Transférer le trafic encapsulé GENEVE à partir d'un équilibreur de charge de passerelle AWS

Publié: 2023-09-19

Vous pouvez envoyer du trafic encapsulé GENEVE à un capteur ExtraHop en configurant un équilibreur de charge de passerelle AWS (GWLB) comme cible de trafic miroir VPC.

Avant de commencer
Déployez un capteur dans AWS.

Si vous configurez l'interface cible ERSPAN/VXLAN/GENEVE haute performance, assurez-vous de configurer le port de contrôle de santé TCP pour qu'il corresponde au port de contrôle de santé configuré dans AWS

.

Créer un équilibreur de charge de passerelle (GWLB)

Pour des instructions détaillées, voir les instructions AWS pour créer un équilibreur de charge de passerelle.

1. Configurer le groupe de cibles et enregistrer les cibles.
   Paramètres de configuration de base :
   - **Type de cible:** Sélectionner les **adresses IP**
   - **Nom du groupe cible:** Saisir un nom pour identifier le groupe cible
   - **Protocole:** Sélectionner **GENEVE**
   - **VPC:** Sélectionnez le VPC qui héberge l'équilibreur de charge.
2. Assurez-vous que **TCP** est sélectionné pour le protocole du bilan de santé. Dans la section des paramètres avancés du bilan de santé, notez le numéro de port configuré. Lorsque vous configurez une interface Management + RPCAP/ERSPAN/VXLAN/GENEVE Target, le port doit être 80 ou 443. Si vous configurez l'interface ERSPAN/VXLAN/GENEVE Target haute performance, vous pouvez choisir n'importe quel numéro de port valide entre 1 et 65535, mais vous devez entrer le même numéro de port dans le champ TCP Health Check Port (Port de contrôle de santé TCP) sur le capteur.
3. Ajoutez l'adresse IPv4 du capteur ExtraHop comme cible, puis cliquez sur **Créer un groupe cible**.
4. Créez l'équilibreur de charge de la passerelle.
   Paramètres de configuration de base :
   - **Nom de l'équilibreur de charge:** Entrez un nom unique

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

Créer un point d'extrémité Gateway Load Balancer (GWLBe)

Pour des instructions détaillées, voir les instructions AWS pour créer un point d'extrémité Gateway Load Balancer.

1. Dans le tableau de bord VPC, créez un service d'extrémité avec les paramètres suivants :

- **Type d'équilibreur de charge:** Sélectionnez **Gateway**
- **Équilibreurs de charge disponibles:** Sélectionnez l'équilibreur de charge que vous avez créé dans la procédure précédente.
- **Paramètres supplémentaires:** Désélectionnez la case **Acceptation requise**.

2. Cliquez sur **Créer** et notez le nom du service dans l'onglet **Détails**. Le nom du service est requis lorsque vous créez le point d'extrémité.
3. Dans VPC, créez un point d'extrémité avec les paramètres suivants :
   - **Catégorie de service:** Catégorie de service Sélectionnez **Autres services d'extrémité**
   - **Nom du service:** Saisissez 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 la GWLBe.
   - **Sous-réseaux:** Sélectionnez la zone de disponibilité et le sous-réseau où vous souhaitez déployer la GWLBe.

Créer une cible et un filtre de miroir de trafic

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

1. Dans le tableau de bord VPC, créez une nouvelle cible de miroir de trafic avec les paramètres suivants :
   - **Type de cible:** Sélectionnez **Gateway Load Balancer Endpoint**
   - **Cible:** Sélectionnez le GWLBe que vous avez créé dans la procédure précédente.
2. Dans le VPC, créez un filtre miroir de trafic avec les paramètres suivants :
   - **Services réseau:** Cochez la case **amazon-dns**
   - **Règles d'entrée:** Ajoutez une règle et remplissez les champs suivants :
     - **Numéro:** Saisissez un numéro pour la règle, par exemple `100`
     - **Action de la règle:** Sélectionnez **accepter** dans la liste déroulante
     - **Protocole:** Sélectionnez **Tous les protocoles** dans la liste déroulante
     - **Bloc CIDR source:** Type `0.0.0.0/0`
     - **Bloc CIDR de destination:** Type `0.0.0.0/0`
     - **Description de la règle:** Saisissez une description pour la règle
   - **Règles de sortie:** Ajoutez une règle et remplissez les champs suivants :
     - **Numéro:** Saisissez un numéro pour la règle, par exemple `100`
     - **Action de la règle:** Sélectionnez **accepter** dans la liste déroulante
     - **Protocole:** Sélectionnez **Tous les protocoles** dans la liste déroulante
     - **Bloc CIDR source:** Type `0.0.0.0/0`
     - **Bloc CIDR de destination:** Type `0.0.0.0/0`
     - **Description de la règle:** Saisissez une description pour la règle

Vous pouvez maintenant commencer à mettre en miroir le trafic à partir du VPC où la GWLBe a été créée. Répétez cette procédure pour tous les autres VPC à partir desquels vous souhaitez mettre en miroir le trafic.

(Facultatif) Miroir du trafic à partir d'un autre compte

1. Dans le compte dans lequel vous avez créé la GWLB, naviguez vers Endpoint Services in VPC.
2. Sélectionnez le service d'extrémité GWLB que vous avez créé.
3. Cliquez sur l'onglet **Autoriser les mandants**.
4. Cliquez sur **Autoriser les mand**ants.
5. Dans le champ ARN de la page Allow principals, entrez le compte avec lequel vous souhaitez partager le service dans le format suivant :

   ```
   arn:aws:iam::aws-account-id:<ACCOUNTID>:root
   ```
6. Naviguez jusqu'au compte à partir duquel vous souhaitez créer un miroir du trafic.
7. Dans le tableau de bord VPC, créez un nouveau point final avec les paramètres suivants :

   • **Catégorie de service:** Sélectionnez **Other endpoint services (Autres services d'extrémité**)

   • **Nom du service:** Saisissez 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 la GWLBe.

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

   • **Type de cible:** Sélectionnez **Gateway Load Balancer Endpoint**

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

   • **Services réseau:** Cochez la case **amazon-dns**

   • **Règles d'entrée:** Ajoutez une règle et remplissez les champs suivants :

      • **Numéro:** Saisissez un numéro pour la règle, par exemple 100

      • **Action de la règle:** Sélectionnez **accepter** dans la liste déroulante

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

      • **Bloc CIDR source:** Type `0.0.0.0/0`

      • **Bloc CIDR de destination:** Type `0.0.0.0/0`

      • **Description de la règle:** Saisissez une description pour la règle

Répétez cette procédure pour tous les autres VPC à partir desquels vous souhaitez créer un miroir du trafic.