Deploy Reveal(x) 360 sensors for AWS

Published: 2021-08-31

Published: 2021-08-31

This guide provides instructions for deploying ExtraHop-managed Reveal(x) 360 sensors and configuring your AWS resources (ENIs) to mirror traffic to Reveal(x) 360 sensors.

Before you begin

- Familiarize yourself with how traffic mirroring works in AWS.
- You must have an AWS user account that is capable of creating an IAM role and that is able to tag ENI resources.
- Identify the instances in your VPC and their attached network interfaces (source ENIs) from which you want to mirror traffic to Reveal(x) 360 sensors. Note that you can only select interfaces from one availability zone per sensor. For environments with interfaces in multiple availability zones, see Deploy Reveal(x) 360 sensors for AWS in advanced environments.
- You must have an ExtraHop Okta user account with OktaAdmin or ApplianceAdmin privileges to configure Reveal(x) 360.

In the following procedures, you will deploy Reveal(x) 360 sensors and mirror traffic from a source ENI attached to your EC2 instances to a target ENI that is attached to the sensor.

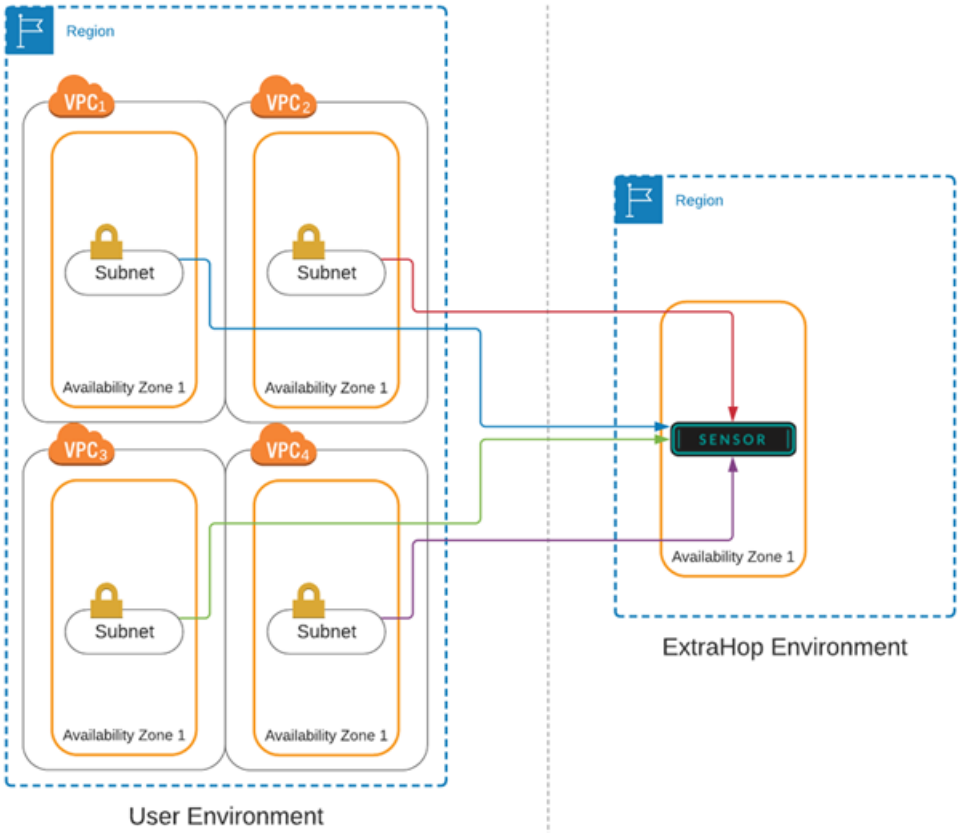
Tip: These procedures require you to configure settings in Reveal(x) 360 and in the AWS Management Console, so it is helpful to have each UI open side-by-side.

Note: For self-managed sensors, see Connect to Reveal(x) 360 from self-managed sensors.

If your AWS workloads are in a single Availability Zone (AZ), you can mirror traffic from the subnets in that AZ to the ExtraHop sensor without incurring data transfer costs.

Elastic Network Interfaces (ENIs) are attached to EC2 instances. An ENI can be configured to mirror network traffic to a mirror target interface. The number of mirror target interfaces that you can connect to a single sensor is determined by the sensor package size.

Sensor Size	Number of Mirror Target Interfaces
Extra Small Premium or Ultra	3
Small Premium or Ultra	3
Medium Premium	7



Retrieve your tenant ID

Your tenant ID is required to create an IAM role and to tag your ENI resources in AWS. Retrieve the ID from the Reveal(x) 360 Administration page by completing the following steps.

1. Log in to the Reveal(x) 360 Console through the URL provided in your welcome email. You can also click the System Settings icon and then click **Administration**.
2. Click **Mirror Targets**.
3. Copy the tenant ID.

Create a target network interface (ENI)

You must create an ENI for each subnet in your VPC that you want to monitor with Reveal(x) 360. A single Reveal(x) 360 sensor can only monitor ENIs from one availability zone.

For more information, see the following AWS documentation: Creating a network interface.

Important: You must create a security group with an inbound rule that allows the VXLAN-encapsulated traffic to be sent over UDP port 4789 from the traffic mirror source to the traffic mirror target. There must be no outbound rules. See AWS documentation about creating a security group.

1. Log in to the Amazon EC2 management console through https://console.aws.amazon.com/ec2/.
2. In the left pane, under Network & Security, click **Network Interfaces**.
3. Click **Create Network Interface** and complete the following fields:

   • **Description:** Type a description. The description text appears in the Description field on the Mirror Target Interfaces page.

- **Subnet:** Select a subnet from the drop-down list.
- **IPv4 Private IP:** Select **Auto-assign**. Alternatively, select **Custom** and then type the primary private IPv4 address in the IPv4 address field. If the subnet has an associated IPv6 CIDR block, you can optionally specify an IPv6 address.
- **Elastic Fabric Adapter:** Do not select the Elastic Fabric Adapter checkbox.
- **Security groups:** Select the security group you created earlier to allow VXLAN traffic into the ENI.

4. Click **Add Tag**.
5. Type `extrahop-tenant` in the Key field and type your tenant ID in the Value field.
6. Click **Create**.

Create an IAM role in AWS

The IAM role enables you to grant ExtraHop access to the traffic mirror targets you created in AWS.

1. Return to the AWS Management Console.
2. In the Security, Identity, & Compliance section, click **IAM**.
3. In the left pane, click **Roles**.
4. Click **Create role**.
5. Click **Another AWS account**.
6. In the Specify accounts that can use this role section, type `895242732570` in the Account ID field.
7. Select the **Require external ID** checkbox and type your tenant ID in the External ID field.
8. Click **Next: Permissions**.
9. Click **Create policy**. The Create policy page opens in a new browser window or tab.
10. Click the JSON tab and paste the following JSON text into the field, replacing all existing text.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterfacePermission"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/extrahop-tenant": "<tenant-id>"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeNetworkInterfaces"
            ],
            "Resource": "*"
        }
    ]
}
```

Note: The `CreateNetworkInterfacePermission` parameter enables you to attach your ENI to the Reveal(x) 360 sensor.

11. Replace `<tenant-id>` with your ExtraHop tenant ID.

12. Click **Review policy**.
13. Type a name in the Policy field. This name can be any string.
14. Click **Create policy**.
15. After the policy is created, close the **Policies** tab and return to the Create role page.
16. Click the Refresh icon. (Do not refresh the browser page.)
17. In the Filter policies field, type the name of the policy you created.
18. Select the checkbox next to the policy name.
19. Click **Next: Tags**. No tags need to be entered.
20. Click **Next: Review**.
21. In the Role name field, type `ExtraHop-Trust-`<*tenant-id*>, where <*tenant-id*> is your ExtraHop tenant ID. For example, if your tenant ID is 12345abcd, type `ExtraHop-Trust-12345abcd`.
22. Click **Create role**.

Add your AWS accounts

Add your AWS account information to the ExtraHop system to enable the discovery of mirror target interfaces.

1. Return to the Reveal(x) 360 Administration page.
2. Click **AWS Accounts**.
3. Click **Add Account**.
4. Type a name in the Name field to identify the account.
5. Type your AWS account ID in the Account ID field.
6. Click **Save**.
7. Repeat the steps for each additional AWS account where you have mirror target interfaces.

To delete an account, remove any sensors attached to the account, select the account name in the list of accounts, and then click **Delete**.

Scan for mirror target interfaces

After tagging your target ENIs in AWS, you must scan for them in Reveal(x) 360 before they can be attached to your sensor.

Important: The ExtraHop system searches for mirror target interfaces by scanning all of the supported AWS regions. It is not possible to configure the system to bypass the scanning of specific regions. If you restrict access to any of these regions in your environment, the scan process will fail. Contact ExtraHop support if you are unable to successfully scan for mirror target interfaces.

1. Return to the Reveal(x) 360 Administration page.
2. Click **Mirror Targets**.
3. On the Mirror Target Interfaces page, click **Scan**.
   All interfaces that you tagged in AWS appear in the Mirror Target Interfaces table.

Table 1: Supported AWS Regions

Region Name	Region
US East (Ohio)	us-east-2
US East (N. Virginia)	us-east-1

Region Name	Region
US West (Oregon)	us-west-2
US West (N. California)	us-west-1
Asia Pacific (Mumbai)	ap-south-1
Asia Pacific (Seoul)	ap-northeast-2
Asia Pacific (Tokyo)	ap-northeast-1
Asia Pacific (Sydney)	ap-southeast-2
Asia Pacific (Singapore)	ap-southeast-1
Canada (Central)	ca-central-1
Europe (Frankfurt)	eu-central-1
Europe (Ireland)	eu-west-1
Europe (London)	eu-west-2
Europe (Paris)	eu-west-3
Europe (Stockholm)	eu-north-1
South America (São Paulo)	sa-east-1

Add sensors

You are now ready to add sensors from the Reveal(x) 360 Administration page.

Important: Mirror target interfaces cannot be added or removed from the sensor after the sensor is deployed. If you want to change the ENI that the sensor is monitoring, terminate the sensor and deploy a new one with the ENIs you want.

1. On the Reveal(x) 360 Administration page, click **Deploy Sensors**.
2. Type a unique name for the sensor in the Name field.
3. Select a sensor package for your deployment.
4. Select an availability zone ID from the drop-down list.
5. From the Mirror Targets drop-down list, select the interfaces you want to attach to the new sensor. Only the ENIs that were tagged with your tenant ID and that are in the selected availability zone appear in the list.
6. Click **Save**.
7. Optional: Select **Enable session key forwarding on this sensor** if you are configuring your Windows and Linux servers to forward session keys. For more information, see Forward session keys to ExtraHop-managed sensors
8. Click **Deploy Sensor**.

When the sensor status changes from Pending to Running, you can view metrics, detections, and records for your AWS traffic in Reveal(x) 360 by clicking **Reveal(x) 360 Console** on the Administration page.

Create a traffic mirror target

Complete these steps for each ENI you created.

For more information, see the following AWS documentation: Getting started with Traffic Mirroring.

1. Return to the AWS Management Console.
2. From the top menu, click **Services**.
3. In the Networking & Content Delivery section, click **VPC**.
4. In the left pane, under Traffic Mirroring, click **Mirror Targets**.
5. Click **Create traffic mirror target** and complete the following fields:
   - **Name tag:** (Optional) Type a descriptive name for the target.
   - **Description:** (Optional) Type a description for the target
   - **Target type:** Select **Network Interface**.
   - **Target:** Select the ENI you previously created.
6. Click **Create**.

Note the Target ID for each ENI. You will need the ID when you create a traffic mirror session.

Create a traffic mirror filter

You must create a filter to allow or restrict traffic from your ENI traffic mirror sources to Reveal(x) 360. We recommend the following filtering rules to help avoid mirroring duplicate frames from peer EC2 instances that are in a single VPC to the Reveal(x) 360 sensor.

- All outbound traffic is mirrored to the sensor, whether the traffic is sent from one peer device to another on the subnet or if the traffic is sent to a device outside of the subnet.
- Inbound traffic is only mirrored to the sensor when the traffic is from an external device. For example, this rule ensures that an app server request is not mirrored twice: once from the sending app server and once from the database that received the request.
- Rule numbers determine the order in which the filters are applied. Rules with lower numbers, such as 100, are applied first.

For more information, see the following AWS documentation: Getting started with Traffic Mirroring.

Important: These filters should only be applied when mirroring all of the instances in a CIDR block.

1. In the AWS Management Console, in the left pane under Traffic Mirroring, click **Mirror Filters**.
2. Click **Create traffic mirror filter** and complete the following fields:
   - **Name tag:** Type a name for the filter.
   - **Description:** Type a description for the filter.
   - **Network services:** Select the **amazon-dns** checkbox.
3. In the Inbound rules section, click **Add rule** and then complete the following fields:
   - **Number:** Type a number for the rule, such as `100`.
   - **Rule action:** Select **reject** from the drop-down list.
   - **Protocol:** Select **All protocols** from the drop-down list.
   - **Source CIDR block:** Type the CIDR block for the subnet.
   - **Destination CIDR block:** Type the CIDR block for the subnet.
   - **Description:** (Optional) Type a description for the rule.
4. In the Inbound rules section, click **Add rule** again and then complete the following fields:
   - **Number:** Type a number for the rule, such as `200`.
   - **Rule action:** Select **accept** from the drop-down list.
   - **Protocol:** Select **All protocols** from the drop-down list.
   - **Source CIDR block:** Type `0.0.0.0/0`.

- **Destination CIDR block:** Type `0.0.0.0/0`.
- **Description:** (Optional) Type a description for the rule.

5. In the Outbound rules section, click **Add rule** and then complete the following fields:
   - **Number:** Type a number for the rule, such as `100`.
   - **Rule action:** Select **accept** from the drop-down list.
   - **Protocol:** Select **All protocols** from the drop-down list.
   - **Source CIDR block::** Type `0.0.0.0/0`.
   - **Destination CIDR block::** Type `0.0.0.0/0`.
   - **Description:** (Optional) Type a description for the rule.
6. Click **Create**.

Create a traffic mirror session

You must create a session for each AWS resource that you want to monitor with Reveal(x) 360. You can create a maximum of 500 traffic mirror sessions per sensor.

For more information, see the following AWS documentation: Getting started with Traffic Mirroring.

1. In the AWS Management Console, in the left pane, under Traffic Mirroring, click **Mirror Session**.
2. Click **Create traffic mirror session** and complete the following fields:
   - **Name tag:** (Optional) Type a descriptive name for the session.
   - **Description:** (Optional) Type a description for the session
   - **Mirror source:** Select the source ENI. The source ENI is typically attached to the EC2 instance that you want to monitor.
   - **Mirror target:** Select the traffic mirror target ID generated for the target ENI.
   - **Session number:** Type `1`.
   - **VNI:** Leave this field empty.
   - **Packet length:** Leave this field empty.
   - **Filter:** From the drop-down menu, select the ID for the traffic mirror filter you created.
3. Click **Create**.

View sensor status

1. Return to the Reveal(x) 360 Administration page.
2. Click **Sensors** in the upper right corner.
3. Find your sensor in the table and view the sensor status.

   When the sensor status changes from Pending to Running, you can view metrics, detections, and records for your AWS traffic in Reveal(x) 360 by clicking **Reveal(x) 360 Console** from the Administration page.

It can take a few minutes for your traffic to appear in the system.