

# 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](https://docs.paloaltonetworks.com).
- To search for a specific topic, go to our search page [docs.paloaltonetworks.com/search.html](https://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>

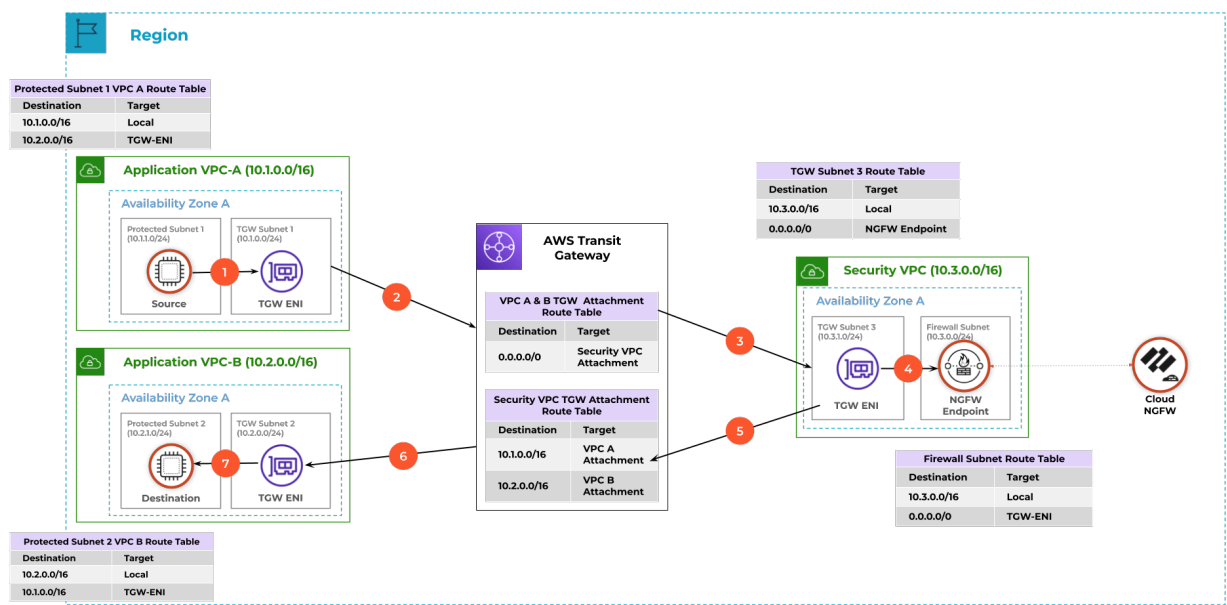
集中型デプロイメントでは、Cloud NGFWコンポーネントは集中化されたセキュリティVPCに展開されます。トラフィックは常にAWS Transit Gateway (TGW) を通過する必要があります。TGWはネットワークハブとして機能し、オンプレミスネットワークだけでなくVPC間の接続を簡素化します。

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。

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

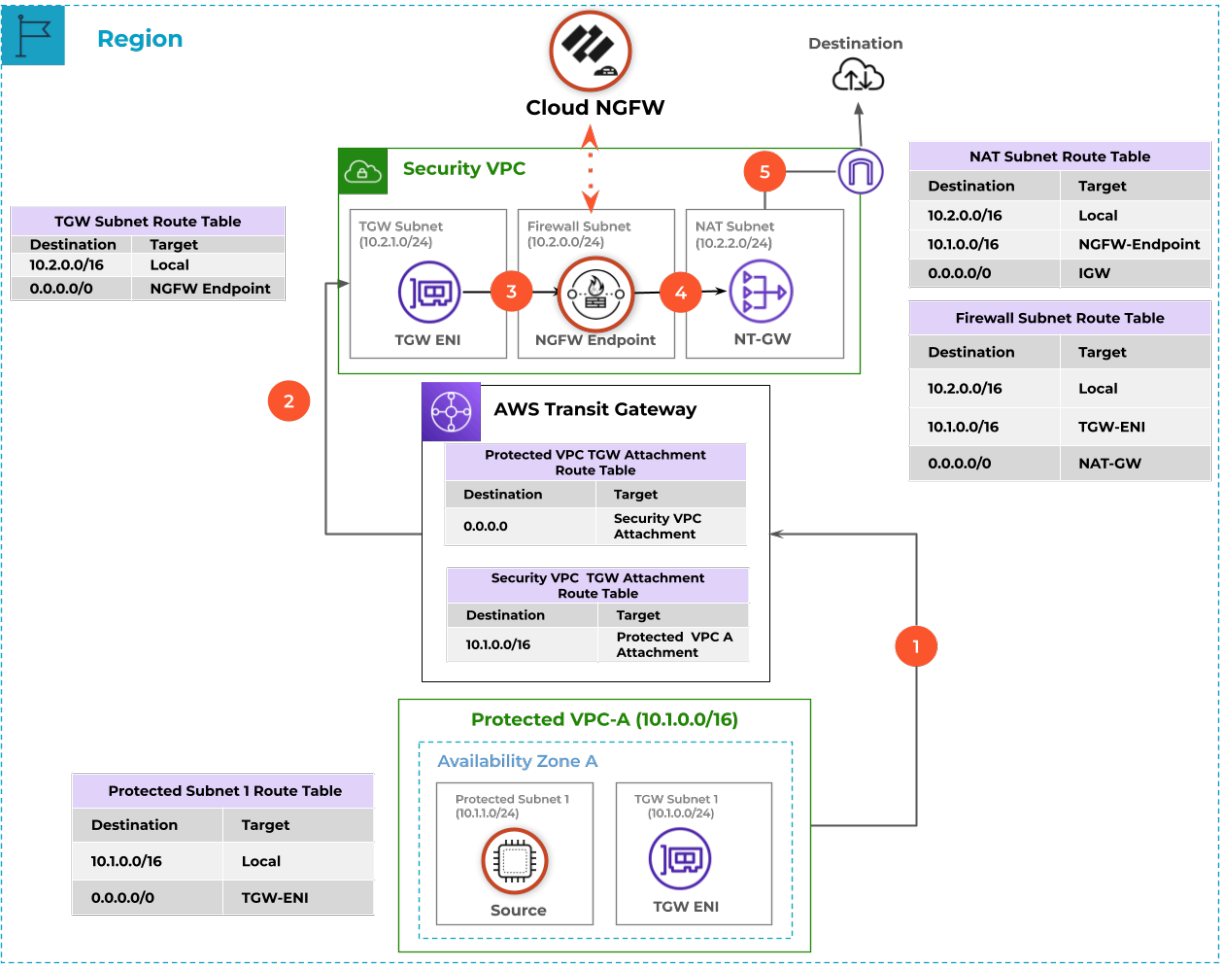




## 集中型アウトバウンド

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。

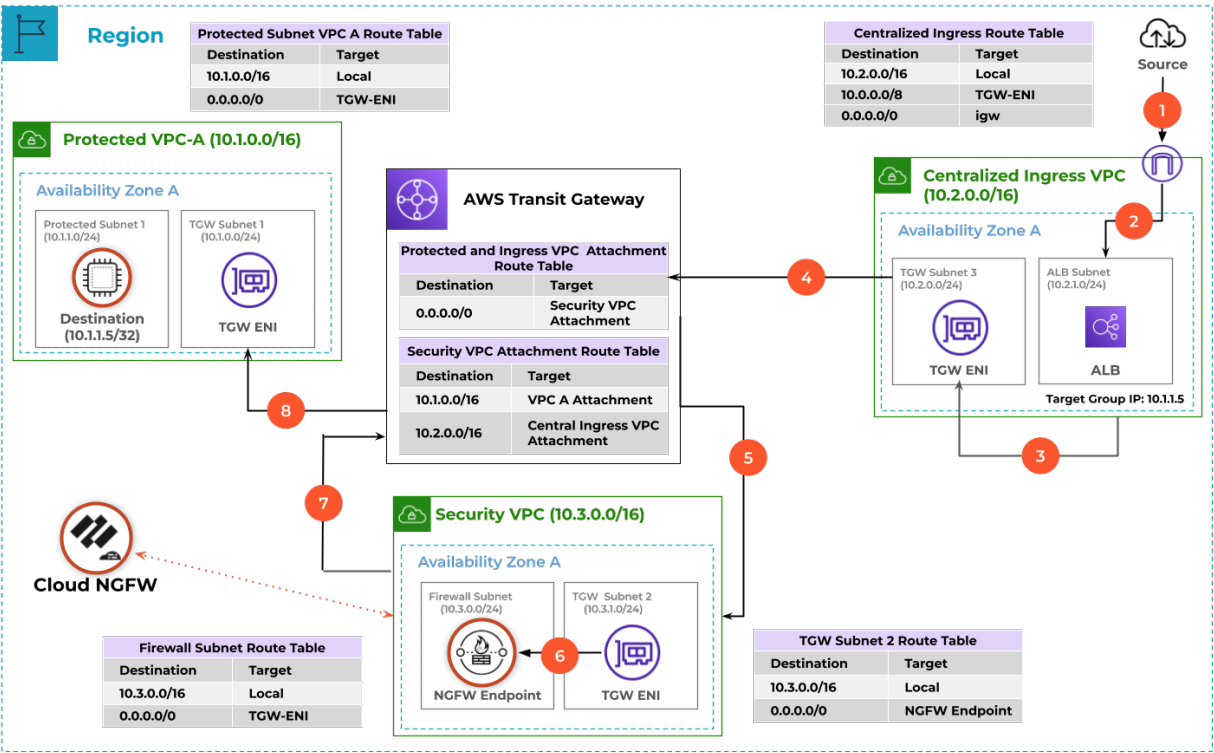
5. NAT ゲートウェイはトラフィックを IGW に転送し、宛先に転送します。



## 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。

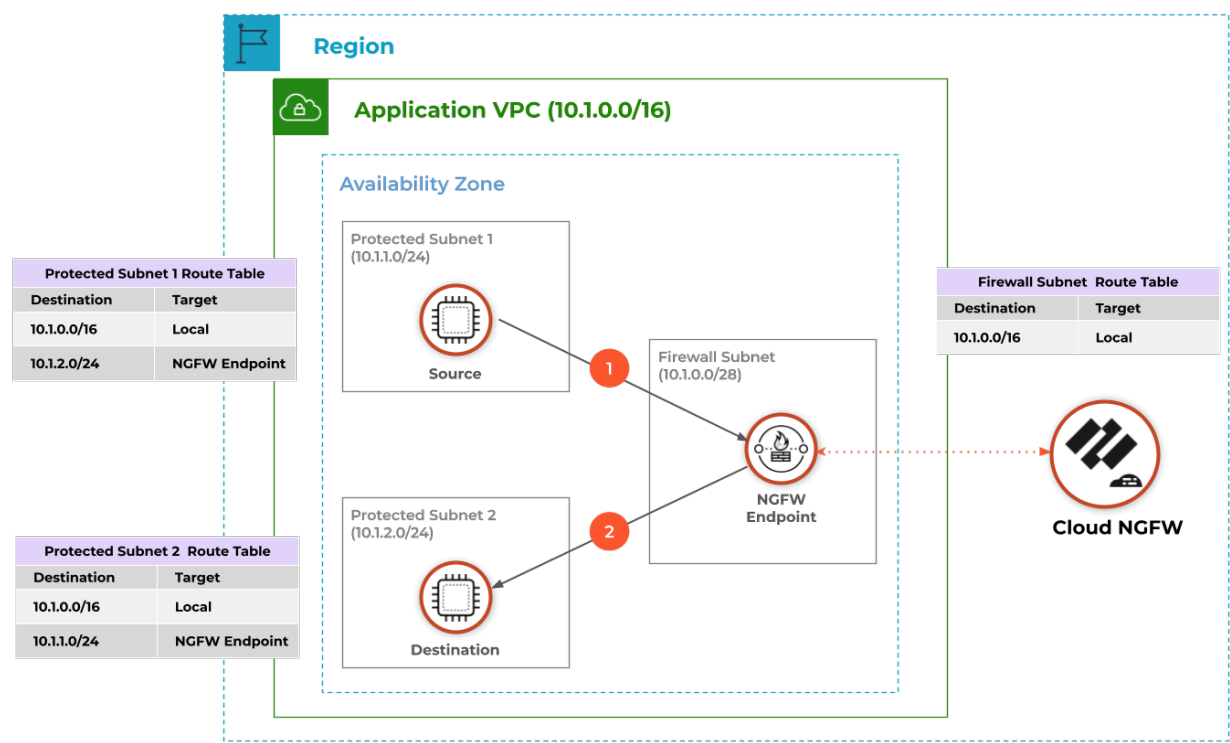
分散型デプロイメントのその他の例については、[Cloud NGFW for AWS デプロイメントアーキテクチャ](#)を参照してください。

## 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。



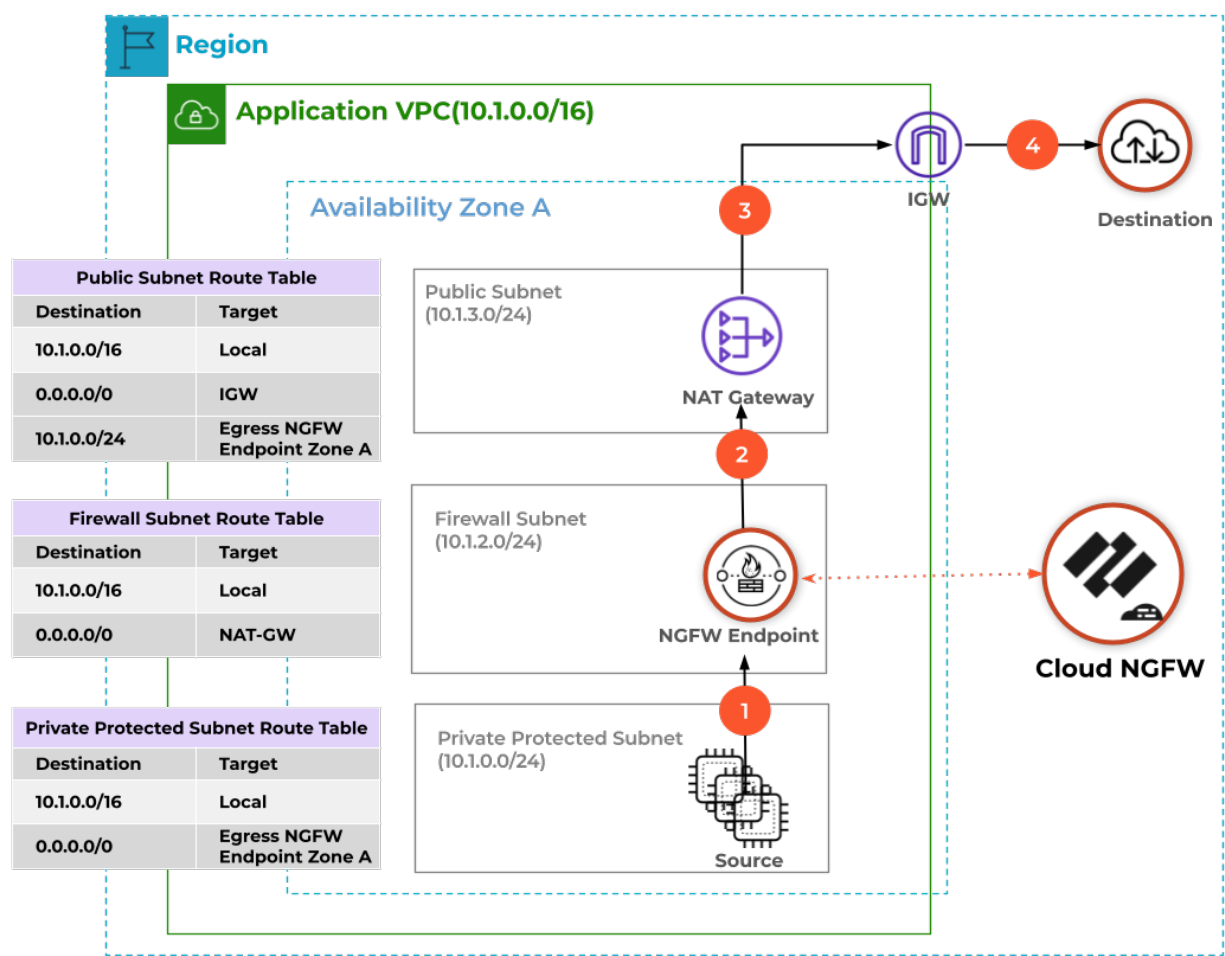
2. トラフィックが許可されている場合、NGFW エンドポイントはトラフィックを宛先に送信します。



## 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。

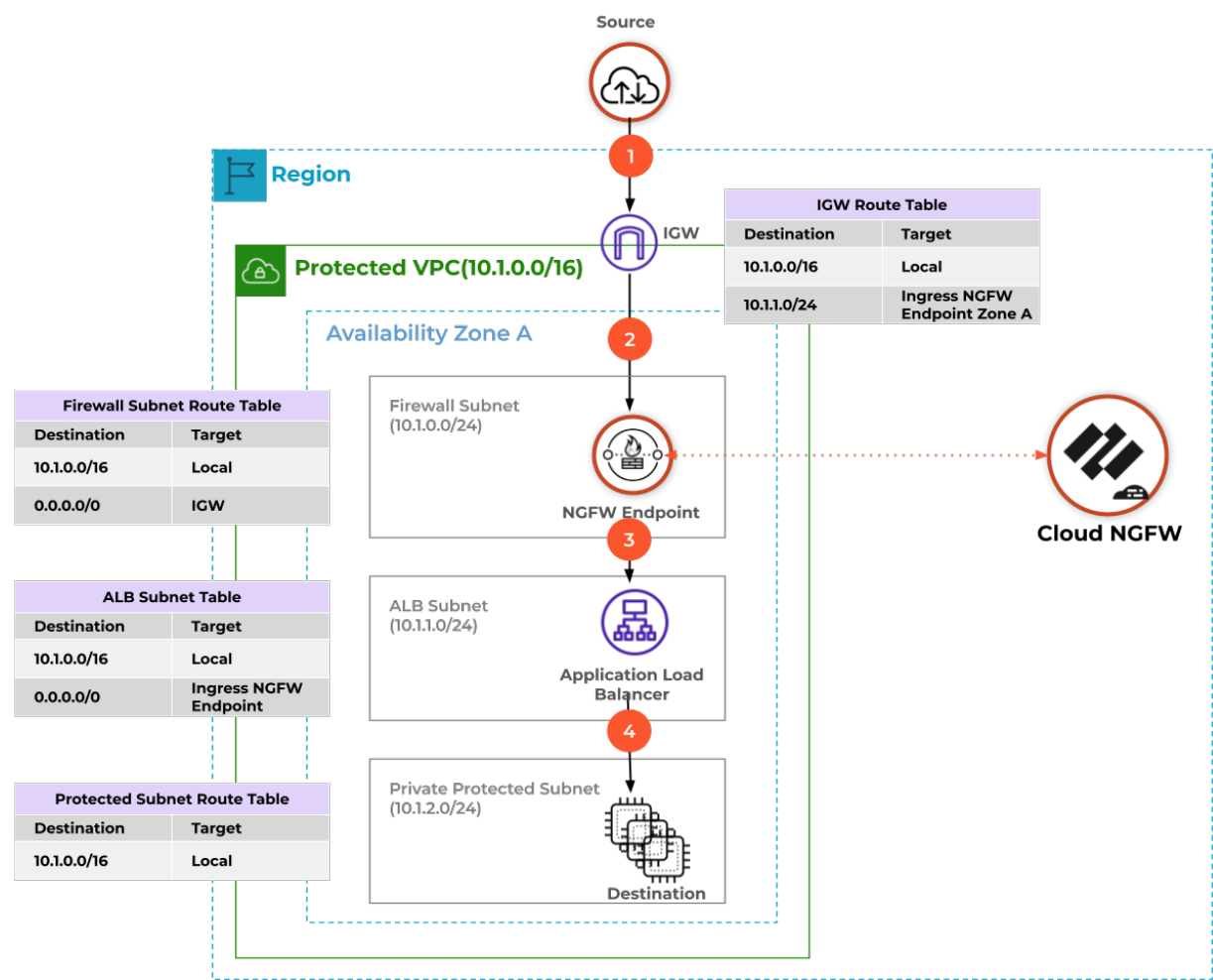
4. トラフィックはインターネットと宛先に続きます。



## 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？
<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。



©2025 Palo Alto Networks, Inc.

- **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。

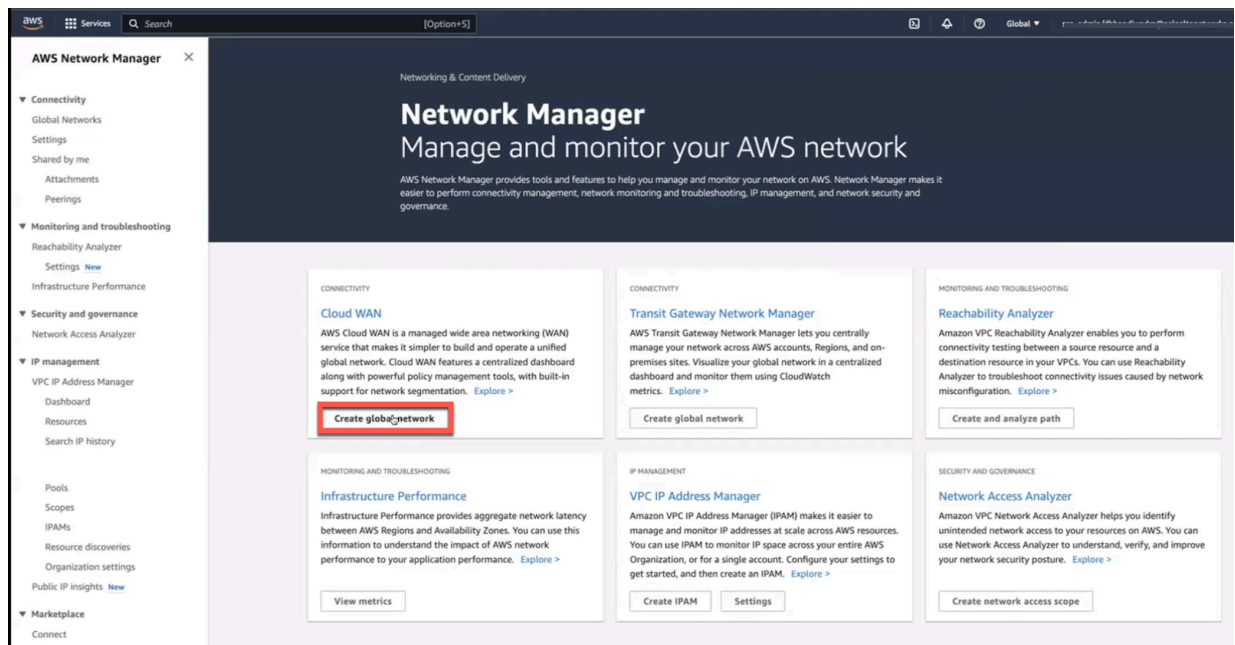


トランジットゲートウェイから完全に移行するには、VPCをCloud WANに直接接続する必要があります。

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 Network Manager** ×

▼ Connectivity  
Global Networks

dbr\_aws\_cloud\_wan  
[Dashboard](#)  
Core network  
Policy versions  
Attachments  
Peerings  
Transit gateway network  
Transit gateways  
Devices  
Sites

▼ Monitoring and troubleshooting  
Reachability Analyzer  
Settings [New](#)  
Infrastructure Performance

▼ Security and governance  
Network Access Analyzer

▼ IP management  
VPC IP Address Manager  
Dashboard  
Resources  
Search IP History

Pools  
Scopes  
IPAMs  
Resource discoveries  
Organization settings

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.

<b>Edge locations</b> 2	<b>Transit gateways</b> 1	<b>Devices</b> 0	<b>Sites</b> 0
----------------------------	------------------------------	---------------------	-------------------

**Geography**

[Transit gateway peering](#) | [Core network Edge connection](#)

The map displays a global network topology. A blue line connects the 'eu-north-1' region in Northern Europe to the 'ap-southeast-2' region in Southeast Asia. The map is powered by Mapbox.

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。



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.

cwan-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.

A core network for testing purposes.

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**

64520 - 64530

ASN range e.x 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**

Choose edge locations

Asia Pacific (Sydney) X Europe (Stockholm) X

ap-southeast-2 eu-north-1

**Segment name**  
This is your default segment enabled in all selected edge locations.

Dev

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.

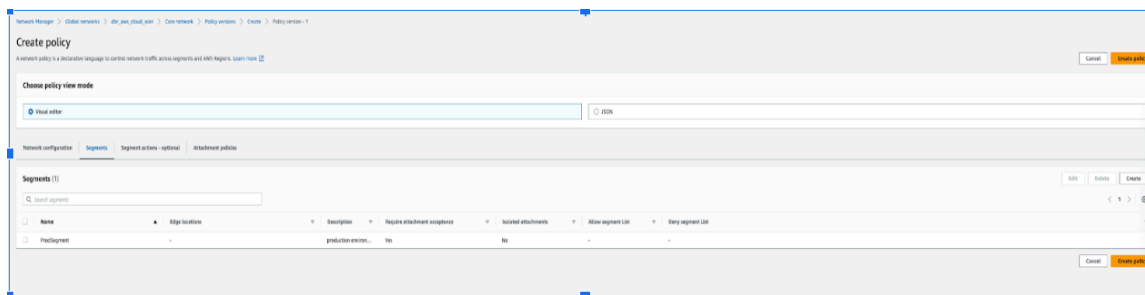
A segment for testing purposes.

Cancel

Previous

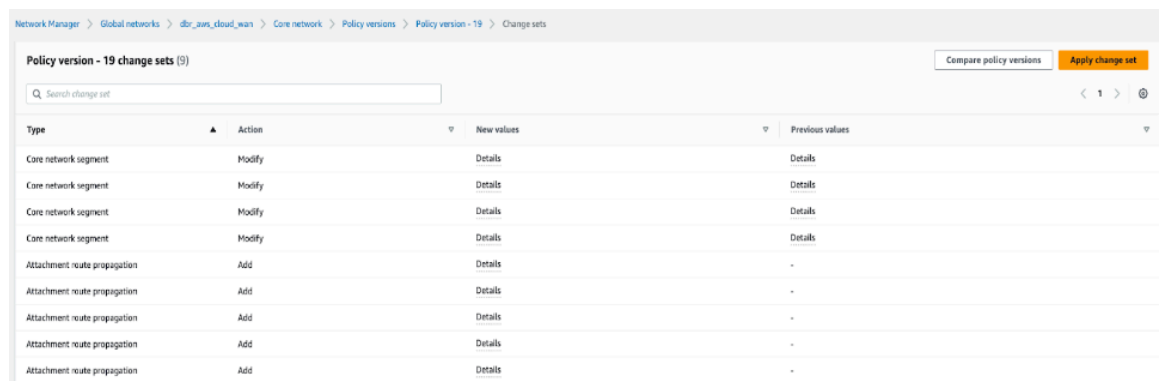
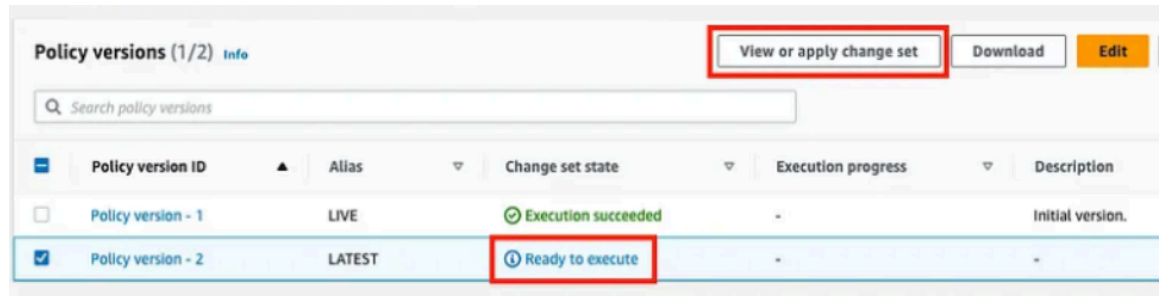
Next

- 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。



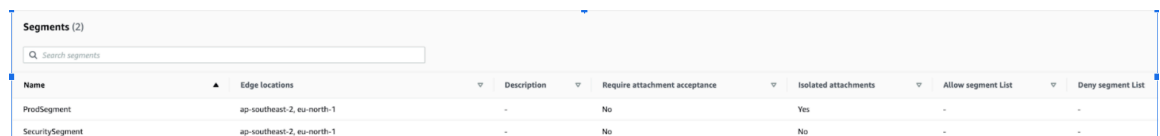
- ポリシーバージョンの変更セット状態が **[Ready to execute(実行準備完了)]**に変更されたら、**[View(表示)]**または**[Apply change set(変更セットの適用)]**をクリックしてポリシーを

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。



- 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。

Sharing (1)		
Q Search sharing		
Segment	Shared with segments	Shared except with segment
SecuritySegment	All	-

Routes (3)		
Q Search routes		
Segment	Destination CIDR block	Destination
ProdSegment	0.0.0.0/0	attachment-08534db1c1a3ed87
SecuritySegment	10.1.0.0/16	attachment-04fd636bdaf4f6e0
SecuritySegment	10.2.0.0/16	attachment-0ffa029e9effa9ba2

- ポリシーアタッチメントを作成します。

Attachment policies (2)							
Q Search attachment policies							
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。

 Services  [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.

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

**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	
<input type="text" value="Enter key"/>	<input type="text" value="Enter value"/>	<input type="button" value="Remove tag"/>
<input type="button" value="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

vpc-0a2ff52d5e27b9238 / app-vpc-sd-gwlb-9c5a Actions ▾

**Details** [Info](#)

VPC ID vpc-0a2ff52d5e27b9238	State <span>Available</span>	DNS hostnames Disabled	DNS resolution Enabled
Tenancy Default	DHCP option set dopt-04d358abcecd53fc0	Main route table rtb-0196c01c6d9f9d614 / app-main-rt-sd-gwlb-9c5a	Main network ACL acl-0a1ecd8c8448070c
Default VPC No	IPv4 CIDR 10.2.0.0/16	IPv6 pool -	IPv6 CIDR (Network border group) -
Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups -	Owner ID 018147215560	

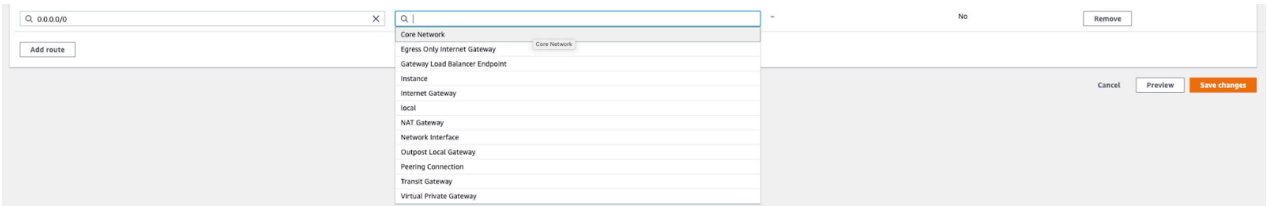
Resource map [New](#) | [CIDRs](#) | [Flow logs](#) | [Tags](#)

**Tags** Manage tags

Search 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。





VPC > Route tables > rtb-0196c01c6d9f9d614 > Edit routes

Edit routes

Destination		Target		Status	Propagated	
10.2.0.0/16		<input type="text" value="local"/>	X	Active	No	
<input type="text" value="199.167.52.5/32"/>	X	<input type="text" value="igw-0c13499196f5afb97"/>	X	Active	No	<button>Remove</button>
<input type="text" value="199.167.54.229/32"/>	X	<input type="text" value="igw-0c13499196f5afb97"/>	X	Active	No	<button>Remove</button>
<input type="text" value="8.47.64.2/32"/>	X	<input type="text" value="igw-0c13499196f5afb97"/>	X	Active	No	<button>Remove</button>
<input type="text" value="8.47.64.11/32"/>	X	<input type="text" value="igw-0c13499196f5afb97"/>	X	Active	No	<button>Remove</button>
<input type="text" value="0.0.0.0/0"/>	X	<input type="text" value="arn:aws:networkmanager-018147215560:core-network/core-network-0e323abbf86a1a758 (sydney-prod-vpc-2)"/>	X	Active	No	<button>Remove</button>
<button>Add route</button>						

Cancel

Preview

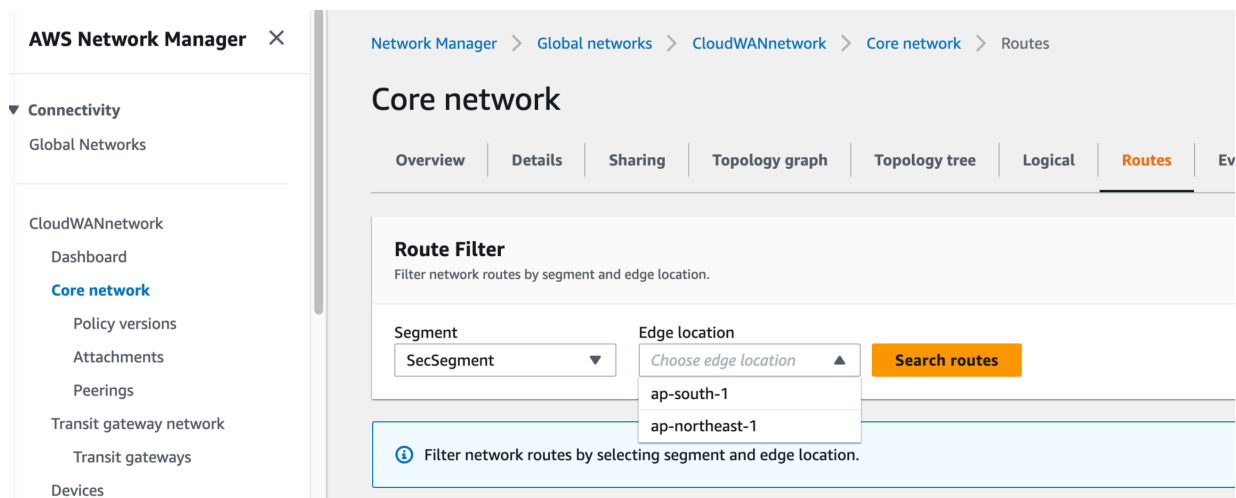
Save changes

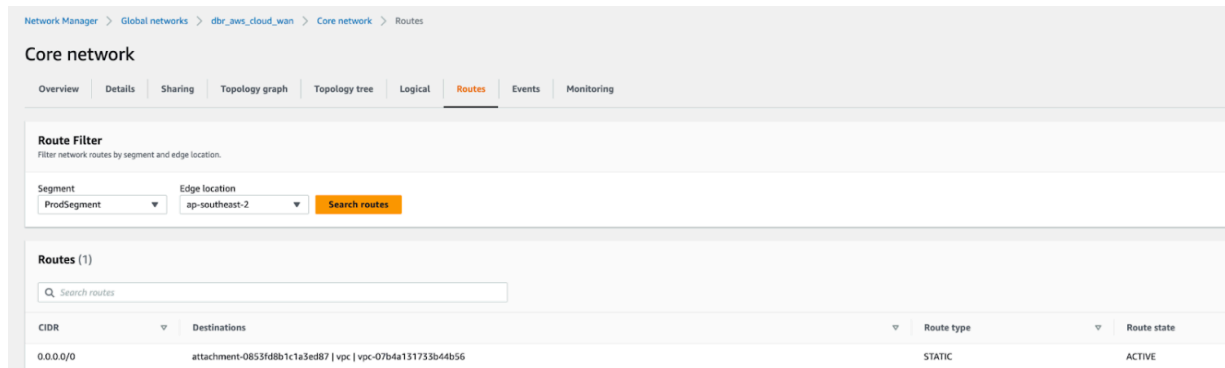
### パケット ウォークスルー

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

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트리と一致し、APP VPC 2にルーティングされます。

Network Manager > Global networks > dbx\_aws\_cloud\_wan > Core network > Routes

### Core network

Overview | Details | Sharing | Topology graph | Topology tree | Logical | **Routes** | Events | Monitoring

**Route Filter**  
Filter network routes by segment and edge location.

Segment: SecuritySegment Edge location: ap-southeast-2 [Search routes](#)

**Routes (3)**

Q Search routes

CIDR	Destinations	Route type	Route state
100.64.0.0/16	attachment-0853f68b1c1a3ed87   vpc   vpc-07b4a131733b44b56	PROPAGATED	ACTIVE
10.2.0.0/16	attachment-0ffa029e9e9fa9ba2   vpc   vpc-0a2ff52d5e27b9238	STATIC	ACTIVE
10.1.0.0/16	attachment-04fd636bdaaf4f6e0   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트리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。

