

**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](http://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](http://docs.paloaltonetworks.com).
- To search for a specific topic, go to our search page [docs.paloaltonetworks.com/search.html](http://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](mailto:documentation@paloaltonetworks.com).

## Copyright

Palo Alto Networks, Inc.  
[www.paloaltonetworks.com](http://www.paloaltonetworks.com)

© 2024-2025 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at [www.paloaltonetworks.com/company/trademarks.html](http://www.paloaltonetworks.com/company/trademarks.html). All other marks mentioned herein may be trademarks of their respective companies.

## Last Revised

April 8, 2025

---

# Table of Contents

|                                       |           |
|---------------------------------------|-----------|
| <b>Cloud NGFW for AWS 集中型デプロイメント</b>  | <b>5</b>  |
| 集中型 East-West                         | 6         |
| 集中型アウトバウンド                            | 9         |
| 集中型インバウンド                             | 12        |
| <b>Cloud NGFW for AWS の分散型デプロイメント</b> | <b>15</b> |
| 分散型 East-West (VPC 内)                 | 16        |
| 分散型アウトバウンド                            | 19        |
| 分散型インバウンド                             | 22        |
| <b>AWS Cloud WANとのCloud NGFW統合</b>    | <b>25</b> |



# 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?  |
|--|---|
| <ul style="list-style-type: none"><li>Cloud NGFW for AWS</li></ul> | <ul style="list-style-type: none"><li>Cloud NGFWサブスクリプション</li><li>Palo Alto Networksカスタマー サポート アカウント (CSP)</li><li>AWS Marketplaceアカウント</li><li>ユーザーのロール (テナントまたは管理者)</li></ul> |

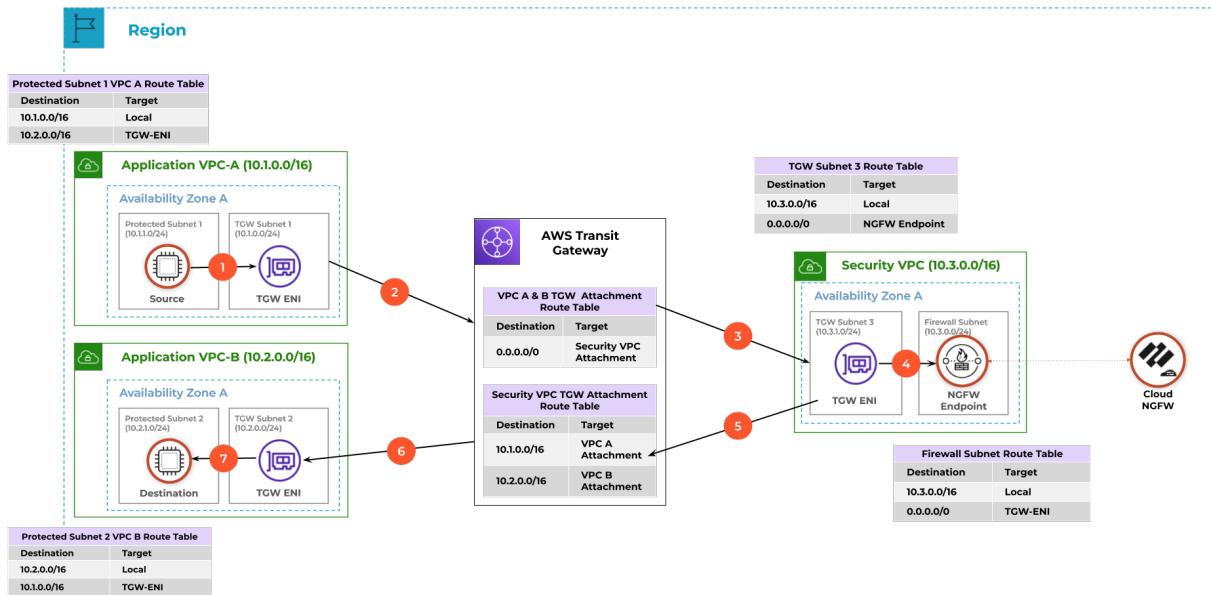
集中型デプロイメントでは、Cloud NGFWコンポーネントは集中化されたセキュリティVPCに展開されます。トライフィックは常にAWS Transit Gateway (TGW) を通過する必要があります。TGWはネットワークハブとして機能し、オンプレミスネットワークだけでなくVPC間の接続を簡素化します。

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。

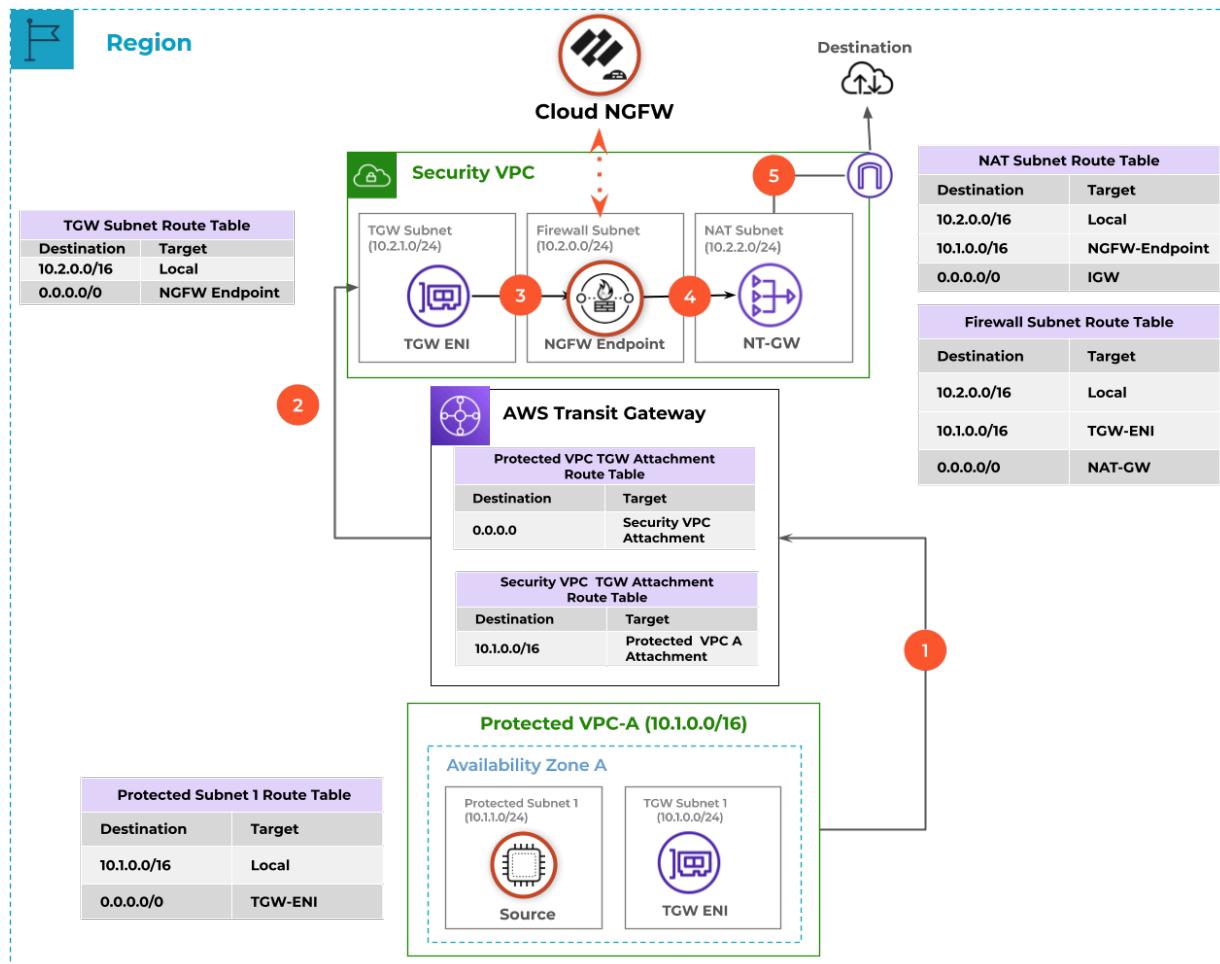
7. 次に、TGW Elastic Network Interfaceがトラフィックを宛先に送信します。



## 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。

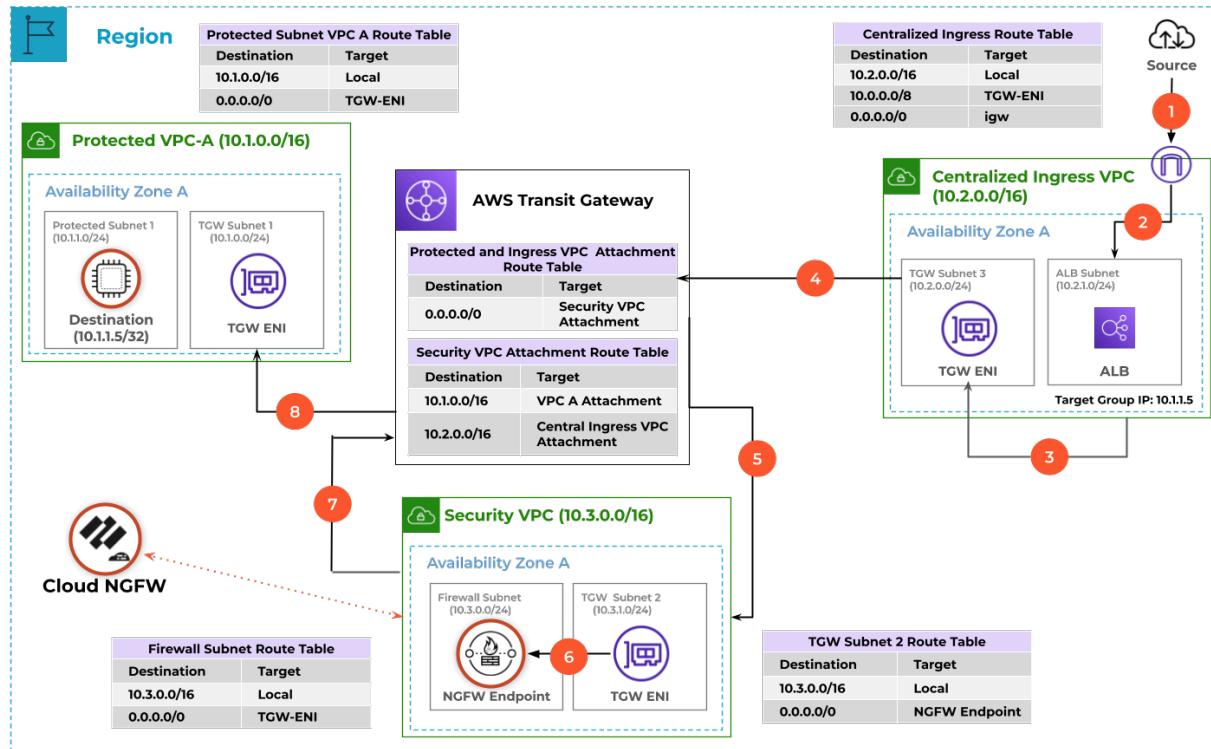
5. NAT ゲートウェイはトラフィックを IGW に転送し、宛先に転送します。



## 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?  |
|--|---|
| <ul style="list-style-type: none"><li>Cloud NGFW for AWS</li></ul> | <ul style="list-style-type: none"><li>Cloud NGFWサブスクリプション</li><li>Palo Alto Networksカスタマー サポート アカウント (CSP)</li><li>AWS Marketplaceアカウント</li><li>ユーザーのロール (テナントまたは管理者)</li></ul> |

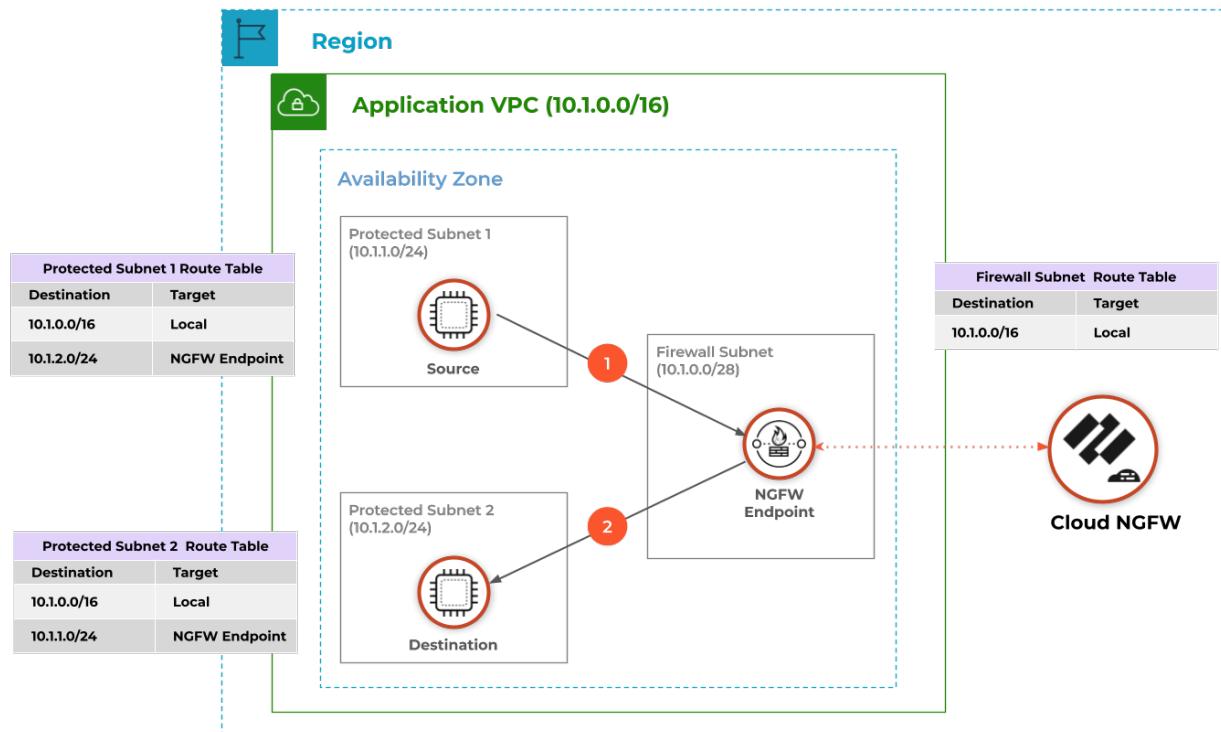
分散型デプロイメントでは、保護が必要な各 VPC に独自の NGFW があります。このデプロイメント方法はそれほど複雑ではないため、設定ミスの可能性が低くなります。

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。

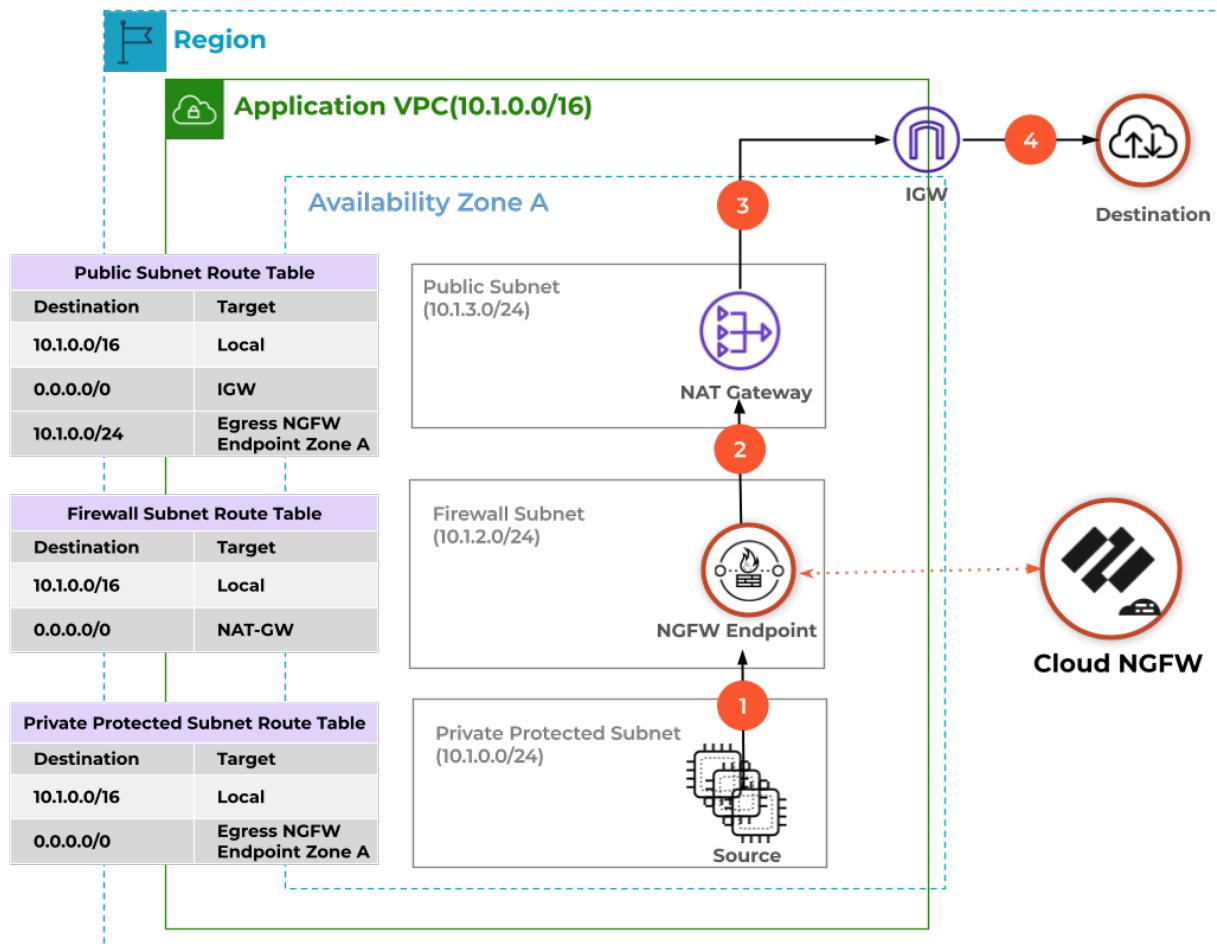
1. ルーティング規則が定義されている場合、Cloud NGFW はルーティング規則を元にパケットを転送します。
2. トラフィックが許可されている場合、NGFW エンドポイントはトラフィックを宛先に送信します。



## 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。

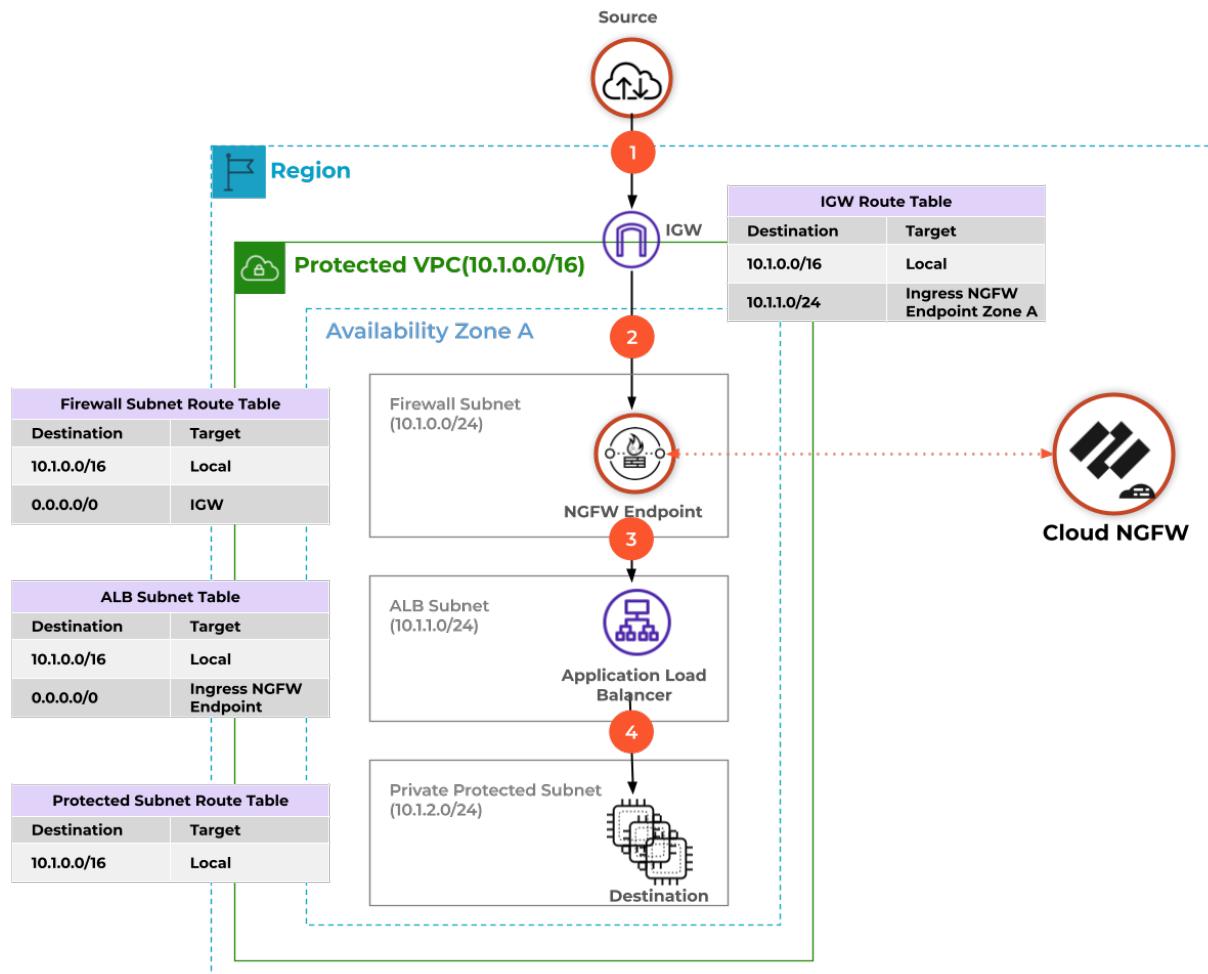
4. トライックはインターネットと宛先に続きます。



## 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?   |
|--|--|
| <ul style="list-style-type: none"> <li>Cloud NGFW for AWS</li> </ul> | <ul style="list-style-type: none"> <li>Cloud NGFWサブスクリプション</li> <li>Palo Alto Networksカスタマー サポート アカウント (CSP)</li> <li>AWS Marketplaceアカウント</li> <li>ユーザーのロール (テナントまたは管理者)</li> </ul> |

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。

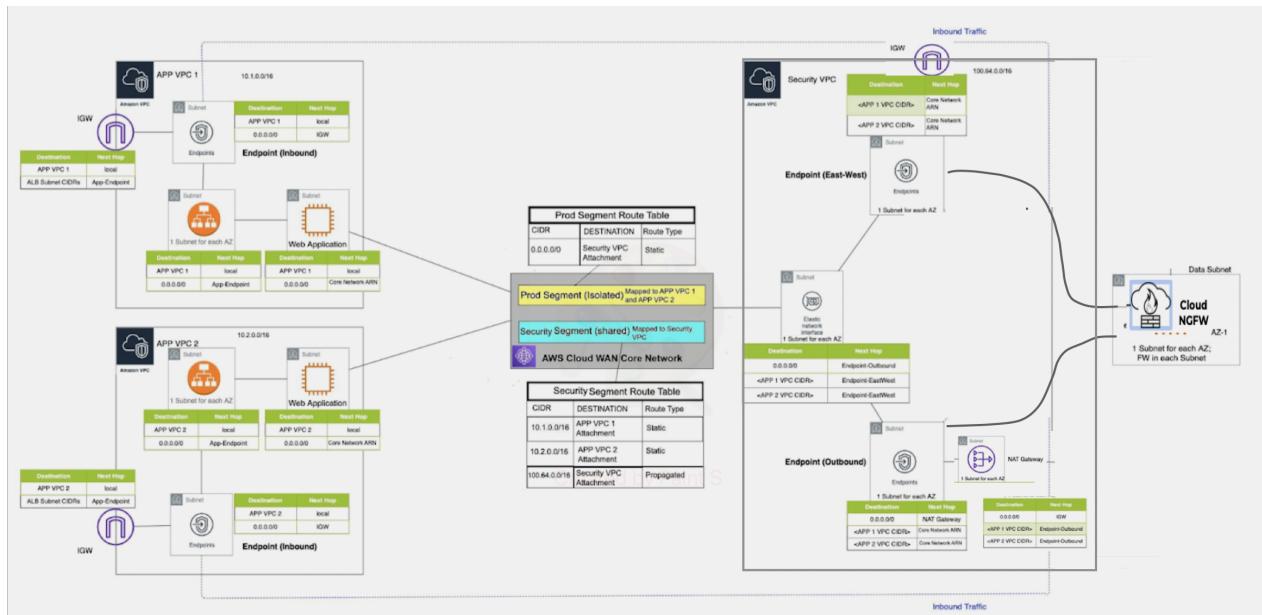
これらのVPCをコア ネットワーク内のセグメントにマッピングできます。これらのセグメントは、VPCアタッチメントやトランジット ゲートウェイ ルート テーブルアタッチメントなどのアタッチメントを使用して接続されます。[組み込みセグメンテーション](#)により、AWS環境とオンプレミス環境全体でネットワークの分離を維持できます。各セグメントは専用のルーティング ドメインを作成します。グローバル ネットワーク内に複数のネットワーク セグメントを作成できます。Cloud WANは、AWSのリソースをセグメント内の通信用に再構成します。簡単に言うと、Cloud WANでは、次のもの間でトラフィックをル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



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、Palo Alto 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。



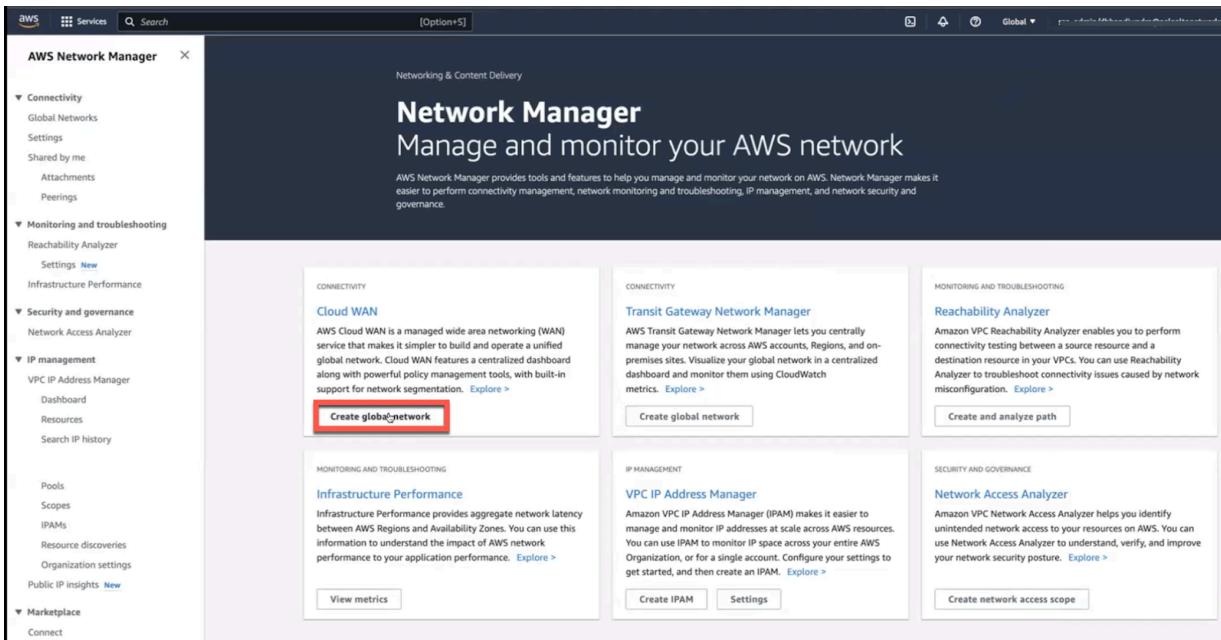
トランジット ゲートウェイから完全に移行するには、VPCをCloud WANに直接接続する必要があります。

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。

## AWS Cloud WANとのCloud NGFW統合



The screenshot shows the AWS Network Manager interface. The left sidebar lists various services: Connectivity (Global Networks, Settings, Shared by me, Attachments, Peering), Monitoring and troubleshooting (Reachability Analyzer, Infrastructure Performance), Security and governance (Network Access Analyzer), IP management (VPC IP Address Manager, Dashboard, Resources, Search IP history), and Marketplace (Connect). The main content area is titled "Network Manager" and "Manage and monitor your AWS network". It features several cards: "Cloud WAN" (a managed wide area networking (WAN) service), "Transit Gateway Network Manager" (lets you centrally manage your network across AWS accounts, Regions, and on-premises sites), "Reachability Analyzer" (Amazon VPC Reachability Analyzer enables you to perform connectivity testing between a source resource and a destination resource in your VPCs), "Infrastructure Performance" (provides aggregate network latency between AWS Regions and Availability Zones), "VPC IP Address Manager" (makes it easier to manage and monitor IP addresses at scale across AWS resources), and "Network Access Analyzer" (helps you identify unintended network access to your resources on AWS). Each card includes a "Create" button: "Create global network" for Cloud WAN, "Create global network" for Transit Gateway Network Manager, "Create and analyze path" for Reachability Analyzer, "Create IPAM" for VPC IP Address Manager, and "Create network access scope" for Network Access Analyzer. The "Create global network" button for Cloud WAN is highlighted with a red box.

## AWS Cloud WANとのCloud NGFW統合

AWS Network Manager

Network Manager > Global networks > dbr\_aws\_cloud\_wan

### dbr\_aws\_cloud\_wan

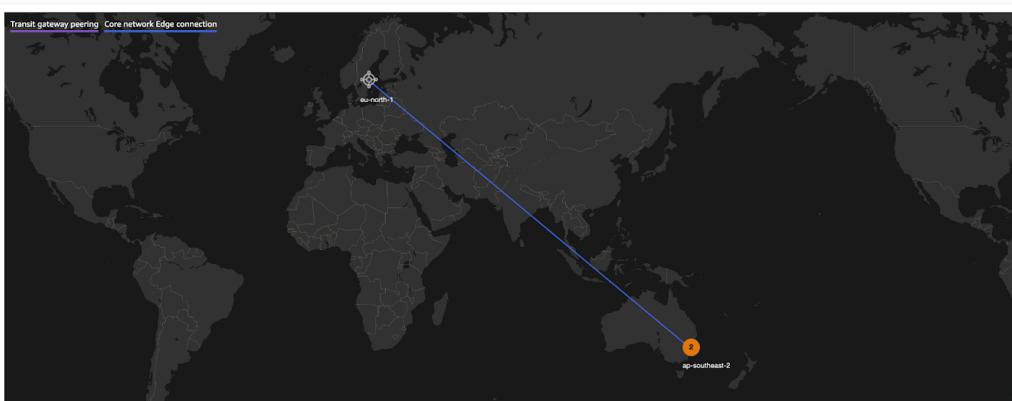
Overview Details Topology graph Topology tree

**Inventory**  
Network resources that are part of your global network.

| Category         | Count |
|------------------|-------|
| Edge locations   | 2     |
| Transit gateways | 1     |
| Devices          | 0     |
| Sites            | 0     |

**Geography**

Transit gateway peering | Core network Edge connection



The map shows a blue line connecting two specific locations on the globe: 'eu-north-1' in Europe and 'ap-southeast-2' in Southeast Asia. The map is a grayscale world map with political boundaries.

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。

## AWS Cloud WANとのCloud NGFW統合

Step 1  
[Create global network](#)

Step 2 - optional  
[Create core network](#)

Step 3  
Review

### Create core network - *optional*

Create a core network to represent your edge network locations and segments. [Learn more](#)

#### Include core network

Add core network in your global network  
Enabling core network will incur additional charges. For more information, see [pricing](#).

#### Core network general settings

**Name - optional**  
A name to help you identify the core network.  
  
Name must contain no more than 100 characters. Valid characters are a-z, A-Z, 0-9, and - (hyphen).

**Description - optional**  
A description to help you identify the core network.  
  
Description must contain no more than 100 characters. Valid characters are a-z, A-Z, 0-9, and - (hyphen).

**► Additional settings**

#### Core network policy settings

**ASN range**  
  
ASN range e.g. 64512 - 65534. The Autonomous System Number for the new Core network. The value must be a range between 64512 - 65534 or 4200000000 - 4294967294.

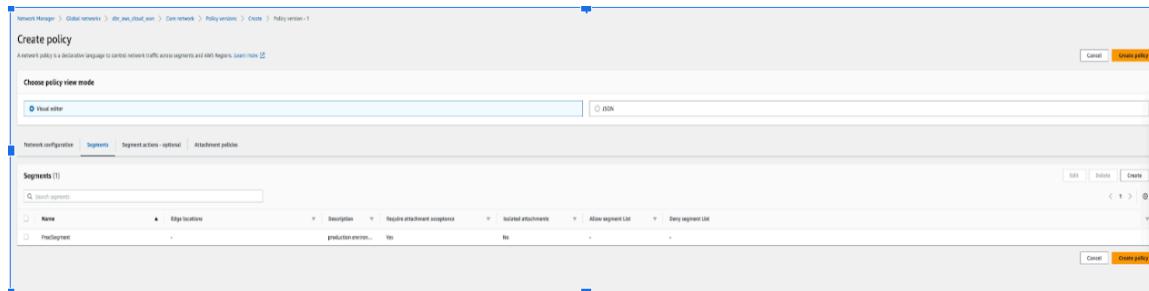
**Edge locations**

**Segment name**  
This is your default segment enabled in all selected edge locations.  
  
Name must contain no more than 100 characters. Valid characters are a-z, A-Z, and 0-9.

**Segment description**  
A description to help you identify the segment.

[Cancel](#) [Previous](#) [Next](#)

- 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。

The screenshot shows the 'Policy versions (1/2)' page. It lists two policy versions: 'Policy version - 1' (LIVE, Execution succeeded) and 'Policy version - 2' (LATEST, Ready to execute). A red box highlights the 'View or apply change set' button and the 'Ready to execute' status of the second policy version.

The screenshot shows the 'Policy version - 19 change sets (9)' page. It lists nine change sets, including modifications to core network segments and attachment route propagations. A red box highlights the 'Compare policy versions' and 'Apply change set' buttons.

- 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。

The screenshot shows the 'Segments (2)' page. It lists two segments: 'ProdSegment' and 'SecuritySegment'. Both segments have 'ap-southeast-2, eu-north-1' as their edge locations. The 'ProdSegment' has 'No' for 'Require attachment acceptance' and 'Yes' for 'Isolated attachments'. The 'SecuritySegment' has 'No' for both 'Require attachment acceptance' and 'Isolated attachments'. A red box highlights the 'Allow segment List' and 'Deny segment List' columns.

- 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。

## AWS Cloud WANとのCloud NGFW統合



| Segment         | Shared with segments |
|-----------------|----------------------|
| SecuritySegment | All                  |



| Segment         | Destination CIDR block | Destination                  |
|-----------------|------------------------|------------------------------|
| ProdSegment     | 0.0.0.0/0              | attachment-0853fd8b1c1a3ed87 |
| SecuritySegment | 10.1.0.0/16            | attachment-04fd636bdaaf4f6e0 |
| SecuritySegment | 10.2.0.0/16            | attachment-0ffu029e9effa9ba2 |

- ポリシーアタッチメントを作成します。



| Rule number | Description | Segment to attach              | Require acceptance | Conditions | Operator | Condition values                   | Condition logic |
|-------------|-------------|--------------------------------|--------------------|------------|----------|------------------------------------|-----------------|
| 110         | -           | Segment name - ProdSegment     | -                  | tag-value  | equals   | key=segment, value=ProdSegment     | or              |
| 111         | -           | Segment name - SecuritySegment | -                  | tag-value  | equals   | key=segment, value=SecuritySegment | or              |



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。

The screenshot shows the AWS Cloud WAN 'Create attachment' settings page. The navigation path is: Network Manager > Global networks > dbr\_aws\_cloud\_wan > Core network > Attachments > Create. The main title is 'Create attachment' with the sub-instruction 'Select the type of core network attachment that you would like to create.' Below this, the 'Attachment settings' section is displayed. The 'Name - optional' field contains 'My attachment'. The 'Edge location' dropdown is set to 'Choose edge location'. The 'Attachment type' dropdown is set to 'VPC', with other options like 'VPN', 'Connect', and 'Transit gateway route table' available. Under 'VPC ID', there is a dropdown menu. The 'Tags' section allows adding key-value pairs, with an 'Add tag' button and a note that 49 more tags can be added. The top right corner of the page has a search bar and a 'Search' button, and the status '[Option+S]'.

Network Manager > Global networks > dbr\_aws\_cloud\_wan > Core network > Attachments > Create

## Create attachment

Select the type of core network attachment that you would like to create.

### Attachment settings

**Name - optional**  
A name to help you identify the attachment.  
My attachment

Name must contain no more than 100 characters. Valid characters are a-z, A-Z, 0-9, and - (hyphen).

**Edge location**  
Choose edge location

**Attachment type**

- VPC
- VPN
- VPC**
- Connect
- Transit gateway route table

**Appliance mode support**  
Enable Appliance mode for this attachment.

**IPv6 support**  
Enable IPv6 for this attachment.

**VPC ID**  
Select the VPC to attach to the core network.

**Tags**  
Specified tags to help identify a Network Manager resource.

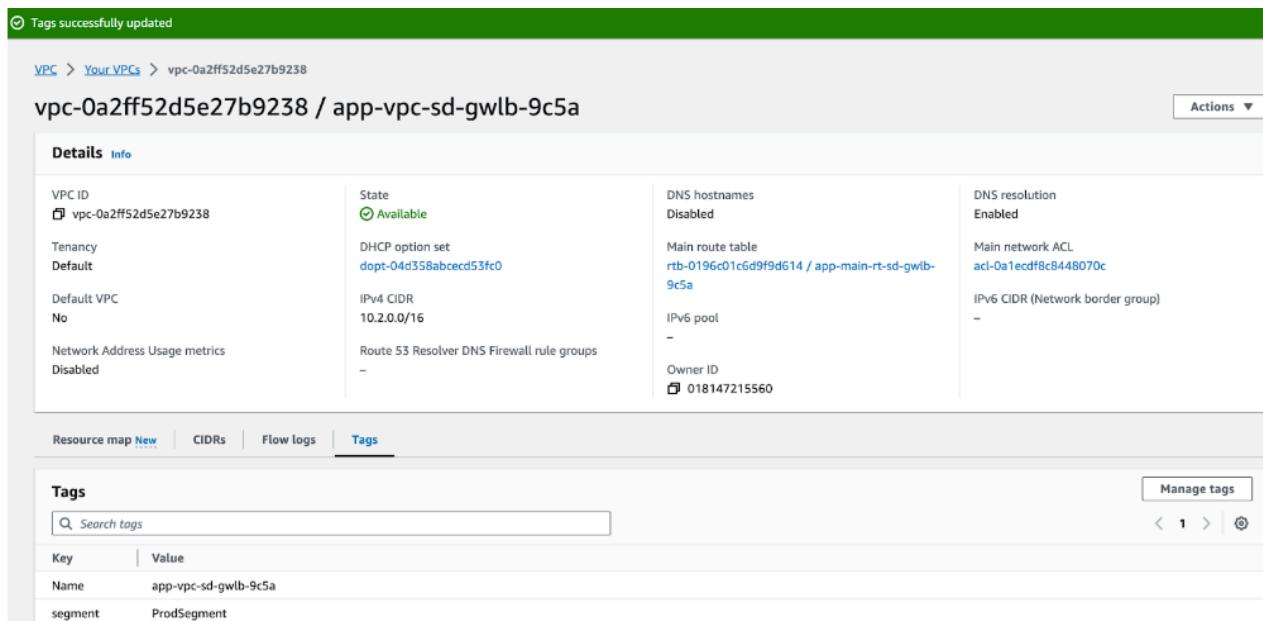
| Key       | Value       | Remove tag |
|-----------|-------------|------------|
| Enter key | Enter value | Remove tag |

Add tag

You can add 49 more tags.

#### 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。



Tags successfully updated

VPC > Your VPCs > vpc-0a2ff52d5e27b9238 / app-vpc-sd-gwlb-9c5a

Actions ▾

**Details** **Info**

|   |   |  |   |
|---|---|--|---|
| VPC ID<br>vpc-0a2ff52d5e27b9238           | State<br>Available                              | DNS hostnames<br>Disabled  | DNS resolution<br>Enabled                 |
| Tenancy<br>Default                        | DHCP option set<br>dopt-04d358abced53fc0        | Main route table<br>rtb-0196c01c6d9f9d614 / app-main-rt-sd-gwlb-9c5a | Main network ACL<br>acl-0a1ecdf8c8448070c |
| Default VPC<br>No                         | IPv4 CIDR<br>10.2.0.0/16                        | IPv6 pool<br>-   | IPv6 CIDR (Network border group)<br>-     |
| Network Address Usage metrics<br>Disabled | Route 53 Resolver DNS Firewall rule groups<br>- | Owner ID<br>018147215560   |   |

Resource map [New](#) | CIDRs | Flow logs | **Tags**

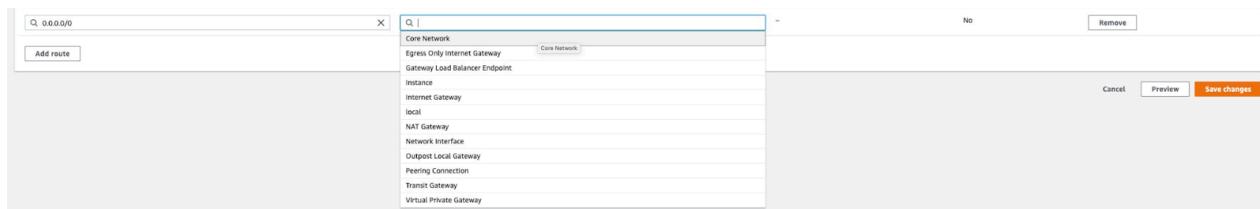
Tags

Manage tags

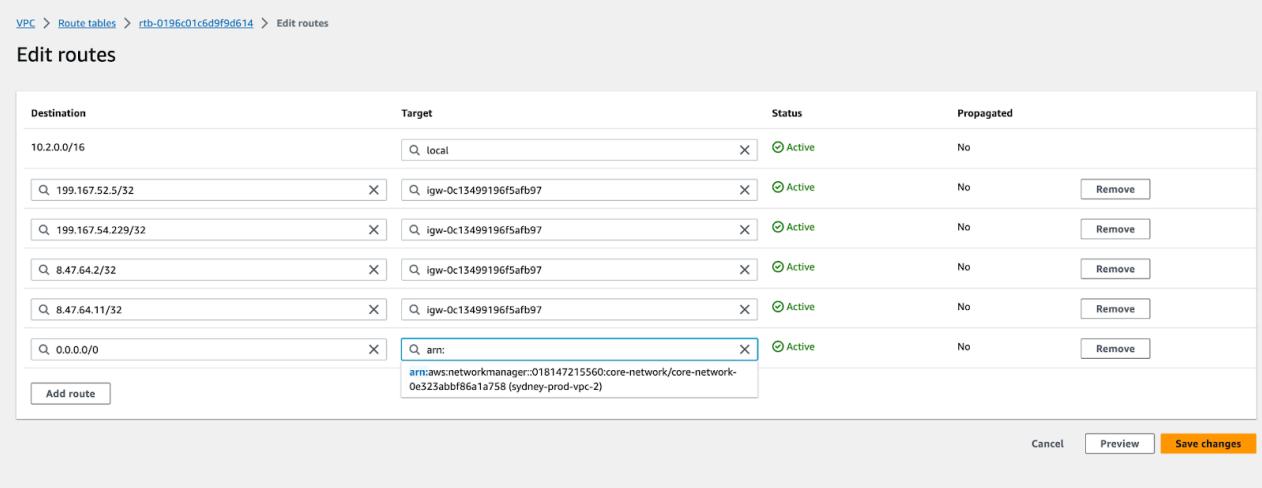
| Key     | Value                |
|---------|----------------------|
| Name    | app-vpc-sd-gwlb-9c5a |
| segment | ProdSegment          |

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。

## AWS Cloud WANとのCloud NGFW統合



## AWS Cloud WANとのCloud NGFW統合



The screenshot shows the 'Edit routes' interface for a specific route table. The table has columns for Destination, Target, Status, and Propagated. There are six existing routes and one new route being added.

| Destination       | Target  | Status | Propagated |
|-------------------|---|--------|------------|
| 10.2.0.0/16       | local   | Active | No         |
| 199.167.52.5/32   | igw-0c13499196f5afb97   | Active | No         |
| 199.167.54.229/32 | igw-0c13499196f5afb97   | Active | No         |
| 8.47.64.2/32      | igw-0c13499196f5afb97   | Active | No         |
| 8.47.64.11/32     | igw-0c13499196f5afb97   | Active | No         |
| 0.0.0.0/0         | arn:aws:networkmanager:018147215560:core-network/core-network-0e323abb861a758 (sydney-prod-vpc-2) | Active | No         |
| Add route         |   |        |            |

At the bottom right, there are buttons for 'Cancel', 'Preview', and 'Save changes'.

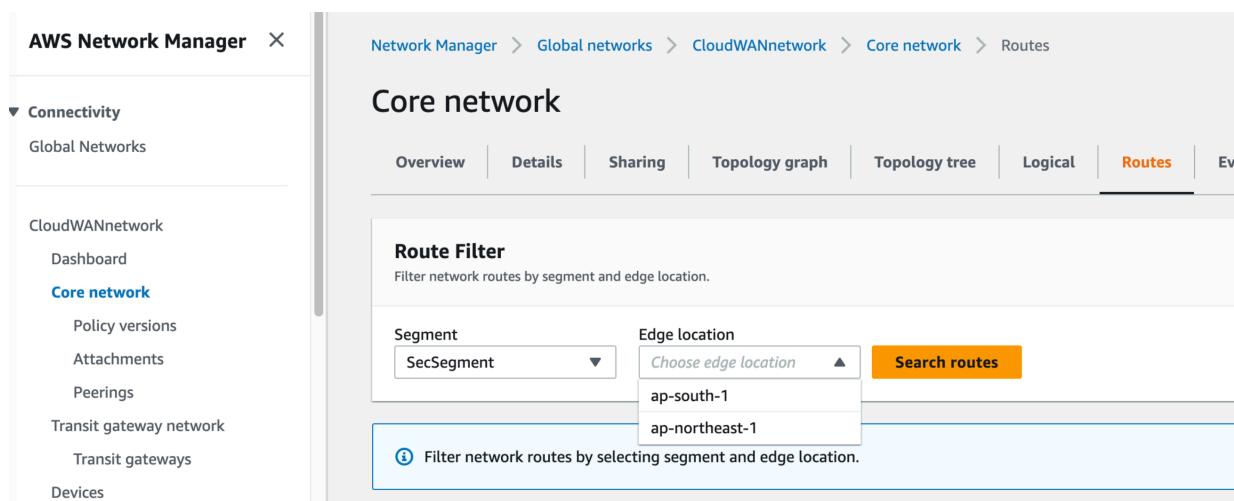
### パケット ウォークスルー

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

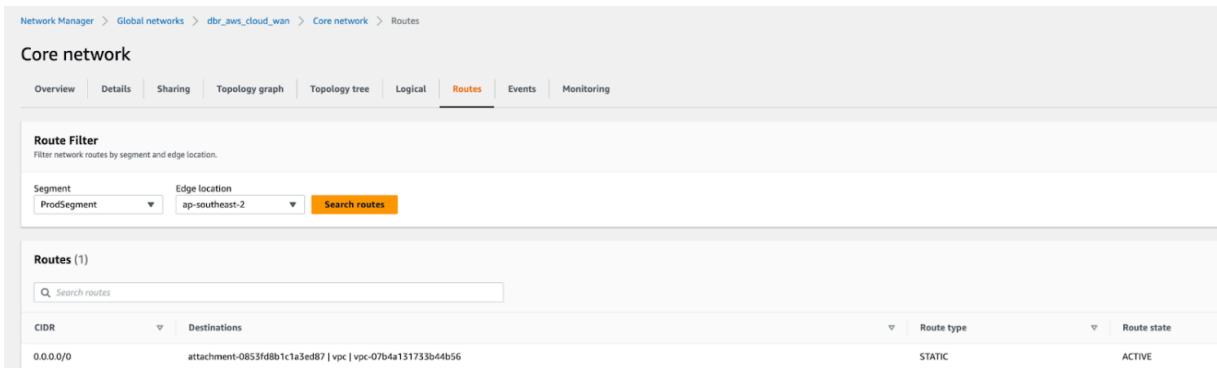
## AWS Cloud WANとのCloud NGFW統合

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。



The screenshot shows the AWS Network Manager interface. The left sidebar is titled 'AWS Network Manager' and has a 'Connectivity' section with 'Global Networks' and 'CloudWANnetwork' expanded. Under 'CloudWANnetwork', 'Core network' is selected, and its sub-options include 'Policy versions', 'Attachments', 'Peerings', 'Transit gateway network', 'Transit gateways', and 'Devices'. The main content area is titled 'Core network' and shows the 'Routes' tab selected. A 'Route Filter' section is present, with 'Segment' set to 'SecSegment' and 'Edge location' set to 'ap-south-1'. A dropdown menu for 'Edge location' shows 'ap-south-1' and 'ap-northeast-1'. A 'Search routes' button is also visible. A tooltip at the bottom of the filter section says: 'Filter network routes by selecting segment and edge location.'

## AWS Cloud WANとのCloud NGFW統合



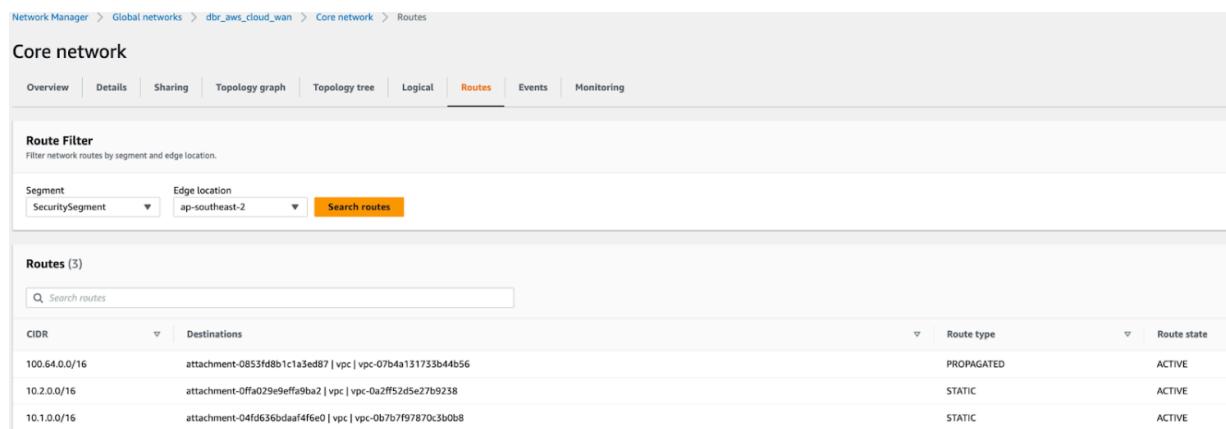
The screenshot shows the AWS Network Manager interface for a 'Core network'. The 'Routes' tab is selected. A 'Route Filter' section allows filtering by 'Segment' (ProdSegment) and 'Edge location' (ap-southeast-2), with a 'Search routes' button. Below this, a table titled 'Routes (1)' displays one route entry:

| CIDR      | Destinations   | Route type | Route state |
|-----------|--|------------|-------------|
| 0.0.0.0/0 | attachment-0853fd8b1c1a3ed87   vpc   vpc-07b4a131733b44b56 | STATIC     | ACTIVE      |

- 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

## AWS Cloud WANとのCloud NGFW統合

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。



The screenshot shows the AWS Network Manager Core network Routes page. The navigation path is: Network Manager > Global networks > db\_r\_aws\_cloud\_wan > Core network > Routes. The 'Routes' tab is selected. A 'Route Filter' section allows filtering by Segment (SecuritySegment) and Edge location (ap-southeast-2). A search bar is present. The main table displays three routes:

| CIDR          | Destinations   | Route type | Route state |
|---------------|--|------------|-------------|
| 100.64.0.0/16 | attachment-0853fd8b1c1a3ed87   vpc   vpc-07b4a131733b44b56   | PROAGATED  | ACTIVE      |
| 10.2.0.0/16   | attachment-0ffa029e9effa9ba2   vpc   vpc-0a2ff52d5e27b9238   | STATIC     | ACTIVE      |
| 10.1.0.0/16   | attachment-04fd636bdcaaaf4f6e0   vpc   vpc-0b7b7f97870c3b0b8 | STATIC     | ACTIVE      |

- 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。

