

Bereitstellungen in Cloud NGFW für AWS

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

Palo Alto Networks, Inc.
www.paloaltonetworks.com

© 2024-2024 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. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

December 5, 2024

Table of Contents

Zentralisierte Bereitstellungen in Cloud NGFW für AWS.....	5
Zentralisierter Ost-West-Datenverkehr.....	6
Zentralisierter ausgehender Datenverkehr.....	9
Zentralisierter eingehender Datenverkehr.....	12
Verteilte Bereitstellungen in Cloud NGFW für AWS.....	15
Verteilter Ost-West-Datenverkehr (innerhalb der VPC).....	16
Verteilter ausgehender Datenverkehr.....	19
Verteilter eingehender Datenverkehr.....	22
Cloud NGFW-Integration mit AWS Cloud WAN.....	25

Table of Contents

Zentralisierte Bereitstellungen in Cloud NGFW für AWS

Wo kann ich das verwenden?	Was brauche ich?
<ul style="list-style-type: none">Cloud NGFW für AWS	<ul style="list-style-type: none"><input type="checkbox"/> Cloud NGFW-Abonnement<input type="checkbox"/> Konto beim Kunden-Support-Portal (CSP) von Palo Alto Networks<input type="checkbox"/> AWS Marketplace-Konto<input type="checkbox"/> Benutzerrolle (Mandant oder Administrator)

Bei einer zentralisierten Bereitstellung werden Ihre Cloud NGFW-Komponenten in einer zentralisierten Sicherheits-VPC bereitgestellt. Der Datenverkehr muss immer durch ein AWS Transit Gateway (TGW) geleitet werden, das als Netzwerk-Hub fungiert und die Konnektivität zwischen VPCs sowie lokalen Netzwerken vereinfacht.

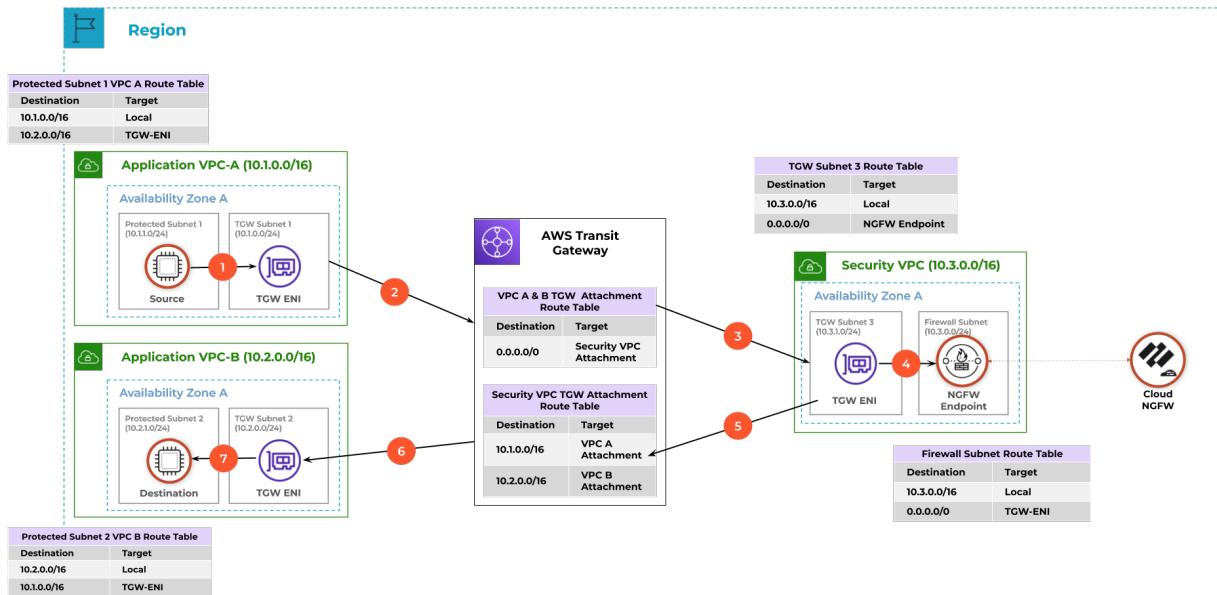
Weitere Beispiele für zentralisierte Bereitstellungen finden Sie unter [Bereitstellungsarchitekturen in Cloud NGFW für AWS](#).

Zentralisierter Ost-West-Datenverkehr

1. Datenverkehr von der Quellinstanz wird an das TGW Elastic Network Interface (ENI) gesendet.
2. Das TGW Elastic Network Interface leitet den Datenverkehr an das TGW.
3. Das TGW leitet den Datenverkehr an das TGW Elastic Network Interface der Sicherheits-VPC weiter.
4. Das TGW Elastic Network Interface sendet den Datenverkehr an den NGFW-Endpunkt und weiter zur NGFW zur Prüfung.
5. Wenn der Datenverkehr zulässig ist, sendet die NGFW ihn an den NGFW-Endpunkt zurück. Der Datenverkehr wird dann über den TGW-Endpunkt der Sicherheits-VPC an das TGW zurückgesendet.
6. Der TGW leitet den Datenverkehr an das TGW Elastic Network Interface im Ziel-VPC weiter.

7. Dann sendet das TGW Elastic Network Interface den Datenverkehr an das Ziel.

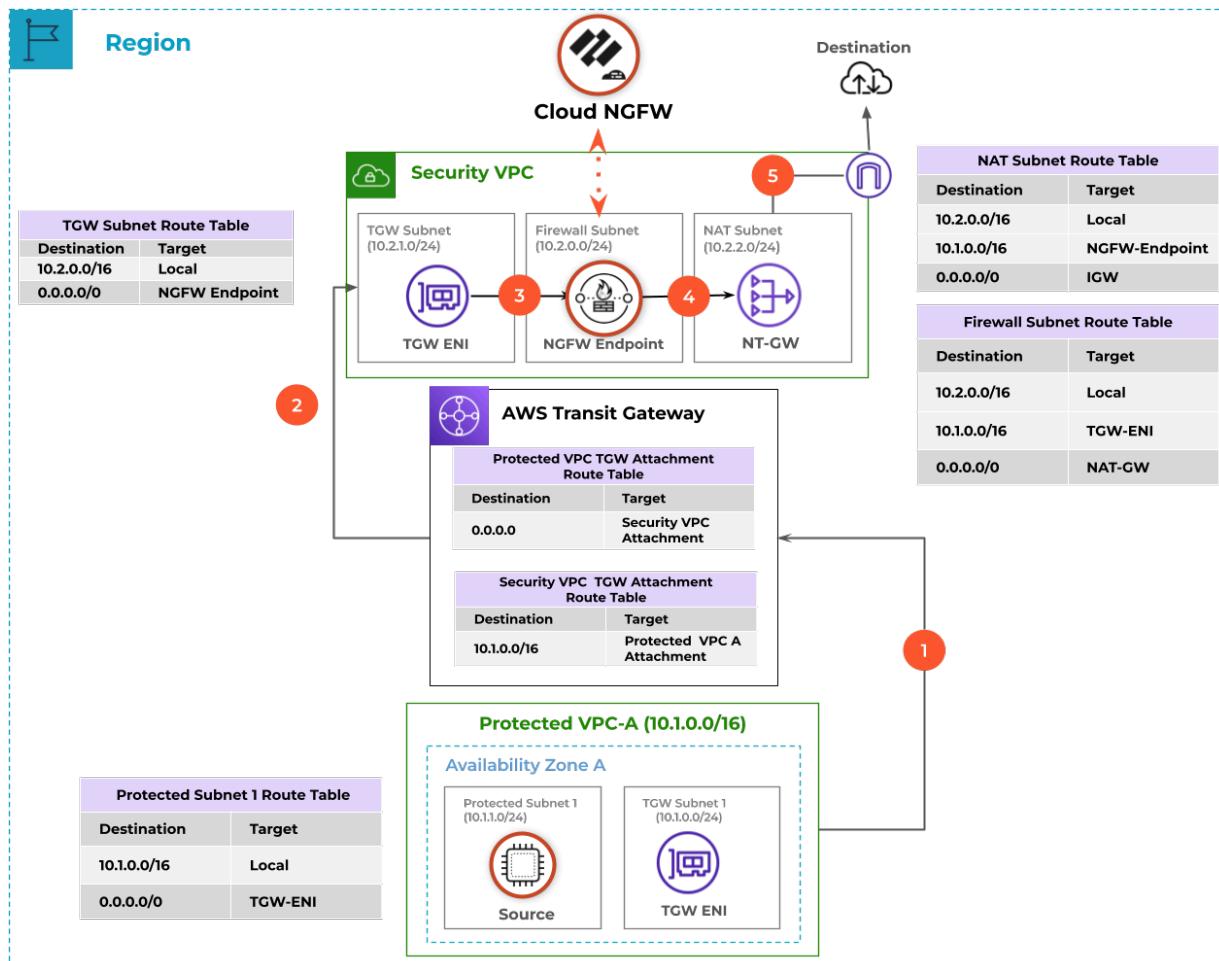
Zentralisierte Bereitstellungen in Cloud NGFW für AWS



Zentralisierter ausgehender Datenverkehr

1. Datenverkehr von der Quellinstanz wird an das TGW Elastic Network Interface und weiter an das TGW gesendet.
2. Das TGW leitet den Datenverkehr an das TGW Elastic Network Interface der Sicherheits-VPC weiter.
3. Das TGW Elastic Network Interface sendet den Datenverkehr an den NGFW-Endpunkt und weiter an die NGFW zur Prüfung.
4. Wenn der Datenverkehr zulässig ist, leitet der NGFW-Endpunkt ihn an das NAT-Gateway weiter.

5. Das NAT-Gateway leitet den Datenverkehr an das IGW und dann weiter an das Ziel.

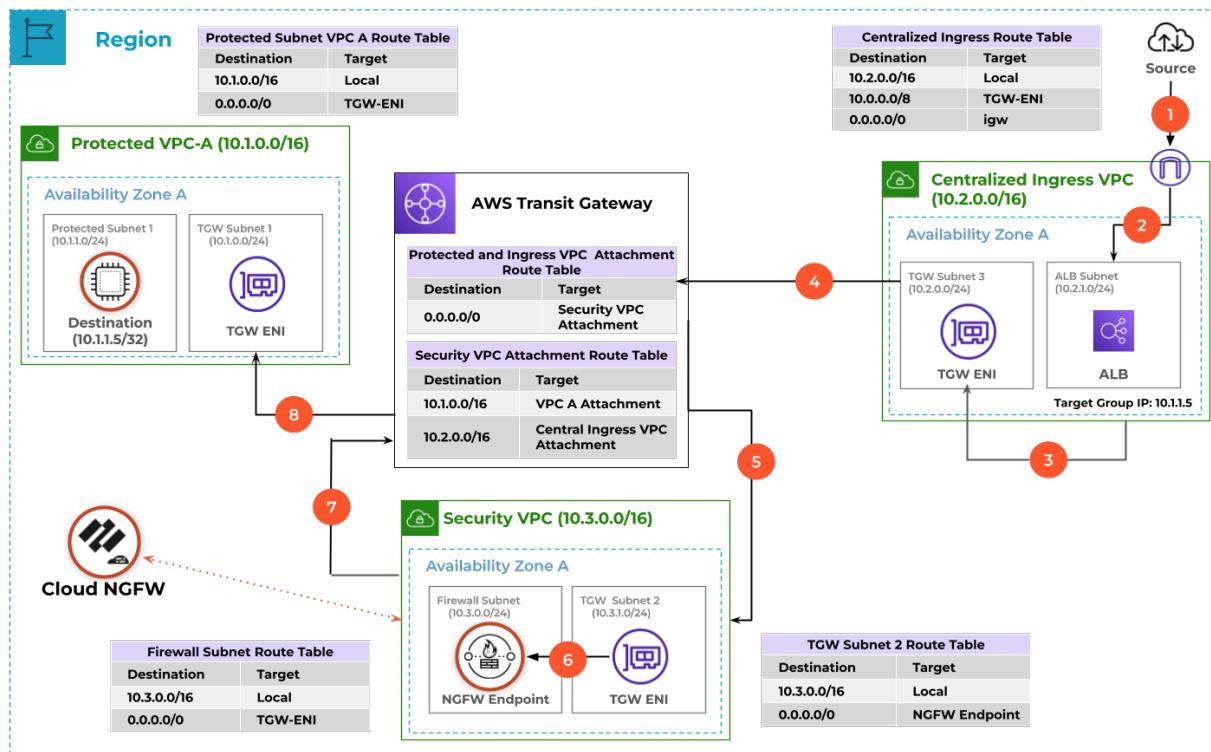


Zentralisierter eingehender Datenverkehr

1. Datenverkehr aus dem Internet kommt am Internetgateway an.
2. Das Internetgateway leitet den Datenverkehr an den Application Load Balancer (ALB) weiter.
3. Der ALB sendet dann den Datenverkehr an das TGW Elastic Network Interface der Eingangs-VPC.
4. Das TGW Elastic Network Interface sendet den Datenverkehr an das TGW.
5. Das TGW leitet den Datenverkehr an das TGW Elastic Network Interface der Sicherheits-VPC weiter.
6. Das TGW Elastic Network Interface sendet den Datenverkehr an den NGFW-Endpunkt und weiter zur NGFW zur Prüfung.
7. Wenn der Datenverkehr zulässig ist, sendet der NGFW-Endpunkt ihn an das TGW.

8. Das TGW leitet den Datenverkehr dann an das TGW Elastic Network Interface der geschützten VPC und anschließend an das Ziel weiter.

Zentralisierte Bereitstellungen in Cloud NGFW für AWS



Verteilte Bereitstellungen in Cloud NGFW für AWS

Wo kann ich das verwenden?	Was brauche ich?
<ul style="list-style-type: none">Cloud NGFW für AWS	<ul style="list-style-type: none"><input type="checkbox"/> Cloud NGFW-Abonnement<input type="checkbox"/> Konto beim Kunden-Support-Portal (CSP) von Palo Alto Networks<input type="checkbox"/> AWS Marketplace-Konto<input type="checkbox"/> Benutzerrolle (Mandant oder Administrator)

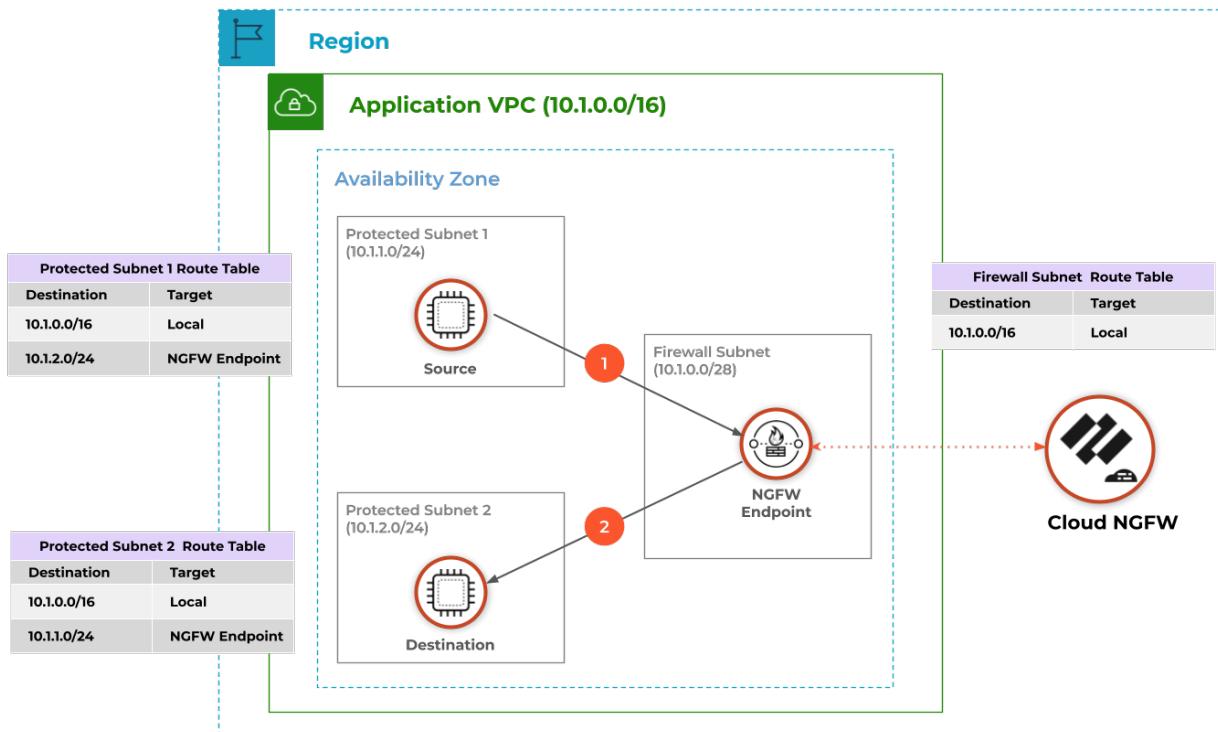
In einer verteilten Bereitstellung verfügt jede VPC, die geschützt werden muss, über eine eigene NGFW. Diese Bereitstellungsmethode ist weniger kompliziert und eine Fehlkonfiguration ist daher weniger wahrscheinlich.

Weitere Beispiele für verteilte Bereitstellungen finden Sie unter [Bereitstellungsarchitekturen in Cloud NGFW für AWS](#).

Verteilter Ost-West-Datenverkehr (innerhalb der VPC)

1. Datenverkehr von der Quellinstanz wird zur Prüfung an den NGFW-Endpunkt und weiter an die NGFW geleitet.

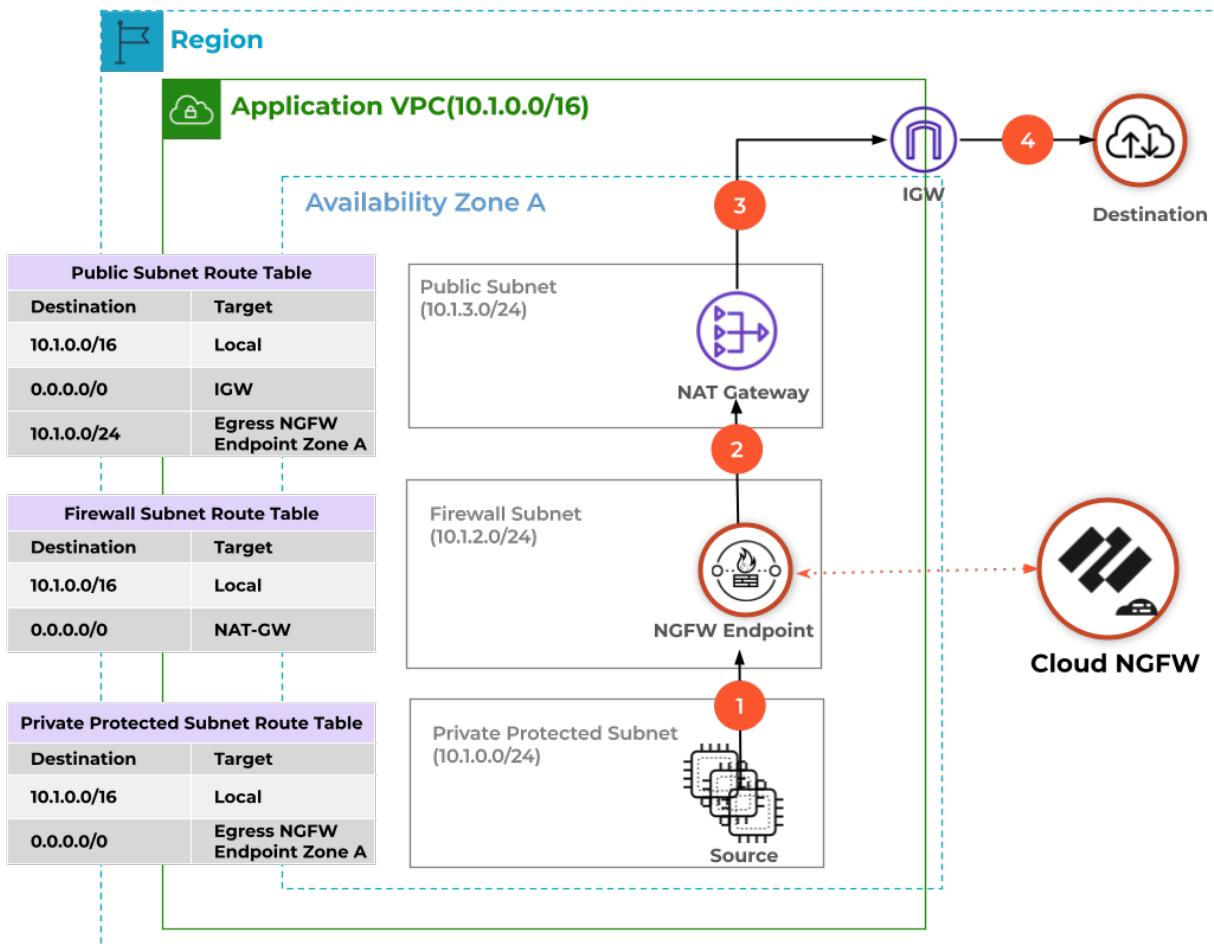
2. Wenn der Datenverkehr zulässig ist, sendet der NGFW-Endpunkt ihn an das Ziel.



Verteilter ausgehender Datenverkehr

1. Datenverkehr von der Quellinstanz wird zur Prüfung an den NGFW-Endpunkt und weiter an die NGFW geleitet.
2. Wenn der Datenverkehr zulässig ist, sendet der NGFW-Endpunkt den geprüften Datenverkehr an das NAT-Gateway.
3. Das NAT-Gateway sendet den Datenverkehr an das Internetgateway.

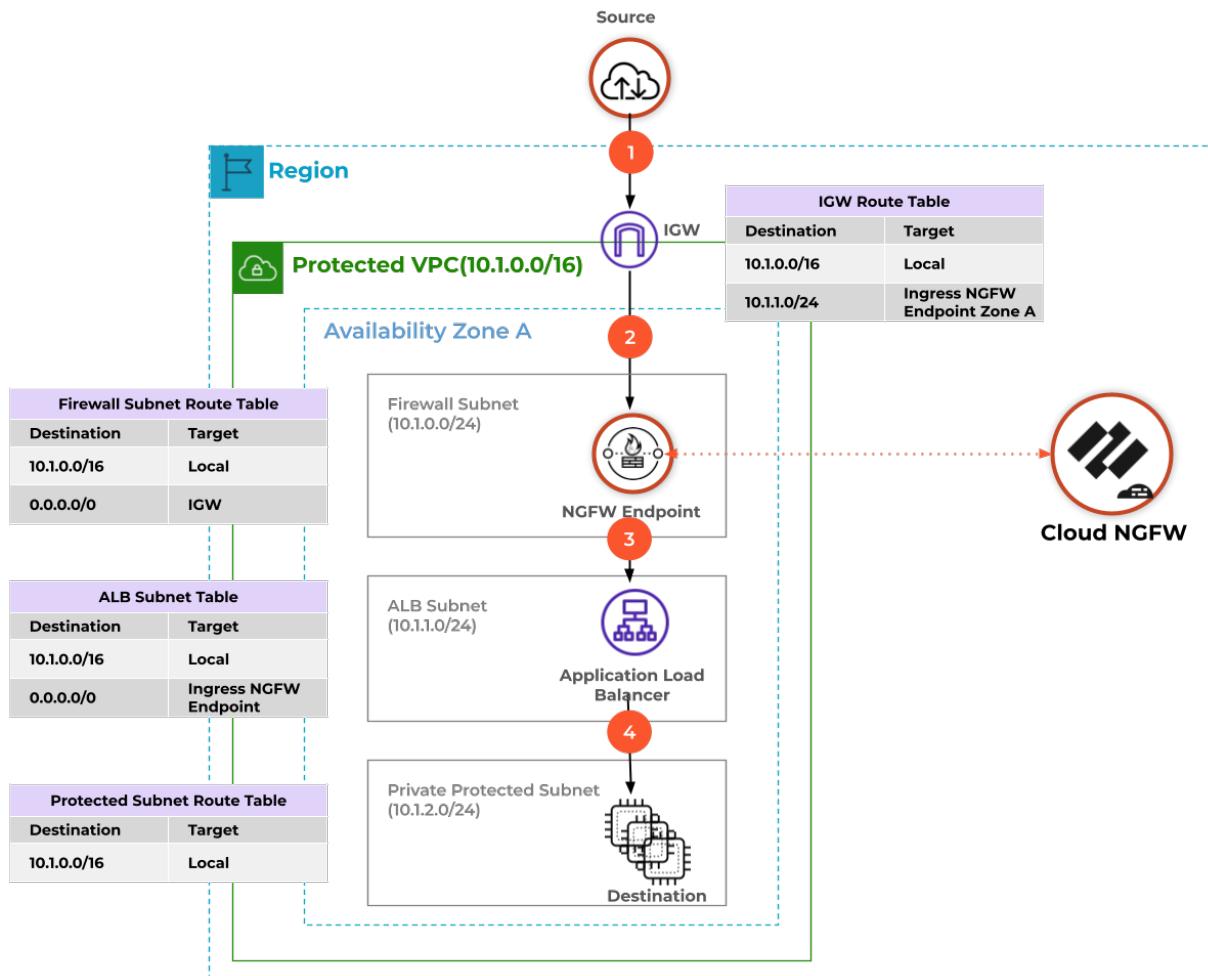
4. Der Datenverkehr wird ins Internet und an das Ziel weitergeleitet.



Verteilter eingehender Datenverkehr

1. Der Datenverkehr von der Quelle kommt am Internetgateway an.
2. Das Internetgateway leitet den Datenverkehr an den NGFW-Endpunkt und dann zur Prüfung an die NGFW weiter.
3. Wenn der Datenverkehr zulässig ist, leitet der NGFW-Endpunkt ihn an den Application Load Balancer weiter.

4. Der Application Load Balancer leitet den Datenverkehr an das Ziel weiter.



Cloud NGFW-Integration mit AWS Cloud WAN

Wo kann ich das verwenden?	Was brauche ich?
<ul style="list-style-type: none"> Cloud NGFW für AWS 	<ul style="list-style-type: none"> Cloud NGFW-Abonnement Konto beim Kunden-Support-Portal (CSP) von Palo Alto Networks AWS Marketplace-Konto Benutzerrolle (Mandant oder Administrator)

AWS Cloud WAN ist ein verwalteter Wide-Area-Networking(WAN)-Dienst, mit dem Sie ein einheitliches Netzwerk aufbauen können, das Cloud- und lokale Umgebungen miteinander verbindet. Er bietet ein zentrales Dashboard zum Verbinden von lokalen Standorten, Zweigstellen, Rechenzentren und Amazon Virtual Private Clouds (VPCs) über das globale AWS-Netzwerk und selbst andere Cloud-Anbieter.

Cloud WAN unterstützt die Konnektivität innerhalb von AWS durch den AWS Network Manager, eine Schnittstelle, die Ihr globales Netzwerk zentral verwaltet. Ein globales Netzwerk ist ein einzelnes privates Netzwerk, das als Container auf Stammebene für Ihre Netzwerkobjekte fungiert und sowohl Transit-Gateways als auch ein Kernnetzwerk enthalten kann. Das Kernnetzwerk besteht aus Netzwerkrichtlinien, Anhängen wie VPCs und Transit-Gateway-Routentabellen.

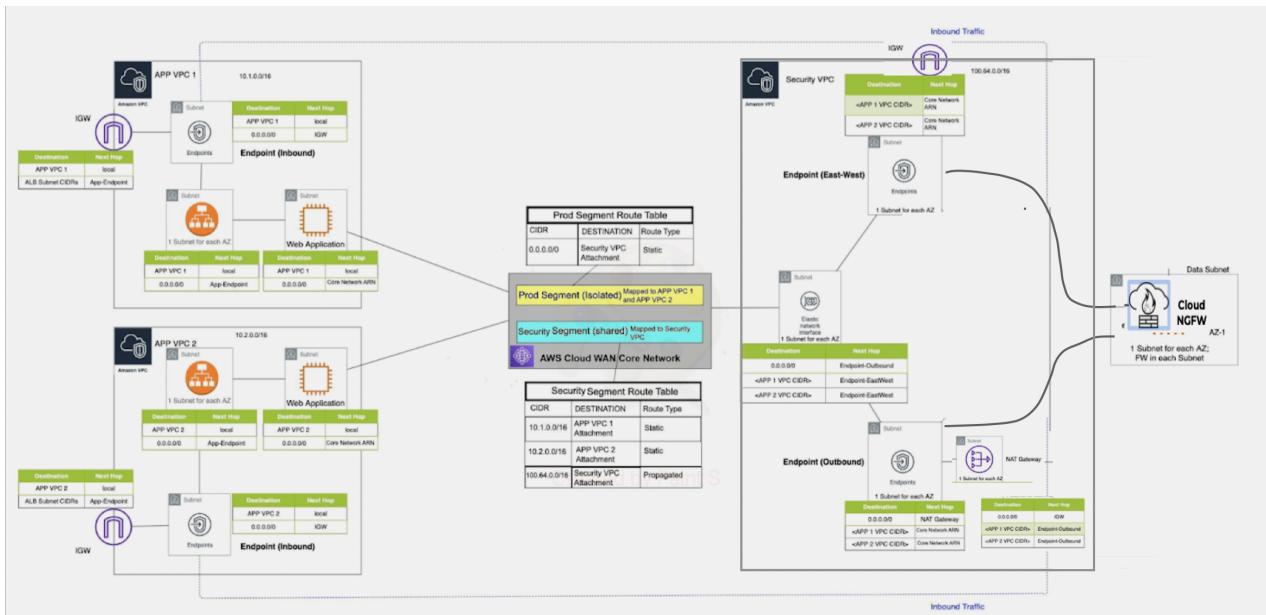
Sie können diese VPCs Segmenten im Kernnetzwerk zuordnen. Diese Segmente werden durch Anhänge wie VPC-Anhänge oder Transit-Gateway-Routentabellen-Anhänge verbunden. Die [integrierte Segmentierung](#) hilft Ihnen, die Netzwerkssegmente über AWS- und lokale Umgebungen hinweg aufrechtzuerhalten. Jedes Segment erstellt eine dedizierte Routingdomäne. Sie können innerhalb Ihres globalen Netzwerks mehrere Netzwerksegmente erstellen. Cloud WAN schränkt die Kommunikation der AWS-Ressourcen innerhalb des Segments ein. Kurz gesagt ermöglicht Ihnen Cloud WAN die Weiterleitung des Datenverkehrs zwischen:

- VPCs im selben Segment und in derselben Region (isierte Anhänge).
- VPCs in verschiedenen Segmenten derselben Region.
- VPCs im selben Segment über verschiedene Regionen hinweg (isierte Anhänge).
- VPCs in verschiedenen Segmenten und in verschiedenen Regionen.

Überlegungen vor der Bereitstellung von AWS Cloud WAN:

- Peering zwischen Transit-Gateways und Cloud WAN wird in derselben Region und nicht regionsübergreifend unterstützt.
- Stellen Sie sicher, dass Sie für Anwendungsfälle, die AWS-Site-to-Site-VPN-Verbindungen über Direct Connect mithilfe von [privaten IP-Adressen](#) erfordern, Cloud WAN mit einem Transit-Gateway verbinden.

- Achten Sie beim Bereitstellen von Cloud WAN zusammen mit Transit-Gateways darauf, dass sich die ASN des Transit-Gateways von der ASN unterscheidet, die für die Kernnetzwerk-Edges von Cloud WAN verwendet wird.
- Achten Sie beim Erstellen des Kernnetzwerks darauf, dass Sie im Abschnitt mit den Edge-Standorten unter den Richtlinieneinstellungen des Kernnetzwerks alle Regionen hinzufügen, für die Ihre VPCs konfiguriert sind. Sie müssen außerdem Segmente erstellen und unter dem Segmentnamen den Segmenttyp – „dev“ (Entwicklung), „prod“ (Produktion), „management“ (Verwaltung) oder „security“ (Sicherheit) – hinzufügen, zu dem diese Regionen gehören.



AWS Cloud WAN kann mit zwei Methoden bereitgestellt werden:

- **Verbund aus Transit-Gateways und Cloud WAN erstellen** – Bei dieser Methode ersetzen Sie statisch erstellte Transit-Gateway-Peering-Verbindungen durch Cloud WAN. Während Sie einen Verbund von Transit-Gateways und Cloud WAN erstellen, müssen Sie die Transit-Gateways mithilfe des AWS Network Managers registrieren, ein Peering zwischen den Transit-Gateways erstellen, Anhänge für die Transit-Gateways erstellen und dann die Cloud WAN-Konfiguration anwenden.

- **Nur Cloud WAN** – Bei dieser Methode wird Cloud WAN für die gesamte Konnektivität verwendet und Transit-Gateways werden entfernt.

AWS Cloud WAN bereitstellen

Cloud WAN ist die Verbindung zwischen VPCs und lokalen Netzwerken. Im Folgenden soll näher darauf eingegangen werden, wie Sie mithilfe der Cloud NGFWs von Palo Alto Networks den mit Cloud WAN verbundenen Datenverkehr absichern können. Obwohl Cloud WAN ein globales Konstrukt ist, empfiehlt Palo Alto Networks die Bereitstellung von Cloud NGFW in jeder AWS-Region, die es umfasst, um einen Sicherheitsstatus mit geringer Latenz und optimierten Kosten aufrechtzuerhalten.

Cloud NGFW kann in einer zentralisierten Sicherheits-VPC in jeder Region bereitgestellt werden. Die Sicherheits-VPC kann per Anhang direkt mit dem Cloud-WAN-Sicherheitssegment verbunden werden. Das den Anhängen und Segmenten zugeordnete Routing definiert, wie der Datenverkehr zur Bedrohungsabwehr an die Cloud NGFW-Ressource weitergeleitet wird. Sie können den von Cloud-Anhängen eingehenden Datenverkehr vor der Weiterleitung an das Ziel zur Sicherheits-VPC umleiten. Wenn Cloud NGFW innerhalb einer Region bereitgestellt wird, kann Folgendes geschützt und gesichert werden:

- East-West-Datenverkehr mit interregionalen und intraregionalen Datenverkehrsflüssen
- Ausgehender Datenverkehr kann überprüft und gesichert werden
- Datenverkehr aus der lokalen und Zweigstellenumgebung kann überprüft und geschützt werden

Betrachten wir einen Anwendungsfall, bei dem sich VPCs in derselben Region befinden (isolierte Anhänge). Um diese Einrichtung zu konfigurieren, [stellen Sie die Cloud NGFW-Firewall innerhalb der Sicherheits-VPC bereit](#). Sie können die Cloud NGFW-Firewall in einer Sicherheits-VPC bereitstellen, die direkt mit einem Cloud-WAN oder über ein Transit-Gateway mit einem Cloud-WAN-Anhang verbunden ist.



Um eine vollständige Migration vom Transit-Gateway durchzuführen, müssen Sie Ihre VPCs direkt mit dem Cloud-WAN verbinden.

Der ausgehende Datenverkehr von der Produktions-VPC wird an das Cloud-WAN weitergeleitet, von dort aus wird er zur Überprüfung an die Sicherheits-VPC weitergeleitet und über das NAT-Gateway und das interne Gateway gesendet. In der umgekehrten Richtung erreicht der Datenverkehr von der Sicherheits-VPC das Sicherheitssegment und wird dann basierend auf der Routing-Konfiguration an den VPC-Anhang gesendet.

Um den Datenverkehr zwischen VPCs im selben Segment und in derselben Region mit einer Bereitstellung von **AWS Cloud WAN (ausschließlich)** zu prüfen, führen Sie die folgenden Aufgaben aus:

1. Melden Sie sich beim AWS Network Manager an und erstellen Sie ein globales Netzwerk.

Cloud NGFW-Integration mit AWS Cloud WAN

The screenshot shows the AWS Network Manager interface. The left sidebar lists various services under 'AWS Network Manager'. The main content area is titled 'Network Manager' and 'Manage and monitor your AWS network'. It features several cards:

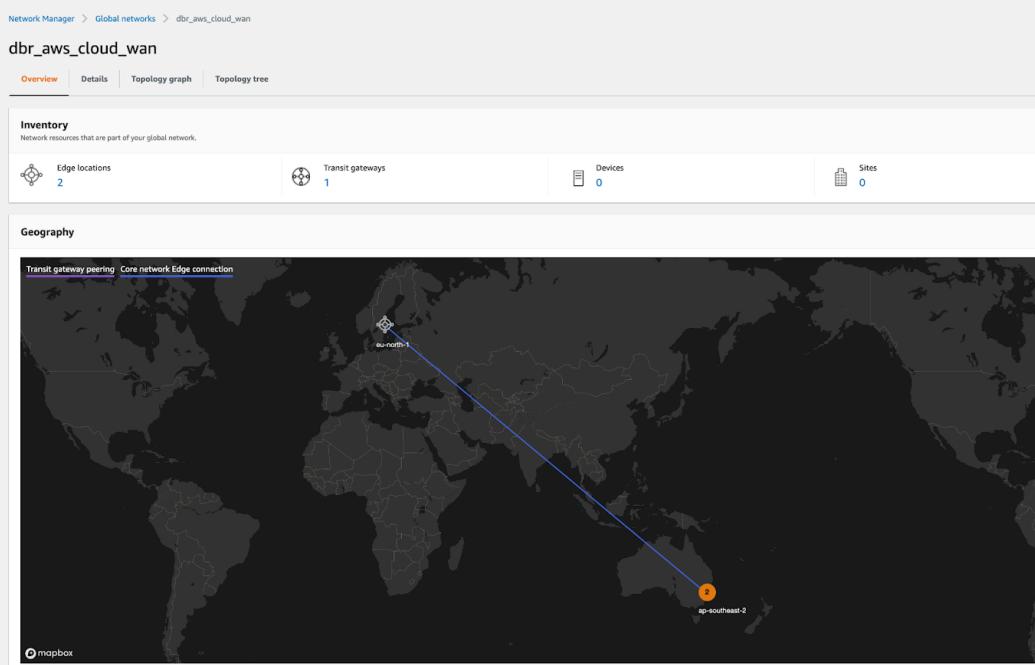
- Cloud WAN**: Describes AWS Cloud WAN as a managed wide area networking (WAN) service. A red box highlights the 'Create global network' button.
- Transit Gateway Network Manager**: Describes AWS Transit Gateway Network Manager. A red box highlights the 'Create global network' button.
- Reachability Analyzer**: Describes Amazon VPC Reachability Analyzer. A red box highlights the 'Create and analyze path' button.
- Infrastructure Performance**: Describes Infrastructure Performance, which provides aggregate network latency between AWS Regions and Availability Zones. A red box highlights the 'View metrics' button.
- VPC IP Address Manager**: Describes Amazon VPC IP Address Manager (IPAM). A red box highlights the 'Create IPAM' and 'Settings' buttons.
- Network Access Analyzer**: Describes Amazon VPC Network Access Analyzer. A red box highlights the 'Create network access scope' button.

Cloud NGFW-Integration mit AWS Cloud WAN

Screenshot of the AWS Network Manager interface showing the Cloud WAN setup.

The left sidebar shows the navigation menu:

- 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



2. Erstellen Sie ein Kernnetzwerk und eine Kernnetzwerkrichtlinie.

Verwenden Sie die AWS Cloud WAN-Konsole, um eine Kernnetzwerkrichtlinienversion zu erstellen, indem Sie die folgenden Schritte ausführen:

- Konfigurieren Sie die Netzwerkeinstellungen.

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

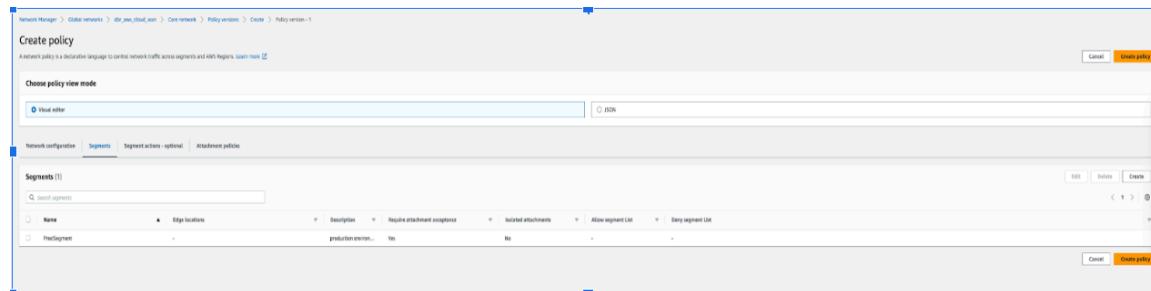
Segment name
This is your default segment enabled in all selected edge locations.

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](#)

- Klicken Sie zum Bearbeiten einer Richtlinienversion auf **Policy versions** (**Richtlinienversionen**), wählen Sie die gewünschte Richtlinie aus und klicken Sie auf **Edit** (**Bearbeiten**). Nehmen Sie die erforderlichen Änderungen vor und klicken Sie auf **Create Policy** (**Richtlinie erstellen**).



- Nachdem sich der Änderungssatzstatus der Richtlinienversion in **Bereit zur Ausführung** geändert hat, führen Sie die Richtlinie aus, indem Sie auf **Änderungssatz anzeigen** oder

anwenden klicken. Klicken Sie alternativ auf **Richtlinienversion vergleichen**, um das JSON-Dokument anzuzeigen.

Policy versions (1/2) Info					
View policy versions				View or apply change set	
				Download	
				Edit	
Policy version ID		Alias	Change set state	Execution progress	Description
Policy version - 1		LIVE	Execution succeeded	-	Initial version.
<input checked="" type="checkbox"/> Policy version - 2		LATEST	Ready to execute	-	-

Policy version - 19 change sets (9)					
Compare policy versions Apply change set					
Type	Action	New values	Previous values		
Core network segment	Modify	Details	Details		
Core network segment	Modify	Details	Details		
Core network segment	Modify	Details	Details		
Core network segment	Modify	Details	Details		
Attachment route propagation	Add	Details	-		
Attachment route propagation	Add	Details	-		
Attachment route propagation	Add	Details	-		
Attachment route propagation	Add	Details	-		
Attachment route propagation	Add	Details	-		

- Erstellen Sie Netzwerkrichtliniensegmente innerhalb Ihres Kernnetzwerks.

Achten Sie beim Konfigurieren der Richtlinienversionen darauf, dass Sie die Anwendungen hinzufügen: APP VPC 1 (10.1.0.0/16) und APP VPC 2 (10.2.0.0/16) im Produktionssegment und in der Firewall sowie die Sicherheits-VPC (100.64.0.0/16) im Sicherheitssegment.

Segments (2)								
Search segments								
Name	Edge locations	Description	Require attachment acceptance	Isolated attachments	Allow segment List	Deny segment List		
ProdSegment	ap-southeast-2, eu-north-1	-	No	Yes	-	-		
SecuritySegment	ap-southeast-2, eu-north-1	-	No	No	-	-		

- Erstellen Sie Segmentfreigabe- und Segmentroutenaktionen.

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

Routes (3)		Destination
Segment	Destination CIDR block	
ProdSegment	0.0.0.0/0	attachment-0853fd8b1c1a3ed87
SecuritySegment	10.1.0.0/16	attachment-04fd636bdaaf4f6e0
SecuritySegment	10.2.0.0/16	attachment-0ffa029d9effa9ba2

- Erstellen Sie Richtlinienanhänge.

Attachment policies (2)		Description	Segment to attach	Require acceptance	Conditions	Operator	Condition values	Condition logic
Rule number	▲							
110	-		Segment name - ProdSegment	-	tag-value	equals	key=segment, value=ProdSegment	or
111	-		Segment name - SecuritySegment	-	tag-value	equals	key=segment, value=SecuritySegment	or



Sie können wahlweise dem Segment (Schlüssel) Tags wie „prod segment“ (Wert) hinzufügen. Diese Tags werden erst angezeigt, nachdem Sie die Segmente im Cloud-WAN hinzugefügt haben.

3. Erstellen Sie einen Anhang.



- *Verwenden Sie beim Erstellen eines Anhangs die VPC- oder Transit-Gateway-Routentabelle als Anhangstyp.*
- *Um sicherzustellen, dass die Cloud NGFW-Firewall den zwischen VPC-Anhängen weitergeleiteten Datenverkehr prüfen kann, müssen Sie den Appliance-Modus im VPC-Anhang für die Sicherheits-VPC aktivieren, die die Cloud NGFW-Firewall enthält.*

The screenshot shows the AWS Cloud WAN interface for creating a core network attachment. The top navigation bar includes the AWS logo, Services, a search bar, and a [Option+S] button. The breadcrumb trail indicates the path: 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. Aktualisieren Sie VPC-Routentabellen.

Nachdem die erforderlichen Cloud WAN-Konstrukte nun vorhanden sind, müssen die VPCs angepasst werden, um die Paketweiterleitung zum Kernnetzwerk zu erleichtern. Die Anwendungs- und Firewall-Instanzen oder die jeweiligen VPCs müssen mit ähnlichen Tags wie das Segment gekennzeichnet werden. Fügen Sie dem Anhang spezifische Tags hinzu, damit er mit dem Anhang übereinstimmt, der während Schritt 2, [Erstellen Sie Richtlinienanhänge](#), erstellt wurde.

VPC ID: vpc-0a2ff52d5e27b9238

State: Available

DHCP option set: dopt-04d358abcecd53fc0

IPv4 CIDR: 10.2.0.0/16

Route 53 Resolver DNS Firewall rule groups: -

DNS hostnames: Disabled

Main route table: rtb-0196c01c6d9f9d614 / app-main-rt-sd-gwlb-9c5a

IPv6 pool: -

Owner ID: 018147215560

DNS resolution: Enabled

Main network ACL: acl-0a1ecdf8c8448070c

IPv6 CIDR (Network border group): -

Tags:

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

Um die Kommunikation zwischen angeschlossenen VPCs und dem Kernnetzwerk zu ermöglichen, müssen die VPC-Routentabellen von der vorhandenen Ziel-Transit-Gateway-Route auf den entsprechenden Kernnetzwerk-ARN aktualisiert werden, wie unten veranschaulicht.

Cloud NGFW-Integration mit AWS Cloud WAN



Cloud NGFW-Integration mit AWS Cloud WAN

The screenshot shows the AWS VPC Route Tables interface. The top navigation bar includes links for VPC, Route tables, rtb-0196c01c6d9f9d614, and Edit routes. The main title is "Edit routes". Below the title is a table with columns: Destination, Target, Status, and Propagated. There are six rows in the table, each representing a route entry. The first row has a destination of 10.2.0.0/16 and a target of "local", marked as Active and No propagated. The second row has a destination of 199.167.52.5/32 and a target of igw-0c13499196f5afb97, marked as Active and No propagated, with a "Remove" button. The third row has a destination of 199.167.54.229/32 and a target of igw-0c13499196f5afb97, marked as Active and No propagated, with a "Remove" button. The fourth row has a destination of 8.47.64.2/32 and a target of igw-0c13499196f5afb97, marked as Active and No propagated, with a "Remove" button. The fifth row has a destination of 8.47.64.11/32 and a target of igw-0c13499196f5afb97, marked as Active and No propagated, with a "Remove" button. The sixth row has a destination of 0.0.0.0/0 and a target of "arn:aws:networkmanager::018147215560:core-network/core-network-0e323abb861a758 (sydney-prod-vpc-2)", marked as Active and No propagated, with a "Remove" button. At the bottom left is an "Add route" button. At the bottom right are "Cancel", "Preview", and "Save changes" buttons.

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

Weg eines Pakets

Im Folgenden ist der Weg eines Pakets beschrieben, wenn eine EC2-Instanz in APP VPC 1 mit einer EC2-Instanz in APP VPC 2 kommuniziert:

- Wenn ein Client in APP VPC 1 (10.1.0.0/16) eine Verbindung zu einem Server in APP VPC 2 (10.2.0.0/16) beginnt, führt er eine Suche in der VPC-Routentabelle (App-Subnetz) durch. Das Paket stimmt mit dem Standardrouteneintrag überein, wobei der ARN des Kernnetzwerks als Ziel angegeben ist, und wird an das Kernnetzwerk weitergeleitet.
- Wenn das Paket im Kernnetzwerk ankommt, führt es eine Suche in der Routentabelle des Produktionssegments durch, da APP VPC 1 dem Produktionssegment zugeordnet ist. Das Paket stimmt

Cloud NGFW-Integration mit AWS Cloud WAN

mit dem Standardeintrag überein, wobei der Sicherheitsanhang als Ziel angegeben ist, und wird an die Sicherheits-VPC weitergeleitet.

The screenshot shows the AWS Network Manager interface. The left sidebar has a 'Connectivity' section with 'Global Networks' and a 'CloudWANnetwork' section containing 'Dashboard', 'Core network' (which is selected), 'Policy versions', 'Attachments', 'Peerings', 'Transit gateway network', 'Transit gateways', and 'Devices'. The main area is titled 'Core network' and shows a 'Route Filter' with tabs for 'Overview', 'Details', 'Sharing', 'Topology graph', 'Topology tree', 'Logical', and 'Routes' (which is selected). A dropdown menu for 'Segment' is open, showing 'SecSegment'. A dropdown menu for 'Edge location' is open, showing 'Choose edge location' at the top, followed by 'ap-south-1' and 'ap-northeast-1'. An orange button labeled 'Search routes' is visible. A tooltip at the bottom says: 'Filter network routes by selecting segment and edge location.'

The screenshot shows the Network Manager interface with the following navigation path: Network Manager > Global networks > dbr_aws_cloud_wan > Core network > Routes.

The main title is "Core network". Below it, there are tabs: Overview, Details, Sharing, Topology graph, Topology tree, Logical, **Routes**, Events, and Monitoring. The "Routes" tab is highlighted.

A "Route Filter" section allows filtering by Segment (ProdSegment) and Edge location (ap-southeast-2), with a "Search routes" button.

The results table shows one route entry:

Routes (1)			Route type	Route state
CIDR	Destinations			
0.0.0.0/0	attachment-0853fd8b1c1a3ed87 vpc vpc-07b4a13173b44b56		STATIC	ACTIVE

- Wenn das Paket beim Sicherheits-VPC-Anhang (100.64.0.0/16) ankommt, führt es eine Suche in der VPC-Routentabelle (CWAN-Subnetz) durch. Das Paket stimmt mit der Standardroute überein, wobei Firewall-Endpunkt 1 als Ziel angegeben ist, und wird – zunächst über den Endpunkt der Firewall zur Überprüfung – an eine Firewall weitergeleitet.
- Die Firewall prüft den Datenverkehr, vergleicht ihn mit ihrer Sicherheitsrichtlinie und lässt ihn durch. Die Firewall leitet das Paket zurück an den Endpunkt der Firewall, wo es eine Suche in der VPC-Routentabelle (Firewall-Subnetz) durchführt. Das Paket stimmt mit dem Standardrouteneintrag überein, wobei der ARN des Kernnetzwerks als Ziel angegeben ist, und wird an das Kernnetzwerk weitergeleitet.
- Wenn das Paket im Kernnetzwerk ankommt, führt es eine Suche in der gemeinsamen Sicherheitsroutentabelle durch, da die Sicherheits-VPC dem Sicherheitssegment zugeordnet ist. Das

Cloud NGFW-Integration mit AWS Cloud WAN

Paket stimmt mit dem APP VPC 2 CIDR(10.2.0.0/16)-Eintrag überein, wobei der APP VPC 2-Anhang als Ziel angegeben ist, und wird an APP VPC 2 weitergeleitet.

The screenshot shows the AWS Network Manager interface under the 'Core network' section, specifically the 'Routes' tab. A 'Route Filter' is applied to 'Segment: SecuritySegment' and 'Edge location: ap-southeast-2'. The results show three routes:

CIDR	Destinations	Route type	Route state
100.64.0.0/16	attachment-0853fd8b1c1a3ed87 vpc vpc-07b4a131733b44b56	PROBABLY	ACTIVE
10.2.0.0/16	attachment-0ffa029e9effa9ba2 vpc vpc-0a2ff52d5e27b9238	STATIC	ACTIVE
10.1.0.0/16	attachment-04fd636bdaaf4f6e0 vpc vpc-0b7b7f9780c3b0b8	STATIC	ACTIVE

- Wenn das Paket bei APP VPC 2 ankommt, führt es eine Suche in der VPC-Routentabelle (CWAN-Subnetz) durch. Das Paket stimmt mit dem VPC CIDR-Eintrag überein, wobei „local“ (lokal) als Ziel angegeben ist, und wird an die Instanz weitergeleitet.

Der zurückgegebene Datenverkehr folgt demselben Weg in die entgegengesetzte Richtung.

