Amazon Virtual Private Cloud

Traffic Mirroring

Amazon Virtual Private Cloud: Traffic Mirroring

Table of Contents

What is Traffic Mirroring? ... 1
- Traffic Mirroring concepts ... 1
- Work with Traffic Mirroring ... 1
- Traffic Mirroring benefits ... 1
- Pricing ... 2

How Traffic Mirroring works ... 3
- Targets ... 3
  - Network interfaces ... 4
  - Network Load Balancer ... 4
  - Gateway Load Balancer endpoints ... 5
  - VXLAN encapsulation ... 6
  - Routing and security groups ... 6
  - Processing mirrored traffic ... 7
- Filters ... 7
- Sessions ... 7
  - Traffic mirror sources ... 8
- Connectivity options ... 8
- Packet format ... 9

Get started ... 10
- Prerequisites ... 10
- Step 1: Create the traffic mirror target ... 10
- Step 2: Create the traffic mirror filter ... 11
- Step 3: Create the traffic mirror session ... 11
- Step 4: Analyze the data ... 12

Traffic Mirroring examples ... 13
- Mirror inbound TCP traffic to a single appliance ... 13
  - Step 1: Create a traffic mirror target ... 13
  - Step 2: Create a traffic mirror filter ... 13
  - Step 3: Create a traffic mirror session ... 14
- Mirror inbound TCP and UDP traffic to multiple appliances ... 14
  - Step 1: Create a traffic mirror target for appliance a ... 15
  - Step 2: Create a traffic mirror target for appliance b ... 15
  - Step 3: Create a traffic mirror filter with a rule for TCP traffic ... 15
  - Step 4: Create a traffic mirror filter with a rule for UDP traffic ... 15
  - Step 5: Create a traffic mirror session for the TCP traffic ... 16
  - Step 6: Create a traffic mirror session for the UDP traffic ... 16
- Mirror non-local VPC traffic ... 17
  - Step 1: Create a traffic mirror target ... 17
  - Step 2: Create a traffic mirror filter ... 17
  - Step 3: Create a traffic mirror session ... 19
- Mirror traffic to a Gateway Load Balancer endpoint ... 19
  - Step 1: Create a traffic mirror target in Spoke VPC1 ... 20
  - Step 2: Create a traffic mirror target in Spoke VPC2 ... 21
  - Step 3: Create a traffic mirror filter rule ... 21
  - Step 4: Create a traffic mirror session in Spoke VPC1 ... 21
  - Step 5: Create a traffic mirror session in Spoke VPC2 ... 21

Work with Traffic Mirroring ... 23
- Targets ... 23
  - Create a traffic mirror target ... 23
  - View traffic mirror target details ... 24
  - Modify traffic mirror target tags ... 24
  - Delete a traffic mirror target ... 24
- Cross-account targets ... 25
  - Share a traffic mirror target ... 25

Accept a resource share 25
Delete a resource share 26
Filters 26
Create a traffic mirror filter 26
View your traffic mirror filters 27
Modify your traffic mirror filter rules 27
Modify traffic mirror filter tags 28
Modify traffic mirror filter network services 28
Delete a traffic mirror filter 28
Sessions 29
Create a traffic mirror session 29
View your traffic mirror sessions 30
Modify your traffic mirror session 30
Modify traffic mirror session tags 31
Delete a traffic mirror session 31
Work with open-source tools 32
Step 1: Install the Suricata software on the EC2 instance target 32
Step 2: Create a traffic mirror target 33
Step 3: Create a traffic mirror filter 33
Step 4: Create a traffic mirror session 33
Monitor mirrored traffic 34
Traffic Mirroring metrics and dimensions 34
View Traffic Mirroring CloudWatch metrics 36
Quotas and limitations 37
Quotas 37
Sessions 37
Targets 37
Filters 37
Throughput 38
Packets 38
Sources 38
Limitations 39
MTU 39
Traffic bandwidth and prioritization 40
Checksum offloading 40
Identity and access management 41
..... 41
Document history 42

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 or a Gateway Load Balancer with a UDP listener. Traffic Mirroring supports filters and packet truncation, so that you can extract only the traffic of interest, using the monitoring tools of your choice.

Traffic Mirroring concepts

The following are the key concepts for Traffic Mirroring:

- **Source** — The network interface to monitor.
- **Filter** — A set of rules that defines the traffic that is mirrored.
- **Target** — The destination for mirrored traffic.
- **Session** — Establishes a relationship between a source, a filter, and a target.

Work with Traffic Mirroring

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

- **Amazon Web Services Management Console**— Provides a web interface that you can use to access your traffic mirror resources.
- **Amazon Command Line Interface (Amazon CLI)** — Provides commands for a broad set of Amazon services, including Amazon VPC. The Amazon CLI is supported on Windows, macOS, and Linux. For more information, see Amazon Command Line Interface.
- **Amazon SDKs** — Provide language-specific APIs. The Amazon SDKs take care of many of the connection details, such as calculating signatures, handling request retries, and handling errors. For more information, see Amazon 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 Amazon VPC actions in 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

You are charged on an hourly basis for each active traffic mirror session. You'll continue to be charged for Traffic Mirroring until you delete all active traffic mirror sessions. For example, you'll still be charged in the following scenarios:

- You detached the network interface from the mirror source
- You stopped or terminated the mirror source
- You changed the instance type of the mirror source to an unsupported instance type

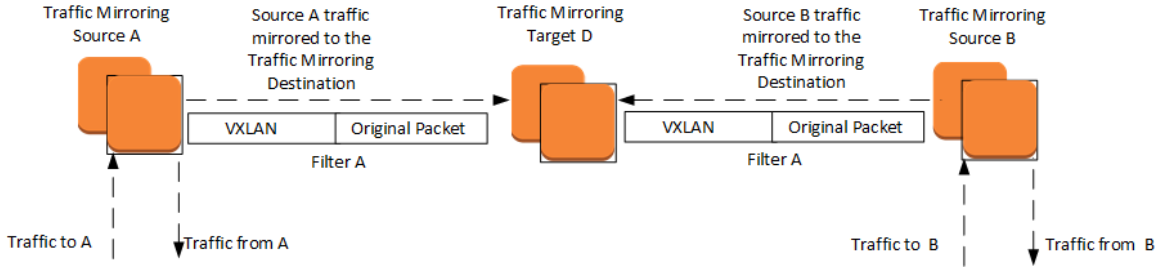
For the steps to delete a traffic mirror session, see the section called “Delete a traffic mirror session” (p. 31).

For information about pricing for Traffic Mirroring, see **Network Analysis** on the Amazon VPC pricing page.

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 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

Contents

- Traffic mirror target concepts (p. 3)
- Traffic mirror filter concepts (p. 7)
- Traffic mirror session concepts (p. 7)
- Traffic mirror source and target connectivity options (p. 8)
- Traffic Mirroring packet format (p. 9)

Traffic mirror target concepts

A *traffic mirror target* is the destination for mirrored traffic.

You can use the following resources as traffic mirror targets:

- Network interfaces (p. 4) of type `interface`

- Network Load Balancers (p. 4)
- Gateway Load Balancer endpoints (p. 5)

For high availability, we recommend that you use a Network Load Balancer or a Gateway Load Balancer endpoint as a mirror target.

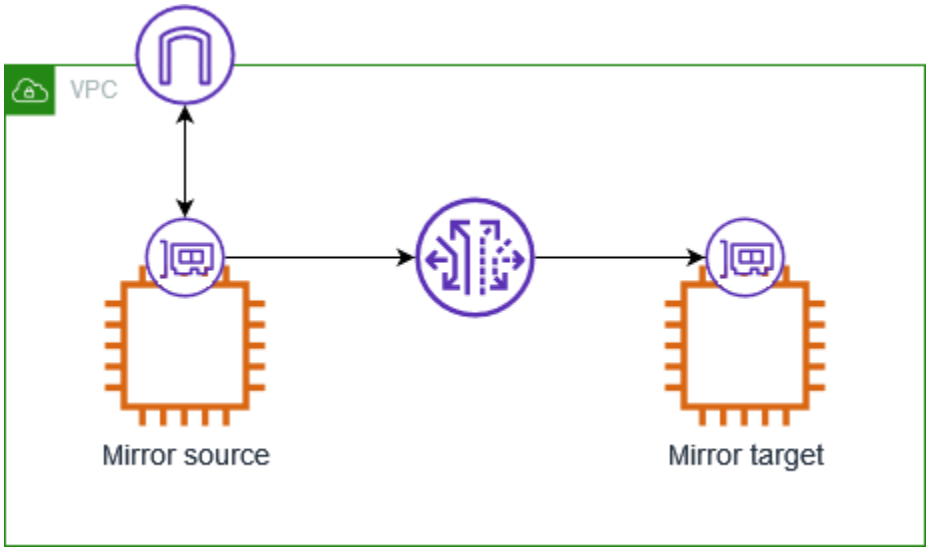
You might experience out-of-order delivery of mirrored packets when you use a Network Load Balancer or Gateway Load Balancer endpoint as your traffic mirror target. If your monitoring appliance can't handle out-of-order packets, we recommend using a network interface as your traffic mirror target.

A traffic mirror target can be owned by an Amazon Web Services account that is different from the traffic mirror source. For more information, see Cross-account targets (p. 25).

After you create a traffic mirror target, you add it to a traffic mirror session. You can use a traffic mirror target in more than one traffic mirror session. For more information, see the section called "Sessions" (p. 7).

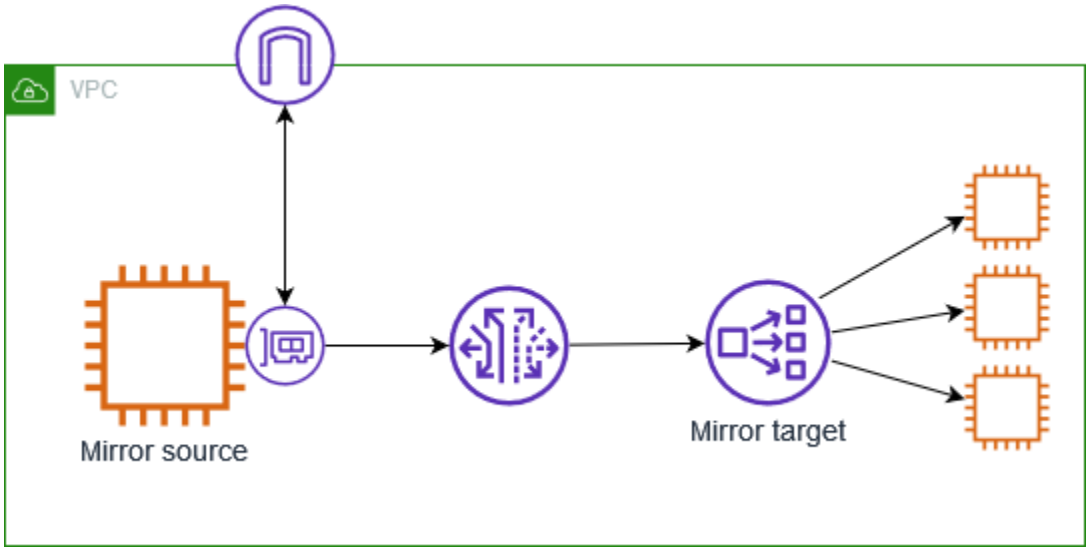
Network interfaces

The following diagram shows a traffic mirror session where the traffic mirror target is a network interface for an EC2 instance. Traffic Mirroring filters the traffic from the network interface of the mirror source and sends the accepted mirrored traffic to the mirror target.



Network Load Balancer

The following diagram shows a traffic mirror session where the traffic mirror target is a Network Load Balancer. You install the monitoring software on the target instances, and then register them with the load balancer. Traffic Mirroring filters the traffic from the network interface of the mirror source and sends the accepted mirrored traffic to the load balancer. The load balancer sends the mirrored traffic to the target instances.

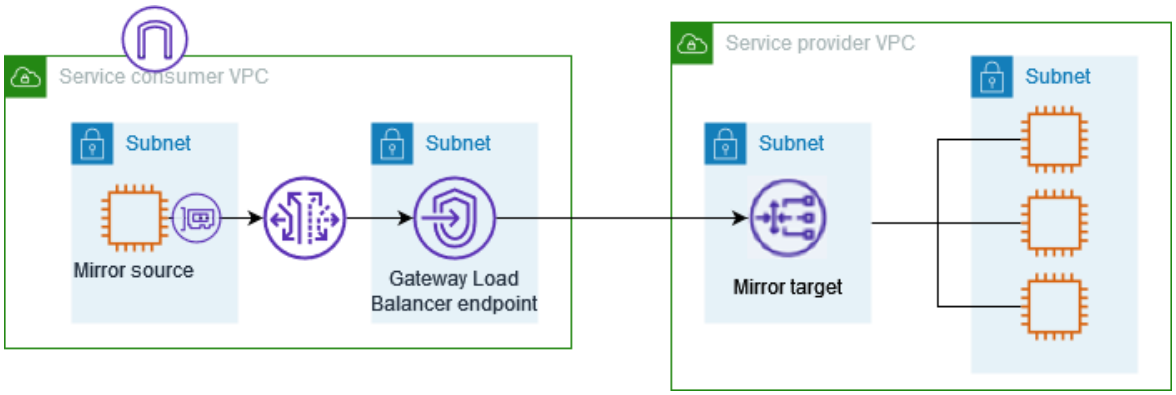


Considerations

- Traffic mirroring can't occur unless the load balancer has UDP listeners on port 4789. If you remove the UDP listeners, Traffic Mirroring fails without an error indication.
- To improve availability and fault tolerance, we recommend that you select at least two Availability Zones when you create the Network Load Balancer, and that you register target instances in each selected Availability Zone.
- We recommend that you enable cross-zone load balancing for your Network Load Balancer. If all registered target instances in an Availability Zone become unhealthy and cross-zone load balancing is disabled, the load balancer can't send the mirrored traffic to target instances in another Availability Zone. If you enable cross-zone load balancing, the load balancer can send the mirrored traffic to healthy target instances in another Availability Zone.
- If you select an additional Availability Zone for your Network Load Balancer after you create it, Traffic Mirroring does not send mirrored traffic to target instances in the new Availability Zone unless you enable cross-zone load balancing.
- When the Network Load Balancer removes a load balancer node from the DNS table, Traffic Mirroring continues to send the mirrored traffic to that node.

Gateway Load Balancer endpoints

The following diagram shows a traffic mirror session where the traffic mirror target is a Gateway Load Balancer endpoint. The mirror source is in the service consumer VPC and the Gateway Load Balancer is in the service provider VPC. You install the monitoring software on the target appliances, and then register them with the load balancer. Traffic Mirroring filters the traffic from the network interface of the mirror source and sends the accepted mirrored traffic to the Gateway Load Balancer endpoint. The load balancer sends the mirrored traffic to the target appliances.



Considerations

- A listener for Gateway Load Balancers listens for all IP packets across all ports, and then forwards traffic to the target group.
- To improve availability and fault tolerance, we recommend that you select at least two Availability Zones when you create the Gateway Load Balancer, and that you register target appliances in each selected Availability Zone.
- If all registered target appliances in an Availability Zone become unhealthy and cross-zone load balancing is disabled, the load balancer can't send the mirrored traffic to target appliances in another Availability Zone. If you enable cross-zone load balancing, the load balancer can send the mirrored traffic to healthy target appliances in another Availability Zone.
- The maximum MTU supported by the Gateway Load Balancer is 8500. 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 an 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 VPC endpoints to monitor the volume of traffic being sent over the Gateway Load Balancer endpoint. You can also use CloudWatch metrics for Traffic Mirroring. For more information, see *Monitor mirrored traffic* (p. 34).

VXLAN encapsulation

Mirrored traffic is encapsulated in VXLAN packets and then routed to the mirror target. The security groups for a traffic mirror target must allow VXLAN traffic (UDP port 4789) from the traffic mirror source. The route table for the subnet with the traffic mirror source must have a route that sends the mirrored traffic to the traffic mirror target. The monitoring software that you run on the mirror target must be able to process encapsulated VXLAN packets.

Routing and security groups

Encapsulated mirror traffic is routed to the traffic mirror target by using the VPC route table. Make sure that your route table is configured to send the mirrored traffic to the traffic mirror target.

Inbound traffic that is dropped at the traffic mirror source, because of the inbound security group rules or the inbound network ACL rules, is not mirrored.

Mirrored outbound traffic is not subject to the outbound security group rules for the traffic mirror source.

Processing mirrored traffic

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

Traffic mirror filter concepts

A *traffic mirror filter* is a set of inbound and outbound rules that determines which traffic is copied from the traffic mirror source and sent to the traffic mirror target. 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.

We evaluate traffic mirror filter rules from the lowest value to the highest value. The first rule that matches the traffic determines whether the traffic is mirrored. If you don't add any rules, then no traffic is mirrored.

For example, in the following set of filter rules, rule 10 ensures that SSH traffic from my network to my VPC is not mirrored and rule 20 mirrors all other IPv4 TCP traffic.

Inbound

Number	Rule action	Protocol	Source port range	Destination port range	Source CIDR block	Destination CIDR block
10	reject	TCP (6)		22	*my-network*	*vpc-cidr*
20	accept	TCP (6)			0.0.0.0/0	0.0.0.0/0

In the following set of filter rules, rule 10 mirrors HTTPS traffic from all IPv4 addresses and rule 20 mirrors HTTPS traffic from all IPv6 addresses.

Inbound

Number	Rule action	Protocol	Source port range	Destination port range	Source CIDR block	Destination CIDR block
10	accept	TCP (6)		443	0.0.0.0/0	0.0.0.0/0
20	accept	TCP (6)		443	::/0	::/0

Note that if you don't add outbound rules, then no outbound traffic is mirrored.

Traffic mirror session concepts

A *traffic mirror session* establishes a relationship between a traffic mirror source and a traffic mirror target. Traffic mirror sessions are evaluated based on the ascending session number that you define when you create the session.

A traffic mirror session contains the following resources:

- A traffic mirror source (p. 8)
- A traffic mirror target (p. 3)
- A traffic mirror filter (p. 7)

Each packet is mirrored once. However, you can use multiple traffic mirror sessions on the same mirror 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 sources

A traffic mirror source is the network interface of type `interface`. For example, a network interface for an EC2 instance or an RDS instance.

A network interface can't be a traffic mirror target and a traffic mirror source in the same traffic mirror session.

Traffic Mirroring is not available on all instance types.

Instance types

- Traffic Mirroring is not available on the following virtualized Nitro instance types:
  - General purpose: M6a, M6i, M6in, M7g, M7i, M7i-flex
  - Compute optimized: C6a, C6gn, C6i, C6id, C6in, C7g, Hpc6a
  - Memory optimized: R6a, R6i, R6id, R6idn, R6in, R7g, R7iz, X2idn, X2iedn, X2iezn
  - Storage optimized: I4g, I4i, Im4gn, Is4gen
  - Accelerated computing: Inf2, Trn1
- Traffic Mirroring is not available on bare metal instances.
- Traffic Mirroring is available only on the following non-Nitro instances types: C4, D2, G3, G3s, H1, I3, M4, P2, P3, R4, X1, and X1e. Note that this does not include T2 instances.

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 Amazon Web Services 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.

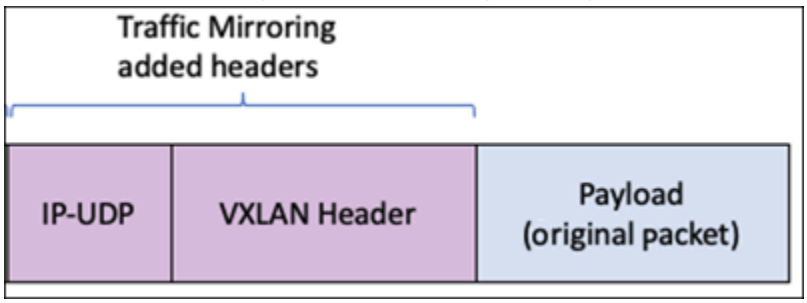
The following table describes the available resource configurations.

Source owner	Source VPC	Target owner	Target VPC	Connectivity option
Account A	VPC 1	Account A	VPC1	No additional configuration

Source owner	Source VPC	Target owner	Target VPC	Connectivity option
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:

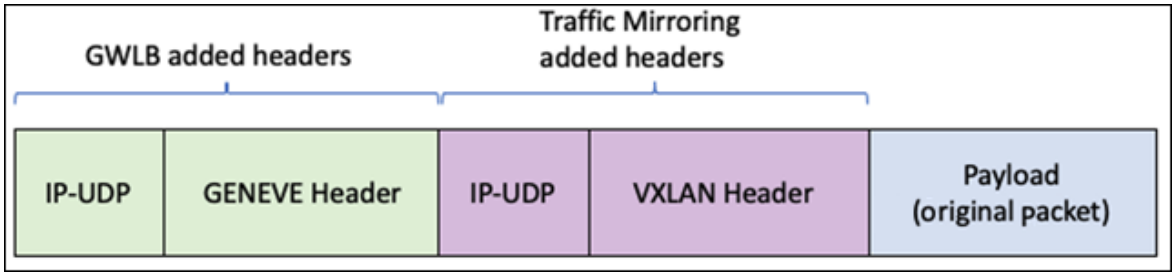


For more information about the VXLAN protocol, see RFC 7348.

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.
- **Source port** — The port is determined by a 5-tuple hash of the original L2 packet, for ICMP, TCP, and UDP flows. For other flows, the port is determined by a 3-tuple hash of the original L2 packet.
- **Destination IP address** — The primary IP address of the appliance, Gateway Load Balancer endpoint, or Network Load Balancer (when the appliance is deployed behind one).
- **Destination port** — The port is 4789, which is the well known port for VXLAN.

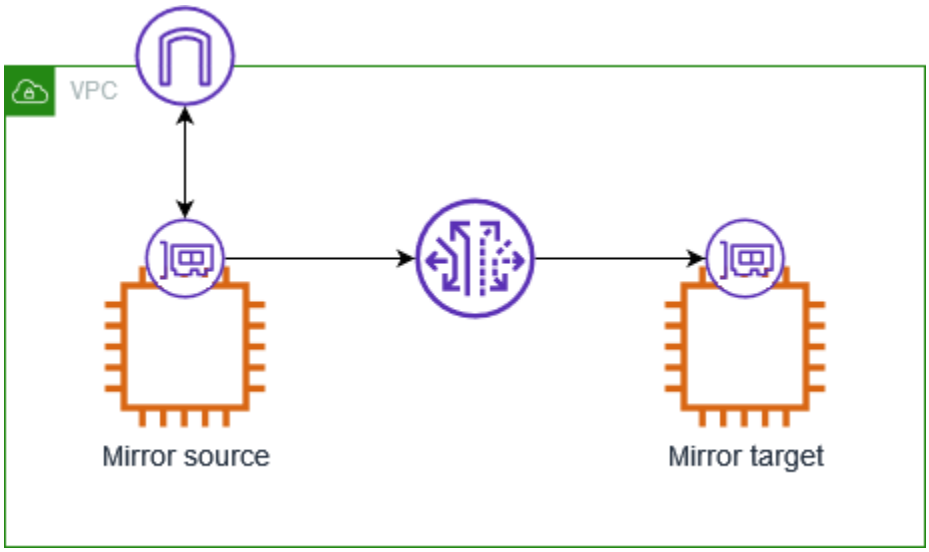
Appliances that received mirrored traffic through a Gateway Load Balancer should be able to parse both outer GENEVE encapsulation (from Gateway Load Balancer) and an inner VXLAN encapsulation (from VPC Traffic Mirroring) to retrieve the original L3 packet. The following shows an example:



Get started with Traffic Mirroring

To get started with Traffic Mirroring, we'll explore traffic mirror targets, filters, and sessions.

A mirror session is a connection between a mirror source and a mirror target. In the following diagram, both the mirror source and the mirror target are EC2 instances. The mirror filter determines which network packets are mirrored. For example, you can add inbound and outbound rules to the filter such that it rejects SSH traffic but accepts all other traffic. Traffic Mirroring applies the filter rules, and then copies the accepted traffic from the network interface of the mirror source to the network interface of the mirror target. You can run your capture and analysis tools on the packets delivered to the mirror target.



Tasks

- Prerequisites (p. 10)
- Step 1: Create the traffic mirror target (p. 10)
- Step 2: Create the traffic mirror filter (p. 11)
- Step 3: Create the traffic mirror session (p. 11)
- Step 4: Analyze the data (p. 12)

Prerequisites

- The traffic mirror source and traffic mirror target must be in the same VPC or in VPCs that are connected (for example, using VPC peering or a transit gateway).
- The traffic mirror target 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 the mirrored traffic.

To create a traffic mirror target

1. Open the Amazon VPC console at https://console.amazonaws.cn/vpc/.
2. In the **Region** selector, choose the Amazon Region that you used when you created the mirror target.
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 **Network Interface**.
8. For **Target**, choose the network interface of the instance.
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. For each rule, inbound or outbound, choose **Add rule**, and then specify the following information:

   - **Number**: The rule priority.
   - **Rule action**: Indicates whether to accept or reject the packets.
   - **Protocol**: The protocol.
   - (Optional) **Source port range**: The source port range.
   - (Optional) **Destination port range**: The destination port range.
   - **Source CIDR block**: The source CIDR block.
   - **Destination CIDR block**: The destination CIDR block.
   - **Description**: A description for the rule.
6. (Optional) For each tag to add, choose **Add new tag** and enter the tag key and tag value.
7. 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 mirror source.
6. For **Mirror target**, choose your traffic mirror target.
7. For **Additional settings**, do the following:

   a. For **Session number**, enter **1**, which 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.

      To mirror the entire packet, do not enter a value. To mirror only a portion of each packet, set this value to the number of bytes 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.
   d. For **Filter**, choose your traffic mirror filter.
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 copied to the traffic mirror target, you can use a tool from the Amazon 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. 13)
- Mirror inbound TCP and UDP traffic to multiple appliances (p. 14)
- Mirror non-local VPC traffic (p. 17)
- Mirror traffic to a Gateway Load Balancer endpoint (p. 19)

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. 23).

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. 26).

Traffic mirror filter rule for inbound TCP traffic

Option	Value
Rule action	Accept

Option	Value
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 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. 29).

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. 23).

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. 23).

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. 26)

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. 26)

Traffic mirror filter rule for inbound UDP traffic

Option	Value
Rule action	Accept
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. 29).

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. 29).

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. 23).

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. 26).

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. 29).

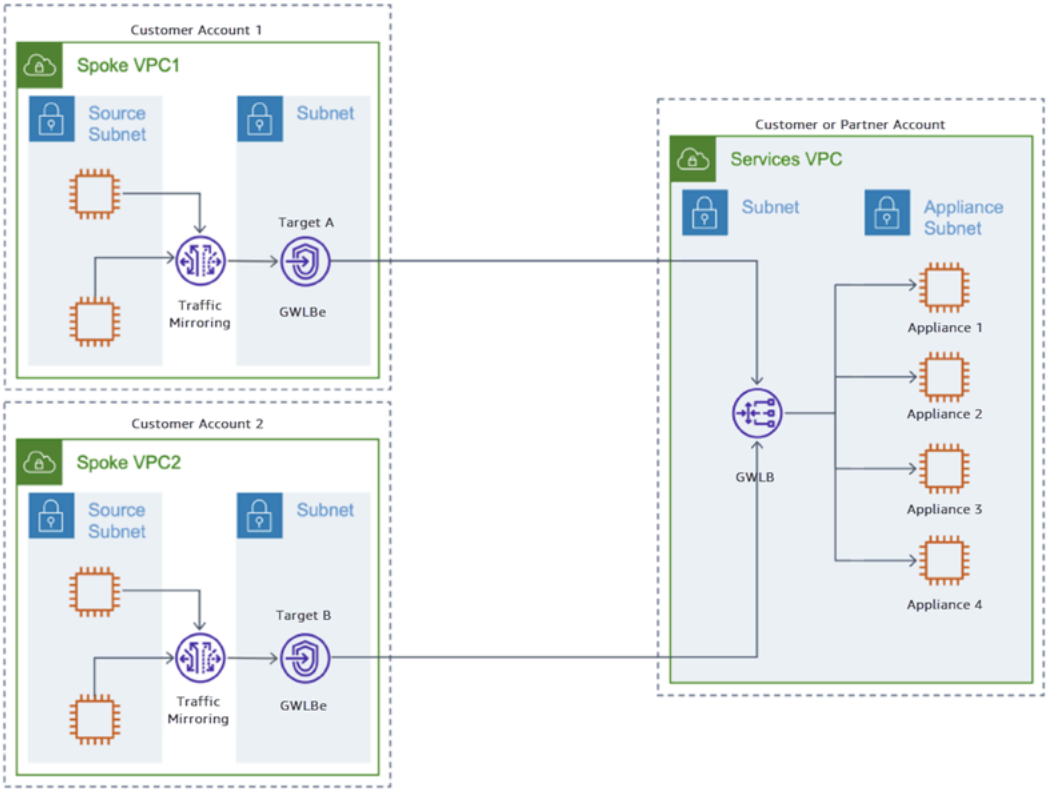
Traffic mirror session to monitor inbound TCP traffic

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. 23).

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. 23).

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. 26).

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. 29).

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. 29).

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 Amazon CLI.

Contents

- Traffic mirror targets (p. 23)
- Cross-account traffic mirror targets (p. 25)
- Traffic mirror filters (p. 26)
- Traffic mirror sessions (p. 29)

Traffic mirror targets

A traffic mirror target is the destination for mirrored traffic. For more information, see the section called "Targets" (p. 3).

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. 29).

You must configure a security group for the traffic mirror target that allows VXLAN traffic (UDP port 4789) from the traffic mirror source.

You can share a traffic mirror target across accounts. For more information, see Cross-account targets (p. 25).

Tasks

- Create a traffic mirror target (p. 23)
- View traffic mirror target details (p. 24)
- Modify traffic mirror target tags (p. 24)
- Delete a traffic mirror target (p. 24)

Create a traffic mirror target

To create a traffic mirror target using the console

1. Open the Amazon VPC console at https://console.amazonaws.cn/vpc/.
2. In the **Region** selector, choose the Amazon Region that you used when you created the mirror target.
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 type of the traffic mirror target:

   - **Network interface**
   - **Network Load Balancer**
   - **Gateway Load Balancer endpoint**

8. For **Target**, choose the traffic mirror target. We display targets based on the target type that you selected in the previous step.
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 Amazon CLI

Use the create-traffic-mirror-target command.

View traffic mirror target details

To view your traffic mirror targets using the console

1. Open the Amazon VPC console at https://console.amazonaws.cn/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 Amazon CLI

Use the describe-traffic-mirror-targets command.

Modify traffic mirror target tags

To modify your traffic mirror target tags using the console

1. Open the Amazon VPC console at https://console.amazonaws.cn/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 Amazon 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 can delete a traffic mirror target, you must remove it from any traffic mirror sessions.

To delete your traffic mirror target using the console

1. Open the Amazon VPC console at https://console.amazonaws.cn/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 Amazon CLI

Use the delete-traffic-mirror-target command.

Cross-account traffic mirror targets

A traffic mirror target can be owned by an Amazon 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 Amazon Resource Access Manager. When you are in different Amazon 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.

Tasks

- Share a traffic mirror target (p. 25)
- Accept a resource share (p. 25)
- Delete a resource share (p. 26)

Share a traffic mirror target

You can use Amazon 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. 23).

To share a traffic mirror target

1. Open the Amazon Resource Access Manager console at https://console.amazonaws.cn/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 Amazon account, OU, or organization, specify its ID and choose **Add**.

   For **Allow external accounts**, choose whether to allow sharing for this resource with Amazon 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 Amazon 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 Amazon Resource Access Manager console at https://console.amazonaws.cn/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 Amazon Resource Access Manager console at https://console.amazonaws.cn/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. When prompted for confirmation, 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. For more information, see the section called “Filters” (p. 7).

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

Tasks

- Create a traffic mirror filter (p. 26)
- View your traffic mirror filters (p. 27)
- Modify your traffic mirror filter rules (p. 27)
- Modify traffic mirror filter tags (p. 28)
- Modify traffic mirror filter network services (p. 28)
- Delete a traffic mirror filter (p. 28)

Create a traffic mirror filter

To create a traffic mirror filter using the console

1. Open the Amazon VPC console at https://console.amazonaws.cn/vpc/.
2. On the navigation pane, choose **Traffic Mirroring**, **Mirror filters**.
3. Choose **Create traffic mirror filter**.

4. (Optional) For **Name tag**, enter a name for the traffic mirror filter.
5. (Optional) For **Description**, enter a description for the traffic mirror filter.
6. (Optional) If you need to mirror Amazon DNS traffic, select **amazon-dns**.
7. For each rule, inbound or outbound, choose **Add rule**, and then specify the following information:

   - **Number**: The rule priority.
   - **Rule action**: Indicates whether to accept or reject the packets.
   - **Protocol**: The protocol.
   - (Optional) **Source port range**: The source port range.
   - (Optional) **Destination port range**: The destination port range.
   - **Source CIDR block**: The source CIDR block. The source and destination CIDR blocks must both be either IPv4 ranges or IPv6 ranges.
   - **Destination CIDR block**: The destination CIDR block. The source and destination CIDR blocks must both be either IPv4 ranges or IPv6 ranges.
   - **Description**: 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**.

To create a traffic mirror filter using the Amazon 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.amazonaws.cn/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 Amazon CLI

Use the describe-traffic-mirror-filters command.

Modify your traffic mirror filter rules

To modify your traffic mirror filter using the console

1. Open the Amazon VPC console at https://console.amazonaws.cn/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. For each rule to add, choose either **Inbound rules** , **Add inbound rule** or **Outbound rules**, **Add outbound rule**. Specify the following information, and then choose **Add rule**:

   - **Rule number**: The rule priority.
   - (Optional) **Description**: A description for the rule.
   - **Rule action**: Indicates whether to accept or reject the packets.
   - **Protocol**: The protocol.
   - (Optional) **Source port range**: The source port range.
   - (Optional) **Destination port range**: The destination port range.

- **Source CIDR block**: The source CIDR block. The source and destination CIDR blocks must both be either IPv4 ranges or IPv6 ranges.
- **Destination CIDR block**: The destination CIDR block. The source and destination CIDR blocks must both be either IPv4 ranges or IPv6 ranges.

5. For each inbound rule to modify, select the rule and choose **Modify outbound rule**. Update the rule as needed, and then choose **Modify rule**.
6. For each rule to delete, 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.amazonaws.cn/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 Amazon 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.amazonaws.cn/vpc/.
2. On the navigation pane, choose **Traffic Mirroring**, **Mirror filters**.
3. Select the radio button for the traffic mirror filter.
4. Choose **Actions**, **Modify Network Services**.
5. If you need to mirror Amazon DNS traffic, select **amazon-dns**. Otherwise, clear **amazon-dns**.
6. Choose **Modify**.

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

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

Delete a traffic mirror filter

Before you can delete a traffic mirror filter, you must remove it from any traffic mirror sessions.

To delete a traffic mirror filter using the console

1. Open the Amazon VPC console at https://console.amazonaws.cn/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 Amazon 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. For more information, see the section called “Sessions” (p. 7).

A traffic mirror session contains the following resources:

- A traffic mirror source (p. 8)
- A traffic mirror target (p. 23)
- A traffic mirror filter (p. 26)

You can create a traffic mirror session only if you are the owner of the network interface or the subnet for the traffic mirror source.

Tasks

- Create a traffic mirror session (p. 29)
- View your traffic mirror sessions (p. 30)
- Modify your traffic mirror session (p. 30)
- Modify traffic mirror session tags (p. 31)
- Delete a traffic mirror session (p. 31)

Create a traffic mirror session

To create a traffic mirror session using the console

1. Open the Amazon VPC console at https://console.amazonaws.cn/vpc/.
2. In the **Region** selector, choose the Amazon 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 mirror source.
8. For **Mirror target**, choose an existing traffic mirror target or choose **Create target** to create one. For more information, see the section called “Create a traffic mirror target” (p. 23).

   If the mirror target is owned by another account and shared with you, you must first accept the resource share (p. 25).
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. Sessions are evaluated based on the priority indicated by this session number.
   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.

To mirror the entire packet, do not enter a value. To mirror only a portion of each packet, set this value to the number of bytes 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.

d. For **Filter**, choose an existing traffic mirror filter. Alternatively, choose **Create filter**. For more information, see the section called "Step 2: Create the traffic mirror filter" (p. 11).

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 Amazon 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.amazonaws.cn/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 Amazon 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.amazonaws.cn/vpc/.
2. In the navigation pane, choose **Traffic Mirroring**, **Mirror sessions**.
3. Select the radio button for 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 an existing traffic mirror target or choose **Create target** to create one. For more information, see the section called "Create a traffic mirror target" (p. 23).
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.

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.

To mirror the entire packet, do not enter a value. To mirror only a portion of each packet, set this value to the number of bytes 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.

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 Amazon 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.amazonaws.cn/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 Amazon CLI

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

Delete a traffic mirror session

You are charged on an hourly basis for each active traffic mirror session. To stop all Traffic Mirroring charges, you must delete all active traffic mirror sessions. If you delete the network interface for the traffic mirror source, the traffic mirror sessions for the source are deleted automatically.

To delete your traffic mirror session using the console

1. Open the Amazon VPC console at https://console.amazonaws.cn/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 Amazon 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. 23).

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. 26).

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. 29).

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 at the traffic mirror source:

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.amazonaws.cn/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 Amazon 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 quotas and limitations

Traffic Mirroring has the following quotas and limitations.

Contents

- Quotas (p. 37)
- Limitations (p. 39)
- MTU (p. 39)
- Traffic bandwidth and prioritization (p. 40)
- Checksum offloading (p. 40)

Quotas

The following are the quotas for Traffic Mirroring for your Amazon Web Services account.

Sessions

The following table lists the Traffic Mirroring session limits.

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

Throughput

The following table lists the Traffic Mirroring throughput limits.

Quota	Default	Adjustable
Maximum throughput through a single Gateway Load Balancer endpoint	100 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*.

Limitations

Instance types

- Traffic Mirroring is not available on the following virtualized Nitro instance types:
  - General purpose: M6a, M6i, M6in, M7g, M7i, M7i-flex
  - Compute optimized: C6a, C6gn, C6i, C6id, C6in, C7g, Hpc6a
  - Memory optimized: R6a, R6i, R6id, R6idn, R6in, R7g, R7iz, X2idn, X2iedn, X2iezn
  - Storage optimized: I4g, I4i, Im4gn, Is4gen
  - Accelerated computing: Inf2, Trn1
- Traffic Mirroring is not available on bare metal instances.
- Traffic Mirroring is available only on the following non-Nitro instances types: C4, D2, G3, G3s, H1, I3, M4, P2, P3, R4, X1, and X1e. Note that this does not include T2 instances.

IPv6 traffic

Traffic mirroring is not supported for IPv6-only subnets.

Traffic types

Traffic Mirroring can't mirror the following traffic types:

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

VPC Flow Logs

VPC Flow Logs do not capture mirrored traffic.

Shared VPCs and subnets

- Participants cannot describe, create, modify, or delete a traffic mirror session or target that belongs to the VPC owner. Participants can describe, create, modify, and delete a traffic mirror session or target that belongs to them.
- VPC owners cannot describe, create, modify, or delete a traffic mirror session or target that belongs to the participant.

For more information see, Share your VPC with other accounts in the *Amazon VPC User Guide*.

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) 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.

By default, each Gateway Load Balancer endpoint can support a bandwidth of up to 10 Gbps per Availability Zone and automatically scales up to 100 Gbps. For more information, see Amazon PrivateLink quotas in the *Amazon PrivateLink 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.

If this causes issues, you can disable ENA checksum offloading on the ENA for the source. For example, use the following commands on Amazon Linux 2:

```
[ec2-user ~]$ sudo ethtool --offload eth0 tx off
[ec2-user ~]$ 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

Amazon Identity and Access Management (IAM) is an Amazon service that helps an administrator securely control access to Amazon resources. 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 to an IAM role and users or groups assume that role.

The IAM role must be given permission to use specific traffic mirror resources and API actions. When you attach a policy to a role, 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 the IAM policy attached to the role.

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

Change	Description	Date
Support for Gateway Load Balancer endpoints as traffic mirror targets (p. 42)	Send mirrored traffic to monitoring appliances registered with a Gateway Load Balancer.	May 12, 2022
Support for non-Nitro instance types (p. 42)	Enable Traffic Mirroring on the following non-Nitro instance types: C4, D2, G3, G3s, H1, I3, M4, P2, P3, R4, X1 and X1e.	February 10, 2021
Support for Amazon CloudWatch	Monitor your mirrored traffic using Amazon CloudWatch.	November 25, 2019
Initial release (p. 42)	This release introduces Traffic Mirroring.	June 25, 2019