paloalto TECHDOCS

Cloud NGFW for AWSデプロイメント

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Last Revised

April 8, 2025

Table of Contents

Cloud NGFW for AWS 集中型デプロイメント

どこで使用できますか?	何が必要ですか?
• Cloud NGFW for AWS	❑ Cloud NGFWサブスクリプション ❑ Palo Alto Networksカスタマー サポート アカウント (CSP) ❑ AWS Marketplaceアカウント ❑ ユーザーのロール（テナントまたは管理者）

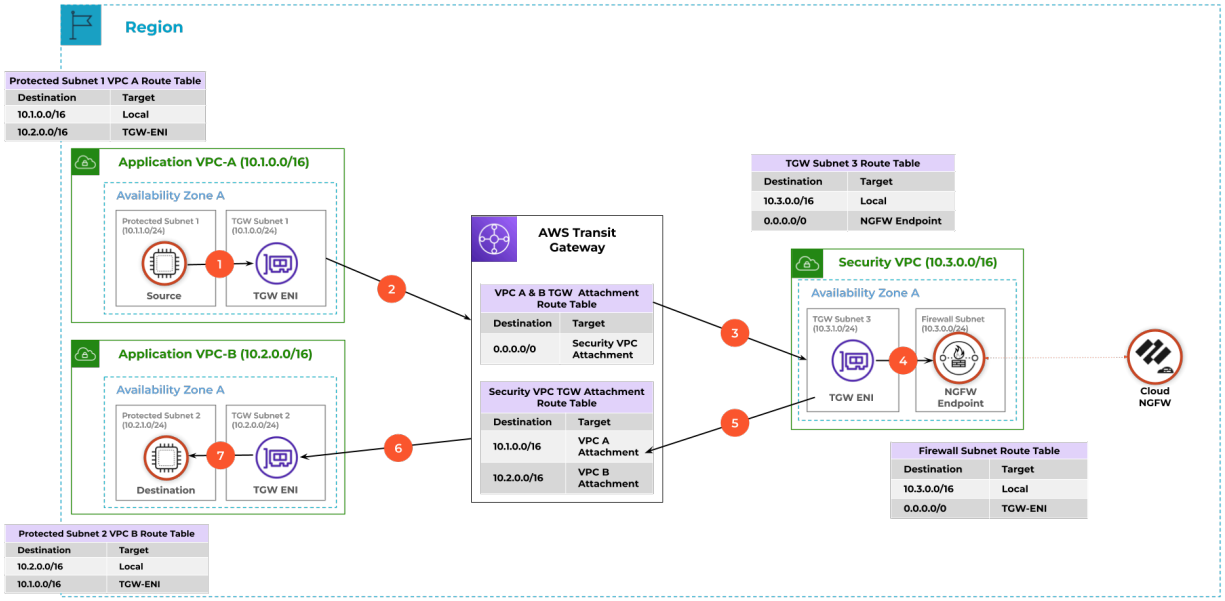
集中型デプロイメントでは、Cloud NGFWコンポーネントは集中化されたセキュリティVPCに展開されます。トラフィックは常にAWS Transit Gateway (TGW) を通過する必要があります。TGWはネットワークハブとして機能し、オンプレミスネットワークだけでなくVPC間の接続を簡素化します。

集中型デプロイメントのその他の例については、「Cloud NGFW for AWS デプロイメントアーキテクチャ」を参照してください。

集中型 East-West

1. ソース インスタンスからのトラフィックは、TGW Elastic Network Interface (ENI) に送られます。
2. TGW Elastic Network Interfaceはトラフィックを TGWに送信します。
3. TGWはトラフィックをセキュリティVPC TGW Elastic Network Interfaceにルーティングします。
4. TGW Elastic Network Interfaceは、トラフィックを NGFWエンドポイントに送信し、検査のためにNGFWに送信します。
5. トラフィックが許可されている場合、NGFW はトラフィックを NGFW エンドポイントに送り返します。その後、トラフィックはセキュリティ VPC TGW エンドポイントを介して TGW に送り返されます。
6. TGWは、トラフィックを宛先VPC内のTGW Elastic Network Interfaceに転送します。

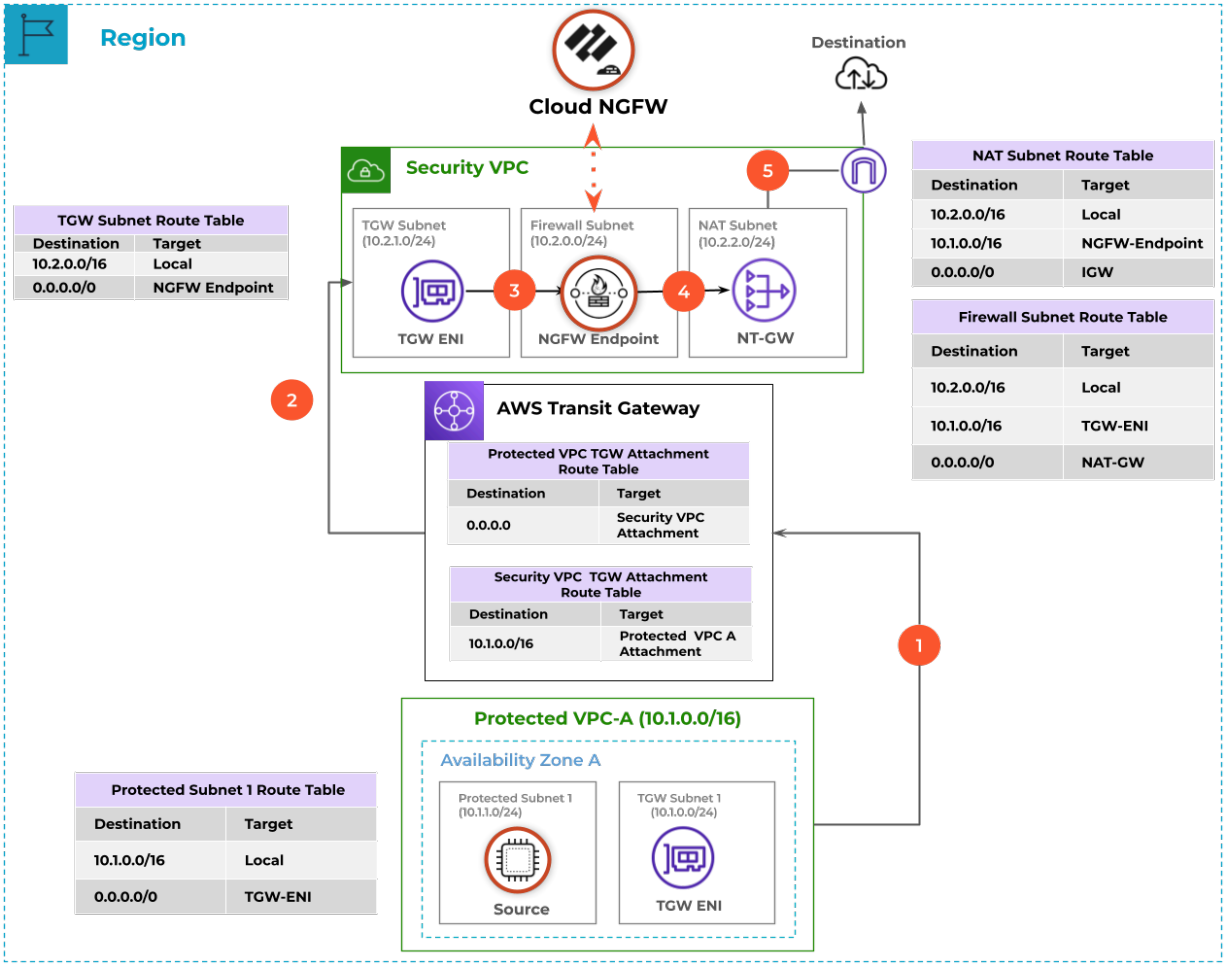
7. 次に、TGW Elastic Network Interfaceがトラフィックを宛先に送信します。



集中型アウトバウンド

1. ソース インスタンスからのトラフィックは、TGW Elastic Network Interfaceに送信され、その後TGWに送信されます。
2. TGWはトラフィックをセキュリティVPC TGW Elastic Network Interfaceにルーティングします。
3. TGW Elastic Network Interfaceは、トラフィックを NGFW エンドポイントに送信し、検査のためにNGFWに送信します。
4. トラフィックが許可されている場合、NGFW エンドポイントはトラフィックを NAT ゲートウェイにルーティングします。

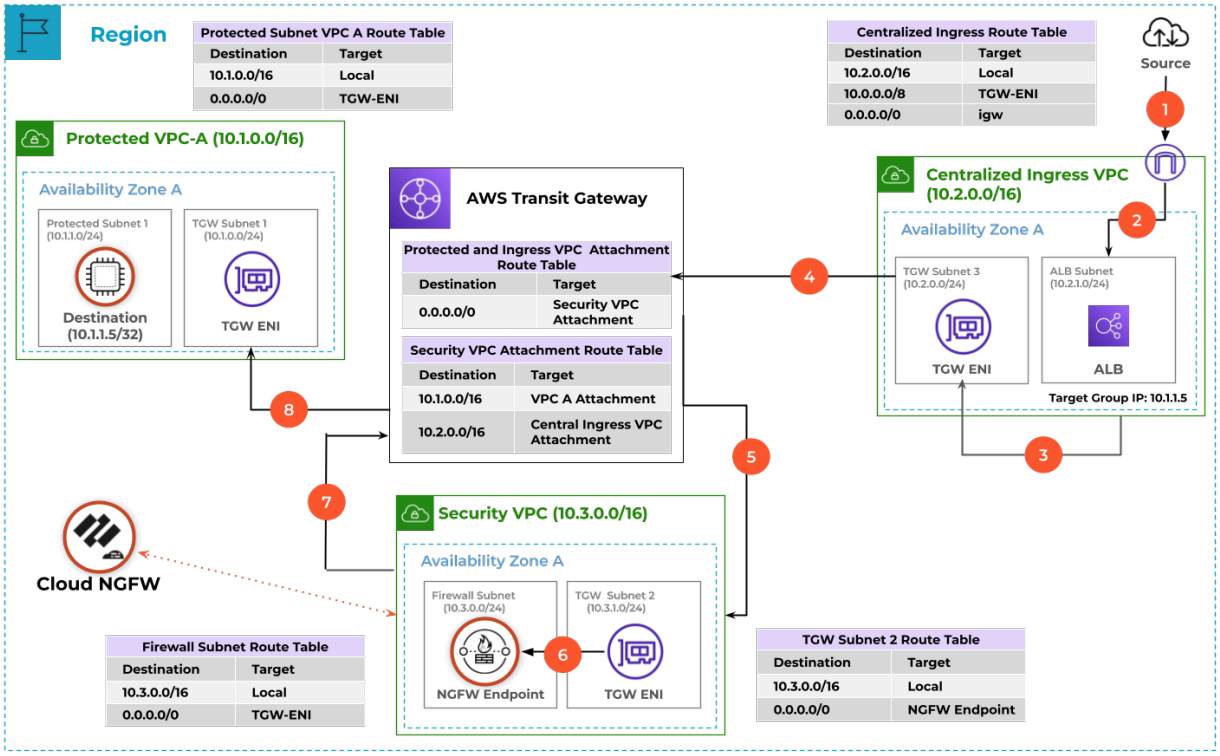
5. NAT ゲートウェイはトラフィックを IGW に転送し、宛先に転送します。



集中型インバウンド

1. インターネットからのトラフィックは、インターネット ゲートウェイに到着します。
2. インターネットゲートウェイは、トラフィックをアプリケーションロードバランサー (ALB) にルーティングします。
3. 次に、ALBはトラフィックを入力VPC TGW Elastic Network Interfaceに送信します。
4. TGW Elastic Network Interfaceは、TGWにトラフィックを送信します。
5. TGWはトラフィックをセキュリティ VPC TGW Elastic Network Interfaceにルーティングします。
6. TGW Elastic Network Interfaceは、トラフィックを NGFWエンドポイントに送信し、検査のためにNGFWに送信します。
7. トラフィックが許可されている場合、NGFW エンドポイントはトラフィックを TGW に送信します。

8. 次に、TGW はトラフィックを保護されたVPC TGW Elastic Network Interfaceにルーティングしてから宛先にルーティングします。



Cloud NGFW for AWS の分散型デプロイメント

どこで使用できますか?	何が必要ですか?
• Cloud NGFW for AWS	❑ Cloud NGFWサブスクリプション ❑ Palo Alto Networksカスタマー サポート アカウント (CSP) ❑ AWS Marketplaceアカウント ❑ ユーザーのロール（テナントまたは管理者）

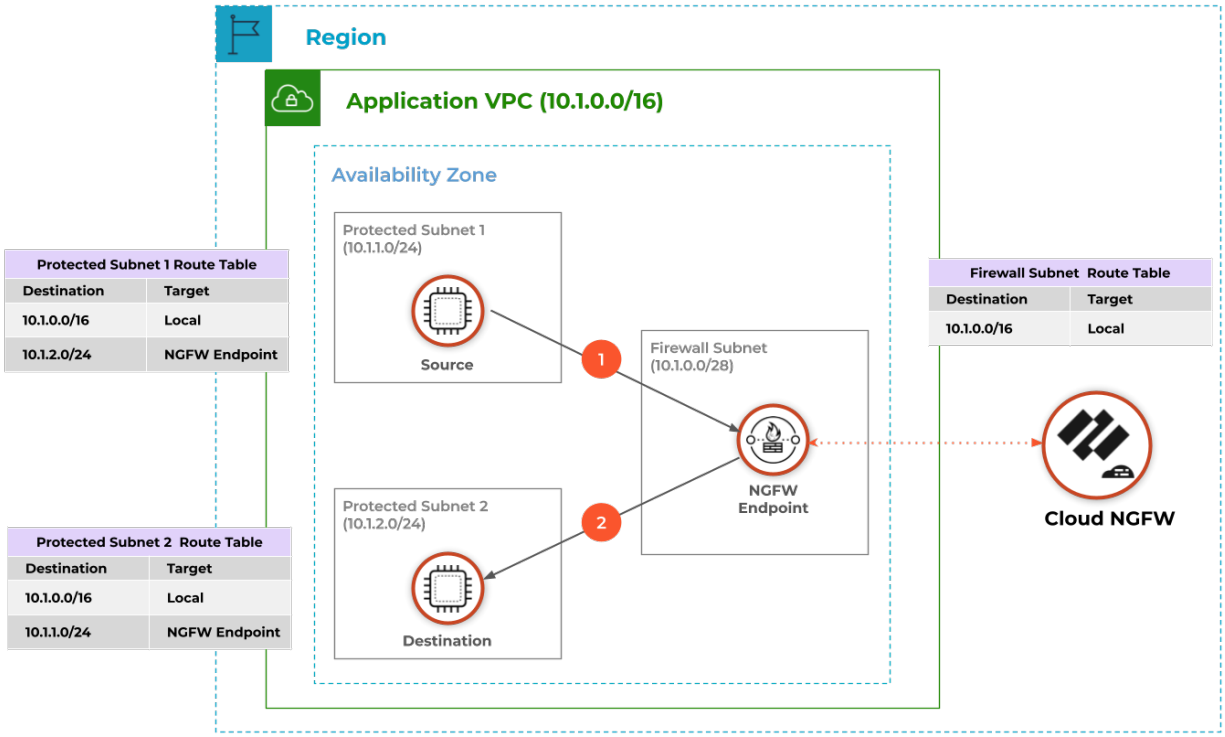
分散型デプロイメントでは、保護が必要な各 VPC に独自の NGFW があります。このデプロイメント方法はそれほど複雑ではないため、設定ミスの可能性が低くなります。

分散型デプロイメントのその他の例については、Cloud NGFW for AWS デプロイメントアーキテクチャを参照してください。

分散型 East-West（VPC 内）

1. ソースインスタンスからのトラフィックは、検査のために NGFW エンドポイントにルーティングされ、NGFW にルーティングされます。

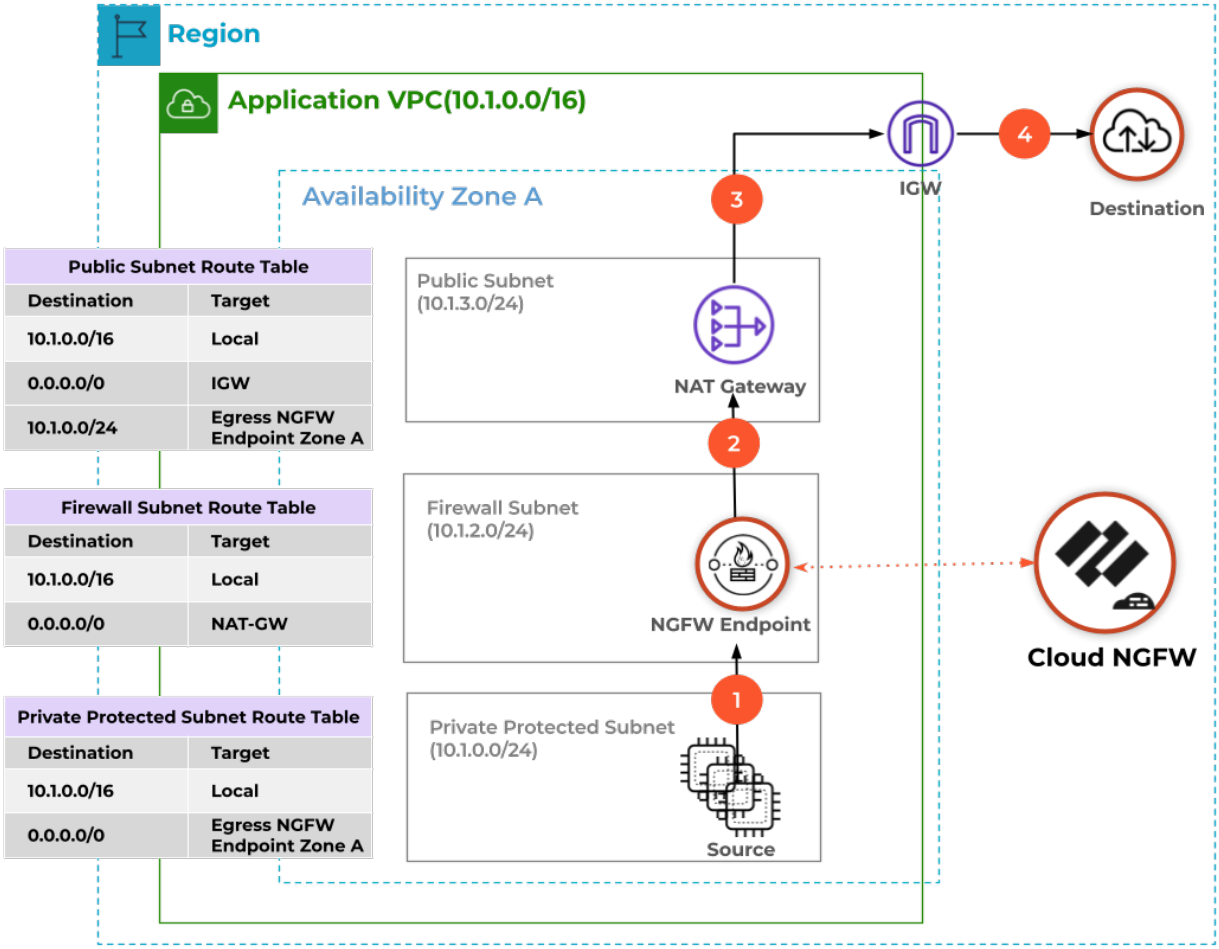
2. トラフィックが許可されている場合、NGFW エンドポイントはトラフィックを宛先に送信します。



分散型アウトバウンド

1. ソースインスタンスからのトラフィックは、検査のために NGFW エンドポイントにルーティングされ、NGFW にルーティングされます。
2. トラフィックが許可されている場合、NGFW エンドポイントは検査されたトラフィックを NAT ゲートウェイに送信します。
3. NAT ゲートウェイはトラフィックをインターネットゲートウェイに送信します。

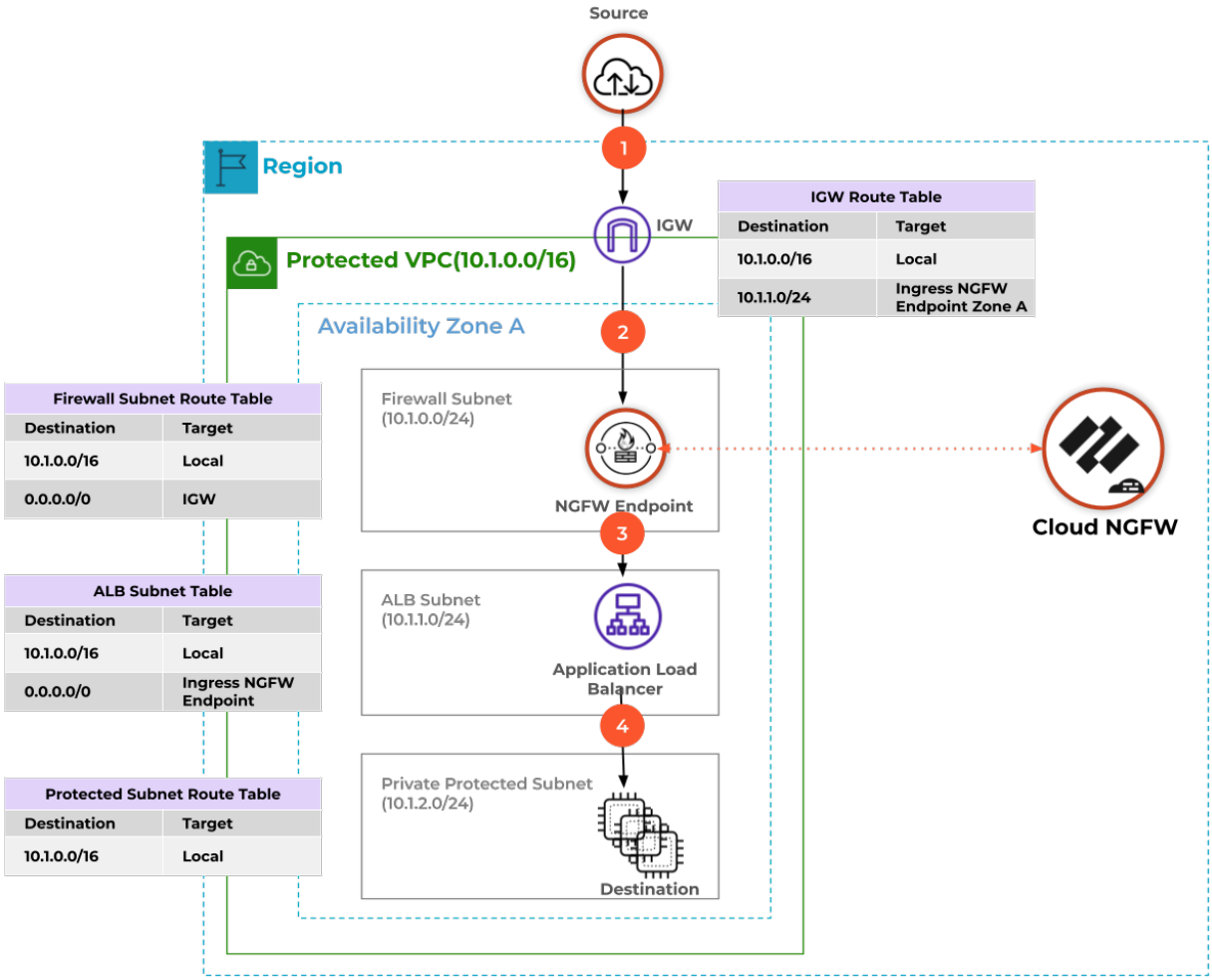
4. トラフィックはインターネットと宛先に続きます。



分散型インバウンド

1. ソースからのトラフィックは、インターネットゲートウェイに到着します。
2. インターネットゲートウェイはトラフィックを NGFW エンドポイントにルーティングし、次に検査のために NGFW にルーティングします。
3. トラフィックが許可されている場合、NGFW エンドポイントはトラフィックをアプリケーション ロードバランサーにルーティングします。

4. アプリケーションロードバランサーは、トラフィックを宛先に転送します。



AWS Cloud WANとのCloud NGFW統合

どこで使用できますか?	何が必要ですか?
• Cloud NGFW for AWS	❑ Cloud NGFWサブスクリプション ❑ Palo Alto Networksカスタマー サポート アカウント (CSP) ❑ AWS Marketplaceアカウント ❑ ユーザーのロール（テナントまたは管理者）

AWS Cloud WANは、クラウド環境とオンプレミス環境を相互接続した統合ネットワークを構築できるマネージドWAN（ワイドエリアネットワーキング）サービスです。オンプレミス、ブランチ オフィス、データセンター、Amazon Virtual Private Cloud (バーチャル プライベート クラウド - VPC)をAWSグローバルネットワーク全体、さらには他のクラウド プロバイダーに接続するための一元化されたダッシュボードを提供します。

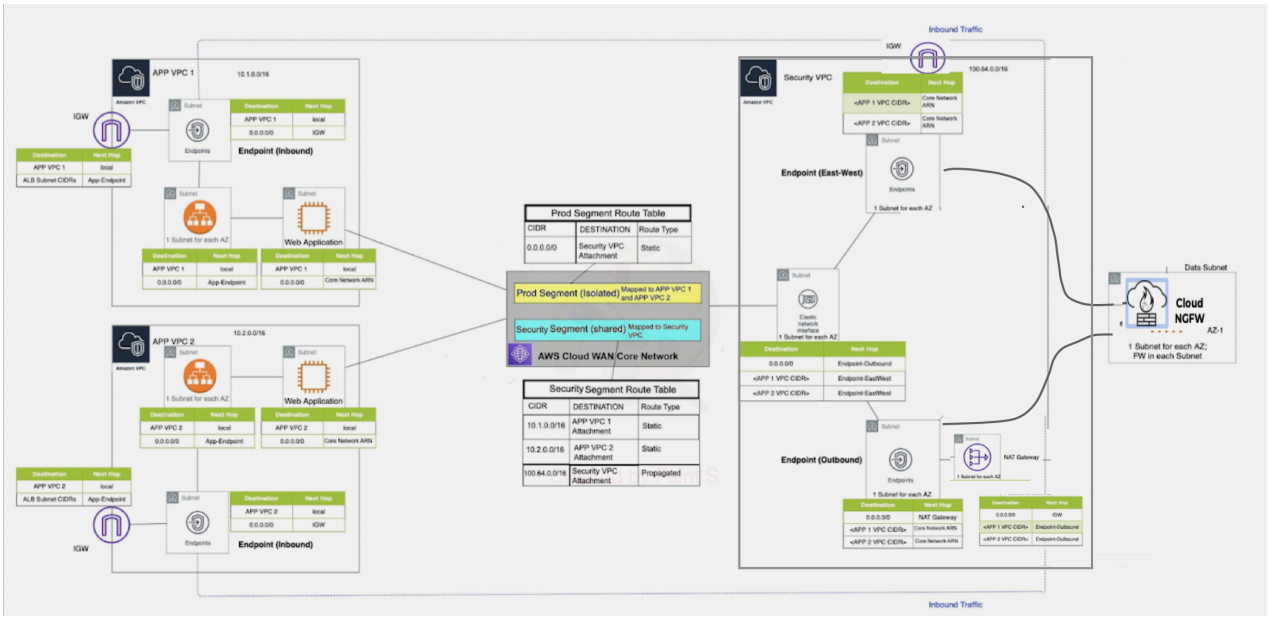
Cloud WANは、グローバルネットワークを一元管理するインターフェイスであるAWS Network Managerを通じて、AWS内の接続を支援します。グローバル ネットワークは、ネットワーク オブジェクトのルートレベルのコンテナとして機能する単一のプライベート ネットワークで、中継ゲートウェイとコア ネットワークの両方を含めることができます。コア ネットワークは、ネットワーク ポリシー、VPCなどのアタッチメント、およびトランジット ゲートウェイ ルート テーブルで構成されます。

これらのVPCをコア ネットワーク内のセグメントにマッピングできます。これらのセグメントは、VPCアタッチメントやトランジット ゲートウェイ ルート テーブル アタッチメントなどのアタッチメントを使用して接続されます。組み込みセグメンテーションにより、AWS環境とオンプレミス環境全体でネットワークの分離を維持できます。各セグメントは専用のルーティング ドメインを作成します。グローバル ネットワーク内に複数のネットワーク セグメントを作成できます。Cloud WANは、AWSのリソースをセグメント内の通信用に再構成します。簡単に言うと、Cloud WANでは、次のものの間でトラフィックをルーティングできます。

- 同じセグメント、同じリージョンのVPC（分離されたアタッチメント）。
- 同じリージョンの異なるセグメントにあるVPC。
- 異なるリージョンにまたがる同一セグメント内のVPC（分離されたアタッチメント）。
- 地域ごとに異なるセグメントのVPC。

AWS Cloud WANをデプロイする前の検討事項:

- トランジット ゲートウェイとCloud WAN間のピアリングは同じリージョンでサポートされ、リージョン間ではサポートされません。
- プライベートIPアドレスを使用してダイレクト接続でAWSサイト間VPN接続を必要とするユース ケースでは、Cloud WANをトランジット ゲートウェイで接続するようにしてください。
- トランジット ゲートウェイとともにCloud WANをデプロイする際、トランジット ゲートウェイのASNとCloud WANのコア ネットワーク エッジに使用されるASNが異なることを確認してください。
- コア ネットワークの作成中に、コア ネットワーク ポリシー設定のエッジ ロケーション セクションで、VPCが構成されているすべてのリージョンを確実に追加します。また、セグメントを作成し、これらのリージョンが属するセグメントのタイプ（dev、prod、management、security）をセグメント名の下に追加する必要があります。



AWS Cloud WANは、次の2つの方法でデプロイできます。

- トランジットゲートウェイと**Cloud WAN**の統合 – この方法では、静的に作成されたトランジット ゲートウェイ ピアリング接続をCloud WANで置き換えます。Cloud WANでトランジット ゲートウェイを連携させる場合は、AWS Network Managerを使用してトランジッ トゲート

ウェイを登録し、トランジット ゲートウェイ間のピアリングを作成してトランジット ゲートウェイにアタッチメントを作成してから、Cloud WANの設定を適用する必要があります。

- **Cloud WAN**のみ: この方法では、すべての接続にCloud WANが使用され、トランジット ゲートウェイは削除されます。

AWS Cloud WANをデプロイする

Cloud WANは、VPCとオンプレミス ネットワークの相互接続です。ここでは、PaloAlto Networks Cloud NGFWを使用して、Cloud WANと相互接続されたトラフィックを保護する方法について詳しく説明します。Cloud WANはグローバル構築ですが、Palo Alto Networksでは、Cloud NGFWをすべてのAWSリージョンにデプロイし、低レイテンシーでセキュリティ体制を維持し、コストを最適化することを推奨しています。

Cloud NGFWは、すべての地域の一元化されたセキュリティVPCにデプロイできます。セキュリティVPCは、アタッチメントを介してクラウドWANセキュリティセグメントに直接接続できます。アタッチメントとセグメントに関連付けられたルーティングは、脅威防御のためにトラフィックをCloud NGFWリソースにルーティングする方法を定義します。宛先に転送する前に、クラウドアタッチメントからセキュリティVPCに到着したトラフィックをリダイレクトできます。リージョン内にデプロイされたCloud NGFWが保護とセキュリティを実現。

- 地域間フローと地域内フローによるEast-Westトラフィック
- アウトバウンド トラフィックフローの検査と保護
- オンプレミスおよびブランチ環境からのトラフィックの検査とセキュリティ保護

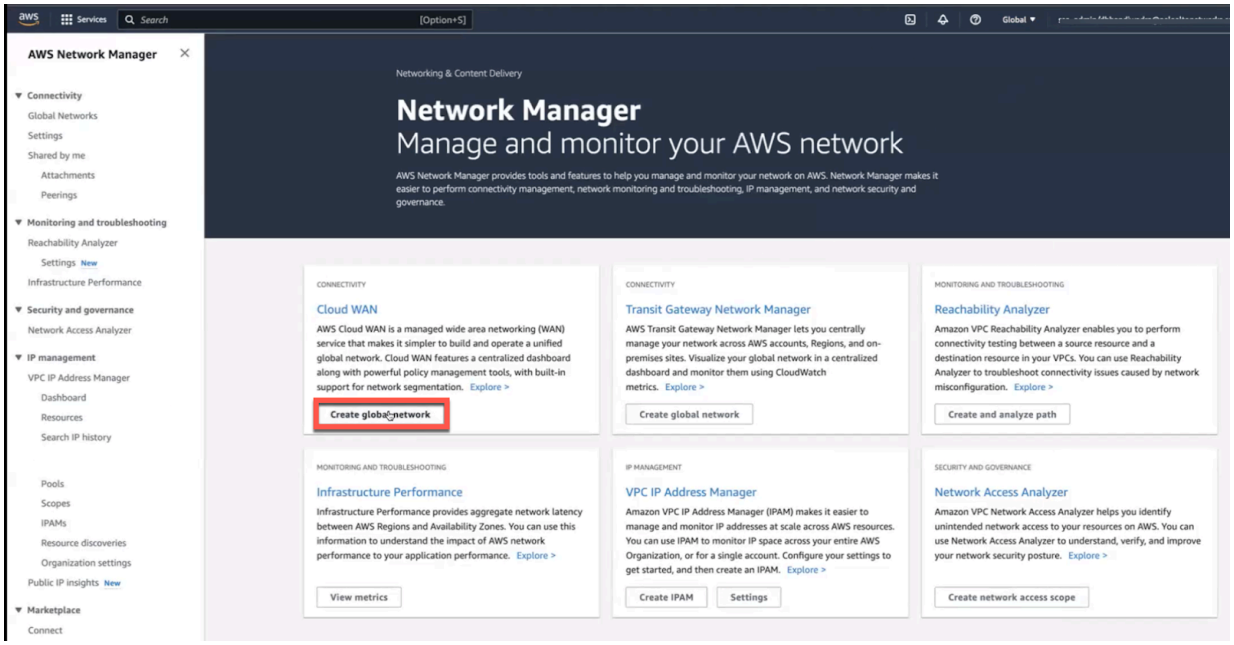
VPCが同じリージョン（分離されたアタッチメント）にあるというユースケースを考えてみます。このセットアップを設定するには、セキュリティVPC内にCloud NGFWファイアウォールをデプロイします。Cloud NGFWファイアウォールは、セキュリティVPCにデプロイできます。セキュリティVPCは、Cloud WANに直接接続されているか、またはCloud WANアタッチメントを備えたトランジット ゲートウェイを介して接続されています。

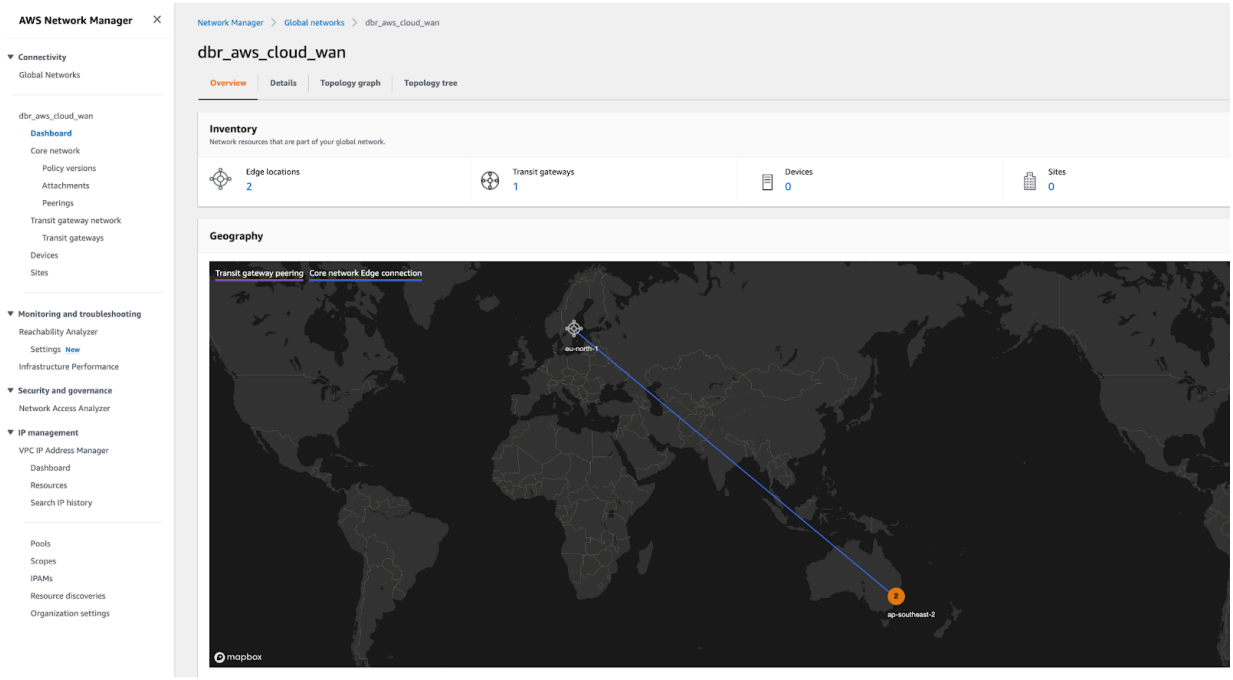
トランジットゲートウェイから完全に移行するには、*VPCをCloud WAN*に直接接続する必要があります。

本番VPCからの出口トラフィックは、Cloud WANにルーティングされ、セキュリティVPCにルーティングされて検査され、NATゲートウェイと内部ゲートウェイを介して送信されます。逆方向では、セキュリティVPCからのトラフィックはセキュリティ セグメントに到達し、ルーティング設定に基づいてVPCアタッチメントに送信されます。

AWS Cloud WAN（のみ）デプロイメントで、同一セグメント、同一リージョンのVPC間のトラフィックを検査するには、以下のタスクを実行します。

1. AWS Network Managerにログインし、グローバルネットワークを作成します。

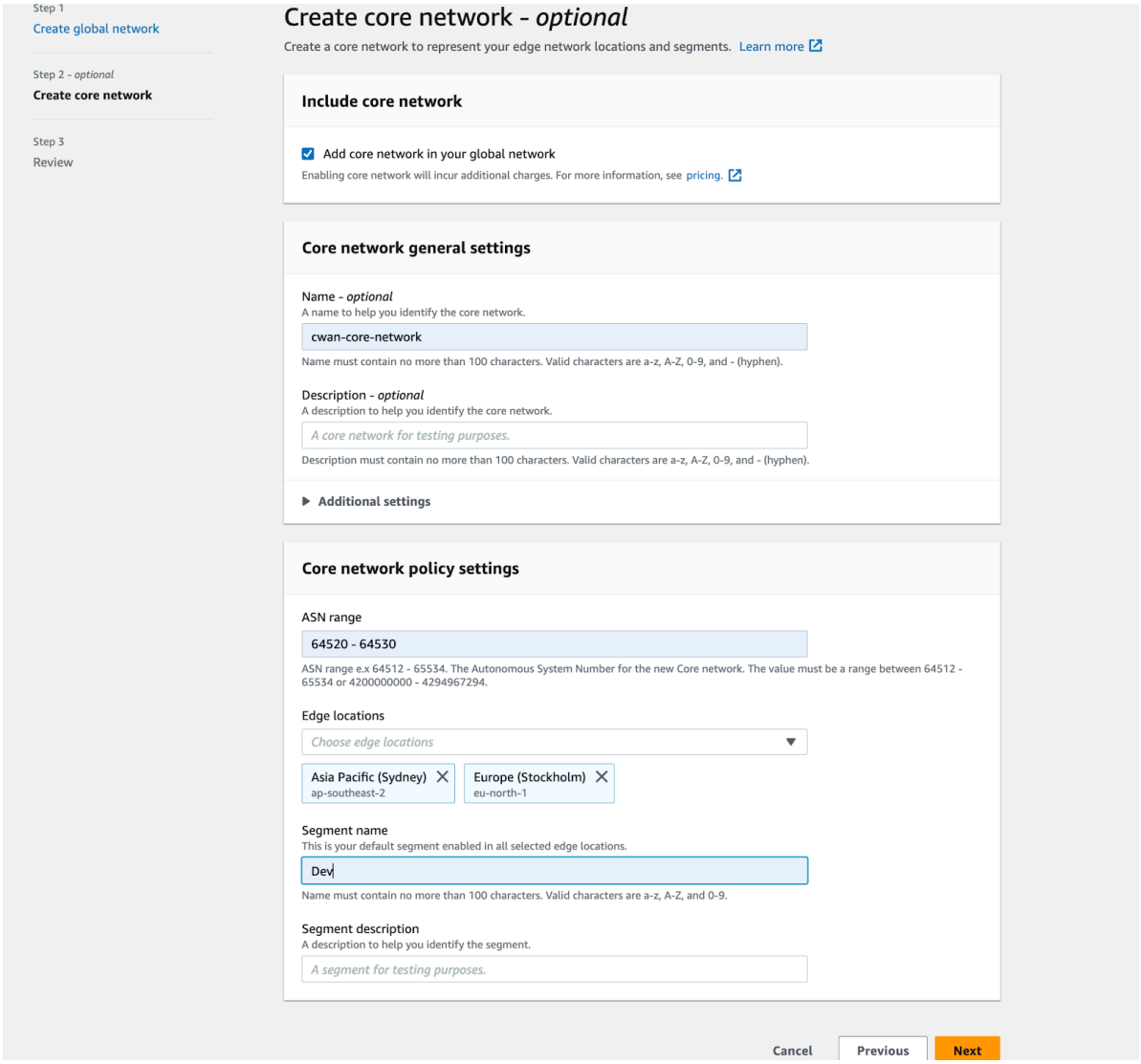




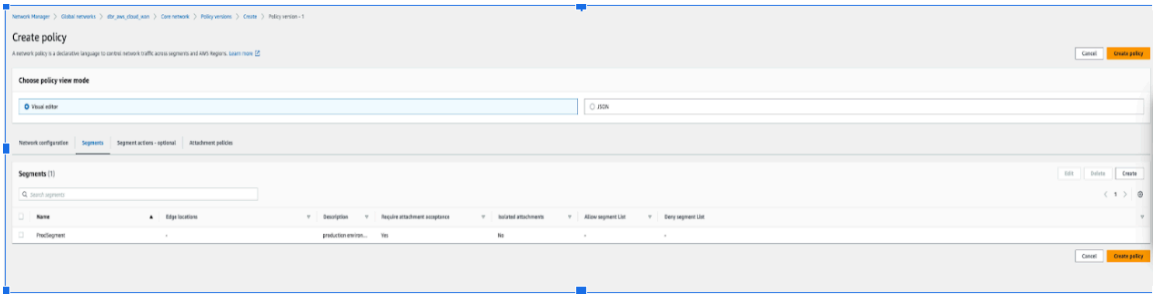
2. コア ネットワークとコア ネットワーク ポリシーを作成します。

   AWS Cloud WANコンソールを使用して、次のタスクに従ってコア ネットワーク ポリシー バージョンを作成します。

   - ネットワークの設定を行います。

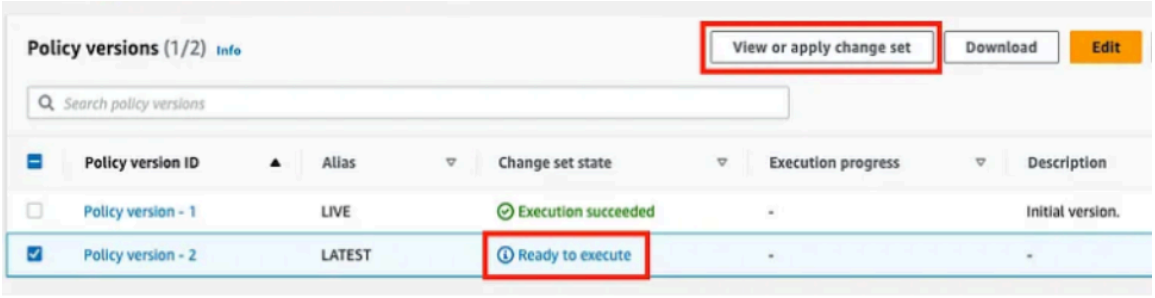


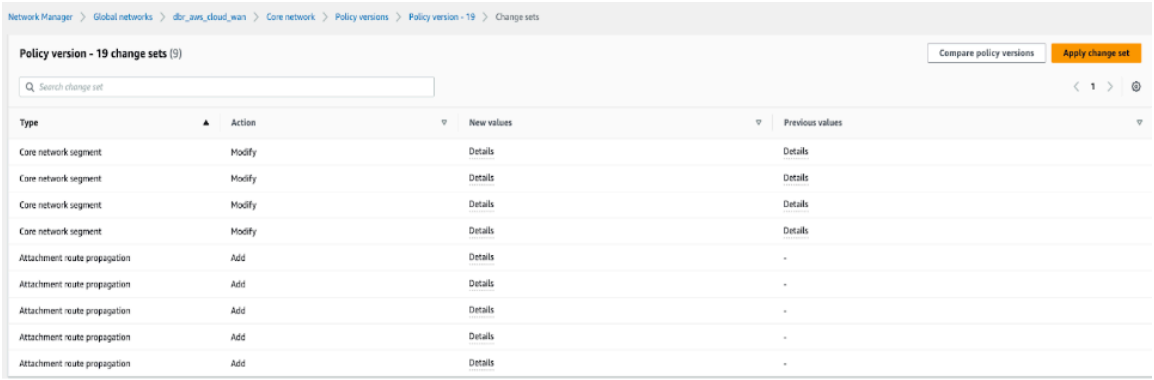
- ポリシーバージョンを編集するには、**[Policy versions(**ポリシーバージョン**)]**をクリックし、必要なポリシーを選択して**[Edit(**編集**)]**をクリックします。必要な変更を行い、**[Create Policy(**ポリシーの作成**)]**をクリックします。



- ポリシーバージョンの変更セット状態が **[Ready to execute(**実行準備完了**)]**に変更されたら、**[View(**表示**)]**または**[Apply change set(**変更セットの適用**)]**をクリックしてポリシーを

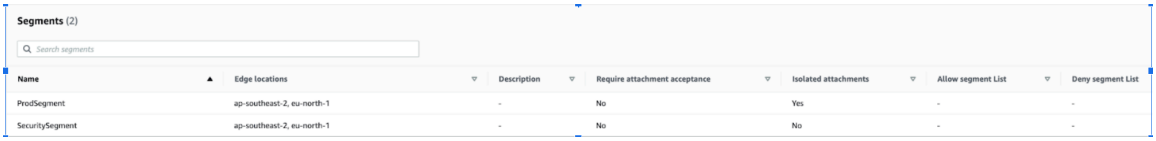
実行します。または、**[Compare policy version(**ポリシー バージョンを比較**)**］をクリックしてJSONドキュメントを表示します。



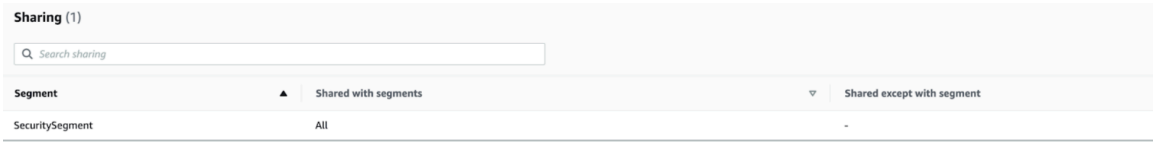


- コア ネットワーク内にネットワーク ポリシー セグメントを作成します。

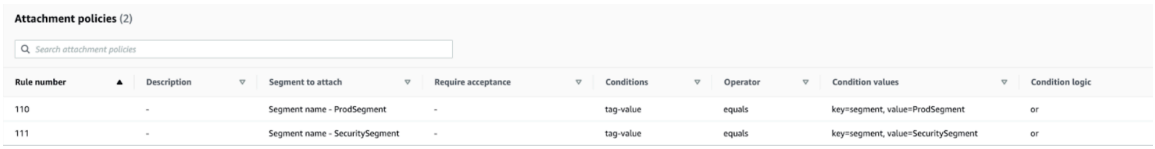
  ポリシー バージョンを構成する際に、実動セグメントとファイアウォールにアプリケーション#APP VPC 1（10.1.0.0/16）とAPP VPC 2（10.2.0.0/16 ）、セキュリティ セグメントにセキュリティVPC（100.64.0.0/16）を追加するようにしてください。



- セグメント共有アクションとセグメントルートアクションを作成します。



- ポリシーアタッチメントを作成します。

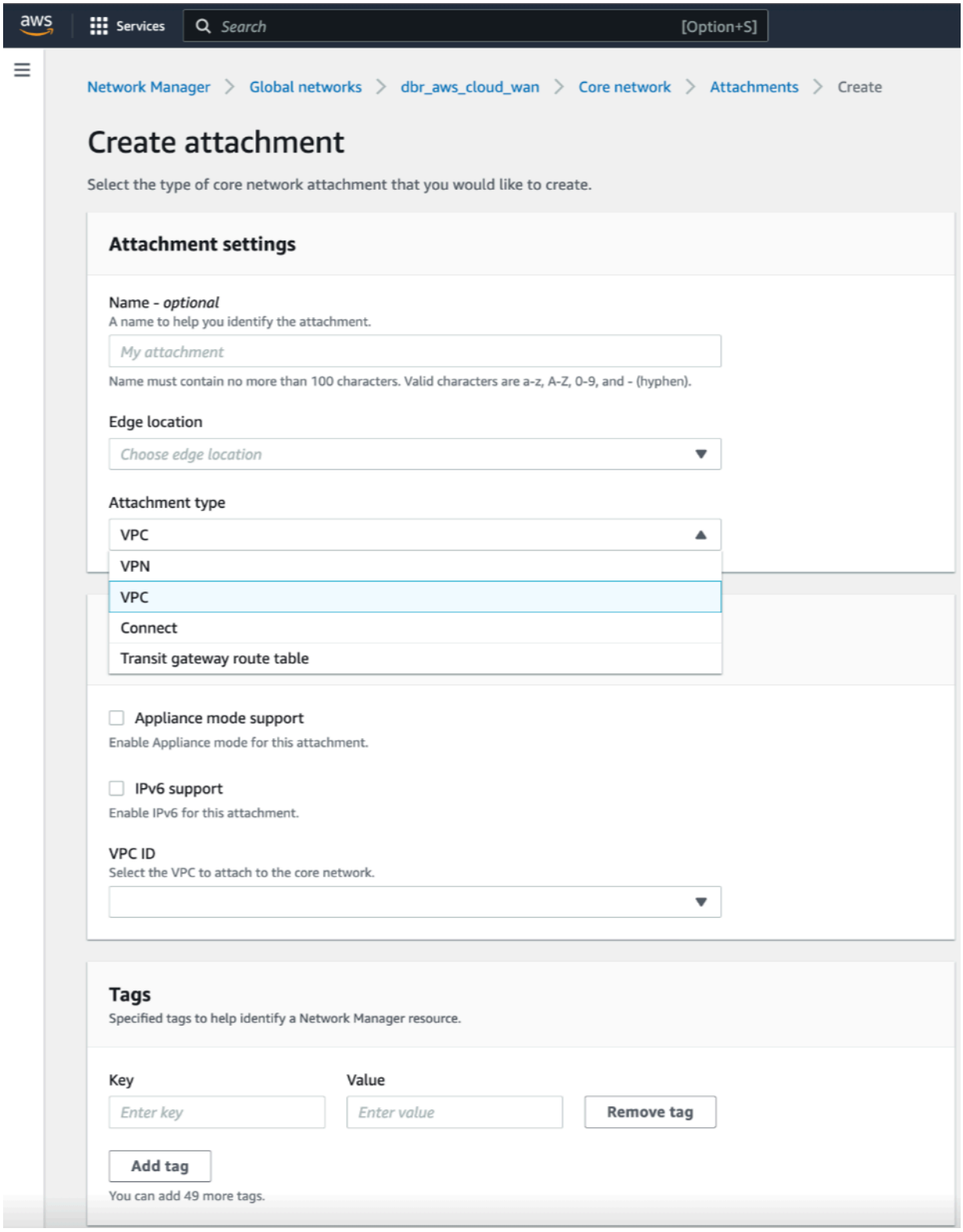


セグメント*(*キー*)*に実動セグメント*(*値*)*などのタグを追加できます。これらのタグは、*Cloud WAN*にセグメントを追加した後にのみ反映されます。

3. アタッチメントを作成します。

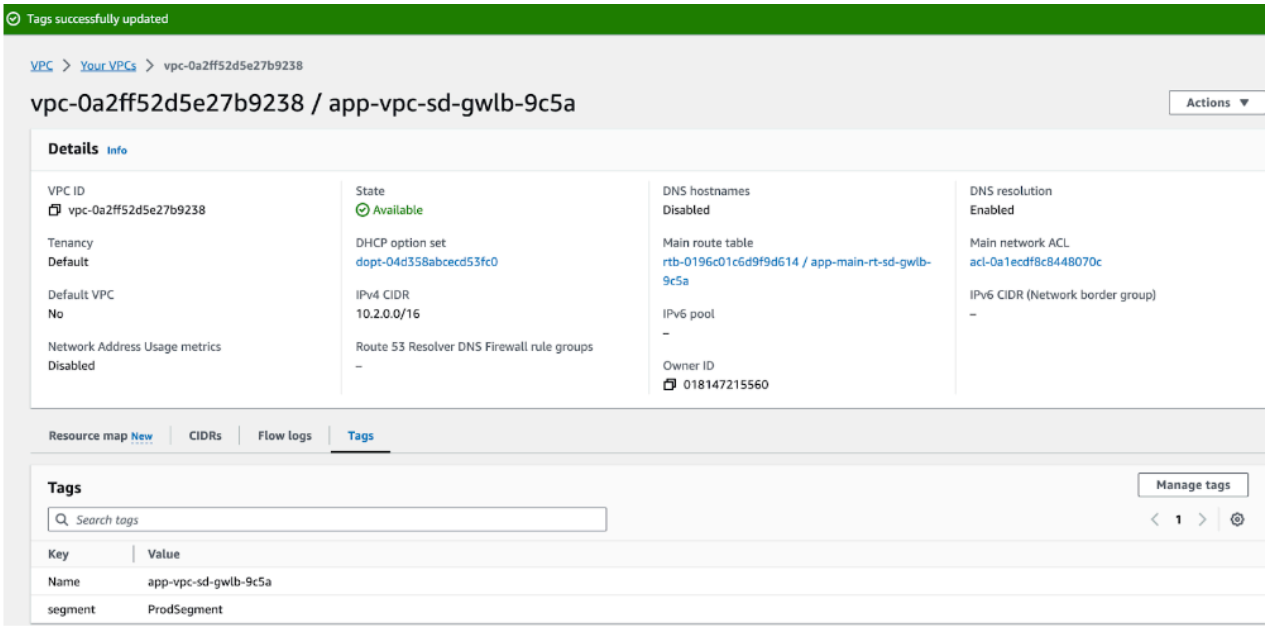
   - アタッチメントの作成時に、アタッチメントの種類として*VPC*またはトランジット ゲートウェイ ルート テーブルを使用します

     。
   - *VPC*アタッチメント間でルーティングされるトラフィックを*Cloud NGFW*ファイアウォールが検査できるように、*Cloud NGFW*ファイアウォールが含まれているセキュリティ *VPC*の*VPC*アタッチメント上で、アプライアンス モードを有効にする必要があります。

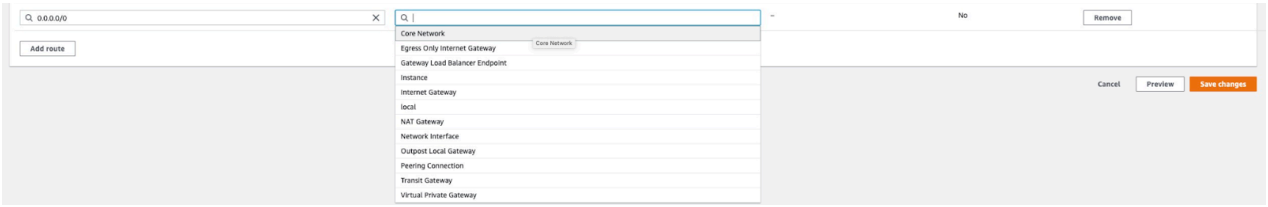


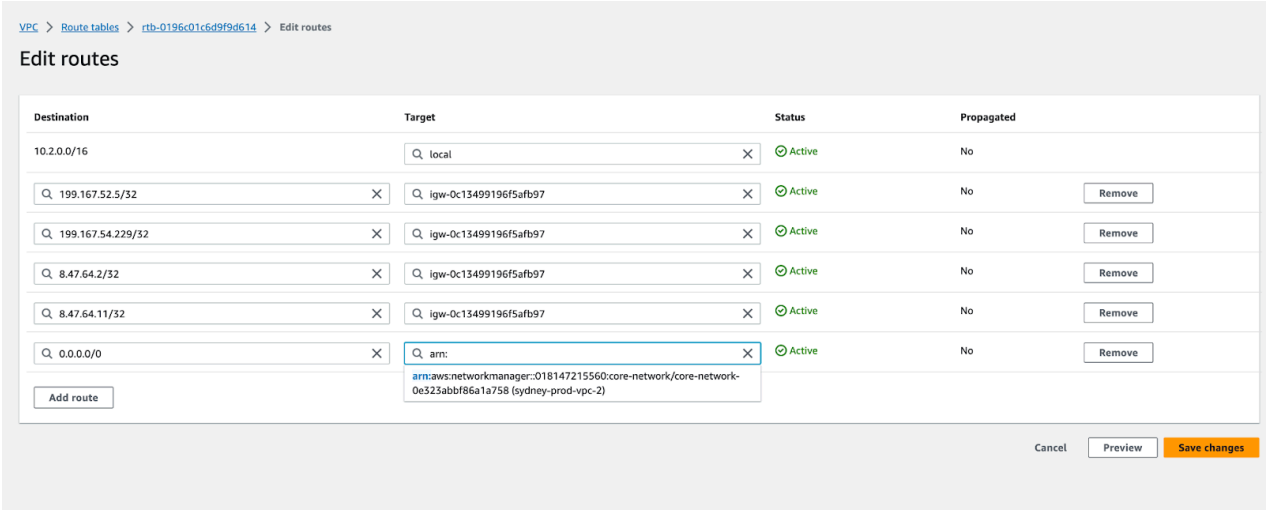
4. VPC Route Tables（ルートテーブル）を更新します。

   必要なCloud WAN構成が整ったので、コア ネットワークへのパケット転送を容易にするためにVPCを調整する必要があります。アプリケーションとファイアウォールのインスタンス、またはそれぞれのVPCには、セグメントのインスタンスと同様のタグを付ける必要があります。手順2の「ポリシーアタッチメントの作成」で作成したアタッチメントに合わせて、アタッチメントに特定のタグを追加します。



アタッチメントVPCとコア ネットワーク間の通信を有効にするには、以下に示すように、VPCルート テーブルを既存のターゲット トランジット ゲートウェイ ルートから対応するコアネットワークARNに更新する必要があります。



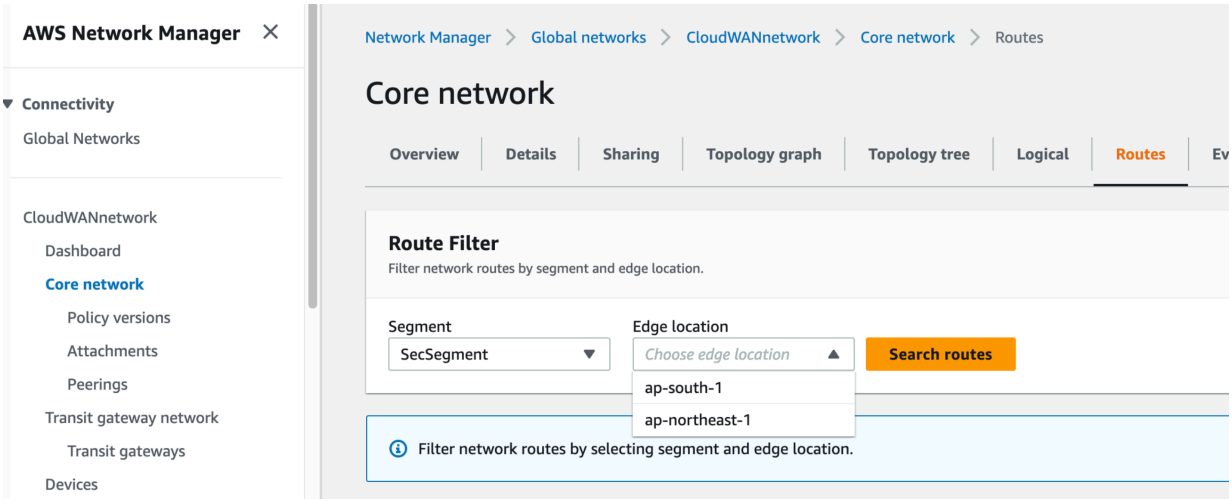


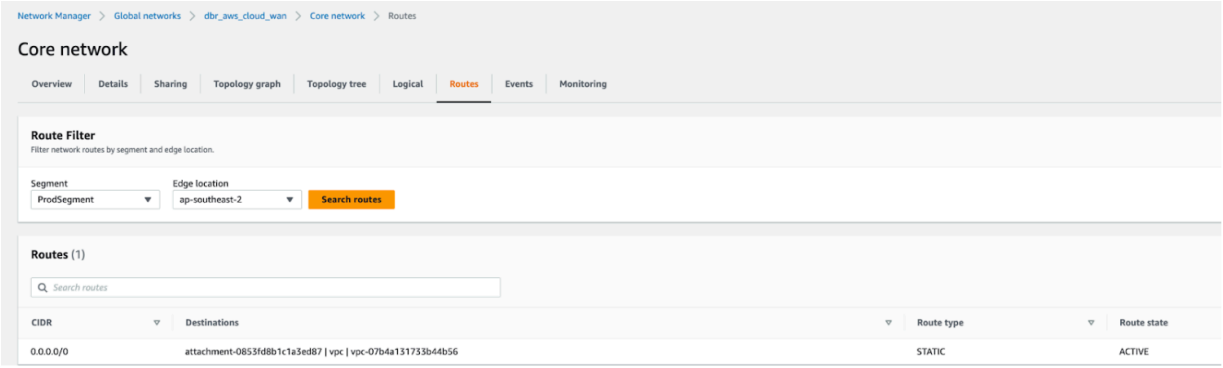
パケット ウォークスルー

以下の手順では、アプリケーションVPC 1のEC2インスタンスがアプリケーション VPC 2 のEC2インスタンスと通信する場合のパケット ウォークスルーについて説明します。

- APP VPC 1（10.1.0.0/16）のクライアントがAPP VPC 2（10.2.0.0/16）のサーバーへの接続を開始すると、VPC（App Subnet）ルート テーブル検索を実行します。パケットはコア ネットワークARNをターゲットとするデフォルト ルート エントリと一致し、コア ネットワークにルーティングされます。
- APP VPC 1はprodセグメントに関連付けられているため、パケットがコア ネットワークに到着すると、prodセグメントのルート テーブル検索を実行します。パケットはセキュリティ ア

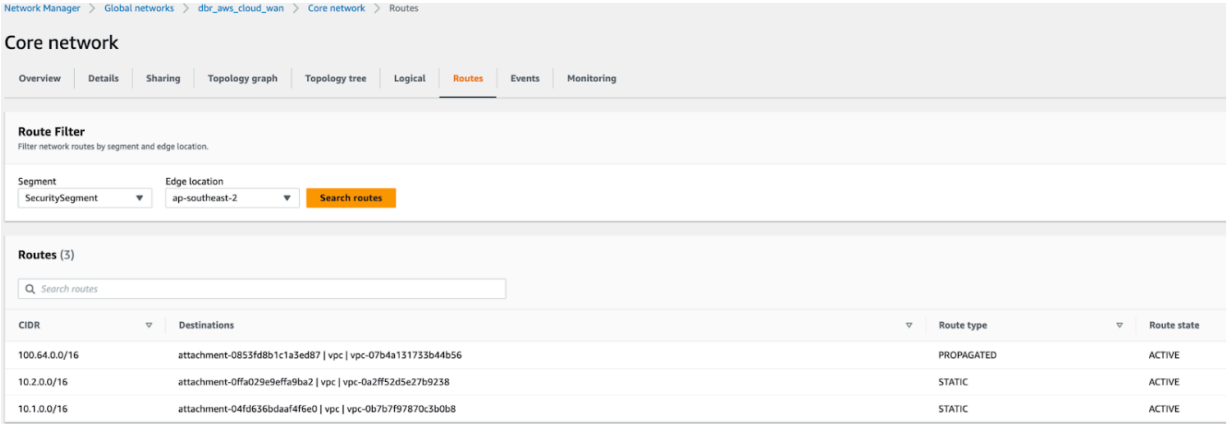
タッチメントをターゲットとするデフォルト エントリと一致し、セキュリティVPCにルーティングされます。





- パケットがセキュリティ VPC (100.64.0.0/16) アタッチメントに到達すると、VPC (CWANサブネット) ルートテーブル検索を実行します。パケットは、ファイアウォール エンドポイント1をターゲットとするデフォルト ルートと一致し、ファイアウォールにルーティングされ、ファイアウォールのエンドポイントを経由して検査されます。
- ファイアウォールはトラフィックを検査し、セキュリティ ポリシーと比較し、通過を許可します。ファイアウォールはパケットをファイアウォールのエンドポイントにルーティングして戻し、そこでVPC（ファイアウォール サブネット）ルート テーブル検索を行います。パケットはコア ネットワーク ARN をターゲットとするデフォルト ルート エントリと一致し、コア ネットワークにルーティングされます。
- セキュリティVPCはセキュリティ セグメントに関連付けられているため、パケットがコア ネットワークに到着すると、共有セキュリティ ルート テーブル検索を実行します。パケット

は、APP VPC 2アタッチメントをターゲットとするAPP VPC 2 CIDR(10.2.0.0/16)エントリと一致し、APP VPC 2にルーティングされます。



- パケットがAPP VPC 2に到着すると、VPC（CWANサブネット）ルート テーブル検索を実行します。パケットはローカルをターゲットとしてVPC CIDRエントリと一致し、インスタンスにルーティングされます。

リターン トラフィックは同じパスを逆方向にトレースします。