Weiterleiten von geneve-gekapseltem Datenverkehr von einem AWS Gateway Load Balancer

Veröffentlicht: 2025-02-12

Sie können in Genf gekapselten Datenverkehr an einen ExtraHop-Sensor senden, indem Sie einen AWS Gateway Load Balancer (GWLB) als VPC-Mirror-Traffic-Ziel konfigurieren.

Bevor Sie beginnen
Einen Sensor in AWS bereitstellen. Stellen Sie sicher, dass wählen Sie Management + RPCAP/ERSPAN/VXLAN/GENEVE für die Capture-Schnittstelle.

Wenn Sie die leistungsstarke ERSPAN/VXLAN/GENEVE Target-Schnittstelle konfigurieren, stellen Sie sicher, dass konfigurieren Sie den TCP Health Check Port um dem in AWS konfigurierten Health Check-Port zu entsprechen.

Erstellen Sie einen Gateway Load Balancer (GWLB)

Eine ausführliche Anleitung finden Sie in den AWS-Anweisungen zu einen Gateway Load Balancer erstellen.

1. Konfigurieren Sie die Zielgruppe und registrieren Sie Ziele.
   Grundlegende Konfigurationseinstellungen:
   - **Art des Ziels:** Wählen **IP-Adressen**
   - **Name der Zielgruppe:** Geben Sie einen Namen ein, um die Zielgruppe zu identifizieren
   - **Protokoll:** Wählen **GENF**
   - **VPC:** Wählen Sie die VPC aus, die den Load Balancer hostet
2. Stellen Sie sicher, dass **TCP** ist für das Health Check-Protokoll ausgewählt. Notieren Sie sich im Abschnitt Einstellungen für die erweiterte Integritätsprüfung die konfigurierte Portnummer. Bei der Konfiguration einer Management + RPCAP/ERSPAN/VXLAN/GENEVE Target-Schnittstelle muss der Port 80 oder 443 sein. Wenn Sie die leistungsstarke ERSPAN/VXLAN/GENEVE Target-Schnittstelle konfigurieren, können Sie eine beliebige gültige Portnummer zwischen 1 und 65535 wählen. Sie müssen jedoch dieselbe Portnummer in das Feld TCP Health Check Port auf dem Sensor eingeben.
3. Fügen Sie die IPv4-Adresse des ExtraHop-Sensors als Ziel hinzu und klicken Sie dann auf **Zielgruppe erstellen**.
4. Erstellen Sie den Gateway Load Balancer.
   Grundlegende Konfigurationseinstellungen:
   - **Name des Load Balancers:** Geben Sie einen eindeutigen Namen ein

   Einstellungen für die Netzwerkzuweisung:
   - **VPC:** Wählen Sie die VPC für Ihre Ziele aus.
   - **Zuordnungen:** Wählen Sie die gewünschten Zonen und die entsprechenden Subnetze aus.
   - **IP-Listener-Routing:** Wählen Sie im Standardaktionsfeld die Zielgruppe aus, die Sie im vorherigen Schritt erstellt haben.

Erstellen Sie einen Gateway Load Balancer-Endpunkt (GWLBE)

Eine detaillierte Anleitung finden Sie in den AWS-Anweisungen zu einen Gateway Load Balancer-Endpunkt erstellen.

1. Erstellen Sie im VPC-Dashboard einen Endpunktdienst mit den folgenden Einstellungen:
   - **Load Balancer-Typ:** Wählen **Tor**
   - **Verfügbare Load Balancer:** Wählen Sie den Load Balancer aus, den Sie im vorherigen Verfahren erstellt haben.
   - **Zusätzliche Einstellungen:** Deaktivieren Sie das **Annahme erforderlich** Ankreuzfeld.
2. Klicken Sie **Erstellen** und notieren Sie den Dienstnamen auf der **Einzelheiten** Tab. Der Dienstname ist erforderlich, wenn Sie den Endpunkt erstellen.
3. Erstellen Sie in VPC einen Endpunkt mit den folgenden Einstellungen:
   - **Servicekategorie:** Wählen **Andere Endpunktdienste**
   - **Name des Dienstes:** Geben Sie den Dienstnamen ein, den Sie im vorherigen Schritt notiert haben, und klicken Sie dann auf **Service verifizieren**.
   - **VPC:** Wählen Sie im Dropdownmenü die VPC aus, in der Sie die GWLBE erstellen möchten.
   - **Subnetze:** Wählen Sie die Verfügbarkeitszone und das Subnetz aus, in dem Sie die GWLBE bereitstellen möchten.

Erstellen Sie ein Verkehrsspiegelziel und einen Filter

Eine detaillierte Anleitung finden Sie in den AWS-Anweisungen zu Erstellen Sie ein Verkehrsspiegelziel und einen Verkehrsspiegelfilter.

1. Erstellen Sie im VPC-Dashboard ein neues Traffic Mirror-Ziel mit den folgenden Einstellungen:
   - **Typ des Ziels:** Wählen **Gateway Load Balancer-Endpunkt**
   - **Ziel:** Wählen Sie die GWLBE aus, die Sie im vorherigen Verfahren erstellt haben
2. Erstellen Sie in VPC einen Traffic Mirror-Filter mit den folgenden Einstellungen:
   - **Netzwerkdienste:** Wählen Sie die **Amazon-DNS** Ankreuzfeld
   - **Regeln für eingehenden Verkehr:** Fügen Sie eine Regel hinzu und füllen Sie die folgenden Felder aus:
     - **Zahl:** Geben Sie eine Zahl für die Regel ein, z. B. `100`
     - **Regelaktion:** Wählen **akzeptieren** aus dem Drop-down-Menü
     - **Protokoll:** Wählen **Alle Protokolle** aus dem Drop-down-Menü
     - **Quell-CIDR-Block:** Typ `0,0,0,0/0`
     - **Ziel-CIDR-Block:** Typ `0,0,0,0/0`
     - **Beschreibung:** Geben Sie eine Beschreibung für die Regel ein
   - **Regeln für ausgehenden Verkehr:** Fügen Sie eine Regel hinzu und füllen Sie die folgenden Felder aus:
     - **Zahl:** Geben Sie eine Zahl für die Regel ein, z. B. `100`
     - **Regelaktion:** Wählen **akzeptieren** aus dem Drop-down-Menü
     - **Protokoll:** Wählen **Alle Protokolle** aus dem Drop-down-Menü
     - **Quell-CIDR-Block:** Typ `0,0,0,0/0`
     - **Ziel-CIDR-Block:** Typ `0,0,0,0/0`
     - **Beschreibung:** Geben Sie eine Beschreibung für die Regel ein

Sie können jetzt mit der Spiegelung des Datenverkehrs von der VPC aus beginnen, auf der die GWLBE erstellt wurde. Wiederholen Sie diesen Vorgang für alle anderen VPCs, von denen Sie den Datenverkehr spiegeln möchten.

(Optional) Spiegeln Sie den Traffic von einem alternativen Konto ab

1. Navigieren Sie in dem Konto, in dem Sie die GWLB erstellt haben, zu Endpoint Services in VPC.
2. Wählen Sie den GWLB Endpoint Service aus, den Sie erstellt haben.
3. Klicken Sie auf **Prinzipale zulassen** Tab.
4. Klicken Sie **Prinzipale zulassen**.
5. Geben Sie im Feld ARN auf der Seite „Principals zulassen“ das Konto ein, mit dem Sie den Service teilen möchten, und zwar im folgenden Format:

   ```
   arn:aws:iam::aws-account-id:<ACCOUNTID>:root
   ```

6. Navigiere zu dem Konto, von dem du den Traffic spiegeln möchtest.
7. Erstellen Sie im VPC-Dashboard einen neuen Endpunkt mit den folgenden Einstellungen:

   • **Kategorie Service:** Wählen **Andere Endpunktdienste**

   • **Name des Dienstes:** Geben Sie den Dienstnamen ein, den Sie im vorherigen Schritt notiert haben, und klicken Sie dann auf **Service verifizieren**.

   • **VPC:** Wählen Sie im Dropdownmenü die VPC aus, in der Sie die GWLBE erstellen möchten.

   • **Subnetze:** Wählen Sie die Verfügbarkeitszone und das Subnetz aus, in dem Sie die GWLBE bereitstellen möchten.
8. Erstellen Sie in VPC ein Traffic Mirror-Ziel mit den folgenden Einstellungen:

   • **Typ des Ziels:** Wählen **Gateway Load Balancer-Endpunkt**

   • **Ziel:** Wählen Sie die GWLBE aus, die Sie erstellt haben
9. Erstellen Sie in VPC einen Traffic Mirror-Filter mit den folgenden Einstellungen:

   • **Netzwerkdienste:** Wählen Sie die **Amazon-DNS** Ankreuzfeld

   • **Regeln für eingehenden Verkehr:** Fügen Sie eine Regel hinzu und füllen Sie die folgenden Felder aus:

      • **Zahl:** Geben Sie eine Zahl für die Regel ein, z. B. 100

      • **Regelaktion:** Wählen **akzeptieren** aus der Dropdownliste

      • **Protokoll:** Wählen **Alle Protokolle** aus dem Drop-down-Menü

      • **Quell-CIDR-Block:** Typ `0,0,0,0/0`

      • **CIDR-Zielblock:** Typ `0,0,0,0/0`

      • **Beschreibung:** Geben Sie eine Beschreibung für die Regel ein

Wiederholen Sie diesen Vorgang für alle anderen VPCs, von denen Sie den Datenverkehr spiegeln möchten.