paloalto TECHDOCS

Bereitstellungen in Cloud NGFW für AWS

docs.paloaltonetworks.com

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

December 5, 2024

Table of Contents

Zentralisierte Bereitstellungen in Cloud NGFW für AWS

Wo kann ich das verwenden?	Was brauche ich?
• Cloud NGFW für AWS	❑ Cloud NGFW-Abonnement ❑ Konto beim Kunden-Support-Portal (CSP) von Palo Alto Networks ❑ AWS Marketplace-Konto ❑ Benutzerrolle (Mandant oder Administrator)

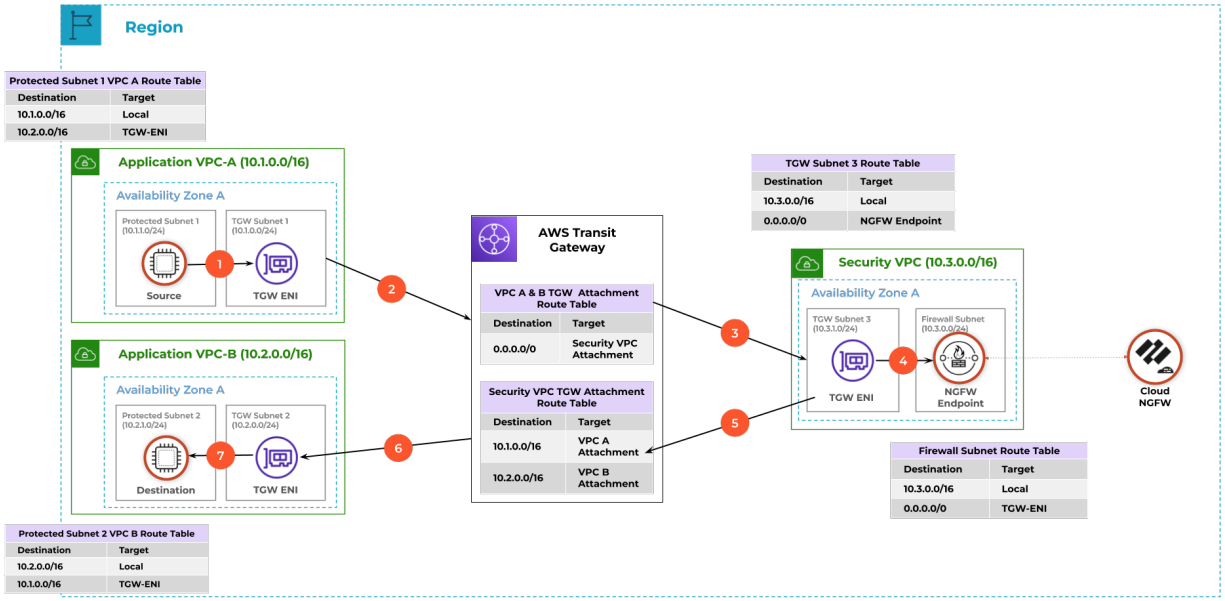
Bei einer zentralisierten Bereitstellung werden Ihre Cloud NGFW-Komponenten in einer zentralisierten Sicherheits-VPC bereitgestellt. Der Datenverkehr muss immer durch ein AWS Transit Gateway (TGW) geleitet werden, das als Netzwerk-Hub fungiert und die Konnektivität zwischen VPCs sowie lokalen Netzwerken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

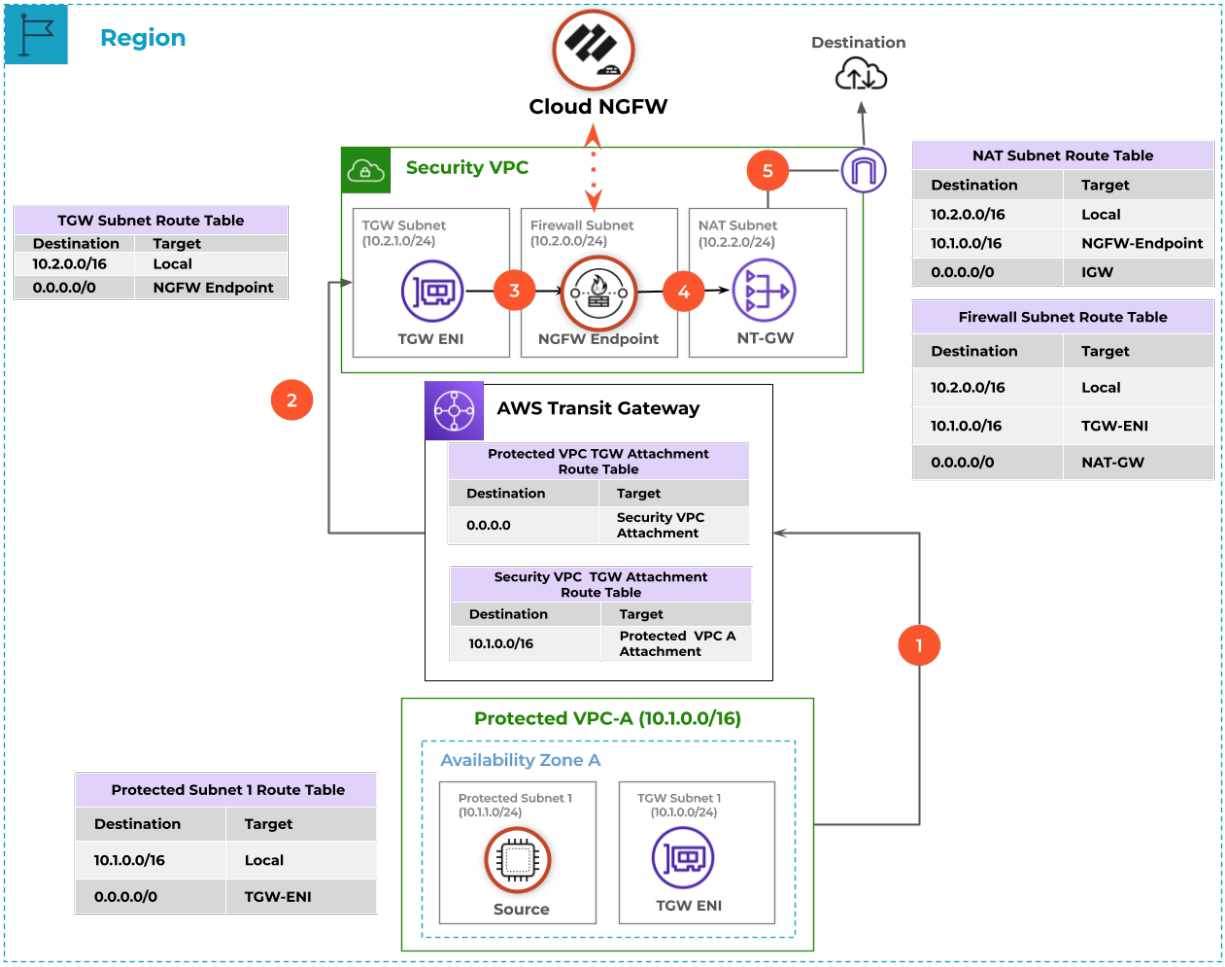
7. Dann sendet das TGW Elastic Network Interface den Datenverkehr an das Ziel.



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.

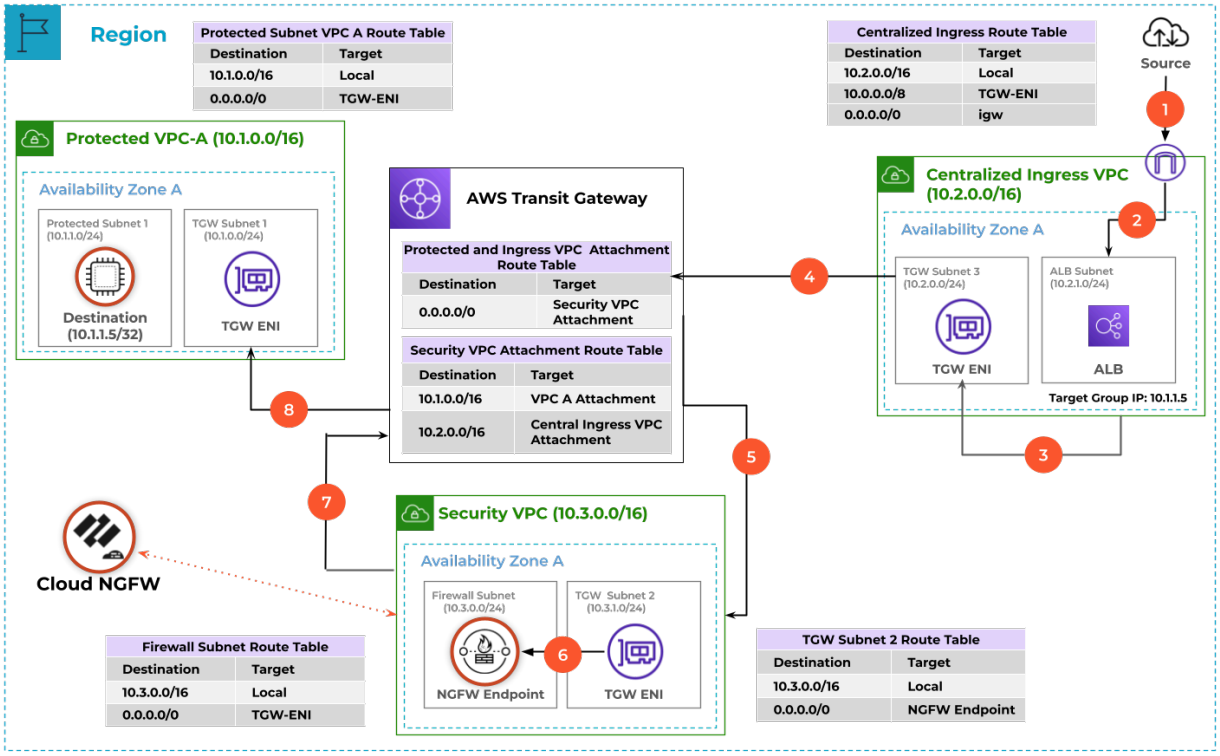
5. Das NAT-Gateway leitet den Datenverkehr an das IGW und dann weiter an das Ziel.



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.



Verteilte Bereitstellungen in Cloud NGFW für AWS

Wo kann ich das verwenden?	Was brauche ich?
• Cloud NGFW für AWS	❑ Cloud NGFW-Abonnement ❑ Konto beim Kunden-Support-Portal (CSP) von Palo Alto Networks ❑ AWS Marketplace-Konto ❑ Benutzerrolle (Mandant oder Administrator)

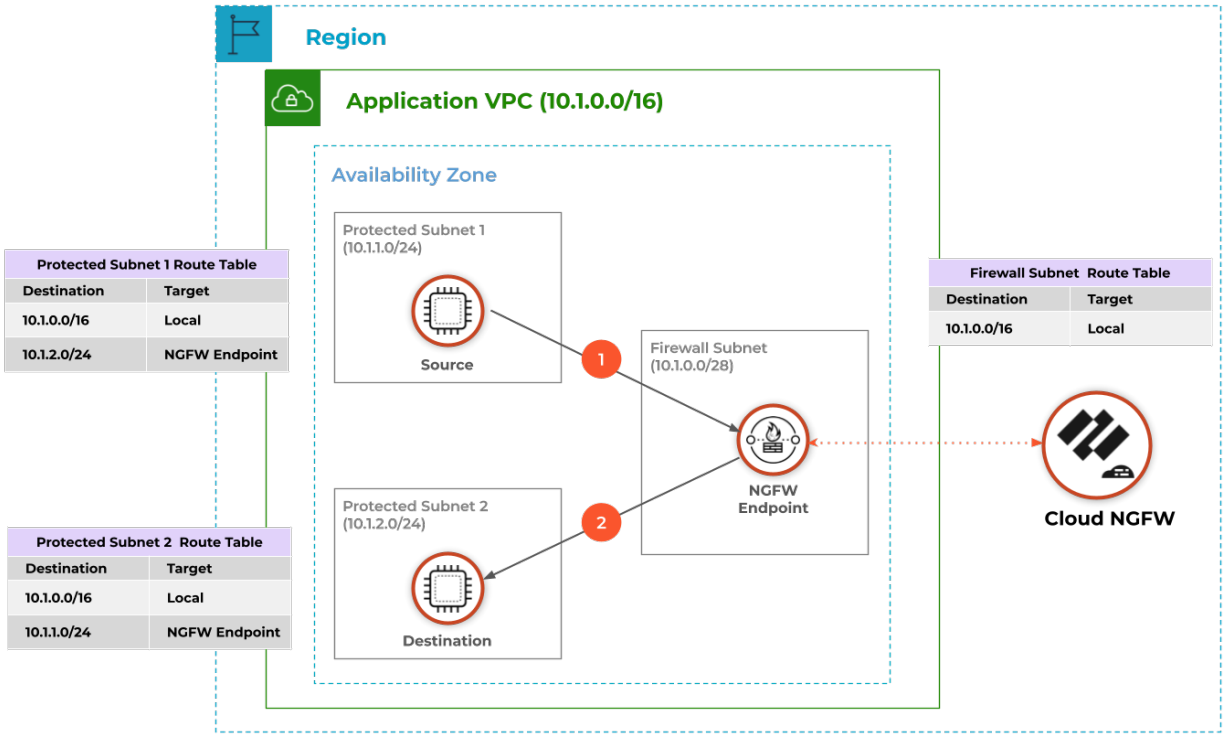
In einer verteilten Bereitstellung verfügt jede VPC, die geschützt werden muss, über eine eigene NGFW. Diese Bereitstellungsmethode ist weniger kompliziert und eine Fehlkonfiguration ist daher weniger wahrscheinlich.

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.

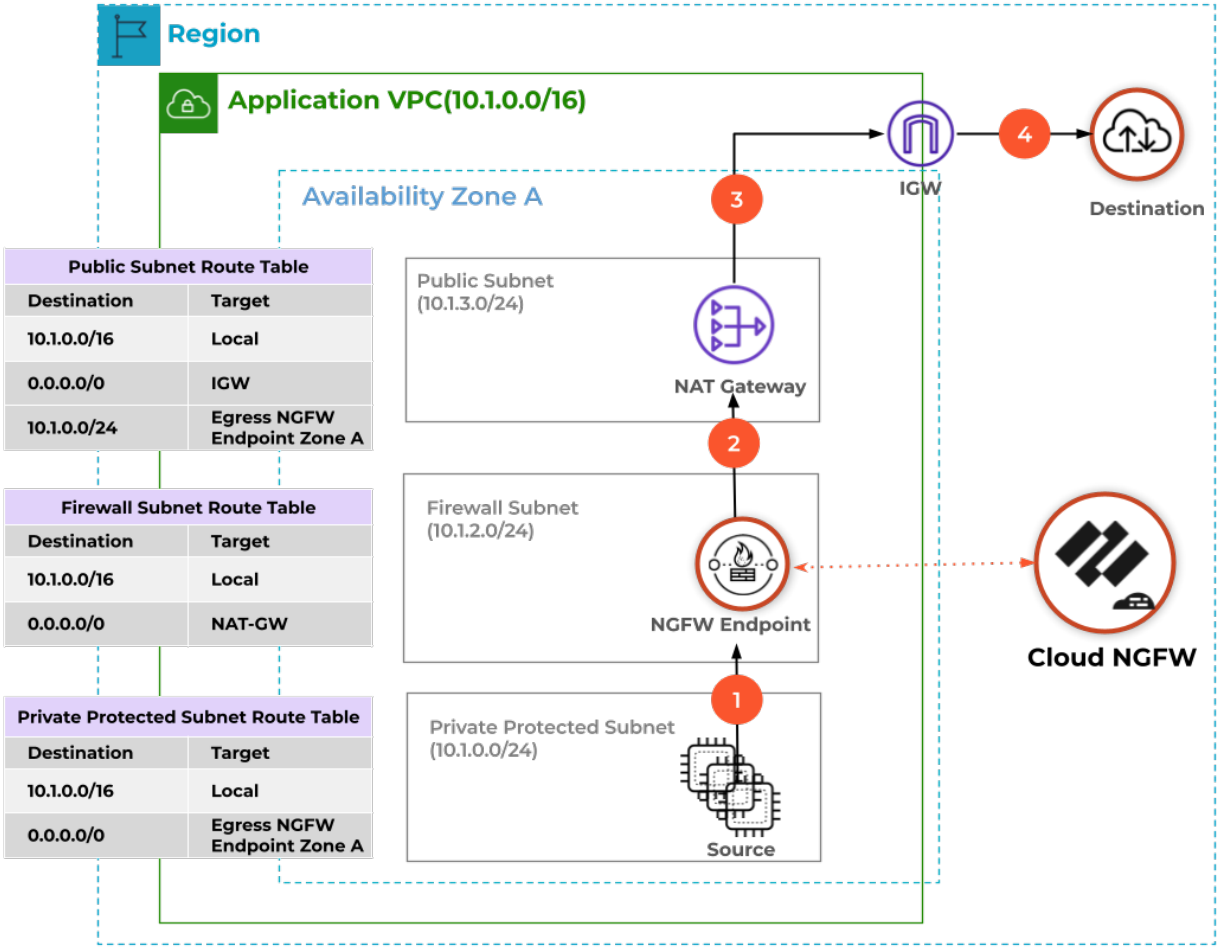
2. Wenn der Datenverkehr zulässig ist, sendet der NGFW-Endpunkt ihn an das Ziel.



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.

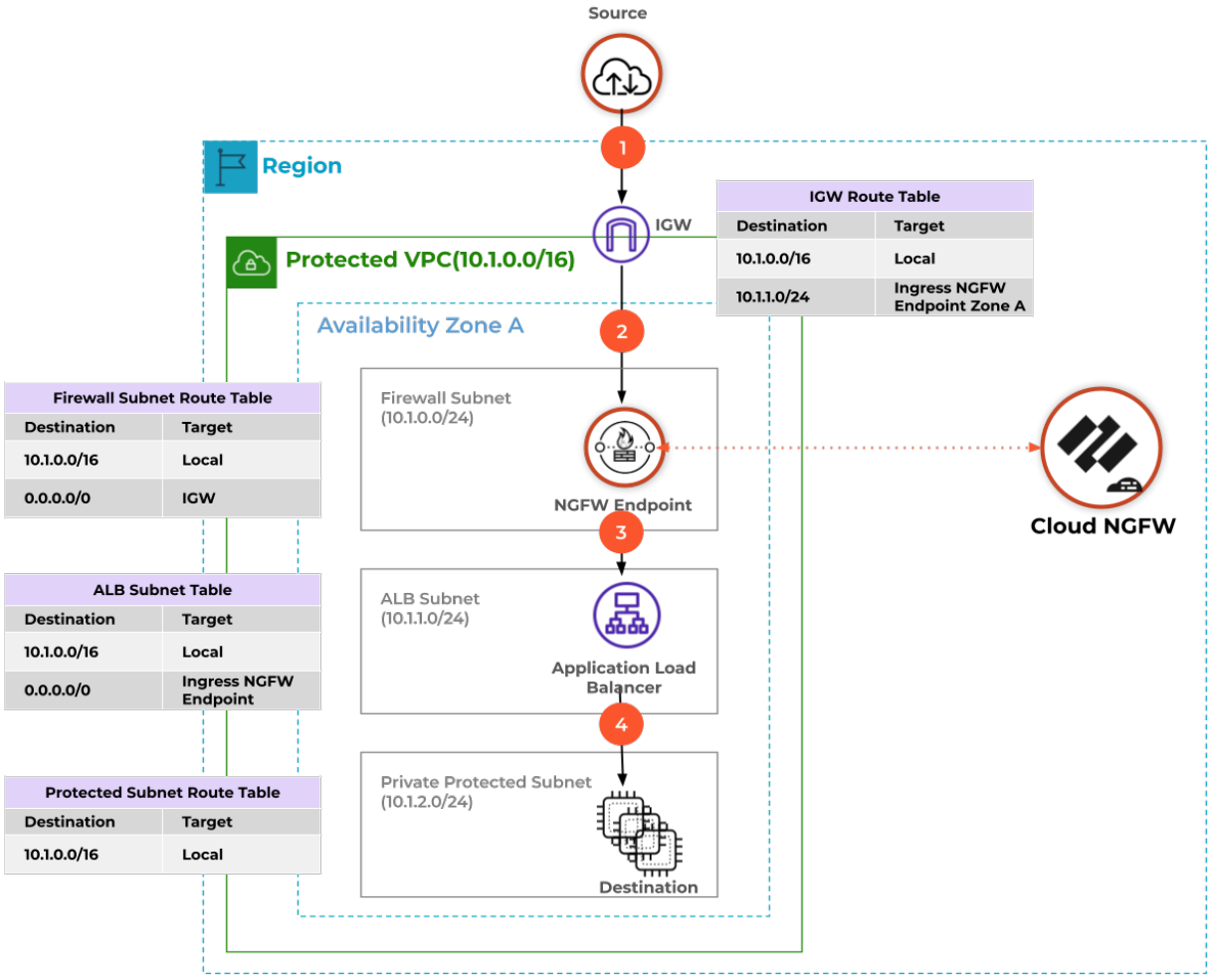
4. Der Datenverkehr wird ins Internet und an das Ziel weitergeleitet.



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?
• Cloud NGFW für AWS	❑ 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.

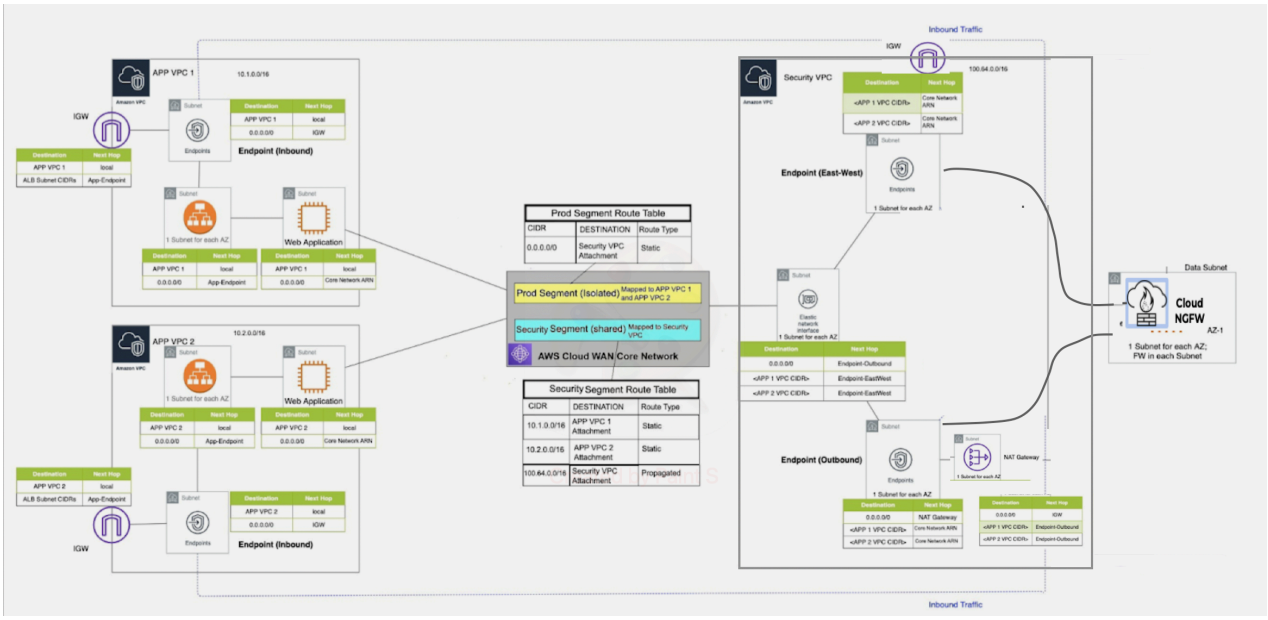
Sie können diese VPCs Segmenten im Kernnetzwerk zuordnen. Diese Segmente werden durch Anhänge wie VPC-Anhänge oder Transit-Gateway-Routentabellen-Anhänge verbunden. Die integrierte Segmentierung hilft Ihnen, die Netzwerkisolation über AWS- und lokale Umgebungen hinweg aufrechtzuerhalten. Jedes Segment 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 (isolierte Anhänge).
- VPCs in verschiedenen Segmenten derselben Region.
- VPCs im selben Segment über verschiedene Regionen hinweg (isolierte 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

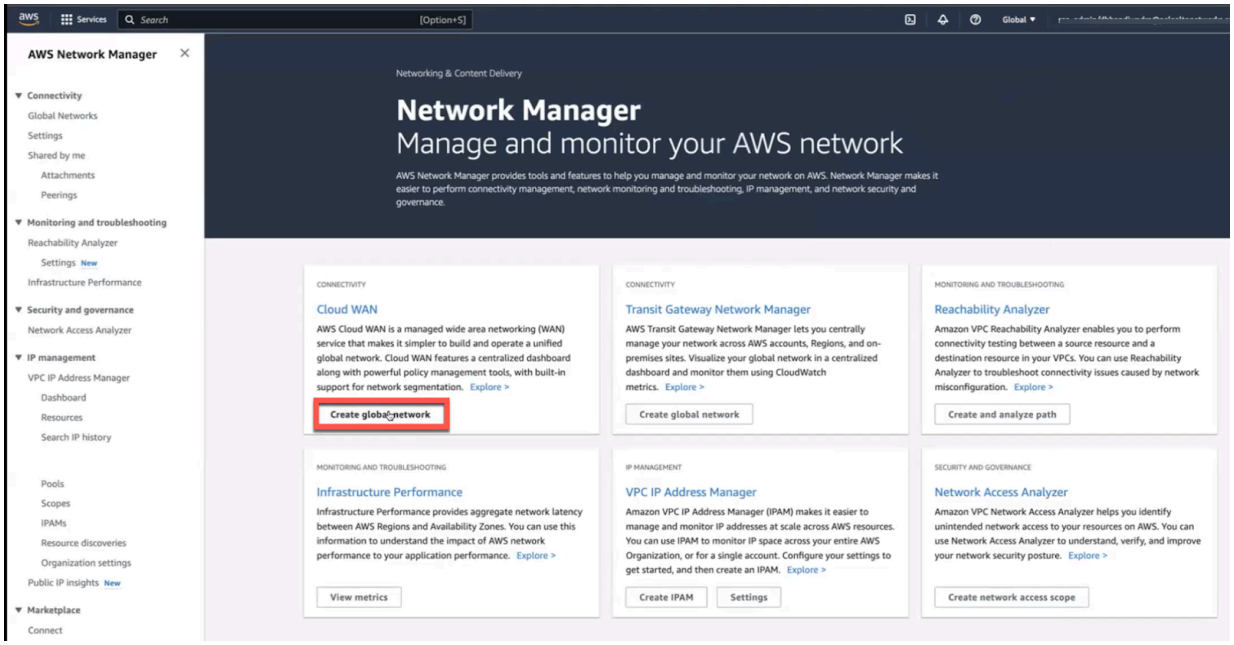
Betrachten wir einen Anwendungsfall, bei dem sich VPCs in derselben Region befinden (isolierte Anhänge). Um diese Einrichtung zu konfigurieren, stellen Sie die Cloud NGFW-Firewall innerhalb der Sicherheits-VPC bereit. Sie können die Cloud NGFW-Firewall in einer Sicherheits-VPC bereitstellen, die direkt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

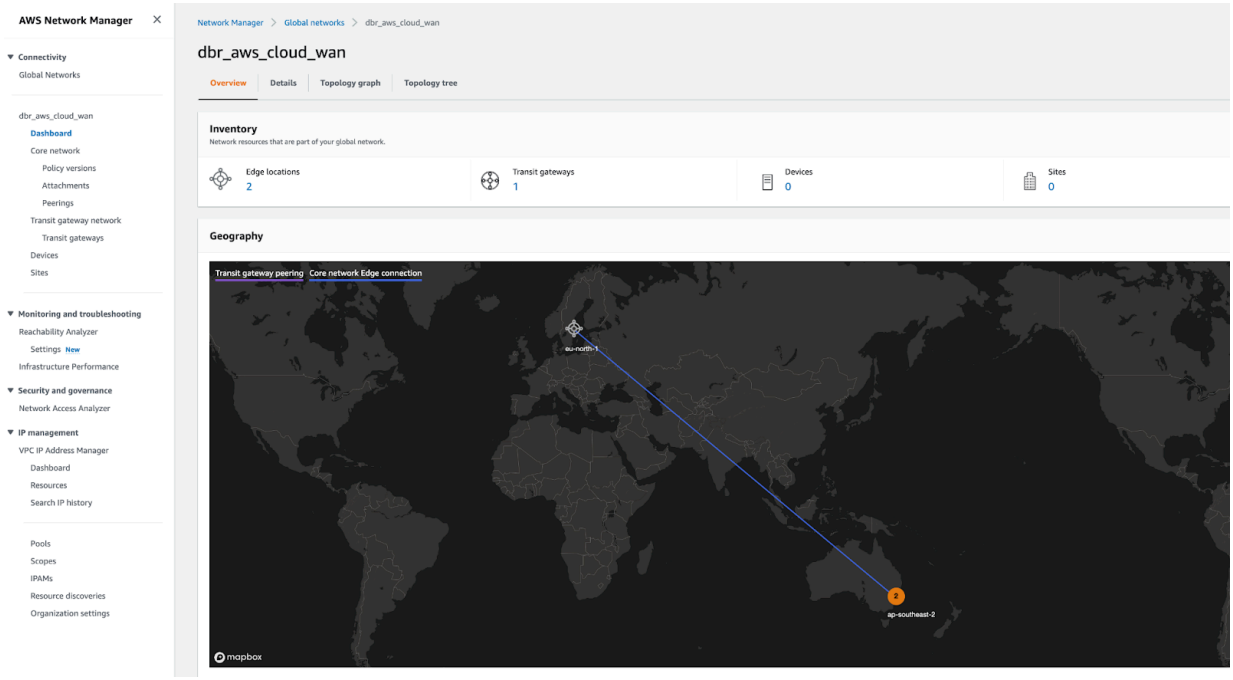
Um eine vollständige Migration vom Transit-Gateway durchzuführen, müssen Sie Ihre VPCs direkt mit dem Cloud-WAN verbinden.

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.

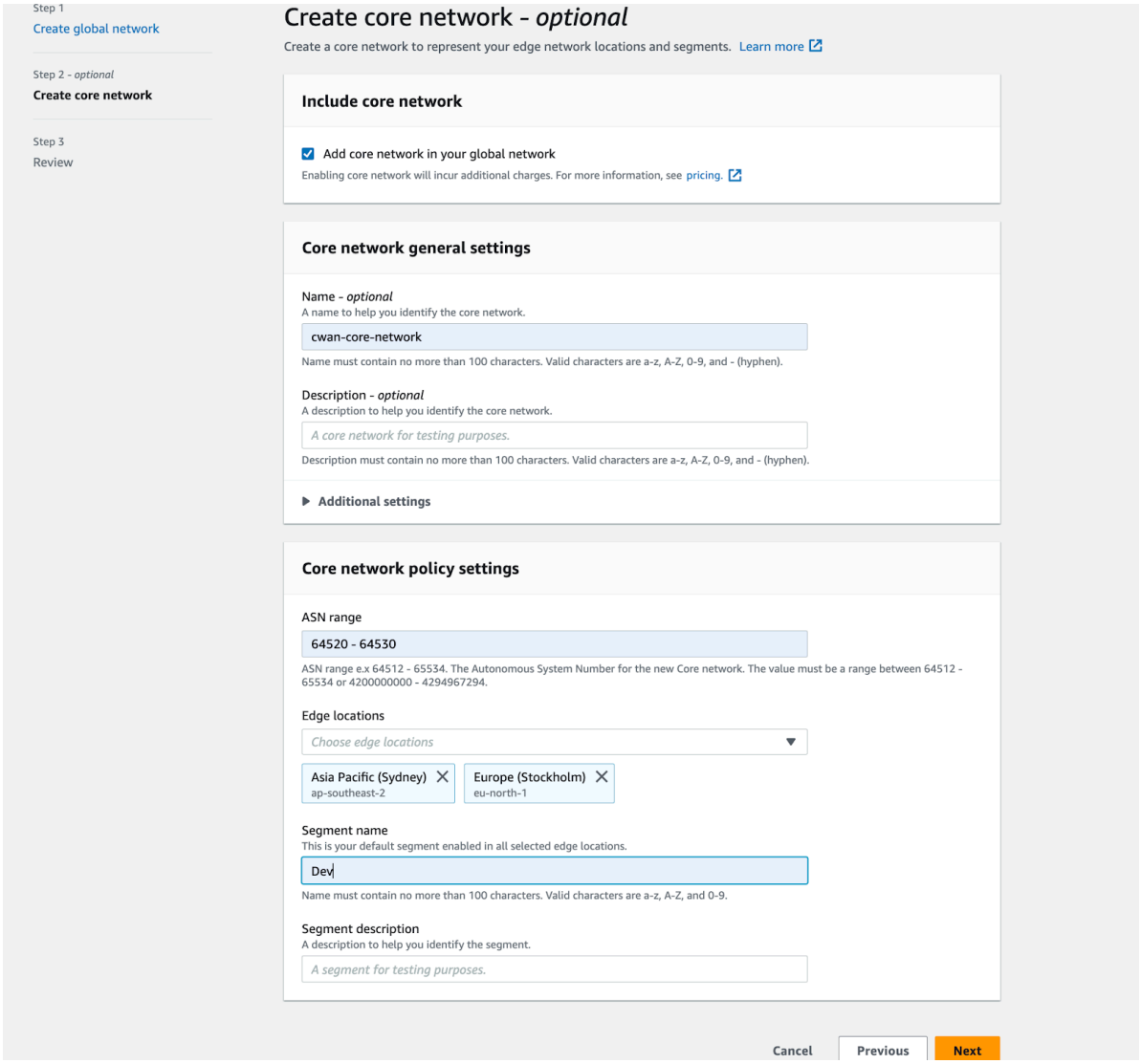




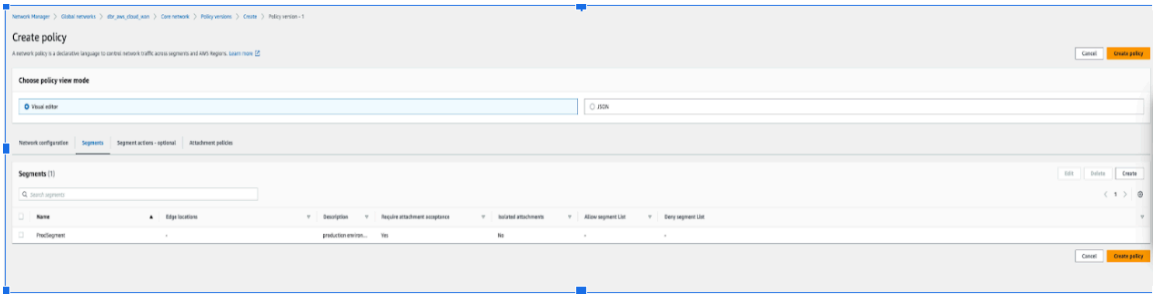
2. Erstellen Sie ein Kernnetzwerk und eine Kernnetzwerkrichtlinie.

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

   - Konfigurieren Sie die Netzwerkeinstellungen.

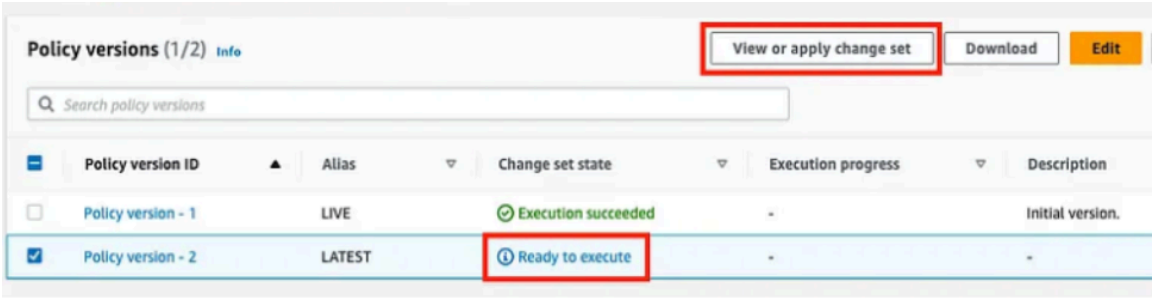


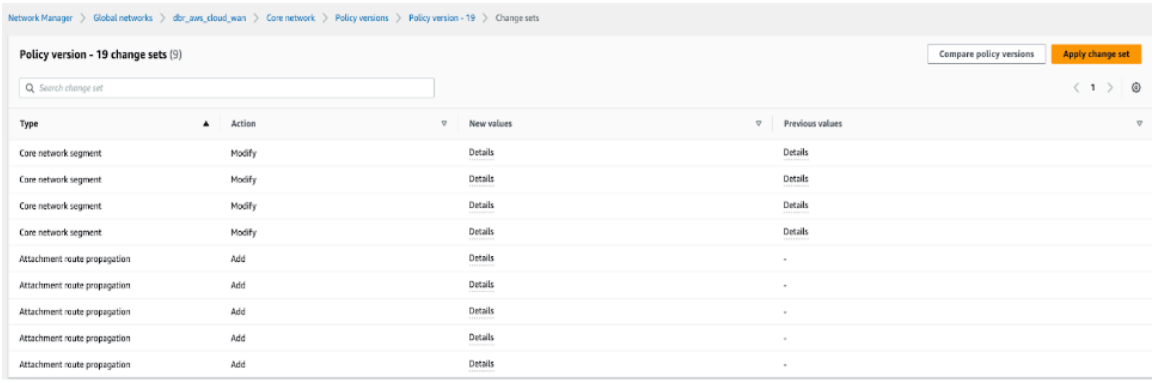
- Klicken Sie zum Bearbeiten einer Richtlinienversion auf **Policy versions (Richtlinienversionen)**, wählen Sie die gewünschte Richtlinie aus und klicken Sie auf **Edit (Bearbeiten)**. Nehmen Sie die erforderlichen Änderungen vor und klicken Sie auf **Create Policy (Richtlinie erstellen)**.



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

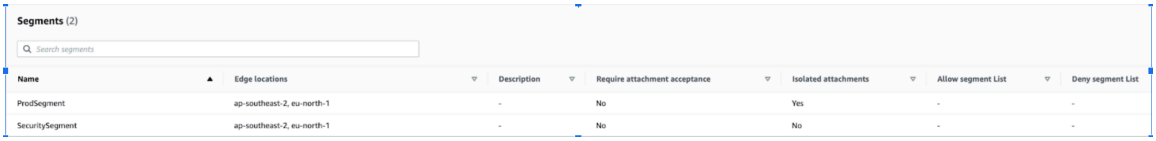
anwenden klicken. Klicken Sie alternativ auf **Richtlinienversion vergleichen**, um das JSON-Dokument anzuzeigen.



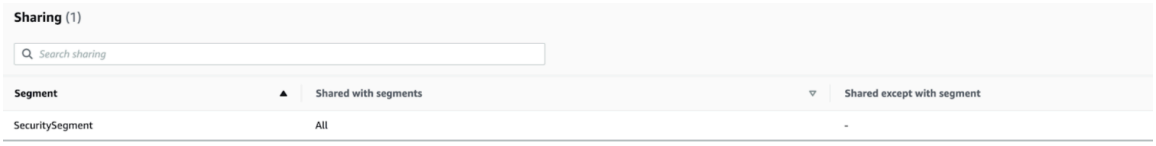


- Erstellen Sie Netzwerkrichtliniensegmente innerhalb Ihres Kernnetzwerks.

  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.



- Erstellen Sie Segmentfreigabe- und Segmentroutenaktionen.

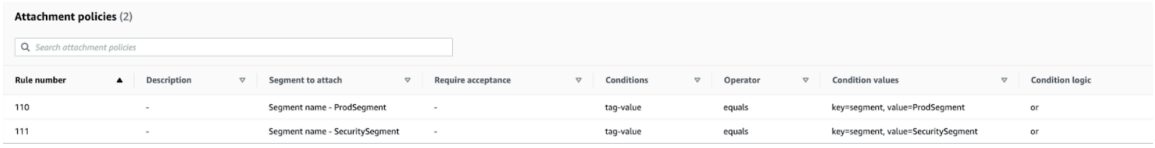


Routes (3)

Search routes

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-0ffa029e9effa9ba2

- Erstellen Sie Richtlinienanhänge.



Attachment policies (2)

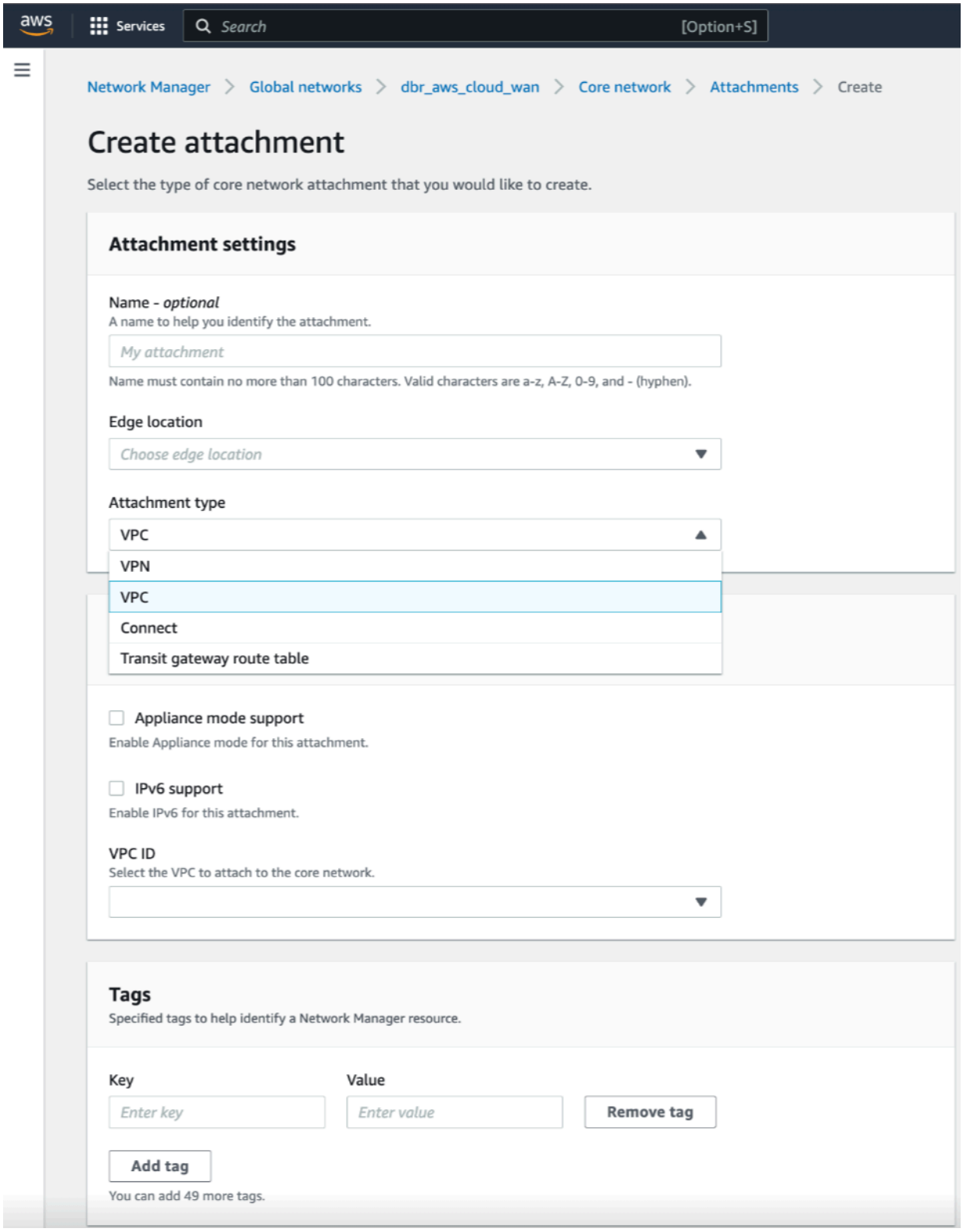
Search attachment policies

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

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.

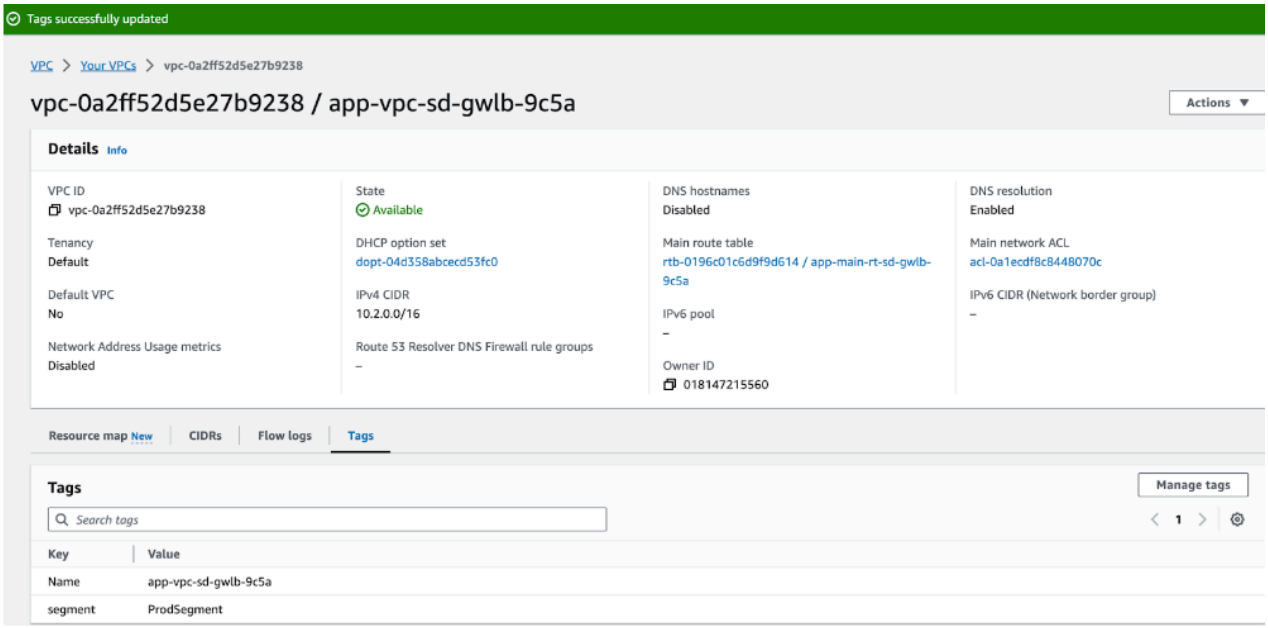
3. Erstellen Sie einen Anhang.

- *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.*

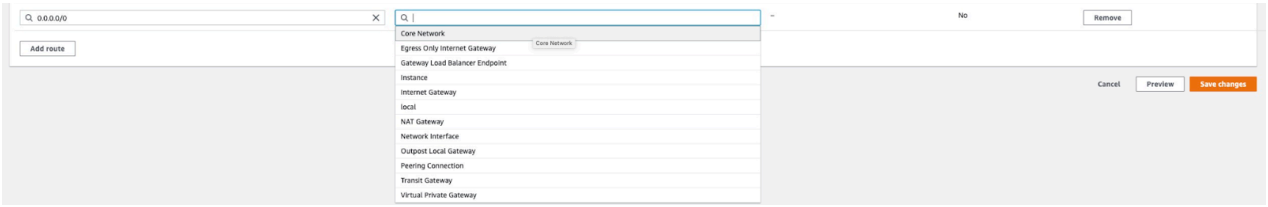


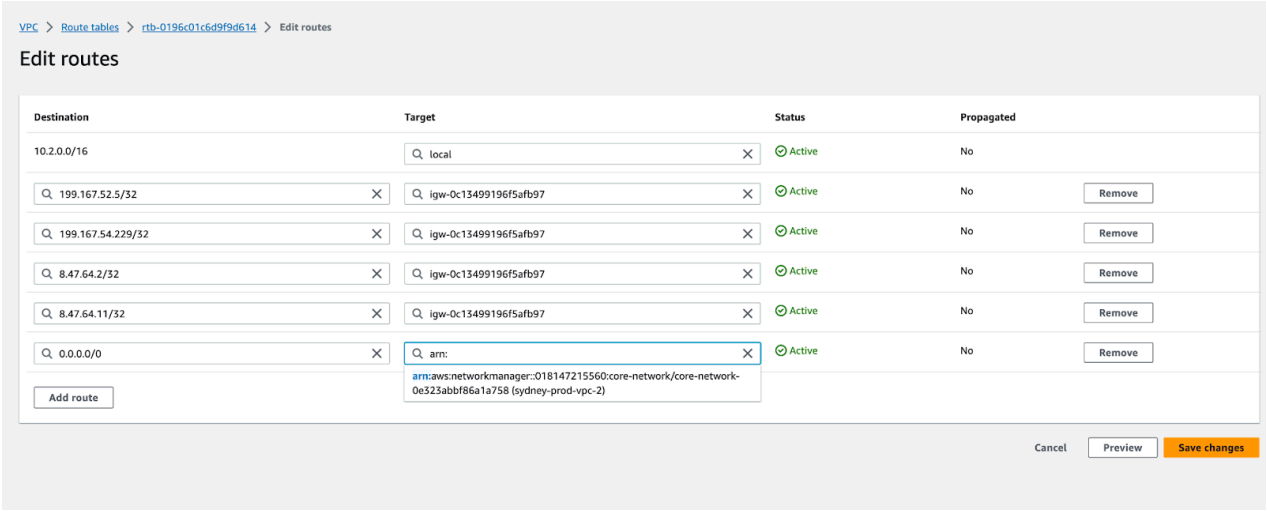
4. Aktualisieren Sie VPC-Routentabellen.

   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.



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.



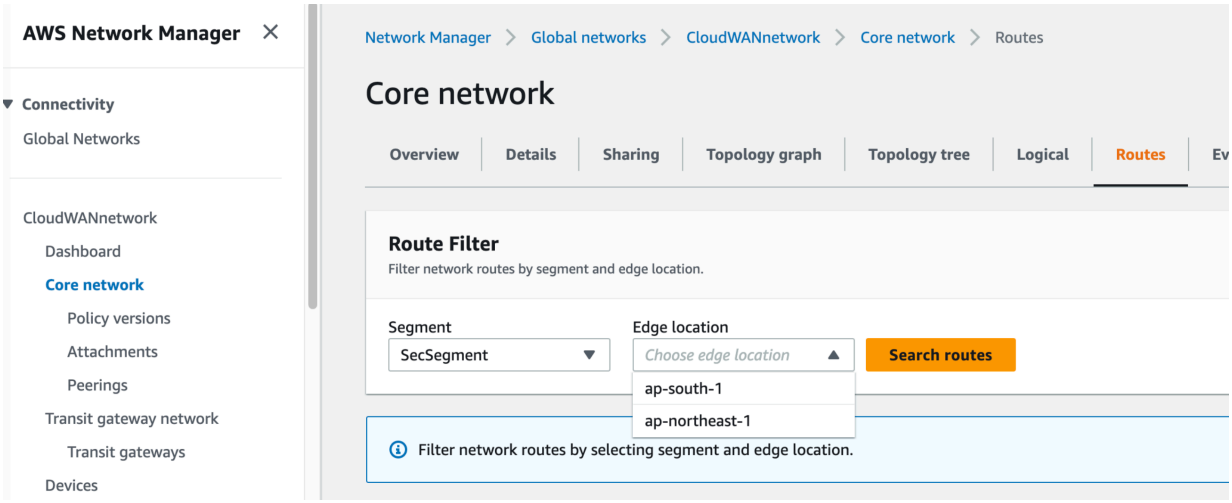


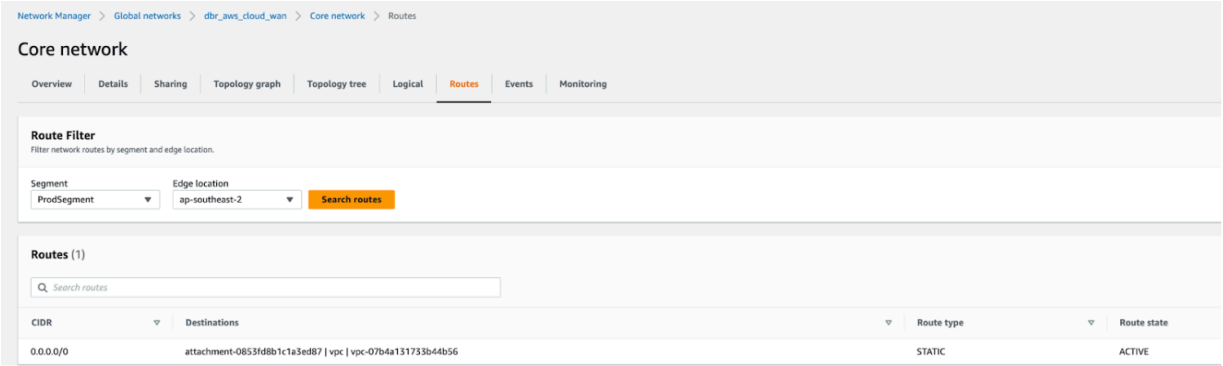
Weg eines Pakets

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

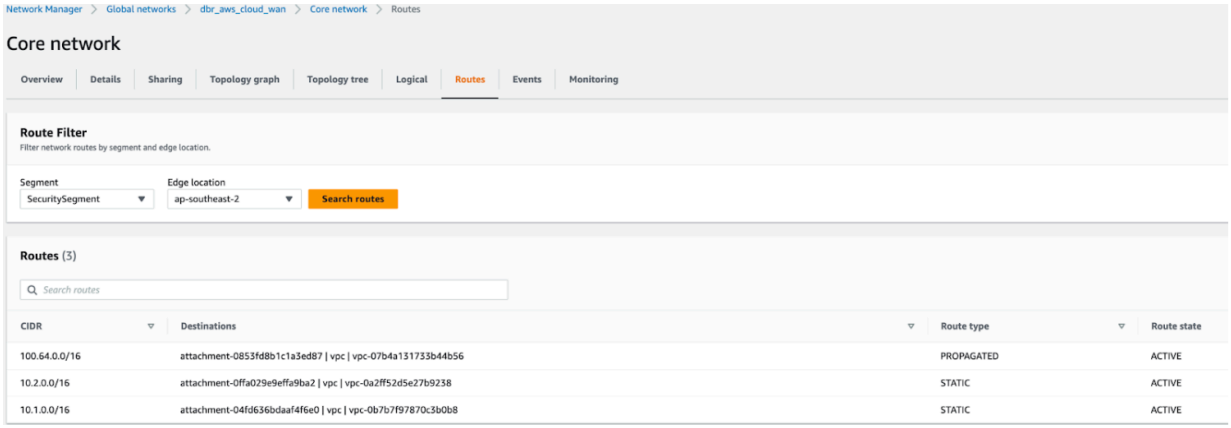
mit dem Standardeintrag überein, wobei der Sicherheitsanhang als Ziel angegeben ist, und wird an die Sicherheits-VPC weitergeleitet.





- 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

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.



- 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.

