Reveal(x) 360 Best Practices

Published: 2021-09-04

Reveal(x) 360 offers a flexible and highly-customizable environment. Depending on how your AWS traffic is structured, you can deploy Reveal(x) 360 sensors in a number of configurations and filter your AWS traffic to minimize duplication. This guide provides recommendations that can help optimize your Reveal(x) 360 experience and avoid unnecessary costs.

See the following related guides about Reveal(x) 360:

- Reveal(x) 360 Setup and Administration Guide
- Deploy Reveal(x) 360 sensors for AWS
- Connect to Reveal(x) 360 from self-managed sensors

Deployment Architecture

We recommend that you organize your AWS workloads in a way that optimizes for cost by assessing potential data transfer charges against the cost of deploying additional sensors. In general, you should deploy only the number of sensors necessary for your total throughput and number of mirror target interfaces.

While you can deploy one sensor per Virtual Private Cloud (VPC) and Availability Zone (AZ) pair to avoid data transfer fees, in some low-traffic environments it might be more cost-effective to deploy fewer sensors and pay for minor cross-VPC, cross-AZ transfer fees.

Note: You can share a mirror target interface across multiple AWS accounts

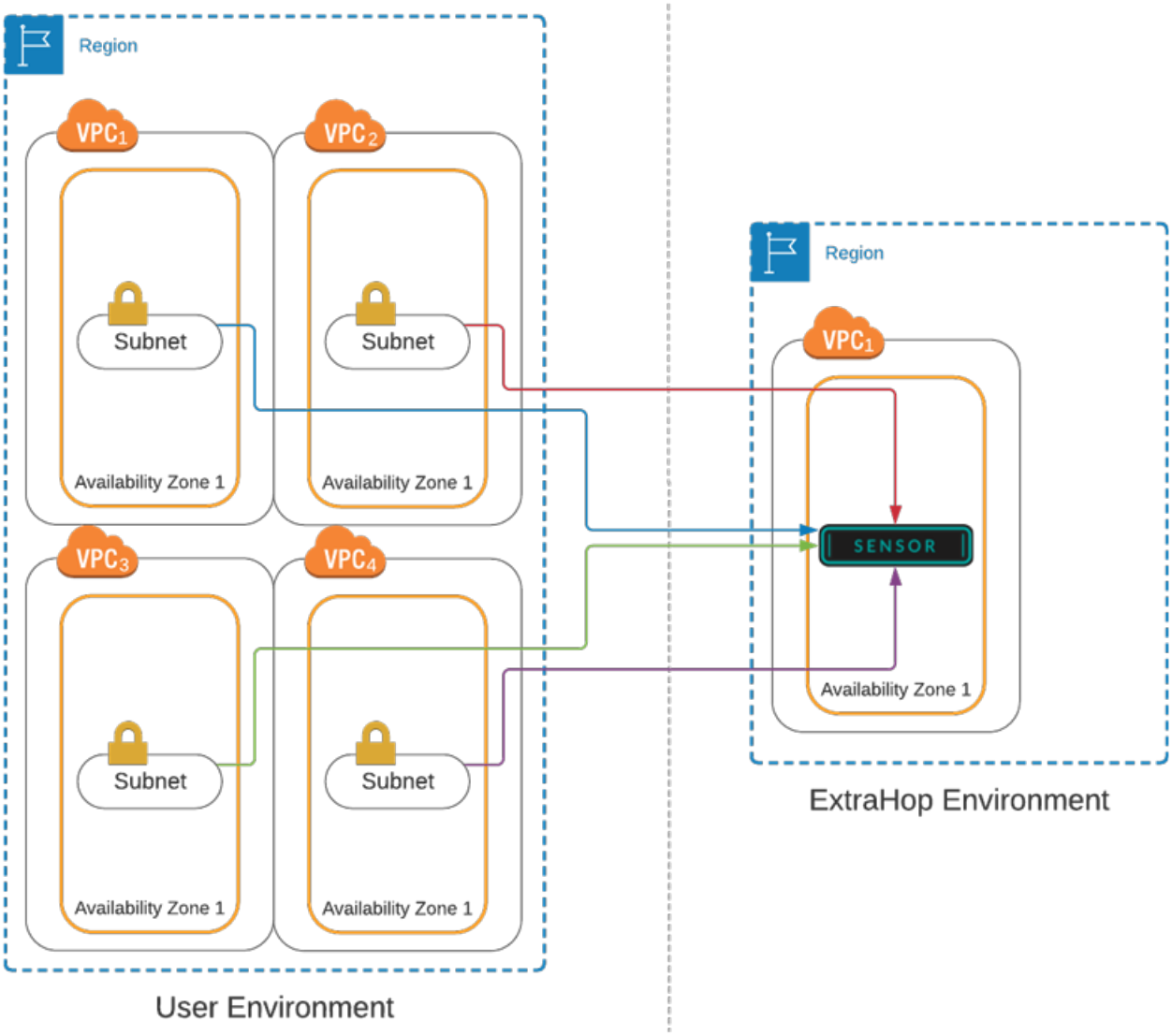
The following sections show a few ways that you can organize your workloads and connect to Reveal(x) 360 sensors.

Single Availability Zone

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 are determined by the sensor package size.

For example, you can connect up to 7 mirror target interfaces to a sensor in the medium-sized package.



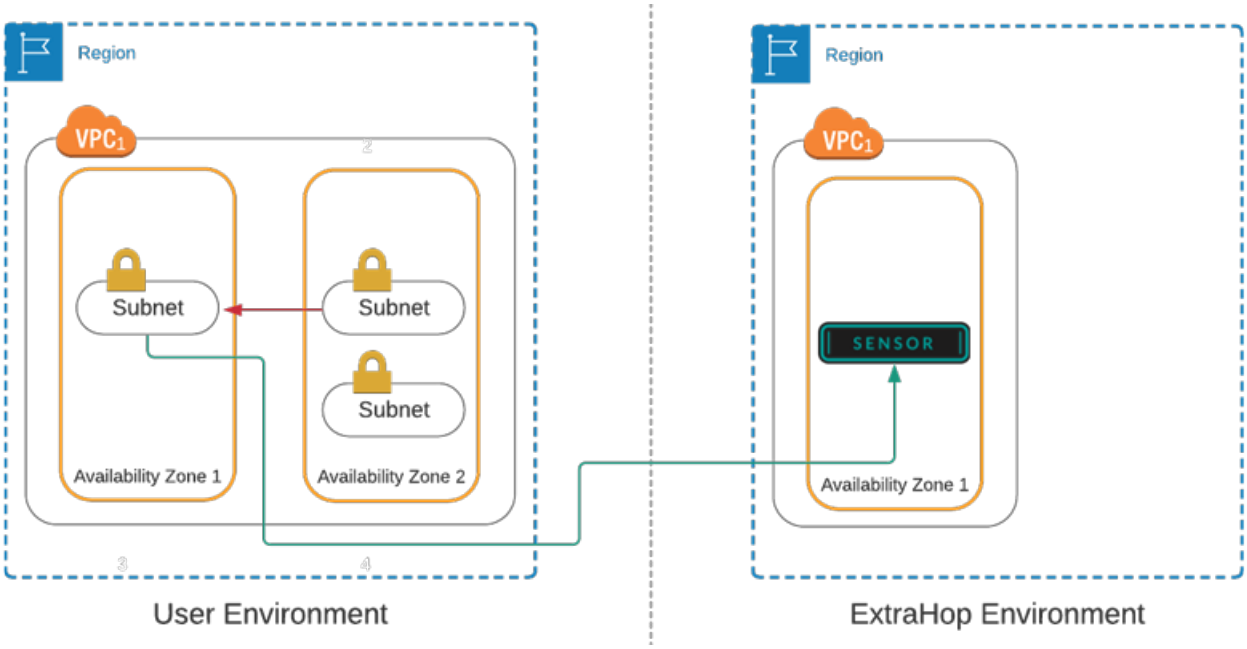
As long as the AZ is the same across your VPCs and matches the AZ that the sensor is in, there are no data transfer charges.

Multiple Availability Zones

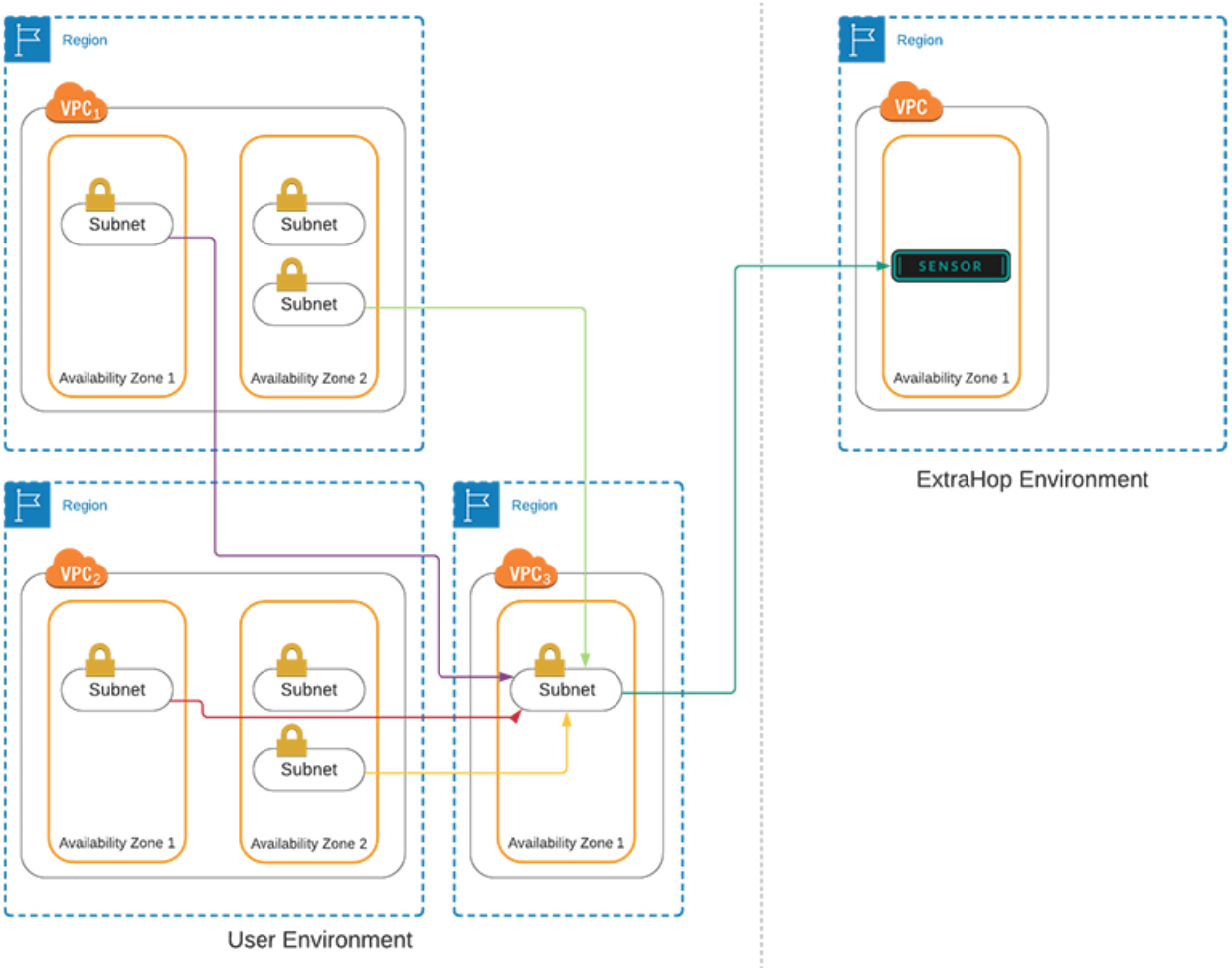
If you have subnets in multiple AZs, you can organize your workloads to mirror traffic directly from the subnets in each AZ to a single sensor. In this type of configuration, you must create a mirror target instance for each subnet that has traffic that you want to mirror to the sensor.

> **Important:** This configuration incurs data transfer fees between your AZs. Make sure that the data transfer fees for your traffic are less than the cost of deploying additional sensors.

While the mirror target interfaces do not have to be in the same VPC or even AWS account, the mirror target interfaces and the sensor must be in the same AZ.



For AWS workloads that span multiple AZs and VPCs, we recommend that you create a dedicated monitoring VPC with two subnets—one configured for 172.16.0.0/12 and one for 192.168.0.0/16. You can create the dedicated monitoring VPC in either the same or different AWS accounts than your workloads depending on your infrastructure.



This type of configuration ensures that your mirrored traffic is unaffected by any changes to your production environment and enables you to mirror traffic from the subnets in your VPCs with non-routable addresses to a subnet with an alternate non-routable address.

- Route workload traffic from subnets on 10.0.0.0/8 to the monitoring subnets of either 172.16.0.0/12 or 192.168.0.0/16.
- Route workload traffic from a subnet on 192.168.0.0/16 to the monitoring subnet of 172.16.0.0/12.
- Route workload traffic from a subnet on 172.16.0.0/12 to the monitoring subnet of 192.168.0.0/16.

In this type of configuration, you only need to create one mirror target interface on the monitoring VPC to mirror traffic to the sensor in the same AZ.

Note: This configuration incurs data transfer fees between your AZs. Make sure that the data transfer fees for your traffic are less than the cost of deploying additional sensors.

Filtering traffic

The following filtering rules 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. This rule ensures that a web server request is not mirrored twice: once from the sending web 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. These filters should only be applied when mirroring all of the instances in a CIDR block.

Table 1: Inbound Rules

Number	Rule Action	Protocol	Source CIDR Block	Destination CIDR Block
100	Reject	All	CIDR block for the subnet	CIDR block for the subnet
200	Accept	All	0.0.0.0/0	0.0.0.0/0

Table 2: Outbound Rules

Number	Rule Action	Protocol	Source CIDR Block	Destination CIDR Block
100	Accept	All	0.0.0.0/0	0.0.0.0/0

See Create a traffic mirror filter in the Deploy Reveal(x) 360 sensors for AWS guide for help adding these rules to your AWS VPC.