Amazon Virtual Private Cloud

Traffic Mirroring

Amazon Virtual Private Cloud: Traffic Mirroring

Copyright © Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

Table of Contents

What is Traffic Mirroring?

Traffic Mirroring is an Amazon VPC feature that you can use to copy network traffic from an elastic network interface of type `interface`. You can then send the traffic to out-of-band security and monitoring appliances for:

- Content inspection
- Threat monitoring
- Troubleshooting

The security and monitoring appliances can be deployed as individual instances, or as a fleet of instances behind either a Network Load Balancer with a UDP listener or a Gateway Load Balancer with a UDP listener. Traffic Mirroring supports filters and packet truncation, so that you only extract the traffic of interest to monitor by using monitoring tools of your choice.

Traffic Mirroring concepts

The following are the key concepts for Traffic Mirroring:

- **Source** — The network interface to monitor.
- **Target** — The destination for mirrored traffic.
- **Filter** — A set of rules that defines the traffic that is copied in a traffic mirror session.
- **Session** — An entity that describes Traffic Mirroring from a source to a target using filters.

Working with Traffic Mirroring

You can create, access, and manage your traffic mirror resources using any of the following:

- **AWS Management Console**— Provides a web interface that you can use to access your traffic mirror resources.
- **AWS Command Line Interface (AWS CLI)** — Provides commands for a broad set of AWS services, including Amazon VPC. The AWS CLI is supported on Windows, macOS, and Linux. For more information, see AWS Command Line Interface.
- **AWS SDKs** — Provide language-specific APIs. The AWS SDKs take care of many of the connection details, such as calculating signatures, handling request retries, and handling errors. For more information, see AWS SDKs.
- **Query API**— Provides low-level API actions that you call using HTTPS requests. Using the Query API is the most direct way to access Amazon VPC. However, it requires that your application handle low-level details such as generating the hash to sign the request and handling errors. For more information, see the Amazon EC2 API Reference.

Traffic Mirroring benefits

Traffic Mirroring offers the following benefits:

- **Simplified operation** — Mirror any range of your VPC traffic without having to manage packet forwarding agents on your EC2 instances.
- **Enhanced security** — Capture packets at the elastic network interface, which cannot be disabled or tampered with from a user space.
- **Increased monitoring options** — Send your mirrored traffic to any security device.

Pricing

For information about pricing, see VPC pricing.

How Traffic Mirroring works

Traffic Mirroring copies inbound and outbound traffic from the network interfaces that are attached to your instances. You can send the mirrored traffic to the network interface of another instance, a Network Load Balancer that has a UDP listener, or a Gateway Load Balancer that has a UDP listener. The traffic mirror source and the traffic mirror target (monitoring appliance) can be in the same VPC. Or they can be in a different VPCs that are connected through intra-Region VPC peering, a transit gateway, or by a Gateway Load Balancer endpoint to connect to a Gateway Load Balancer in a different VPC.

Consider the following scenario, where you want to mirror traffic from two sources (Source A and Source B) to a single traffic mirror target (Target D). The following procedures are required:

- Identify the traffic mirror source (Source A)
- Identify the traffic mirror source (Source B)
- Configure the traffic mirror target (Target D)
- Configure the traffic mirror filter (Filter A)
- Configure the traffic mirror session for Source A, Filter A, and Target D
- Configure the traffic mirror session for Source B, Filter A, and Target D

After you create the traffic mirror session, any traffic that matches the filter rules is encapsulated in a VXLAN header. It is then sent to the target.

Contents

Architecture diagram

Consider the following scenario, where you want to mirror traffic from two sources (Source A and Source B) to a single traffic mirror target (Target D). After you create the traffic mirror session, any traffic that matches the filter rules is encapsulated in a VXLAN header. It is then sent to the target.

The following procedures are required:

- Identify the traffic mirror source (Source A)
- Identify the traffic mirror source (Source B)
- Configure the traffic mirror target (Target D)

- Configure the traffic mirror filter (Filter A)
- Configure the traffic mirror session for Source A, Filter A, and Target D
- Configure the traffic mirror session for Source B, Filter A, and Target D

Traffic mirror targets

A *traffic mirror target* is the destination for mirrored traffic. A traffic mirror target can be owned by an AWS account that is different from the traffic mirror source.

Use any of the following resources for a traffic mirror target:

- A network interface
- A Network Load Balancer
- Gateway Load Balancer endpoint

You can use a traffic mirror target in more than one traffic mirror session. Make sure to allow VXLAN traffic (UDP port 4789) from the traffic mirror source in the security groups that are associated with the traffic mirror target.

Traffic mirror target options

You can either use open-source tools or choose a monitoring solution available on AWS Marketplace. You can stream replicated traffic to any network packet collector or analytics tool, without having to install vendor-specific agents.

Network Load Balancer considerations

When the traffic mirror target is a Network Load Balancer, the following rules apply:

- There must be UDP listeners on port 4789.
- If all of the Network Load Balancer targets in an Availability Zone become unhealthy, the mirrored traffic can still be sent to traffic mirror targets in other zones. In this case, enable cross-zone load balancing to allow the Network Load Balancer to forward the mirrored traffic to a healthy target in another zone. For more information, see Availability Zones and load balancer nodes in the *Elastic Load Balancing User Guide*.
- For more information on Traffic Mirroring considerations, see Traffic Mirroring considerations (p. 36).

Gateway Load Balancer considerations

When the traffic mirror target is a Gateway Load Balancer endpoint the following rules apply:

- A listener for Gateway Load Balancers listens for all IP packets across all ports, and then forwards traffic to the target group you've chosen.
- If all of the Gateway Load Balancers in an Availability Zone become unhealthy, the mirrored traffic can still be sent to traffic mirror targets in other zones. In this case, cross-zone load balancing is used to allow the Gateway Load Balancer to forward the mirrored traffic to a healthy target in another zone. For more information, see Gateway Load Balancer target failure scenarios in the *User Guide for Gateway Load Balancers*.

- For more information on Traffic Mirroring considerations, see Traffic Mirroring considerations (p. 36).

Traffic mirror filters and filter rules

A *traffic mirror filter* is a set of inbound and outbound traffic rules that determine the traffic that is copied from the traffic mirror source and sent to the traffic mirror destination. By default, no traffic is mirrored. To mirror traffic, add traffic mirror rules to the filter. The combination of rules that you add define what traffic is mirrored. You can also choose to mirror certain network services traffic, including Amazon DNS. When you add network services traffic, all traffic (inbound and outbound) related to that network service is mirrored.

Traffic mirror filter rules define what traffic is mirrored. You define the parameters to apply to the traffic mirror source traffic to determine the traffic to mirror. The following traffic mirror filter rule parameters are available:

- Traffic direction (inbound or outbound)
- Action (accept or reject the packet)
- Protocol (L4 protocol)
- Source port range
- Destination port range
- Source CIDR block
- Destination CIDR block

Rules are evaluated from the lowest value to the highest value. The first rule that matches the traffic determines the action to take.

Traffic mirror sessions

A *traffic mirror session* establishes a relationship between a traffic mirror source and a traffic mirror target.

A traffic mirror session contains the following resources:

- A traffic mirror source
- A traffic mirror target
- A traffic mirror filter

The source is the network interface of type `interface` (for example, a network interface for an EC2 instance or an RDS instance). For more information, see *Limitations and quotas* (p. 41).

Each packet is mirrored once. However, you can use multiple traffic mirror sessions on the same source. This is useful if you want to send a subset of the mirrored traffic from a traffic mirror source to multiple tools. For example, you can filter HTTP traffic in a higher priority traffic mirror session and send it to a specific monitoring appliance. At the same time, you can filter all other TCP traffic in a lower priority traffic mirror session and send it to another monitoring appliance.

Traffic mirror sessions are evaluated based on the ascending session number that you define when you create the session.

Traffic mirror source and target connectivity options

The traffic mirror source and the traffic mirror target (monitoring appliance) can be in the same VPC, or different VPCs, connected using an intra-Region VPC peering connection or with a transit gateway using a Gateway Load Balancer endpoint to connect to a Gateway Load Balancer in a different VPC.

The traffic mirror target can be owned by an AWS account that is different from the traffic mirror source.

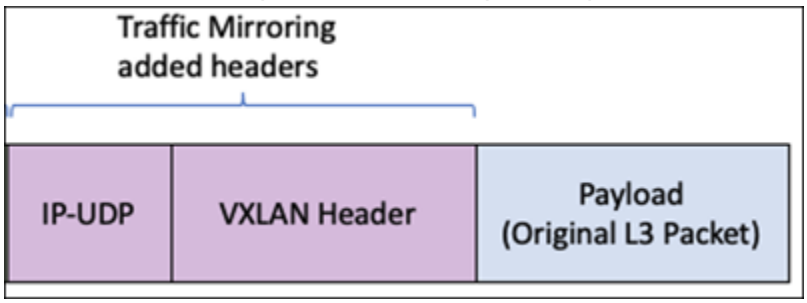
The mirrored traffic is sent to the traffic mirror target using the source VPC route table. Before you configure Traffic Mirroring, make sure that the traffic mirror source can route to the traffic mirror target.

The following table describes the available resource configurations.

Source owner	Source VPC	Target owner	Target VPC	Connectivity option
Account A	VPC 1	Account A	VPC1	No additional configuration
Account A	VPC 1	Account A	VPC 2	Intra-Region peering or a transit gateway or Gateway Load Balancer endpoint
Account A	VPC 1	Account B	VPC 2	Cross-account intra-Region peering connection, a transit gateway, or a Gateway Load Balancer endpoint
Account A	VPC 1	Account B	VPC 1	VPC sharing

Traffic Mirroring packet format

Mirrored traffic is encapsulated with a VXLAN header. All appliances that receive traffic directly with this feature should be able parse a VXLAN-encapsulated packet, as shown in the following example:

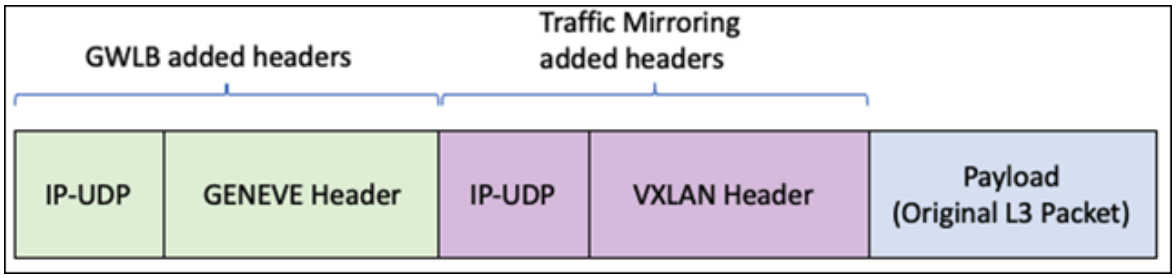


For more information about the VXLAN protocol, see RFC 7348.

The following fields apply to Traffic Mirroring:

- **VXLAN ID** — The virtual network ID that you can assign to a traffic mirror session. If you do not assign a value, we assign a random value that is unique to all sessions in the account.
- **Source IP address** — The primary IP address of the source network interface.
- **Destination IP address** — The primary IP address of the appliance, or the Network Load Balancer when the appliance is deployed behind one.

Appliances that received mirrored traffic through a Gateway Load Balancer should be able to parse both outer GENEVE encapsulation (from Gateway Load Balancer) and an inner VXLAN encapsulation (from VPC Traffic Mirroring) to retrieve the original L3 packet. The following shows an example:



Get started with Traffic Mirroring

The following tasks help you to become familiar with traffic mirror targets, filters, and sessions. Follow the instructions to create a traffic mirror target and filter, and then use those resources to create a session.

Tasks

Prerequisites

Review the Traffic Mirroring considerations. For more information, see *Considerations* (p. 36). Also verify the following.

- Make sure that the traffic mirror source and traffic mirror target are either:
  - In the same VPC, or
  - In different VPCs that are connected via VPC peering, a transit gateway, or a Gateway Load Balancer endpoint.
- The traffic mirror target instance must allow traffic to UDP port 4789.
- The traffic mirror source must have a route table entry for the traffic mirror target.
- Security group rules and network ACL rules on the traffic mirror target cannot drop the mirrored traffic from the traffic mirror source.

Step 1: Create the traffic mirror target

Create a destination for mirrored traffic.

Create a traffic mirror target

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the **Region** selector, choose the AWS Region that you used when you created the VPCs.
3. On the navigation pane, choose **Traffic Mirroring**, **Mirror Targets**.
4. Choose **Create traffic mirror target**.
5. (Optional) For **Name tag**, enter a name for the traffic mirror target.
6. (Optional) For **Description**, enter a description for the traffic mirror target.
7. For **Target type**, choose the traffic mirror target type.
8. For **Target**, choose the traffic mirror target.
9. (Optional) For each tag to add, choose **Add new tag** and enter the tag key and tag value.
10. Choose **Create**.

Step 2: Create the traffic mirror filter

A traffic mirror filter contains one or more traffic mirror rules, and a set of network services. The filters and rules that you add define the traffic that is mirrored.

To create a traffic mirror filter

1. On the navigation pane, choose **Traffic Mirroring**, **Mirror Filters**.
2. Choose **Create traffic mirror filter**.
3. (Optional For **Name tag**, enter a name for the traffic mirror filter.
4. (Optional) For **Description**, enter a description for the traffic mirror filter.
5. (Optional) Mirror network services.

   [Mirror Amazon DNS traffic] Select **amazon-dns**.
6. (Optional) For each inbound rule, choose **Inbound rules**, **Add rule**, and then specify the following information:

   - **Number**: Enter a priority to assign to the rule.
   - **Rule action**: Choose the action to take for the packet.
   - **Protocol**: Choose the L4 protocol to assign to the rule.
   - (Optional) **Source port range**: Enter the source port range.
   - (Optional) **Destination port range**: Enter the destination port range.
   - **Source CIDR block**: Enter a source CIDR block.
   - **Destination CIDR block**: Enter a destination CIDR block.
   - **Description**: Enter a description for the rule.
7. (Optional) For each outbound rule, choose **Outbound rules**, **Add rule**, and then specify the following information:

   - **Number**: Enter a priority to assign to the rule.
   - **Rule action**: Choose the action to take for the packet.
   - **Protocol**: Choose the IP protocol to assign to the rule.
   - (Optional) **Source port range**: Enter the source port range.
   - (Optional) **Destination port range**: Enter the destination port range.
   - **Source CIDR block**: Enter a source CIDR block.
   - **Destination CIDR block**: Enter a destination CIDR block.
   - **Description**: Enter a description for the rule.
8. (Optional) For each tag to add, choose **Add new tag** and enter the tag key and tag value.
9. Choose **Create**.

Step 3: Create the traffic mirror session

Create a traffic mirror session that sends mirrored packets from the source to a target so that you can monitor and analyze traffic.

To create a traffic mirror session

1. In the navigation pane, choose **Traffic Mirroring**, **Mirror Sessions**.
2. Choose **Create traffic mirror session**.
3. (Optional) For **Name tag**, enter a name for the traffic mirror session.

4. (Optional) For **Description**, enter a description for the traffic mirror session.
5. For **Mirror source**, choose the network interface of the instance that you want to monitor.
6. For **Mirror target**, choose the traffic mirror target.
7. For **Additional settings**, do the following:

   a. For **Session number**, enter the session number. The valid values are 1 to 32,766, where 1 is the highest priority.

      The session number determines the order that traffic mirror sessions are evaluated in both of the following situations:

      - When an interface is used by multiple sessions.
      - When an interface is used by different traffic mirror targets and traffic mirror filters.

      Traffic is only mirrored one time.

   b. (Optional) For **VNI**, enter the VXLAN ID to use for the traffic mirror session. For more information about the VXLAN protocol, see RFC 7348.

      If you do not enter a value, we assign a random unused number.

   c. (Optional) For **Packet Length**, enter the number of bytes in each packet to mirror.

      If you do not want to mirror the entire packet, set **Packet Length** to the number of bytes in each packet to mirror. For example, if you set this value to 100, the first 100 bytes after the VXLAN header that meet the filter criteria are copied to the target.

      To mirror the entire packet, do not enter a value in this field.

   d. For **Filter**, choose the traffic mirror filter that determines what traffic gets mirrored.
8. (Optional) For each tag to add, choose **Add new tag** and enter the tag key and tag value.
9. Choose **Create**.

Step 4: Analyze the data

After the mirrored traffic is on the traffic mirror target, you can use a tool from the AWS Partner Network to analyze the data.

Traffic Mirroring examples

The following are common use cases for Traffic Mirroring.

- Mirror inbound TCP traffic to a single appliance (p. 11)
- Mirror inbound TCP and UDP traffic to multiple appliances (p. 12)
- Mirror non-local VPC traffic (p. 15)
- To mirror traffic from multiple network interfaces, see VPC Traffic Mirroring Source Automation Application on github.

Example: Mirror inbound TCP traffic to a single monitoring appliance

Consider the scenario where you want to mirror inbound TCP traffic on an instance, and send it to a single monitoring appliance. You need the following traffic mirror resources for this example:

- A traffic mirror target for the appliance (Target A)
- A traffic mirror filter with a traffic mirror rule for the TCP inbound traffic (Filter 1)
- A traffic mirror session that has the following:
  - A traffic mirror source
  - A traffic mirror target for the appliance
  - A traffic mirror filter with a traffic mirror rule for the TCP inbound traffic

Step 1: Create a traffic mirror target

Create a traffic mirror target (Target A) for the monitoring appliance. Depending on your configuration, the target is one of the following types:

- The network interface of the monitoring appliance
- The Network Load Balancer when the appliance is deployed behind one
- The Gateway Load Balancer endpoint when the appliance is deployed behind a Gateway Load Balancer

For more information, see the section called “Create a traffic mirror target” (p. 21).

Step 2: Create a traffic mirror filter

Create a traffic mirror filter (Filter 1) that has the following inbound rule. For more information, see the section called “Create a traffic mirror filter” (p. 24).

Traffic mirror filter rule for inbound TCP traffic

Option	Value
Rule action	Accept
Protocol	TCP
Source port range	

Option	Value
Destination port range	
Source CIDR block	0.0.0.0/0
Destination CIDR block	0.0.0.0/0
Description	TCP Rule

Step 3: Create a traffic mirror session

Create and configure a traffic mirror session with the following options. For more information, see the section called "Create a traffic mirror session" (p. 27).

Traffic mirror session to monitor inbound TCP traffic

Option	Value
Mirror source	The network interface of the instance that you want to monitor.
Mirror target	Target A
Filter	Filter 1

Example: Mirror inbound TCP and UDP traffic to multiple appliances

Consider the scenario where you want to mirror inbound TCP and UDP traffic on an instance. But you want to send the TCP traffic to one appliance (Appliance A), and the UDP traffic to a second appliance (Appliance B). You need the following traffic mirror entities for this example:

- A traffic mirror target for Appliance A (Target A)
- A traffic mirror target for Appliance B (Target B)
- A traffic mirror filter with a traffic mirror rule for the TCP inbound traffic (Filter 1)
- A traffic mirror filter with a traffic mirror rule for the UDP inbound traffic (Filter 2)
- A traffic mirror session that has the following:
  - A traffic mirror source
  - A traffic mirror target (Target A) for Appliance A
  - A traffic mirror filter (Filter 1) with a traffic mirror rule for the TCP inbound traffic
- A traffic mirror session that has the following:
  - A traffic mirror source
  - A traffic mirror target (Target B) for Appliance B
  - A traffic mirror filter (Filter 2) with a traffic mirror rule for the UDP inbound traffic

Step 1: Create a traffic mirror target for appliance a

Create a traffic mirror target for Appliance A (Target A). Depending on your configuration, the target is one of the following types:

- The network interface of the monitoring appliance
- The Network Load Balancer when the appliance is deployed behind one
- The Gateway Load Balancer endpoint when the appliance is deployed behind a Gateway Load Balancer

For more information, see the section called “Create a traffic mirror target” (p. 21).

Step 2: Create a traffic mirror target for appliance b

Create a traffic mirror target (Target B) for Appliance B. Depending on your configuration, the target is one of the following types:

- The network interface of the monitoring appliance
- The Network Load Balancer when the appliance is deployed behind one
- The Gateway Load Balancer endpoint when the appliance is deployed behind a Gateway Load Balancer

For more information, see the section called “Create a traffic mirror target” (p. 21).

Step 3: Create a traffic mirror filter with a rule for TCP traffic

Create a traffic mirror filter (Filter 1) with the following inbound rule for TCP traffic. For more information, see the section called “Create a traffic mirror filter” (p. 24)

Traffic mirror filter rule for inbound TCP traffic

Option	Value
Rule action	Accept
Protocol	TCP
Source port range	
Destination port range	
Source CIDR block	0.0.0.0/0
Destination CIDR block	0.0.0.0/0
Description	TCP Rule

Step 4: Create a traffic mirror filter with a rule for UDP traffic

Create a traffic mirror filter (Filter 2) with the following inbound rule for UDP traffic. For more information, see the section called “Create a traffic mirror filter” (p. 24)

Traffic mirror filter rule for inbound UDP traffic

Option	Value
Rule action	Accept

Option	Value
Protocol	UDP
Source port range	
Destination port range	
Source CIDR block	0.0.0.0/0
Destination CIDR block	0.0.0.0/0
Description	UDP Rule

Step 5: Create a traffic mirror session for the TCP traffic

Create and configure a traffic mirror session with the following options. For more information, see the section called "Create a traffic mirror session" (p. 27).

Traffic mirror session to monitor inbound TCP traffic

Option	Value
Mirror source	The network interface of the instance that you want to monitor.
Mirror target	Target A
Filter	Filter 1
Session number	1

Step 6: Create a traffic mirror session for the UDP traffic

Create and configure a traffic mirror session with the following options. For more information, see the section called "Create a traffic mirror session" (p. 27).

Traffic mirror session to monitor inbound UDP traffic

Option	Value
Mirror source	The network interface of the instance that you want to monitor.
Mirror target	Target B
Filter	Filter 2
Session number	2

Example: Mirror non-local VPC traffic

Consider the scenario where you want to monitor traffic leaving your VPC or traffic whose source is outside your VPC. In this case, you will mirror all traffic except traffic passing within your VPC and send it to a single monitoring appliance. You need the following traffic mirror resources:

- A traffic mirror target for the appliance (Target A)
- A traffic mirror filter that has two sets of rules for outbound and inbound traffic. For outbound traffic, it will reject all packets which have a destination IP in the VPC CIDR block and accept all other outbound packets. For inbound traffic, it will reject all packets which have a source IP in the VPC CIDR block and accept all other inbound packets.
- A traffic mirror session that has the following:
  - A traffic mirror source
  - A traffic mirror target for the appliance (Target A)
  - A traffic mirror filter with a traffic mirror rule for the TCP inbound traffic (Filter F)

In this example, the VPC CIDR block is 10.0.0.0/16.

Step 1: Create a traffic mirror target

Create a traffic mirror target (Target A) for the monitoring appliance. Depending on your configuration, the target is one of the following types:

- The network interface of the monitoring appliance
- The Network Load Balancer when the appliance is deployed behind one
- The Gateway Load Balancer endpoint when the appliance is deployed behind a Gateway Load Balancer

For more information, see the section called “Create a traffic mirror target” (p. 21).

Step 2: Create a traffic mirror filter

Create a traffic mirror filter (Filter F) that has the following rules. For more information, see the section called “Create a traffic mirror filter” (p. 24).

Outbound traffic mirror filter rules

Create the following outbound rules:

- Reject all outbound packets which have a destination IP in the VPC CIDR block
- Accept all other outbound packets (destination CIDR block 0.0.0.0/0)

Option	Value
Rule number	10
Rule action	Reject
Protocol	All
Source port range	
Destination port range	

Option	Value
Source CIDR block	0.0.0.0/0
Destination CIDR block	10.0.0.0/16
Description	Reject all intra-VPC traffic

Option	Value
Rule number	20
Rule action	Accept
Protocol	All
Source port range	
Destination port range	
Source CIDR block	0.0.0.0/0
Destination CIDR block	0.0.0.0/0
Description	Accept all outbound traffic

Inbound traffic mirror filter rules

Create the following inbound rules:

- Reject all inbound packets which have a source IP in the VPC CIDR block
- Accept all other inbound packets (source CIDR block 0.0.0.0/0)

Option	Value
Rule number	10
Rule action	Reject
Protocol	All
Source port range	
Destination port range	
Source CIDR block	10.0.0.0/16
Destination CIDR block	0.0.0.0/0
Description	Reject all intra-VPC traffic

Option	Value
Rule number	20

Option	Value
Rule action	Accept
Protocol	All
Source port range	
Destination port range	
Source CIDR block	0.0.0.0/0
Destination CIDR block	0.0.0.0/0
Description	Accept all inbound traffic

Step 3: Create a traffic mirror session

Create and configure a traffic mirror session with the following options. For more information, see the section called "Create a traffic mirror session" (p. 27).

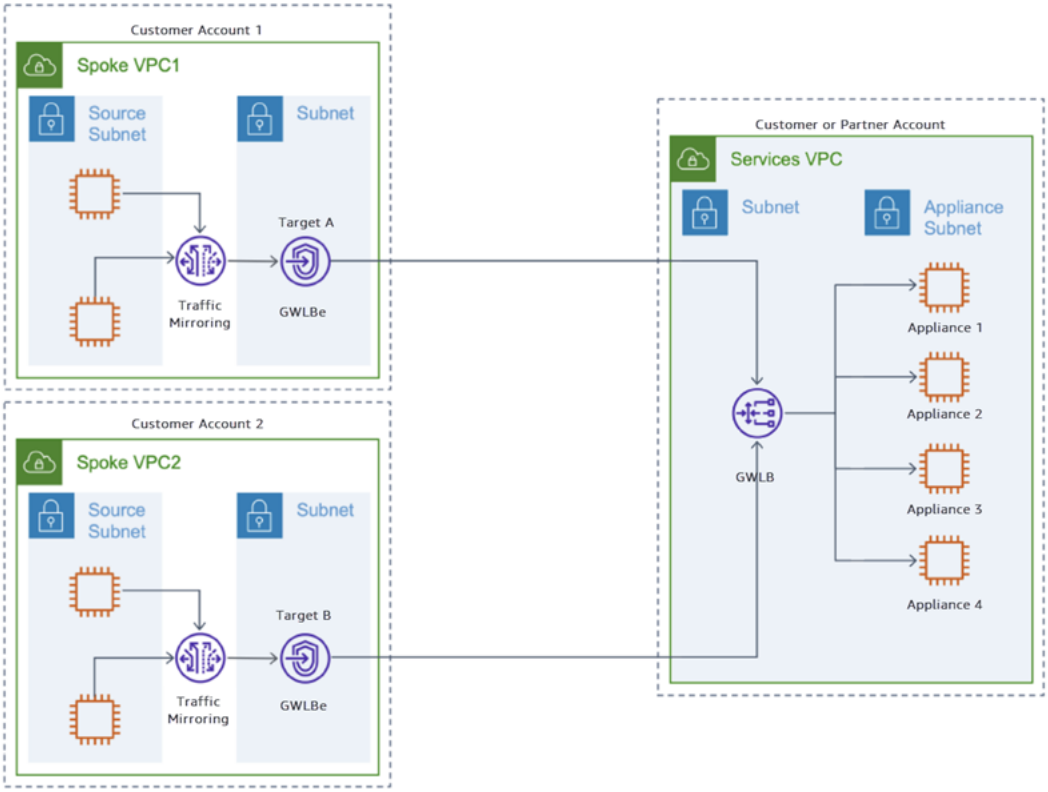
Traffic mirror session to monitor inbound TCP traffic

Option	Value
Mirror source	The network interface of the instance that you want to monitor.
Mirror target	Target A
Filter	Filter F

Example: Mirror traffic to appliances behind a Gateway Load Balancer via Gateway Load Balancer endpoints

You can deploy a Gateway Load Balancer (GWLB) and Gateway Load Balancer endpoint (GWLBe) to securely send mirror traffic across VPC and accounts. The GWLBe is a VPC endpoint that provides private connectivity between VPC with the mirror sources and the monitoring appliances deployed behind the GWLB.

The following diagram shows a deployment of a GWLB for traffic mirroring utilizing GWLBe interfaces. The GWLB is deployed in a centralized Service VPC with multiple appliances as targets. The GWLB is set up for each Availability Zone that the customer wants to monitor traffic, and it can configure their GWLB with cross-zone load balancing as an option to protect against single Availability Zone failures. In the spoke VPCs, GWLBe interfaces are deployed in each spoke VPC. These endpoints are connected to the GWLB to send traffic from the spoke VPC to the Service VPC.



Consider the scenario where you want to mirror inbound TCP traffic on an instance and then send it to a Gateway Load Balancer via a Gateway Load Balancer endpoint. You need the following Traffic Mirroring entities for this example:

- A Traffic Mirroring target for the Gateway Load Balancer endpoint (Target A) in Spoke VPC1
- A Traffic Mirroring target for the Gateway Load Balancer endpoint (Target B) in Spoke VPC2
- A Traffic Mirroring filter with a Traffic Mirroring rule for the TCP inbound traffic (Filter 1) for the Gateway Load Balancer endpoint
- A Traffic Mirroring session for Spoke VPC1 that has the following:
  - A Traffic Mirroring source
  - A Traffic Mirroring target (Target A) for the Gateway Load Balancer endpoint
  - A Traffic Mirroring filter (Filter 1) with a Traffic Mirroring rule for the TCP inbound traffic
- A Traffic Mirroring session for Spoke VPC2 that has the following:
  - A Traffic Mirroring source
  - A Traffic Mirroring target (Target B) for the Gateway Load Balancer endpoint
  - A Traffic Mirroring filter (Filter 1) with a Traffic Mirroring rule for the TCP inbound traffic

Step 1: Create a traffic mirror target in Spoke VPC1

Create a traffic mirror target (Target A) for the Gateway Load Balancer endpoint in Spoke VPC1. For more information, see Create a traffic mirror target (p. 21).

The Gateway Load Balancer endpoint will be the target when the monitoring appliances are deployed behind a Gateway Load Balancer.

Step 2: Create a traffic mirror target in Spoke VPC2

Create a traffic mirror target (Target B) for the Gateway Load Balancer endpoint in Spoke VPC1. For more information, see Create a traffic mirror target (p. 21).

The Gateway Load Balancer endpoint will be the target when the monitoring appliances are deployed behind a Gateway Load Balancer.

Step 3: Create a traffic mirror filter rule

Create a traffic mirror filter (Filter 1) that has the following inbound rule. For more information on creating a filter, see Create a traffic mirror filter (p. 24).

Traffic mirror filter rule for inbound TCP traffic

Option	Value
Rule action	Accept
Protocol	TCP
Source port range	
Destination port range	
Source CIDR block	0.0.0.0/0
Destination CIDR block	0.0.0.0/0
Description	TCP Rule

Step 4: Create a traffic mirror session in Spoke VPC1

Create and configure a traffic mirror session with the following options. For more information, see the section called “Create a traffic mirror session” (p. 27).

Traffic mirror session to monitor inbound TCP traffic for Spoke VPC1

Option	Value
Mirror source	The network interface of the instance that you want to monitor.
Mirror target	Target A
Filter	Filter 1

Step 5: Create a traffic mirror session in Spoke VPC2

Create and configure a traffic mirror session with the following options. For more information, see the section called “Create a traffic mirror session” (p. 27).

Traffic mirror session to monitor inbound TCP traffic for Spoke VPC2

Option	Value
Mirror source	The network interface of the instance that you want to monitor.
Mirror target	Target B
Filter	Filter 1

Work with Traffic Mirroring

You can work with traffic mirror targets, sessions, and filters by using the Amazon VPC console or the AWS CLI.

Contents

Traffic mirror targets

A target is the destination for a traffic mirror session.

The traffic mirror target can be an elastic network interface, a Network Load Balancer, or a Gateway Load Balancer endpoint. After you create a target, assign it to a traffic mirror session. For more information, see the section called “Create a traffic mirror session” (p. 27).

You must configure a security group for the traffic mirror target that allows VXLAN traffic from the source to the target.

You can share a traffic mirror target across accounts. To share a traffic mirror target, create the target, and then share the target. For more information, see the section called “Share a traffic mirror target” (p. 23).

Create a traffic mirror target

Create a destination for mirrored traffic.

To create a traffic mirror target using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the **Region** selector, choose the AWS Region that you used when you created the VPCs.
3. On the navigation pane, choose **Traffic Mirroring**, **Mirror Targets**.
4. Choose **Create traffic mirror target**.
5. (Optional) For **Name tag**, enter a name for the traffic mirror target.
6. (Optional) For **Description**, enter a description for the traffic mirror target.
7. For **Target type**, choose the traffic mirror target type.
8. For **Target**, choose the traffic mirror target.
9. (Optional) For each tag to add, choose **Add new tag** and enter the tag key and tag value.
10. Choose **Create**.

To create a traffic mirror target using the AWS CLI

Use the create-traffic-mirror-target command.

View traffic mirror target details

View the traffic mirror target details.

To view your traffic mirror targets using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Traffic Mirroring**, **Mirror Targets**.
3. Select the ID of the traffic mirror target to open its details page.

To view your traffic mirror targets using the AWS CLI

Use the describe-traffic-mirror-targets command.

Modify traffic mirror target tags

Add a tag to the traffic mirror target, or remove a tag from the traffic mirror target.

To modify your traffic mirror target tags using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Traffic Mirroring**, **Mirror Targets**.
3. Select the ID of the traffic mirror target to open its details page.
4. On the **Tags** tab, choose **Manage tags**.
5. (Optional) For each tag to add, choose **Add new tag** and enter the tag key and tag value. For each tag to remove, choose **Remove**.
6. Choose **Save**.

To modify your traffic mirror target tags using the AWS CLI

Use the create-tags command to add a tag. Use the delete-tags command to remove a tag.

Delete a traffic mirror target

Before you delete a traffic mirror target, pause all traffic mirror sessions that use the traffic mirror target.

To delete your traffic mirror target using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Traffic Mirroring**, **Mirror Targets**.
3. Select the traffic mirror target.
4. Choose **Delete**.
5. When prompted for confirmation, enter **`delete`**, and then choose **Delete**.

To delete a traffic mirror target using the AWS CLI

Use the delete-traffic-mirror-target command.

Cross-account traffic mirror targets

A traffic mirror target can be owned by an AWS account that is different from the traffic mirror source.

Before you can use a cross-account traffic mirror target, the traffic mirror target owner shares the target with you by using the AWS Resource Access Manager. When you are in different AWS Organizations from the owner, after the owner shares the traffic mirror target, you accept the share request. After you accept the share request, you can use the traffic mirror target in a traffic mirror session.

The traffic mirror target is visible to shared accounts in their `DescribeTrafficMirrorTarget` API calls. Only the traffic mirror target owner can modify or delete the traffic mirror target.

Traffic mirror sessions that are created in a different account than the traffic mirror target are visible in `DescribeTrafficMirrorSession` API calls that are made by the traffic mirror target owner.

Share a traffic mirror target

You can use AWS Resource Access Manager (RAM) to share a traffic mirror target across accounts. Use the following procedure to share a traffic mirror target that you own.

You must create a traffic mirror target before you share it. For more information, see the section called "Create a traffic mirror target" (p. 21).

To share a traffic mirror target

1. Open the AWS Resource Access Manager console at https://console.aws.amazon.com/ram/.
2. Choose **Create a resource share**.
3. Under **Description**, for **Name**, enter a descriptive name for the resource share.
4. For **Select resource type**, choose **Traffic Mirror Targets**. Select the traffic mirror target.
5. For **Principals**, add principals to the resource share. For each AWS account, OU, or organization, specify its ID and choose **Add**.

   For **Allow external accounts**, choose whether to allow sharing for this resource with AWS accounts that are external to your organization.
6. (Optional) Under **Tags**, enter a tag key and tag value pair for each tag. These tags are applied to the resource share but not to the traffic mirror target.
7. Choose **Create resource share**.

Accept a resource share

If you are in different AWS Organizations from the share owner, you must accept the resource share before you can access the shared resources.

To accept a resource share

1. Open the AWS Resource Access Manager console at https://console.aws.amazon.com/ram/.
2. On the navigation pane, choose **Shared with me**, **Resource shares**.
3. Select the resource share.
4. Choose **Accept resource share**.
5. To view the shared traffic mirror target, open the **Traffic Mirror Targets** page in the Amazon VPC console.

Delete a resource share

You can delete a resource share at any time. When you delete a resource share, all principals that are associated with the resource share lose access to the shared resources. Deleting a resource share does not delete the shared resources.

When you delete a shared traffic mirror target that is in use, the traffic mirror session becomes inactive.

To delete a resource share

1. Open the AWS Resource Access Manager console at https://console.aws.amazon.com/ram/.
2. On the navigation pane, choose **Shared by me**, **Resource shares**.
3. Select the resource share.

   Be sure to select the correct resource share. You cannot recover a resource share after you delete it.
4. Choose **Delete**.
5. In the **Delete confirmation** dialog box, enter **delete**, and then choose **Delete**.

Traffic mirror filters

Use a traffic mirror filter and its rules to determine the traffic that is mirrored. A traffic mirror filter contains one or more traffic mirror rules. You can also mirror certain network services.

You can define a set of parameters to apply to the traffic mirror source traffic to determine the traffic to mirror. The following traffic mirror filter rule parameters are available:

- Traffic direction: Inbound or outbound
- Action: The action to take, either to accept or reject the packet
- Protocol: The L4 protocol
- Source port range
- Destination port range
- Source CIDR block
- Destination CIDR block

Rules are evaluated from the lowest value to the highest value. The first rule that matches the traffic determines the action to take.

Create a traffic mirror filter

Create a traffic mirror filter.

Create a traffic mirror filter and add rules to the filter to define the traffic that is mirrored. A traffic mirror filter contains one or more traffic mirror rules, and a set of network services.

The **Source CIDR block** and **Destination CIDR block** values must both be either an IPv4 range or an IPv6 range.

To create a traffic mirror filter using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the **Region** selector, choose the AWS Region that you used when you created the VPCs.
3. On the navigation pane, choose **Traffic Mirroring**, **Mirror Filters**.
4. Choose **Create traffic mirror filter**.
5. (Optional) For **Name tag**, enter a name for the traffic mirror filter.
6. (Optional) For **Description**, enter a description for the traffic mirror filter.
7. (Optional) Mirror network services.

   [Mirror Amazon DNS traffic] Select **amazon-dns**.
8. (Optional) For each inbound rule, choose **Inbound rules**, **Add rule**, and then specify the following information:

- **Number**: Enter a priority to assign to the rule.
- **Rule action**: Choose the action to take for the packet.
- **Protocol**: Choose the L4 protocol to assign to the rule.
- (Optional) **Source port range**: Enter the source port range.
- (Optional) **Destination port range**: Enter the destination port range.
- **Source CIDR block**: Enter a source CIDR block.
- **Destination CIDR block**: Enter a destination CIDR block.
- **Description**: Enter a description for the rule.

9. (Optional) Add outbound rules. Choose **Outbound rules**, **Add, rule**, and then specify the following information about the traffic mirror source outbound traffic:

   - **Number**: Enter a priority to assign to the rule.
   - **Rule action**: Choose the action to take for the packet.
   - **Protocol**: Choose the IP protocol to assign to the rule.
   - (Optional) **Source port range**: Enter the source port range.
   - (Optional) **Destination port range**: Enter the destination port range.
   - **Source CIDR block**: Enter a source CIDR block.
   - **Destination CIDR block**: Enter a destination CIDR block.
   - **Description**: Enter a description for the rule.

10. (Optional) For each tag to add, choose **Add new tag** and enter the tag key and tag value.
11. Choose **Create**.

To create a traffic mirror filter using the AWS CLI

Use the create-traffic-mirror-filter command.

View your traffic mirror filters

To view your traffic mirror filters using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Traffic Mirroring**, **Mirror Filters**.
3. Select the ID of the traffic mirror filter to open its details page.

To view your traffic mirror filters using the AWS CLI

Use the describe-traffic-mirror-filters command.

Modify your traffic mirror filter rules

Add or remove inbound and outbound traffic mirror filter rules.

The **Source CIDR block** and **Destination CIDR block** values must both be either an IPv4 range or an IPv6 range.

To modify your traffic mirror filter using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Traffic Mirroring**, **Mirror Filters**.
3. Select the ID of the traffic mirror filter to open its details page.

4. To add inbound rules, choose **Inbound rules** , **Add inbound rule**. Specify the following information, and then choose **Add rule**:

   - **Rule number**: Enter a priority to assign to the rule.
   - (Optional **Description**: Enter a description for the rule.
   - **Rule action**: Choose the action to take for the packet.
   - **Protocol**: Choose the L4 protocol to assign to the rule.
   - (Optional) **Source port range**: Enter the source port range.
   - (Optional) **Destination port range**: Enter the destination port range.
   - **Source CIDR block**: Enter a source CIDR block.
   - **Destination CIDR block**: Enter a destination CIDR block.
5. To add outbound rules, choose **Outbound rules** , **Add outbound rule**. Specify the following information, and then choose **Add rule**:

   - **Rule number**: Enter a priority to assign to the rule.
   - (Optional) **Description**: Enter a description for the rule.
   - **Rule action**: Choose the action to take for the packet.
   - **Protocol**: Choose the IP protocol to assign to the rule.
   - (Optional) **Source port range**: Enter the source port range.
   - (Optional) **Destination port range**: Enter the destination port range.
   - **Source CIDR block**: Enter a source CIDR block.
   - **Destination CIDR block**: Enter a destination CIDR block.
6. To modify a rule, choose **Inbound rules** or **Outbound rules**. Select the rule and choose **Modify inbound rule** or **Modify outbound rule**. Update the rule as needed, and then choose **Modify rule**.
7. To delete a rule, choose **Inbound rules** or **Outbound rules**. Select the rule and choose **Delete**. When prompted for confirmation, enter **`delete`**, and then choose **Delete**.

Modify traffic mirror filter tags

To modify your traffic mirror filters using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Traffic Mirroring**, **Mirror Filters**.
3. Select the ID of the traffic mirror filter to open its details page.
4. From the **Tags** tab, choose**Manage tags**.
5. For each tag to add, choose **Add new tag** and enter the tag key and tag value.
6. For each tag to remove, choose **Remove**.
7. Choose **Save**.

To modify the traffic mirror filter tags using the AWS CLI

Use the create-tags command to add a tag. Use the delete-tags command to remove a tag.

Modify traffic mirror filter network services

To modify your traffic mirror filter network services using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Traffic Mirroring**, **Mirror Filters**.

3. Select the traffic mirror filter.
4. Choose **Actions**, **Modify Network Services**.
5. [Mirror Amazon DNS traffic] Select **amazon dns**.
6. Choose **Modify**.

To modify the network services traffic mirror filters using the AWS CLI

Use the modify-traffic-mirror-filter-network-services command.

Delete a traffic mirror filter

To delete a traffic mirror filter using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Traffic Mirroring**, **Mirror Filters**.
3. Select the traffic mirror filter, and then choose **Actions**, **Delete**.
4. When prompted for confirmation, enter **`delete`**, and then choose **Delete**.

To delete a traffic mirror filter using the AWS CLI

Use the delete-traffic-mirror-filter command.

Traffic mirror sessions

A traffic mirror session establishes a relationship between a traffic mirror source and a traffic mirror target. A traffic mirror session contains the following resources:

- A traffic mirror source
- A traffic mirror target (p. 21)
- A traffic mirror filter (p. 24)

The source is the network interface of type `interface` (for example, the network interface for an EC2 instance or an RDS instance). For more information, see *Limitations and quotas* (p. 41).

Each packet is mirrored once. However, you can use multiple traffic mirror sessions on the same source. This is useful if you want to send a subset of the mirrored traffic from a traffic mirror source to multiple tools. For example, you can filter HTTP traffic in a higher priority traffic mirror session and send it to a specific monitoring appliance. At the same time, you can filter all other TCP traffic in a lower priority traffic mirror session and send it to another monitoring appliance.

Traffic mirror sessions are evaluated based on the ascending priority that you define when you create the session.

Create a traffic mirror session

Create a traffic mirror session.

Before you create a traffic mirror session, make sure that you have the following information:

- The network interface for the source. The network interface type must be `instance`.
- The traffic mirror target
  - To use a target in your account, see the section called “Create a traffic mirror target” (p. 21).

  - To use a target that is owned by another account and shared with you, accept the shared resource before you create the traffic mirror session. For more information, see the section called "Accept a resource share" (p. 23).
- The traffic mirror filter (for more information, see the section called "Create a traffic mirror filter" (p. 24))

To create a traffic mirror session using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the **Region** selector, choose the AWS Region that you used when you created the VPCs.
3. In the navigation pane, choose **Traffic Mirroring**, **Mirror Sessions**.
4. Choose **Create traffic mirror session**.
5. (Optional) For **Name tag**, enter a name for the traffic mirror session.
6. (Optional) For **Description**, enter a description for the traffic mirror session.
7. For **Mirror source**, choose the network interface of the instance that you want to monitor.
8. For **Mirror target**, choose the traffic mirror target or create one. For more information, see the section called "Create a traffic mirror target" (p. 21).
9. For **Additional settings**, do the following:

   a. For **Session number**, enter the session number. The valid values are 1 to 32,766, where 1 is the highest priority.

      The session number determines the order that traffic mirror sessions are evaluated when an interface is used by multiple sessions that have the same interface, but have different traffic mirror targets and traffic mirror filters. Traffic is only mirrored one time.

   b. (Optional) For **VNI**, enter the VXLAN ID to use for the traffic mirror session. For more information about the VXLAN protocol, see RFC 7348.

      If you do not enter a value, we assign a random number.

   c. (Optional) For **Packet Length**, enter the number of bytes in each packet to mirror.

      If you do not want to mirror the entire packet, set **Packet Length** to the number of bytes in each packet to mirror. For example, if you set this value to 100, the first 100 bytes after the VXLAN header that meet the filter criteria are copied to the target.

      To mirror the entire packet, do not enter a value in this field.

   d. For **Filter**, choose the traffic mirror filter that determines what traffic gets mirrored.

      To create a filter, choose **Create filter**. For more information, see the section called "Step 2: Create the traffic mirror filter" (p. 9).
10. (Optional) For each tag to add, choose **Add new tag** and enter the tag key and tag value.
11. Choose **Create**.

To create a traffic mirror session using the AWS CLI

Use the create-traffic-mirror-session command.

View your traffic mirror sessions

To view your traffic mirror sessions using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.

2. In the navigation pane, choose **Traffic Mirroring**, **Mirror Sessions**.
3. Select the ID of the traffic mirror session to open its details page.

To view your traffic mirror session using the AWS CLI

Use the describe-traffic-mirror-sessions command.

Modify your traffic mirror session

To modify your traffic mirror session using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **Traffic Mirroring**, **Mirror Sessions**.
3. Select the traffic mirror session.
4. Choose **Actions**, **Modify session**.
5. (Optional) For **Description**, enter a description for the traffic mirror session.
6. For **Mirror target**, choose the traffic mirror target.

   To create a target, choose **Create target**. For more information, see the section called "Create a traffic mirror target" (p. 21).
7. For **Additional settings**, do the following:

   a. For **Session number**, enter the session number. The session number determines the order that traffic mirror sessions are evaluated. The valid values are 1 to 32,766, where 1 is the highest priority.

   b. (Optional) For **VNI**, enter the VXLAN ID to use for the traffic mirror session. For more information about the VXLAN protocol, see RFC 7348.

      If you do not enter a value, we assign a random unused number.

   c. (Optional) For **Packet Length**, enter the number of bytes in each packet to mirror.

      If you do not want to mirror the entire packet, set **Packet Length** to the number of bytes in each packet to mirror. For example, if you set this value to 100, the first 100 bytes after the VXLAN header that meet the filter criteria are copied to the target.

      To mirror the entire packet, do not enter a value in this field.

   d. For **Filter**, choose the traffic mirror filter that determines what traffic gets mirrored.
8. Choose **Modify**.

To modify your traffic mirror session using the AWS CLI

Use the modify-traffic-mirror-session command.

Modify traffic mirror session tags

To modify your traffic mirror session tags using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **Traffic Mirroring**, **Mirror Sessions**.
3. Select the ID of the traffic mirror session to open its details page.
4. On the **Tags** tab, choose **Manage tags**.

5. (Optional) For each tag to add, choose **Add new tag** and enter the tag key and tag value. For each tag to remove, choose **Remove**.
6. Choose **Modify**.

To modify your traffic mirror session using the AWS CLI

Use the create-tags command to add a tag. Use the delete-tags command to remove a tag.

Delete a traffic mirror session

To delete your traffic mirror session using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Traffic Mirroring**, **Mirror Sessions**.
3. Select the traffic mirror session, and then choose **Actions**, **Delete**.
4. When prompted for confirmation, enter **`delete`**, and then choose **Delete**.

To delete a traffic mirror session using the AWS CLI

Use the delete-traffic-mirror-session command.

Work with open-source tools for Traffic Mirroring

You can use open-source tools to monitor network traffic from Amazon EC2 instances. The following tools work with Traffic Mirroring:

- **Zeek** — For more information, see the Zeek Network Monitor Security website.
- **Suricata** — For more information see the Suricata website.

These open-source tools support VXLAN decapsulation, and they can be used at scale to monitor VPC traffic. For information about how Zeek handles VXLAN support and to download the code, see Zeek vxlan on the GitHub website. For information about how Suricata handles VXLAN support and to download the code, see Suricata on the GitHub website.

The following example uses the Suricata open-source tool. You can follow similar steps for Zeek.

Consider the scenario where you want to mirror inbound TCP traffic on an instance and send the traffic to an instance that has the Suricata software installed. You need the following traffic mirror entities for this example:

- An EC2 instance with the Suricata software installed on it
- A traffic mirror target for the EC2 instance (Target A)
- A traffic mirror filter with a traffic mirror rule for the TCP inbound traffic (Filter rule 1)
- A traffic mirror session that has the following:
  - A traffic mirror source
  - A traffic mirror target for the appliance
  - A traffic mirror filter with a traffic mirror rule for the TCP inbound traffic

Step 1: Install the Suricata software on the EC2 instance target

Launch an EC2 instance, and then install the Suricata software on it by using the following commands.

```
# Become sudo
sudo -s
# Install epel-release
amazon-linux-extras install -y epel
# Install suricata
yum install -y suricata
# Create the default suricata rules directory
mkdir /var/lib/suricata/rules
# Add a rule to match all UDP traffic
echo 'alert udp any any -> any any (msg:"UDP traffic detected"; sid:200001; rev:1;)' > /
var/lib/suricata/rules/suricata.rules
# Start suricata listening on eth0 in daemon mode
suricata -c /etc/suricata/suricata.yaml -k none -i eth0 -D

# Capture logs can be found in /var/log/suricata/fast.log
```

Step 2: Create a traffic mirror target

Create a traffic mirror target (Target A) for the EC2 instance. Depending on your configuration, the target is one of the following types:

- The network interface of the monitoring appliance
- The Network Load Balancer when the appliance is deployed behind one.
- The Gateway Load Balancer endpoint when the appliance is deployed behind a Gateway Load Balancer

For more information, see the section called “Create a traffic mirror target” (p. 21).

Step 3: Create a traffic mirror filter

Create a traffic mirror filter (Filter 1) with the following inbound rule. For more information, see the section called “Create a traffic mirror filter” (p. 24).

Traffic mirror filter rule for inbound TCP traffic

Option	Value
Rule action	Accept
Protocol	TCP
Source port range	
Destination port range	
Source CIDR block	0.0.0.0/0
Destination CIDR block	0.0.0.0/0
Description	TCP Rule

Step 4: Create a traffic mirror session

Create and configure a traffic mirror session with the following options. For more information, see the section called “Create a traffic mirror session” (p. 27).

Traffic mirror session to monitor inbound TCP traffic

Option	Value
Mirror source	The network interface of the instance that you want to monitor.
Mirror target	Target A
Filter	Filter 1

Monitor mirrored traffic using Amazon CloudWatch

You can monitor your mirrored traffic using Amazon CloudWatch, which collects information from your network interface that is part of a traffic mirror session, and creates readable, near real-time metrics. You can use this information to monitor and troubleshoot Traffic Mirroring.

For more information about Amazon CloudWatch, see the Amazon CloudWatch User Guide. For more information, see List the available CloudWatch metrics for your instances in *Amazon EC2 User Guide for Linux Instances*. For more information, see Amazon CloudWatch Pricing.

Traffic Mirroring metrics and dimensions

The following metrics are available for your mirrored traffic.

Metric	Description
`NetworkMirrorIn`	The number of bytes received on all network interfaces by the instance that are mirrored. The number reported is the number of bytes received during the period. If you are using basic (five-minute) monitoring, you can divide this number by 300 to find Bytes/second. If you have detailed (one-minute) monitoring, divide it by 60. Units: Bytes
`NetworkMirrorOut`	The number of bytes sent out on all network interfaces by the instance that are mirrored. The number reported is the number of bytes sent during the period. If you are using basic (five-minute) monitoring, you can divide this number by 300 to find Bytes/second. If you have detailed (one-minute) monitoring, divide it by 60. Units: Bytes
`NetworkPacketsMirrorIn`	The number of packets received on all network interfaces by the instance that are mirrored. This metric is available for basic monitoring only. Units: Count
`NetworkPacketsMirrorOut`	The number of packets sent out on all network interfaces by the instance that are mirrored. This metric is available for basic monitoring only.

Metric	Description
	Units: Count
NetworkSkipMirrorIn	The number of bytes received, that meet the traffic mirror filter rules, that did not get mirrored because of production traffic taking priority. Units: Bytes
NetworkSkipMirrorOut	The number of bytes sent out, that meet the traffic mirror filter rules, that did not get mirrored because of production traffic taking priority. Units: Bytes
NetworkPacketsSkipMirrorIn	The number of packets received, that meet the traffic mirror filter rules, that did not get mirrored because of production traffic taking priority. This metric is available for basic monitoring only. Units: Count
NetworkPacketsSkipMirrorOut	The number of packets sent out, that meet the traffic mirror filter rules, that did not get mirrored because of production traffic taking priority. This metric is available for basic monitoring only. Units: Count

To filter the metric data, use the following dimensions.

Dimension	Description
AutoScalingGroupName	This dimension filters the data you request for all instances in a specified capacity group. An Auto Scaling group is a collection of instances you define if you're using Auto Scaling. This dimension is available only for Amazon EC2 metrics when the instances are in such an Auto Scaling group. Available for instances with Detailed or Basic Monitoring enabled.
ImageId	This dimension filters the data you request for all instances running this Amazon EC2 Amazon Machine Image (AMI). Available for instances with Detailed Monitoring enabled.
InstanceId	This dimension filters the data you request for the identified instance only. This helps you pinpoint an exact instance from which to monitor data. Available for instances with Detailed or Basic Monitoring enabled.
InstanceType	This dimension filters the data you request for all instances running with this specified instance type. This helps you categorize your data by the type of instance running. For example, you might

Dimension	Description
	compare data from an m1.small instance and an m1.large instance to determine which has the better business value for your application. Available for instances with Detailed Monitoring enabled.

View Traffic Mirroring CloudWatch metrics

You can view the metrics for Traffic Mirroring as follows.

To view metrics using the CloudWatch console

Metrics are grouped first by the service namespace, and then by the various dimension combinations within each namespace.

1. Open the CloudWatch console at https://console.aws.amazon.com/cloudwatch/.
2. In the navigation pane, choose **Metrics**.
3. Under **All metrics**, choose the **EC2** metric namespace.
4. To view the metrics, select the metric dimension.

To view metrics using the AWS CLI

At a command prompt, use the following command to list the metrics that are available for Traffic Mirroring:

```
aws cloudwatch list-metrics --namespace "AWS/EC2"
```

The Traffic Mirroring metrics are included with the metrics for Amazon EC2.

Traffic Mirroring considerations

General

- You can only create a traffic mirror session if you are the owner of the source network interface or its subnet.
- We recommend using either a Network Load Balancer or a Gateway Load Balancer endpoint as a target for high availability.
- An elastic network interface cannot be a traffic mirror target and a traffic mirror session source at the same time.
- When you delete a network interface that is a traffic mirror source, the traffic mirror sessions that are associated with the source are automatically deleted.
- Flow logs do not capture mirrored traffic.

Routing and security group rules evaluation

- Encapsulated mirror traffic is routed by using the VPC route table. Make sure that your route table is configured to send the mirrored traffic to the correct traffic mirror target.
- Mirrored outbound traffic from a source instance is not subject to security group evaluation.
- Packets that are dropped at the traffic mirror source by security group rules or by network ACL rules are not mirrored.

MTU

- We truncate the packet to the MTU value when both of the following are true:
  - The traffic mirror target is a standalone instance.
  - The mirrored traffic packet size is greater than the traffic mirror target MTU value.

    For example, if an 8996 byte packet is mirrored, and the traffic mirror target MTU value is 9001 bytes, the mirror encapsulation results in the mirrored packet being greater than the MTU value. In this case, the mirror packet is truncated. To prevent mirror packets from being truncated, set the traffic mirror source interface MTU value to 54 bytes less than the traffic mirror target MTU value for IPv4 and 74 bytes less than the traffic mirror target MTU value when you use IPv6. Therefore, the maximum MTU value supported by Traffic Mirroring with no packet truncation is 8947 bytes. For more information about configuring the network MTU value, see Network Maximum Transmission Unit (MTU) for Your EC2 Instance in the *Amazon EC2 User Guide for Linux Instances*.

Traffic bandwidth and prioritization

- Mirrored traffic counts toward instance bandwidth. For example, if you mirror a network interface that has 1 Gbps of inbound traffic and 1 Gbps of outbound traffic, the instance must handle 4 Gbps of traffic (1 Gbps inbound, 1 Gbps mirrored inbound, 1 Gbps outbound, and 1 Gbps mirrored outbound).
- Production traffic has a higher priority than mirrored traffic when there is traffic congestion. As a result, mirrored traffic is dropped when there is congestion.

- Each Gateway Load Balancer endpoint can support a bandwidth of up to 40 Gbps. For more information about Gateway Load Balancer endpoint quotas, see Availability Zones and load balancer nodes in the *AWS PrivateLink Guide*.

Network Load Balancer

The following rules apply when the Traffic Mirroring is a Network Load Balancer

- There must be UDP listeners on port 4789.
- If you do not have UDP listeners on the Network Load Balancer, you can still use the Network Load Balancer as a target. However, Traffic Mirroring cannot occur because there are no UDP listeners.
- If you remove the UDP listeners from a Network Load Balancer that is a traffic mirror target, Traffic Mirroring fails without an error indication.
- When the Network Load Balancer removes the node in an Availability Zone from the DNS table, Traffic Mirroring continues to send the mirrored packets to that node.
- When you have an existing Network Load Balancer which is a traffic mirror target and you add additional subnets to it, there is no effect. For example, mirrored traffic in the Availability Zone of the new subnet is not routed in the same Availability Zone unless you enable cross-zone load balancing.
- We recommend that you use cross-zone load balancing with your Network Load Balancer to ensure that the packets continue to be mirrored when all targets in an Availability Zone are not healthy. For more information, see Availability Zones and load balancer nodes in the *Elastic Load Balancing User Guide*.

Gateway Load Balancer

The following rules apply when the Traffic Mirroring is a Gateway Load Balancer

- A listener for Gateway Load Balancers listens for all IP packets across all ports, and forwards traffic to the target group that you select.
- The maximum MTU supported by the Gateway Load Balancer is 8500. VPC Traffic Mirroring adds 54 bytes of additional headers to the original packet payload when using IPv4, and 74 bytes when using IPv6. Therefore, the maximum packet size that can be delivered to the appliance without truncation is `8500 - 54 = 8446` when using IPv4, or `8500 - 74 = 8426` when using IPv6.
- You can use the `BytesProcessed` and `PacketsDropped` CloudWatch metrics for Amazon VPC endpoints to monitor the volume of traffic being sent over the Gateway Load Balancer endpoint. You can also use existing Amazon VPC Traffic Mirroring CloudWatch metrics for traffic volumes for each of the traffic mirroring sessions. For more information, see

You can monitor your mirrored traffic using Amazon CloudWatch, which collects information from your network interface that is part of a traffic mirror session, and creates readable, near real-time metrics. You can use this information to monitor and troubleshoot Traffic Mirroring.

For more information about Amazon CloudWatch, see the Amazon CloudWatch User Guide. For more information, see List the available CloudWatch metrics for your instances in *Amazon EC2 User Guide for Linux Instances*. For more information, see Amazon CloudWatch Pricing.

Traffic Mirroring metrics and dimensions

The following metrics are available for your mirrored traffic.

`NetworkMirrorIn`	The number of bytes received on all network interfaces by the instance that are mirrored.
	The number reported is the number of bytes received during the period. If you
	are using basic (five-minute) monitoring,
	you can divide this number by 300 to find
	Bytes/second. If you have detailed (one-minute) monitoring, divide it by 60.
	Units: Bytes
`NetworkMirrorOut`	The number of bytes sent out on all network interfaces by the instance that are mirrored.
	The number reported is the number of bytes sent during the period. If you are
	using basic (five-minute) monitoring, you
	can divide this number by 300 to find
	Bytes/second. If you have detailed (one-minute) monitoring, divide it by 60.
	Units: Bytes
`NetworkPacketsMirrorIn`	The number of packets received on all network interfaces by the instance that
	are mirrored. This metric is available for basic monitoring only.
	Units: Count
`NetworkPacketsMirrorOut`	The number of packets sent out on all network interfaces by the instance that
	are mirrored. This metric is available for basic monitoring only.
	Units: Count
`NetworkSkipMirrorIn`	The number of bytes received, that meet the traffic mirror filter rules, that did not
	get mirrored because of production traffic taking priority.
	Units: Bytes
`NetworkSkipMirrorOut`	The number of bytes sent out, that meet the traffic mirror filter rules, that did not
	get mirrored because of production traffic taking priority.
	Units: Bytes

NetworkPacketsSkipMirrorIn	The number of packets received, that meet the traffic mirror filter rules, that did not get mirrored because of production traffic taking priority. This metric is available for basic monitoring only. Units: Count
NetworkPacketsSkipMirrorOut	The number of packets sent out, that meet the traffic mirror filter rules, that did not get mirrored because of production traffic taking priority. This metric is available for basic monitoring only. Units: Count

Metric	Description

To filter the metric data, use the following dimensions.

AutoScalingGroupName	This dimension filters the data you request for all instances in a specified capacity group. An Auto Scaling group is a collection of instances you define if you're using Auto Scaling. This dimension is available only for Amazon EC2 metrics when the instances are in such an Auto Scaling group. Available for instances with Detailed or Basic Monitoring enabled.
ImageId	This dimension filters the data you request for all instances running this Amazon EC2 Amazon Machine Image (AMI). Available for instances with Detailed Monitoring enabled.
InstanceId	This dimension filters the data you request for the identified instance only. This helps you pinpoint an exact instance from which to monitor data. Available for instances with Detailed or Basic Monitoring enabled.
InstanceType	This dimension filters the data you request for all instances running with this specified instance type. This helps you categorize your data by the type of instance running. For example, you might compare data from an m1.small instance and an m1.large instance to determine which has the better business value for your application. Available for instances with Detailed Monitoring enabled.

Dimension	Description

View Traffic Mirroring CloudWatch metrics

You can view the metrics for Traffic Mirroring as follows.

To view metrics using the CloudWatch console

Metrics are grouped first by the service namespace, and then by the various dimension combinations within each namespace.

1. Open the CloudWatch console at https://console.aws.amazon.com/cloudwatch/.
2. In the navigation pane, choose **Metrics**.
3. Under **All metrics**, choose the **EC2** metric namespace.
4. To view the metrics, select the metric dimension.

To view metrics using the AWS CLI

At a command prompt, use the following command to list the metrics that are available for Traffic Mirroring:

```
aws cloudwatch list-metrics --namespace "AWS/EC2"
```

The Traffic Mirroring metrics are included with the metrics for Amazon EC2.

(p. 33).

- If all of the Gateway Load Balancer targets in an Availability Zone becomes unhealthy, the mirrored traffic can still be sent to traffic mirror targets in other zones. In this case, cross-zone load balancing to allow the Gateway Load Balancer to forward the mirrored traffic to a healthy target in another zone. For more information, see Gateway Load Balancer target failure scenarios in the *User Guide for Gateway Load Balancers*.

Traffic Mirroring limitations and quotas

The following sections describe the limitations, quotas, and checksum offloading for Traffic Mirroring.

Limitations

Traffic Mirroring is available on a majority of the current generation Nitro-based instances and some select non-Nitro instance types.

The following non-Nitro instance types are currently supported:

- C4, D2, G3, G3s, H1, I3, M4, P2, P3, R4, X1, X1e

Traffic Mirroring is not available on the following instance types:

- These current generation instances: C6a, C6gn, C6i, Hpc6a, I4i, Im4gn, Is4gen, M6a, M6i, R6i, T2, X2idn, X2iedn, X2iezn
- Bare metal instances
- Previous generation instances

The following traffic types cannot be mirrored:

- ARP
- DHCP
- Instance metadata service
- NTP
- Windows activation

Quotas

The following are the quotas for Traffic Mirroring for your AWS account.

Sessions

The following table lists the Traffic Mirroring session limits.

Quota	Default	Adjustable
Maximum number of sessions per account	10,000	No

Quota	Default	Adjustable
Maximum number of sessions per source network interface	3	No
Maximum number of sessions for a single Gateway Load Balancer endpoint	Unlimited	Not applicable

Targets

The following table lists the Traffic Mirroring target limits.

Quota	Default	Adjustable
Maximum number of targets per account	10,000	No

Filters

The following table lists the Traffic Mirroring filter limits.

Quota	Default	Adjustable
Maximum number of filters per account	10,000	No
Maximum number of sessions per source network interface	3	No

Throughput

The following table lists the Traffic Mirroring throughput limits.

Quota	Default	Adjustable
Maximum throughput through a single Gateway Load Balancer endpoint	40 Gbps	No

Packets

The following table lists the Traffic Mirroring packet sizes.

Quota	Default	Adjustable
Maximum number of MTUs for a Gateway Load Balancer endpoint	8,500	No

Sources

The following table lists the Traffic Mirroring source limits.

Quota	Default	Adjustable
Maximum number of sources per Network Load Balancer	No limit	No
Maximum number of sources per Gateway Load Balancer endpoint	No limit	No
Maximum number of sessions per target (smaller sizes)	10	No
Maximum number of sources per target (largest size)	100 *	No

* This applies only to the largest instance size. For example, for M5 instances, the maximum is 100 for `m5.24xlarge` and `10` for all other M5 instance sizes. For more information about instance sizes, see Available instance types in the *Amazon EC2 User Guide*.

Checksum offloading

The Elastic Network Adapter (ENA) provides checksum offloading capabilities. If a packet is truncated, this might result in the packet checksum not being calculated for the mirrored packet. The following checksums are not calculated when the mirrored packet is truncated:

- If the mirror packet is truncated, the mirror packet L4 checksum is not calculated.
- If any part of the L3 header is truncated, the L3 checksum is not calculated.

Use the following commands to disable ENA checksum offloading on Amazon Linux 2 AMI:

```
[ec2-user@ip-11-0-0-166 ~]$ sudo ethtool --offload eth0 tx off
[ec2-user@ip-11-0-0-166 ~]$ sudo ethtool --show-offload eth0
Features for eth0:
rx-checksumming: on
tx-checksumming: off
     tx-checksum-ipv4: off
     tx-checksum-ip-generic: off [fixed]
     tx-checksum-ipv6: off [fixed]
     tx-checksum-fcoe-crc: off [fixed]
     tx-checksum-sctp: off [fixed]
```

Identity and access management for Traffic Mirroring

AWS Identity and Access Management (IAM) is an AWS service that helps an administrator securely control access to AWS resources. IAM administrators control who can be *authenticated* (signed in) and *authorized* (have permissions) to use traffic mirror resources.

To allow access to traffic mirror resources, you create and attach an IAM policy either to an IAM user or IAM group.

The IAM user must be given permission to use specific traffic mirror resources and API actions. When you attach a policy to a user or group of users, it allows or denies permission to perform the specified tasks on the specified resources.

You can also use resource-level permissions to restrict what resources users can use when they invoke APIs.

Example Example: CreateTrafficMirrorSession policy

The following IAM policy allows users to use the `CreateTrafficMirrorSession` API, but restricts the action to a specific traffic mirror target (`tmt-12345645678`). To create a traffic mirror session, users must also have permission to use the traffic mirror filter and network interface resources. Therefore, you must include these resources in your IAM policy.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:CreateTrafficMirrorSession",
            "Resource": [
                "arn:aws:ec2:*:*:traffic-mirror-target/tmt-12345645678",
                "arn:aws:ec2:*:*:traffic-mirror-filter/*",
                "arn:aws:ec2:*:*:network-interface/*"
            ]
        }
     ]
}
```

For more information about supported traffic mirror actions, resources, and condition keys, see Actions, Resources, and Condition Keys for Amazon EC2 in the *IAM User Guide*.

Document history for Traffic Mirroring

The following table describes the releases for Traffic Mirroring.

Feature	Description	Release Date
Support for a Gateway Load Balancer endpoint, as a Traffic Mirror target	For more information, see the section called "Targets" (p. 4).	May 12, 2022
Support for additional instances	For more information, see *Considerations* (p. 36).	February 10, 2021
Support for Amazon CloudWatch	Monitor your mirrored traffic using Amazon CloudWatch. For more information, see *Monitor mirrored traffic* (p. 33).	Nov 25, 2019
Initial release	This release introduces Traffic Mirroring.	June 25, 2019