステータスチェックが緑色で 2/2 と表示されればアクセスが可能です

<input type="checkbox"/>	Name	インスタンス ID	インスタンスの状態	インスタンス...	ステータスチェ...
<input type="checkbox"/>	wordpress	i-04551d4630d4b38d0	🟢 実行中	t2.micro	🟢 2/2 のチェックに...

左のチェックボックスにチェックをつけ、パブリック IPv4 DNS の値を、memo.txt の[EC2 PublicDNS]にコピーした後、ブラウザでアクセスしてみてください

- wordpress の画面が表示されれば完了です。記事を書くわけでありませんので、表示される内容はなんでも大丈夫です。
- VPC 画面左ペインからルートテーブルをクリックします。EC2 を起動したサブネットに紐づいているルートテーブルを特定し、その ID を memo.txt の[Route Table ID]にコピーします。また、Name を[public]に変更しておきます。

このルートテーブルは、以下のように VPC 内部の通信は local、それ以外の通信(つまり VPC 外部への通信)は全て Internet Gateway ヘルパーティングする、となっています。後ほど Network Firewall の構築を行ったあと、VPC 外部への通信は Internet Gateway ではなく、Network Firewall のエンドポイントを指定します。

送信先	ターゲット	ステータス	伝播済み
10.10.0.0/16	local	🟢 アクティブ	いいえ
0.0.0.0/0	igw-089ca8e6f3ff7ce21	🟢 アクティブ	いいえ

## Network Firewall 用ネットワークの構築

- 今までの手順で、Network Firewall で保護すべき環境ができました。これから、Network Firewall 専用サブネットを同じ VPC に作成していきます。  
VPC 画面左ペインから、サブネットをクリックし、[サブネットを作成]をおします

New VPC Experience

VPC ダッシュボード

VPC でフィルタリング:

VPC の選択

VIRTUAL PRIVATE CLOUD

VPC

サブネット

ルートテーブル

インターネットゲートウェイ

サブネット (1/7) 情報

サブネットをフィルター

<input type="checkbox"/>	Name	サブネット ID	状態	VPC	IPv4 CIDR
<input checked="" type="checkbox"/>	public	subnet-048434a415b11b11e	🟢 Available	vpc-0f7e82cc3d9932a4e   nwf...	10.10.0.0/24

subnet-048434a415b11b11e / public

詳細 フローログ ルートテーブル ネットワーク ACL 共有 タグ

18. 先程 EC2 を起動した VPC を選びます

### VPC

VPC ID  
この VPC にサブネットを作成します。

vpc-0f7e82cc3d9932a4e (nwfwvpc) ▼

#### 関連付けられた VPC CIDR

IPv4 CIDR  
10.10.0.0/16

19. 以下のように設定して[サブネットを作成]をおします

### サブネットの設定

サブネットの CIDR ブロックとアベイラビリティゾーンを指定します。

#### サブネット 1 (1 個中)

サブネット名  
「Name」というキーと、指定した値を使用してタグを作成します。

fw

名前の長さは最大 256 文字です。

アベイラビリティゾーン [情報](#)  
サブネットが存在するゾーンを選択するか、Amazon が選択するゾーンを受け入れます。

米国東部 (バージニア北部) / us-east-1f ▼

IPv4 CIDR ブロック [情報](#)

10.10.1.0/24 ✕

#### ▼ タグ - オプション

キー	値 - オプション
10.10.1.0/24 ✕	fw ✕

[新しいタグを追加](#)

さらに 49 個の タグ. を追加できます。

AZ は必ず EC2 と同じにしてください。その他の値は memo.txt を参考にして入力してください

20. 現在 VPC には Subnet が 2 つ存在しています。新しくできたサブネット ID を memo.txt にコピーしておきます

サブネット (2) 情報					
<input type="text" value="サブネットをフィルター"/> <span>search: vpc-0f7e82cc3d9932a4e X</span> <span>フィルターをクリア</span>					
<input type="checkbox"/>	Name	サブネット ID	状態	VPC	IPv4 CIDR
<input type="checkbox"/>	public	subnet-048434a415b11b11e	Available	vpc-0f7e82cc3d9932a4e   nwf...	10.10.0.0/24
<input type="checkbox"/>	fw	subnet-0be6820e1ec9032b8	Available	vpc-0f7e82cc3d9932a4e   nwf...	10.10.1.0/24

21. VPC 画面左ペインから、ファイアウォールを選んでクリックします



22. [ファイアウォールの作成]をおします

▼ 概要

### ファイアウォール

ファイアウォールは、保護する VPC を、ファイアウォールポリシーで定義されている保護動作に接続します。保護するアベイラビリティゾーンごとに、ファイアウォールエンドポイント専用のパブリックサブネットをネットワークファイアウォールに提供します。

ファイアウォールを使用するには、VPC ルートテーブルを更新して、ファイアウォールのエンドポイントを介して着信トラフィックと発信トラフィックを送信します。

### ファイアウォールポリシー

ファイアウォールポリシーは、ステートレスおよびステートフルなルールグループおよびその他の設定のコレクションで、ファイアウォールの動作を定義します。

各ファイアウォールは 1 つのファイアウォールポリシーにのみ関連付けることができますが、1 つのファイアウォールポリシーを複数のファイアウォールに使用できます。

### ルールグループ

ネットワークファイアウォールのルールグループは、ネットワークトラフィックの検査と処理方法を定義するステートレスまたはステートフルなルールのコレクションです。

ルールの設定には、5 タプルとドメイン名のフィルタリングが含まれます。Suricata オープンソースルール仕様を使用してステートフルなルールを提供することもできます。

23. 名前を適当につけます

**名前**  
ファイアウォールの一意の名前を入力します。

nwfw0609

名前は 1~128 文字にする必要があります。有効な文字は a~z、A~Z、0~9、- (ハイフン) です。名前の先頭と末尾にハイフンを使用することはできません。また、ハイフンを 2 つ連続して含めることはできません。

**説明 - オプション**

VPC のネットワークトラフィックをモニタリングし、制御するファイアウォール。

説明には 0~256 文字を使用できます。

**VPC**  
このファイアウォールを作成する VPC を選択します。

nwfwvpc ▼

**ファイアウォールサブネット**  
ファイアウォールは、複数のアベイラビリティゾーンで、ゾーンごとに 1 つのサブネットにデプロイできます。各サブネットには、少なくとも 1 つの利用可能な IP アドレスが必要です。

**アベイラビリティゾーン**      **サブネット**

us-east-1f ▼      fw ▼      削除

新しいサブネットを追加

24. VPC は EC2 を起動した VPC を指定します。AZ も同様に同じです。

(NetworkFirewall は AZ 単位で動作するため、必ず揃えてください)。サブネットは EC2 が起動している public ではなく、fw を指定します。つまり以下のような経路を作ります。

Internet ⇔ Internet Gateway ⇔ fw subnet (Network Firewall) ⇔ public subnet

**名前**  
ファイアウォールの一意の名前を入力します。

nwfw0609

名前は 1~128 文字にする必要があります。有効な文字は a~z、A~Z、0~9、- (ハイフン) です。名前の先頭と末尾にハイフンを使用することはできません。また、ハイフンを 2 つ連続して含めることはできません。

**説明 - オプション**

VPC のネットワークトラフィックをモニタリングし、制御するファイアウォール。

説明には 0~256 文字を使用できます。

**VPC**  
このファイアウォールを作成する VPC を選択します。

nwfwvpc ▼

**ファイアウォールサブネット**  
ファイアウォールは、複数のアベイラビリティゾーンで、ゾーンごとに 1 つのサブネットにデプロイできます。各サブネットには、少なくとも 1 つの利用可能な IP アドレスが必要です。

**アベイラビリティゾーン**      **サブネット**

us-east-1f ▼      fw ▼      削除

新しいサブネットを追加

25. ポリシーは後で設定しますが、何か必要なため、[空の…]を選んで適当な名前を付けます。



### 関連付けられたファイアウォールポリシー

ファイアウォールポリシーには、ファイアウォールがウェブトラフィックを検査および管理する方法を定義するルールグループのリストが含まれています。ファイアウォールを作成した後で、関連するファイアウォールポリシーを設定できます。

ファイアウォールポリシーを関連付ける方法を選択する

- ☒ 空のファイアウォールポリシーを作成して関連付ける
- ☐ 既存のファイアウォールポリシーを関連付け

新しいファイアウォールポリシー名

ファイアウォールポリシーの一意の名前を入力します。

nwfwpolicy

名前は 1~128 文字にする必要があります。有効な文字は a~z、A~Z、0~9、- (ハイフン) です。名前の先頭と末尾にハイフンを使用することはできません。また、ハイフンを 2 つ連続して含めることはできません。

説明 - optional

ファイアウォールが VPC のネットワークトラフィックをモニタリングおよび制御する方法を定義するファイアウォール

説明には 0~256 文字を使用できます。

26. [ファイアウォールを作成]をおします

27. ステータスが[プロビジョニング]になるので、しばらく待ちます

**概要**

指示を非表示

<b>ステップ 1: ファイアウォールを作成する 情報</b> ファイアウォールは、保護する VPC とファイアウォールポリシーを接続します。ファイアウォールを作成したら、いつでもステップ 2 に進むことができます。ステップ 3 に進む前に、ファイアウォールのステータスがである必要があります。 <b>準備完了。</b>	<b>ステップ 2: ファイアウォールポリシーを設定する 情報</b> ファイアウォールポリシーは、ファイアウォールが VPC 内のトラフィックをモニタリングおよび処理する方法を定義します。ステートレスでステートフルなルールグループを設定してパケットとトラフィックフローをフィルタリングし、デフォルトのトラフィック処理を定義します。	<b>ステップ 3: ファイアウォール経由でトラフィックをルーティングする 情報</b> VPC ルートテーブルは、ネットワークトラフィックフローを定義します。ルートテーブルを更新して、ファイアウォールのエンドポイントを介してトラフィックを送信します。たとえば、VPC サブネットとインターネットゲートウェイまたはトランジットゲートウェイの間にファイアウォールエンドポイントを挿入できます。
ファイアウォールのステータス 🔄 プロビジョニング	関連付けられたファイアウォールポリシー nwfwpolicy  ⚠️ このファイアウォールポリシーには、ルールグループがありません。 <div>ルールグループを追加 ▼</div>	関連付けられた VPC vpc-0f7e82cc3d9932a4e <div>ルートの更新ガイドを表示</div>

28. 待っている間に、fw subnet 用ルートテーブルを作成します。VPC 画面左ペインからサブネットをクリックし、[ルートテーブルを作成]をおします。名前に[fwrt]をつけ、VPC は EC2 を起動したものを選択します

**ルートテーブル設定**

**名前 - オプション**  
「Name」というキーと、指定した値を使用してタグを作成します。  
fwrt

**VPC**  
このルートテーブルに使用する VPC。  
vpc-0f7e82cc3d9932a4e (nwfwvpc) ▼

29. [ルートテーブルを作成]をおします

30. 作成されたルートテーブル ID を memo.txt の[FW Route Table ID]にコピーします

31. ブラウザでネットワークファイアウォールのタブに戻ります。以下のように、準備完了と表示されていれば起動は完了。fw subnet で Network Firewall が起動されました

概要

指示を非表示

ステップ 1: ファイアウォールを作成する 情報

ファイアウォールは、保護する VPC とファイアウォールポリシーを接続します。ファイアウォールを作成したら、いつでもステップ 2 に進むことができます。ステップ 3 に進む前に、ファイアウォールのステータスがである必要があります。 **準備完了**

ステップ 2: ファイアウォールポリシーを設定する 情報

ファイアウォールポリシーは、ファイアウォールが VPC 内のトラフィックをモニタリングおよび処理する方法を定義します。ステートレスでステートフルなルールグループを設定してパケットとトラフィックフローをフィルタリングし、デフォルトのトラフィック処理を定義します。

ステップ 3: ファイアウォール経由でトラフィックをルーティングする 情報

VPC ルートテーブルは、ネットワークトラフィックフローを定義します。ルートテーブルを更新して、ファイアウォールのエンドポイントを介してトラフィックを送信します。たとえば、VPC サブネットとインターネットゲートウェイまたはトランジットゲートウェイの間にファイアウォールエンドポイントを挿入できます。

ファイアウォールのステータス

準備完了

関連付けられたファイアウォールポリシー

nwfwpolicy

関連付けられた VPC

vpc-0f7e82cc3d9932a4e

ルートの更新ガイドを表示

このファイアウォールポリシーには、ルールグループがありません。

ルールグループを追加 ▼

32. 画面左ペインからルートテーブルをクリックし、[public]の方をクリックします

ルートテーブル (4) 情報						
Q ルートテーブルをフィルター						
<input type="checkbox"/>	Name ▼	ルートテーブル ID ▼	明示的なサブネットの開...	Edge の関連付け	メイン ▼	VPC
<input type="checkbox"/>	public	rtb-022450c1010488a2f	subnet-048434a415b11...	-	いいえ	vpc-0f7e82cc3d9932a4
<input type="checkbox"/>	fwrt	rtb-0fe0bb07fe4b2ec44	-	-	いいえ	vpc-0f7e82cc3d9932a4

現在 VPC には 3 つのルートテーブルが存在しています。

public:明示的に public subnet に紐付けられている

fwrt: Network Firewall ようだがまだ fw subnet に紐付けられていない（後で紐付け作業を行います）

メイン: デフォルトで存在しているもの。明示的に紐付けられたルートテーブルを持たないサブネットが利用する。（現時点だと fw subnet は fwrt に紐付けられていないため、こちらが使われる）

<input type="checkbox"/>	Name ▼	ルートテーブル ID ▼	明示的なサブネットの開...	Edge の関連付け	メイン ▼	VPC
<input type="checkbox"/>	public	rtb-022450c1010488a2f	subnet-048434a415b11...	-	いいえ	vpc-0f7e82cc3d9932a4
<input type="checkbox"/>	fwrt	rtb-0fe0bb07fe4b2ec44	-	-	いいえ	vpc-0f7e82cc3d9932a4
<input type="checkbox"/>	-	rtb-0070d311a67235a04	-	-	はい	vpc-0f7e82cc3d9932a4

これらのルートテーブルを変更しながら

Internet ⇔ Internet Gateway ⇔ fw subnet (Network Firewall) ⇔ public subnet  
を設定していきます。

33. まず public ルートテーブルと public サブネットの紐付けを一度外します。これは本来設計上必要ないのですが、そうしないと設定変更作業が行えません。このため、一度外した後、設定変更を行い、再度紐付けを行います。[アクション]から[サブネット

の関連付けを編集]を選んでチェックを外せば、紐付けが解除されます。

rtb-022450c1010488a2f / public アクション ▼

詳細 情報

ルートテーブル ID rtb-022450c1010488a2f	メイン いいえ	明示的なサブネットの関連付け -	Edge の関連付け -
VPC vpc-0f7e82cc3d9932a4e   nwfwvpc	所有者 ID 294963776963		

34. ルートの編集ボタンを押し[0.0.0.0/0]の設定内容がインターネットゲートウェイになっているものをゲートウェイロードバランサーのエンドポイントに変更し、[変更を保存]をおします

ルートを編集

送信先	ターゲット	ステータス	伝播済み
10.10.0.0/16	local	アクティブ	いいえ
0.0.0.0/0	<div>Q</div> <div>キャリアゲートウェイ Egress Only インターネットゲートウェイ ゲートウェイロードバランサーのエンドポイント インスタンス インターネットゲートウェイ ローカル</div>	アクティブ	いいえ <span>削除</span>

ルートを追加キャンセルプレビュー変更を保存

35. 再度[アクション]からサブネットの関連付けを編集を選び、public subnet と関連付けます。正しく作業されれば、以下になるはずです。

詳細 情報

ルートテーブル ID rtb-022450c1010488a2f	メイン いいえ	明示的なサブネットの関連付け subnet-048434a415b11b11e / public	Edge の関連付け -
VPC vpc-0f7e82cc3d9932a4e   nwfwvpc	所有者 ID 294963776963		

ルート サブネットの関連付け Edge の関連付け ルート伝播 タグ

ルート (2) ルートを編集

Q ルートをフィルタリング 両方 ▼ < 1 > ⚙

送信先 ▼	ターゲット ▼	ステータス ▼	伝播済み ▼
10.10.0.0/16	local	アクティブ	いいえ
0.0.0.0/0	vpc-04c05e86fe84aaebc	アクティブ	いいえ

これで EC2 とインターネットとの通信は、Network Firewall 経由となります。EC 2

から直接 Internet Gateway へアクセスできなくなりました。

36. 続いて fw subnet 用の fwrt を編集します。[ルートの編集]をおしてください

ルートを編集

送信先	ターゲット	ステータス	伝播済み
10.10.0.0/16	<input type="text" value="local"/>	🟢 アクティブ	いいえ

37. 以下のように[0.0.0.0/0]に対してインターネットゲートウェイをセットします

ルート (2)

送信先	ターゲット	ステータス	伝播済み
10.10.0.0/16	local	🟢 アクティブ	いいえ
0.0.0.0/0	igw-089ca8e6f3ff7ce21	🟢 アクティブ	いいえ

これで、fw subnet に存在しているノード（Network Firewall）がインターネットゲートウェイへ通信をルーティングできるようになりました

38. もう一つ、画面左ペイン、ルートテーブルをクリックして[ルートテーブルを作成]をおします。これは、subnet 用ではなく、Internet Gateway 用のルートテーブルです。外部から受ける Internet Gateway の通信を全て、Network Firewall へ振り向けるためのルートテーブルです。名前を[igwrt]にし VPC は EC2 と同じものを指定します。その後ルートを編集し以下のようにします。

ルート

サブネットの関連付け Edge の関連付け ルート伝播 タグ

ルート (1)

送信先	ターゲット	ステータス	伝播済み
10.10.0.0/16	vpce-04c05e86fe84aebc	🟢 アクティブ	いいえ

39. [Edge の関連付け]タブを選び、[Edge の関連付けを編集]ボタンをおします

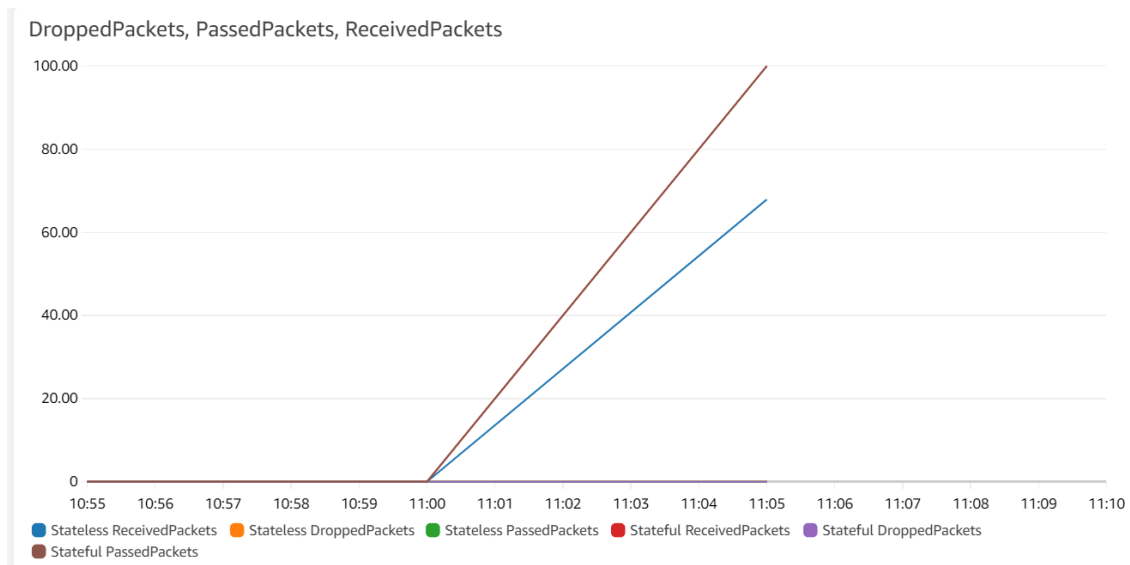
40. インターネットゲートウェイにチェックをつけ[変更を保存]をおします。以下のようになります

41. 最後に、ルートテーブルの fw を fw subnet に紐付けます。以下のようになります。

存在しているすべての Subnet には明示的にルートテーブルが紐付けられているた

め、メインルートテーブルは使われていません。

42. この状態で memo.txt の [EC2 PublicDNS] にアクセスしてみてください
43. Wordpress が表示されたら、ブラウザで少し何度かリロードをして複数回アクセスを行った後、Network Firewall の [モニタリング] タブをクリックすると、通信が通っていることがわかります。



#### ログの設定とセキュリティルール設定

44. 今までの手順で、インターネットから EC2 への通信は Network Firewall を通る環境を作ることができました。これから、ログの設定、そしてセキュリティルールの設定を行っていきます。

ファイアウォールの詳細タブから、ログ記録の編集をおします

ログ記録			編集
ネットワークファイアウォールはステートフルルールグループのログを生成します。ログタイプごとに異なる宛先を設定できます。			
ログタイプ	アラートのログ送信先	フローのログ送信先	
	未設定	未設定	

45. Alert にチェックをつけます
46. [CloudWatch log group]を選び、[ロググループを作成]をおします

**アラートのログ送信先**

ログ宛先  
各ログタイプは、S3 バケット、CloudWatch ロググループ、または Kinesis Data Firehose 配信ストリームに送信できます。

☐ S3  
☒ CloudWatch log group  
☐ Kinesis data firehose

CloudWatch ロググループ  
CloudWatch ロググループの [cloudWatch] ロググループを選択します。

47. [ロググループを作成]を再度押します

CloudWatch > Log groups

**ロググループ (54)**  **アクション ▼** Logs Insights で表示

デフォルトでは、最大 10000 個のロググループのみをロードします。

☒ 完全一致
 < 1 > ⚙️

48. 適当な名前を付け[作成]をおします

CloudWatch > Log groups

**ロググループ (54)**  **アクション ▼** Logs Insights で表示

デフォルトでは、最大 10000 個のロググループのみをロードします。

☒ 完全一致
 < 1 > ⚙️

49. ファイアウォールのログ設定画面に戻ると、先程指定したロググループが指定できるようになっていますので、指定をして[保存]をおします

50. 次に画面左ペインから、ファイアウォールポリシーをクリックし先ほど作成した空のポリシーをクリックして選びます

VPC > ファイアウォールポリシー

**ファイアウォールポリシー (1) 情報**

< 1 > ⚙️

<input type="checkbox"/>	名前	▲
<input type="checkbox"/>	nwfwpolicy	

51. ステートフルグループの[ルールグループを追加]から[新しい・・・]を選びます。ステートレスグループではないので注意してください

**ステートフルルールグループ (0)** 削除 ルールグループを追加 ▲

新しいステートフルルールグループの作成と追加

ステートフルルールグループをファイアウォールポリシーに追加

名前	キャパシティ
ステートフルなルールグループなし	

[ルールグループの追加 (Add rule groups)] を選択して、ステートフルなルールグループをポリシーに追加します。

52. 適当な名前を付け、キャパシティに 100 と入力します

**ステートフルルールグループ**

**名前**  
ステートフルルールグループ内で一意のルールグループの名前を入力します。

suricata

名前は 1~128 文字にする必要があります。有効な文字は a~z、A~Z、0~9、-(ハイフン) です。名前の先頭と末尾にハイフンを使用することはできません。また、ハイフンを 2 つ連続して含めることはできません。

**説明 - オプション**

説明には 0~256 文字を使用できます。

**キャパシティ** 情報  
ルールグループに許可される最大処理キャパシティ。ステートフルルールグループのキャパシティ要件を、追加するルールの数として見積もります。ルールグループの更新時に、この設定を変更したり超えたりすることはできません。

100

キャパシティは 1 以上 10,000 未満である必要があります。

53. [Suricata compatible IPS rules] を選びます

ステートフルルールグループのオプション

☐ **5-tuple**  
5 タプル形式を使用して、送信元 IP、送信元ポート、送信先 IP、送信先ポート、およびプロトコルを指定し、一致するトラフィックに対して実行するアクションを指定します。

☐ **Domain list**  
ドメイン名のリストと、ドメインの 1 つにアクセスしようとするトラフィックに対して実行するアクションを指定します。

☒ **Suricata compatible IPS rules**  
侵入防止システム (IPS) ルール - Suricata ルール構文を使用して高度なファイアウォールルールを提供します。Suricata は、トラフィック検査用の標準ルールベースの言語を含むオープンソースネットワーク IPS です。

54. memo.txt の中に入っている一番最後の文字列をコピーします

alert tcp any any -> any any (msg:"TCP traffic detected"; sid:200001; rev:1;)

**Suricata 互換 IPS ルール** 情報  
Suricata は、トラフィック検査用の標準ルールベースの言語を含むオープンソースネットワーク IPS です。

Suricata 互換 IPS ルール

alert tcp any any -> any any (msg:"TCP traffic detected"; sid:200001; rev:1;)

キャンセル 作成と追加

55. [作成と追加] をおします。これでファイアウォールがすべての TCP 通信を Alert として CloudWatch Logs に出力するようになりました。ブラウザから wordpress に何度かアクセスしてログの出力を確認してください。(数分程度時間がかかります)



```
▼ 2021-06-09T11:27:40.000Z {"firewall_name":"nfw0609","availability_zone":"us-east-1f","event_timestamp":"1623238060","event":{"ti...
{
  "firewall_name": "nfw0609",
  "availability_zone": "us-east-1f",
  "event_timestamp": "1623238060",
  "event": {
    "timestamp": "2021-06-09T11:27:40.805498+0000",
    "flow_id": 1778711945562746,
    "event_type": "alert",
    "src_ip": "162.142.125.86",
    "src_port": 3366,
    "dest_ip": "10.10.0.232",
    "dest_port": 12509,
    "proto": "TCP",
    "alert": {
      "action": "allowed",
      "signature_id": 200001,
      "rev": 1,
      "signature": "TCP traffic detected",
      "category": "",
      "severity": 3
    }
  }
}
```

56. では、Alert ログの出力が確認出来たら、今度は先程のルールを編集します。画面左のペインから、ネットワークファイアウォールのルールグループをクリックして、表示されたルールをさらにクリックして、[ルールを編集]ボタンを押してください。



57. alert の部分を drop に変更して、保存します。数分まって再度ブラウザから wordpress にアクセスしてください。今度はアクセスできなくなっていることが確認できます。

Suricata のルールは、かなり複雑な設定が可能です。詳しくはこちらをご確認ください。

[https://docs.aws.amazon.com/ja\\_jp/network-firewall/latest/developerguide/suricata-examples.html](https://docs.aws.amazon.com/ja_jp/network-firewall/latest/developerguide/suricata-examples.html)

おつかれさまでした！

削除ですが以下の手順で行ってください

1. ルートテーブルからルート編集でターゲットが vpce-となっている行を消す
2. ルートテーブルの Edge 及びサブネットの関連付けをはずす
3. EC2 を削除
4. Network Firewall のログ出力を停止
5. Network Firewall を削除

6. VPC を削除
7. ファイアーウォールポリシーの削除
8. ファイアーウォールのルールグループの削除
9. CloudWatch Logs のロググループを削除