Transférer le trafic encapsulé à Geneve depuis un équilibreur de charge AWS Gateway

Publié: 2024-08-08

Vous pouvez envoyer le trafic encapsulé Geneve vers une sonde ExtraHop en configurant un équilibreur de charge AWS Gateway (GWLB) en tant que cible de trafic miroir VPC.

Avant de commencer
Déployer une sonde dans AWS. Assurez-vous de sélectionnez Management + RPCAP/ERSPAN/VXLAN/GENEVE pour l'interface de capture.

Si vous configurez l'interface cible ERSPAN/VXLAN/GENEVE à hautes performances, assurez-vous que configurer le port de contrôle de santé TCP pour correspondre au port de contrôle de santé configuré dans AWS.

Création d'un équilibreur de charge de passerelle (GWLB)

Pour obtenir des instructions détaillées, consultez les instructions AWS pour créer un équilibreur de charge Gateway.

1. Configurez le groupe cible et enregistrez les cibles.
   Paramètres de configuration de base :
   - **Type de cible:** Sélectionnez **Adresses IP**
   - **Nom du groupe cible:** Entrez un nom pour identifier le groupe cible
   - **Protocole:** Sélectionnez **GENEVE**
   - **VPC:** Sélectionnez le VPC qui héberge l'équilibreur de charge
2. Assurez-vous que **TCP** est sélectionné pour le protocole de contrôle de santé. Dans la section des paramètres de contrôle de santé avancés, notez le numéro de port configuré. Lors de la configuration d'une interface cible Management + RPCAP/ERSPAN/VXLAN/GENEVE, le port doit être 80 ou 443. Si vous configurez l'interface cible ERSPAN/VXLAN/GENEVE à hautes performances, vous pouvez choisir n'importe quel numéro de port valide compris entre 1 et 65535, mais vous devez saisir le même numéro de port dans le champ TCP Health Check Port de la sonde.
3. Ajoutez l'adresse IPv4 de la sonde ExtraHop comme cible, puis cliquez sur **Création d'un groupe cible**.
4. Créez l'équilibreur de charge de passerelle.
   Paramètres de configuration de base :
   - **Nom de l'équilibreur de charge:** Entrez un nom unique

   Paramètres de mappage réseau :
   - **VPC:** Sélectionnez le VPC pour vos cibles.
   - **Mappages:** Sélectionnez les zones souhaitées et les sous-réseaux correspondants.
   - **Routage de l'écouteur IP:** Dans le champ d'action par défaut, sélectionnez le groupe cible que vous avez créé à l'étape précédente.

Création d'un point de terminaison Gateway Load Balancer (GWLbe)

Pour obtenir des instructions détaillées, consultez les instructions AWS pour créer un point de terminaison Gateway Load Balancer.

1. À partir du tableau de bord du VPC, créez un service de point de terminaison avec les paramètres suivants :

- **Type d'équilibreur de charge:** Sélectionnez **Passerelle**
- **Équilibreurs de charge disponibles:** Sélectionnez l'équilibreur de charge que vous avez créé lors de la procédure précédente.
- **Réglages supplémentaires:** Désélectionnez le **Acceptation requise** case à cocher.

2. Cliquez **Créez** et notez le nom du service sur le **Détails** onglet. Le nom du service est obligatoire lorsque vous créez le point de terminaison.
3. Dans VPC, créez un point de terminaison avec les paramètres suivants :
   - **Catégorie de service:** Sélectionnez **Autres services de point de terminaison**
   - **Nom du service:** Tapez le nom du service que vous avez noté à l'étape précédente, puis cliquez sur **Vérifier le service**.
   - **VPC:** Dans la liste déroulante, sélectionnez le VPC dans lequel vous souhaitez créer le GWLbe.
   - **Sous-réseaux:** Sélectionnez la zone de disponibilité et le sous-réseau dans lesquels vous souhaitez déployer le GWLbe.

Création d'une cible et d'un filtre reflétant le trafic

Pour obtenir des instructions détaillées, consultez les instructions AWS pour créer une cible de miroir de trafic et un filtre de miroir de trafic.

1. À partir du tableau de bord du VPC, créez une nouvelle cible miroir du trafic avec les paramètres suivants :
   - **Type de cible:** Sélectionnez **Point de terminaison Gateway Load Balancer**
   - **Cible:** Sélectionnez le GWLbe que vous avez créé lors de la procédure précédente
2. Dans VPC, créez un filtre de miroir du trafic avec les paramètres suivants :
   - **Services de réseau:** Sélectionnez le **amazon dns** case à cocher
   - **Règles relatives au trafic entrant:** Ajoutez une règle et complétez les champs suivants :
     - **Numéro:** Entrez un numéro pour la règle, tel que `100`
     - **Action relative aux règles:** Sélectionnez **accepter** depuis la liste déroulante
     - **Protocole:** Sélectionnez **Tous les protocoles** depuis la liste déroulante
     - **Bloc CIDR source:** Type `0.0.0,0/0`
     - **Bloc CIDR de destination:** Type `0.0.0,0/0`
     - **Descriptif:** Entrez une description pour la règle
   - **Règles relatives au trafic sortant:** Ajoutez une règle et complétez les champs suivants :
     - **Numéro:** Entrez un numéro pour la règle, tel que `100`
     - **Action relative aux règles:** Sélectionnez **accepter** depuis la liste déroulante
     - **Protocole:** Sélectionnez **Tous les protocoles** depuis la liste déroulante
     - **Bloc CIDR source:** Type `0.0.0,0/0`
     - **Bloc CIDR de destination:** Type `0.0.0,0/0`
     - **Descriptif:** Entrez une description pour la règle

Vous pouvez maintenant commencer à mettre en miroir le trafic depuis le VPC où le GWLbe a été créé. Répétez cette procédure pour tous les autres VPC dont vous souhaitez refléter le trafic .

(Facultatif) Refléter le trafic provenant d'un autre compte

1. Dans le compte dans lequel vous avez créé le GWLB, accédez à Endpoint Services in VPC.
2. Sélectionnez le service GWLB Endpoint que vous avez créé.
3. Cliquez sur **Autoriser les directeurs** onglet.
4. Cliquez **Autoriser les directeurs**.
5. Dans le champ ARN de la page Autoriser les principaux, entrez le compte avec lequel vous souhaitez partager le service au format suivant :

   ```
   arn:aws:iam::aws-account-id:<ACCOUNTID>:root
   ```
6. Accédez au compte à partir duquel vous souhaitez refléter le trafic.
7. À partir du tableau de bord du VPC, créez un nouveau point de terminaison avec les paramètres suivants :

   • **Catégorie de service:** Sélectionnez **Autres services de point de terminaison**

   • **Nom du service:** Tapez le nom du service que vous avez noté à l'étape précédente, puis cliquez sur **Vérifier le service**.

   • **VPC:** Dans la liste déroulante, sélectionnez le VPC dans lequel vous souhaitez créer le GWLbe.

   • **Sous-réseaux:** Sélectionnez la zone de disponibilité et le sous-réseau dans lesquels vous souhaitez déployer le GWLbe.
8. Dans VPC, créez une cible miroir du trafic avec les paramètres suivants :

   • **Type de cible:** Sélectionnez **Point de terminaison Gateway Load Balancer**

   • **Cible:** Sélectionnez le GWLbe que vous avez créé
9. Dans VPC, créez un filtre de miroir du trafic avec les paramètres suivants :

   • **Services de réseau:** Sélectionnez le **amazon dns** case à cocher

   • **Règles relatives au trafic entrant:** Ajoutez une règle et complétez les champs suivants :

      • **Numéro:** Entrez un nombre pour la règle, par exemple 100

      • **Action relative aux règles:** Sélectionnez **accepter** depuis la liste déroulante

      • **Protocole:** Sélectionnez **Tous les protocoles** depuis la liste déroulante

      • **Bloc CIDR source:** Type `0.0.0,0/0`

      • **Bloc CIDR de destination:** Type `0.0.0,0/0`

      • **Descriptif:** Entrez une description pour la règle

Répétez cette procédure pour tous les autres VPC dont vous souhaitez refléter le trafic.