Forward GENEVE-encapsulated traffic from an AWS Gateway Load Balancer

Published: 2025-01-10

You can send GENEVE-encapsulated traffic to an ExtraHop sensor by configuring an AWS Gateway Load Balancer (GWLB) as a VPC mirror traffic target.

Before you begin
Deploy a sensor in AWS. Make sure to select Management + RPCAP/ERSPAN/VXLAN/GENEVE for the capture interface.

If you are configuring the High-Performance ERSPAN/VXLAN/GENEVE Target interface, make sure you configure the TCP Health Check Port to match the health check port configured in AWS.

Create a Gateway Load Balancer (GWLB)

For detailed instructions, see the AWS instructions to create a Gateway Load Balancer.

1. Configure the target group and register targets.
   Basic configuration settings:
   - **Target type:** Select **IP addresses**
   - **Target group name:** Type a name to identify the target group
   - **Protocol:** Select **GENEVE**
   - **VPC:** Select the VPC that hosts the load balancer
2. Ensure that **TCP** is selected for the health check protocol. In the advanced health check settings section, note the configured port number. When configuring a Management + RPCAP/ERSPAN/VXLAN/GENEVE Target interface, the port must be 80 or 443. If you are configuring the High-Performance ERSPAN/VXLAN/GENEVE Target interface, you can choose any valid port number between 1 and 65535, but you must enter the same port number in the TCP Health Check Port field on the sensor.
3. Add the IPv4 address of the ExtraHop sensor as the target and then click **Create target group**.
4. Create the gateway load balancer.
   Basic configuration settings:
   - **Load balancer name:** Enter a unique name

   Network mapping settings:
   - **VPC:** Select the VPC for your targets.
   - **Mappings:** Select the desired zones and corresponding subnets.
   - **IP listener routing:** From the default action field, select the target group that you created in the previous step.

Create a Gateway Load Balancer endpoint (GWLBe)

For detailed instructions, see the AWS instructions to create a Gateway Load Balancer endpoint.

1. From the VPC dashboard, create an endpoint service with the following settings:
   - **Load balancer type:** Select **Gateway**
   - **Available load balancers:** Select the load balancer you created in the previous procedure.

- **Additional settings:** Deselect the **Acceptance required** checkbox.

2. Click **Create** and note the service name on the **Details** tab. The service name is required when you create the endpoint.
3. In VPC, create an endpoint with the following settings:
   - **Service category:** Select **Other endpoint services**
   - **Service name:** Type the service name you noted in the previous step and then click **Verify service**.
   - **VPC:** From the drop-down menu, select the VPC where you want to create the GWLBe.
   - **Subnets:** Select the availability zone and the subnet where you want to deploy the GWLBe.

Create a traffic mirror target and filter

For detailed instructions, see the AWS instructions to create a traffic mirror target and traffic mirror filter.

1. From the VPC dashboard, create a new traffic mirror target with the following settings:
   - **Target type:** Select **Gateway Load Balancer Endpoint**
   - **Target:** Select the GWLBe you created in the previous procedure
2. In VPC, create a traffic mirror filter with the following settings:
   - **Network services:** Select the **amazon-dns** checkbox
   - **Inbound rules:** Add a rule and complete the following fields:
     - **Number:** Type a number for the rule, such as `100`
     - **Rule action:** Select **accept** from the drop-down menu
     - **Protocol:** Select **All protocols** from the drop-down menu
     - **Source CIDR block:** Type `0.0.0.0/0`
     - **Destination CIDR block:** Type `0.0.0.0/0`
     - **Description:** Type a description for the rule
   - **Outbound rules:** Add a rule and complete the following fields:
     - **Number:** Type a number for the rule, such as `100`
     - **Rule action:** Select **accept** from the drop-down menu
     - **Protocol:** Select **All protocols** from the drop-down menu
     - **Source CIDR block:** Type `0.0.0.0/0`
     - **Destination CIDR block:** Type `0.0.0.0/0`
     - **Description:** Type a description for the rule

You can now start mirroring traffic from the VPC where the GWLBe was created. Repeat this procedure for all other VPCs you want to mirror traffic from.

(Optional) Mirror traffic from an alternate account

1. In the account you created the GWLB in, navigate to Endpoint Services in VPC.
2. Select the GWLB Endpoint Service you created.
3. Click the **Allow principals** tab.
4. Click **Allow principals**.

5. In the ARN field on the Allow principals page, enter the account you want to share the service with in the following format:

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

6. Navigate to the account you would like to mirror traffic from.
7. From the VPC dashboard, create a new endpoint with the following settings:
   - **Service category:** Select **Other endpoint services**
   - **Service name:** Type the service name you noted in the previous step and then click **Verify service**.
   - **VPC:** From the drop-down menu, select the VPC where you want to create the GWLBe.
   - **Subnets:** Select the availability zone and the subnet where you want to deploy the GWLBe.
8. In VPC, create a traffic mirror target with the following settings:
   - **Target type:** Select **Gateway Load Balancer Endpoint**
   - **Target:** Select the GWLBe you created
9. In VPC, create a traffic mirror filter with the following settings:
   - **Network services:** Select the **amazon-dns** checkbox
   - **Inbound rules:** Add a rule and complete the following fields:
     - **Number:** Type a number for the rule, such as 100
     - **Rule action:** Select **accept** from the drop-down list
     - **Protocol:** Select **All protocols** from the drop-down menu
     - **Source CIDR block:** Type `0.0.0.0/0`
     - **Destination CIDR block:** Type `0.0.0.0/0`
     - **Description:** Type a description for the rule

Repeat this procedure for all other VPCs you want to mirror traffic from.