WHITE PAPER

Corelight Sensor deployment architecture for AWS

Today's organizations understand the benefits of public cloud environments — but it's just as important to understand the associated risks. Network traffic visibility is a critical pillar in overall security assessment. Corelight Cloud Sensors enable customers to extend the benefits of Open Network Detection and Response (NDR) and rich logging to these cloud environments.

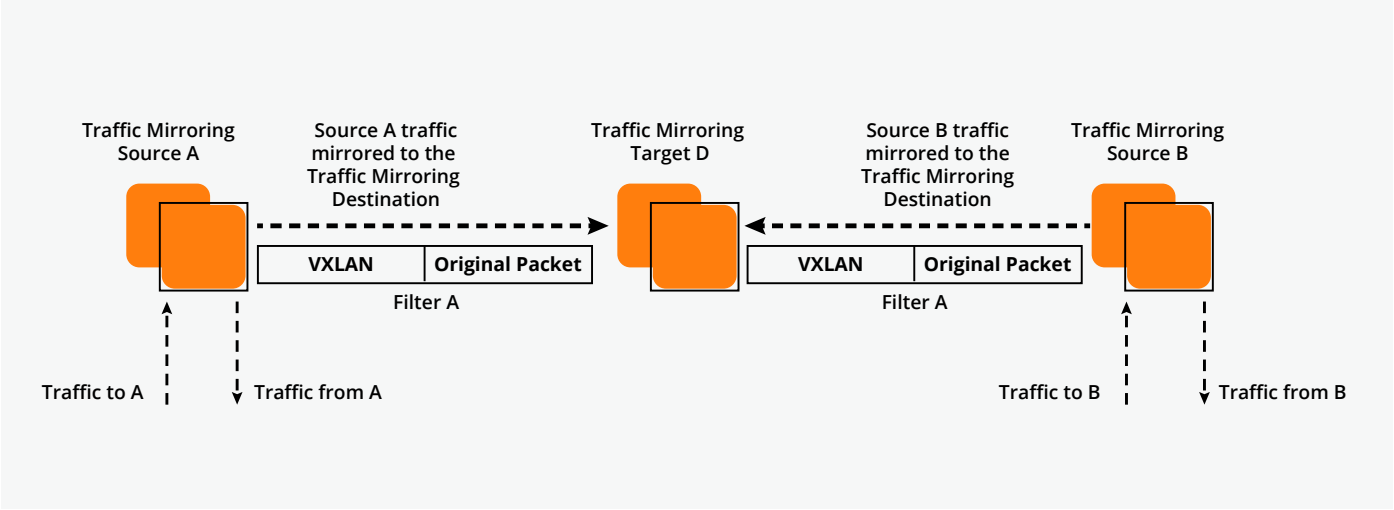
In this paper, we will provide several example architectures using cloud native technologies in conjunction with Corelight Sensors to ensure complete network visibility and protection within AWS. We will highlight the benefits and considerations for each to help identify which cloud deployment is best for your organization and unique environment.

Four examples will be covered in this paper:

- **AWS VPC Traffic Mirroring:** Ideal for smaller environments where the sensor may be colocated with the traffic you are looking to assess
- **AWS Gateway Load Balancer:** For multiple accounts or multiple VPC environments where you may want to utilize AWS Gateway Load Balancers to aggregate your traffic
- **AWS Gateway Load Balancer with Corelight Sensors:** Building on leveraging GWLB, we will walk through an example of their use with Corelight Sensors
- **AWS Gateway Load Balancer with Corelight Cloud Sensor SaaS:** Let Corelight take on the burden of management, updating, and scaling your sensors

AWS VPC TRAFFIC MIRRORING

AWS VPC Traffic Mirroring allows customers to mirror traffic from an elastic network interface (ENI) attached to select EC2 instances. AWS supports Traffic Mirroring on specific instance types listed on the AWS limitations and quota page. Also note that it is not possible to mirror traffic from other devices or services such as IGW, TGW, NAT-GW, or ALB/NLB.



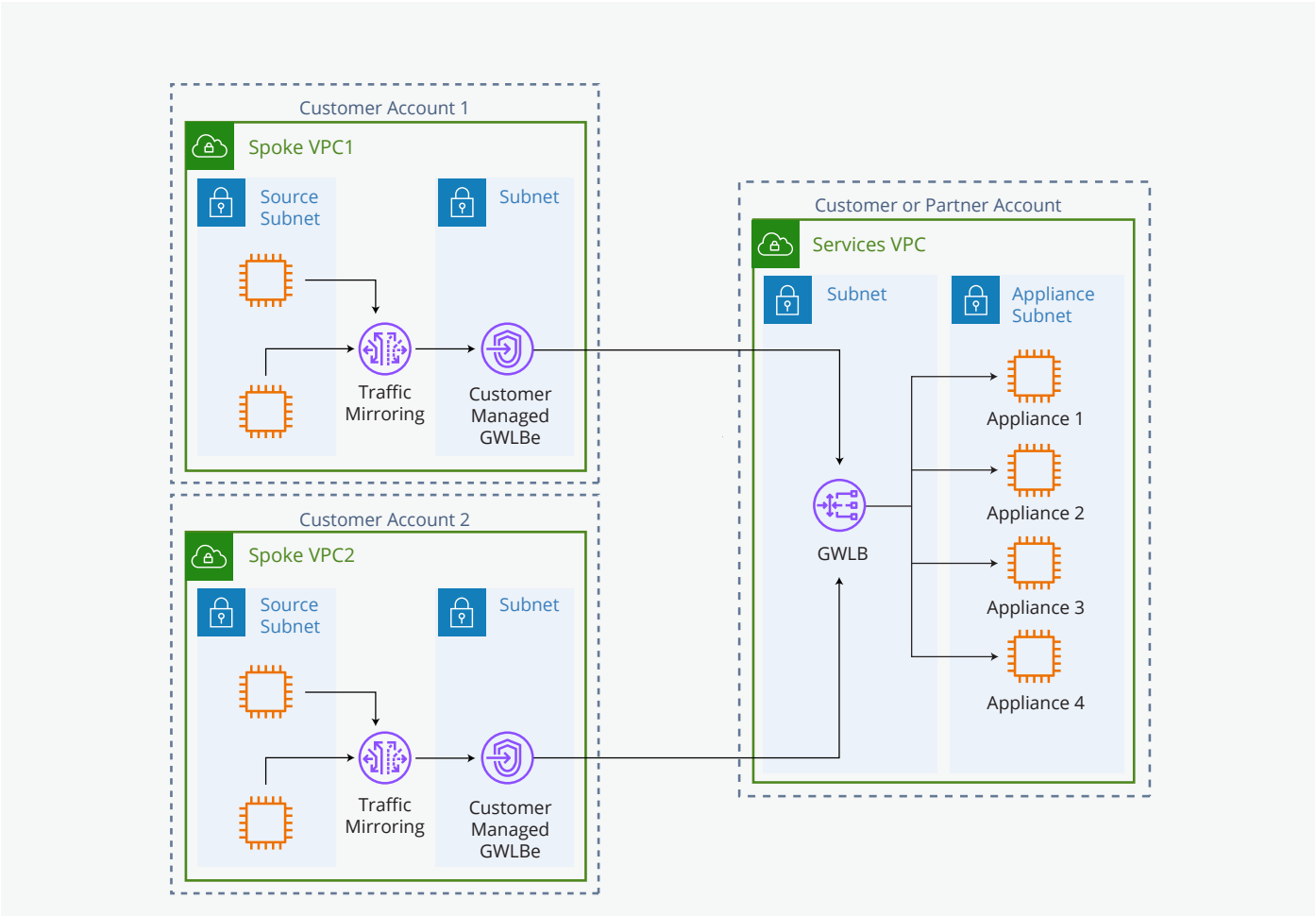
This diagram shows how VPC Traffic Mirroring encapsulates the original network packet with a VXLAN header before sending it to the target instance. A Corelight Cloud Sensor target instance will automatically remove this header.

Traffic Mirroring is helpful for targeted traffic inspection when the source instances are more static in nature. You can utilize AWS Event Bridge and a Lambda function to automate the creation of the Traffic Mirror sessions. This approach involves detecting when a new EC2 instance is started/created and then initiating a predefined mirror session to a predefined target. Other solutions, such as AWS AutoMirror, can also be used via instance metadata tagging. AWS does set a cap at 10,000 mirrored sessions, which should be plenty for most organizations given the dispersion of functions across multiple AWS accounts.

Traffic Mirroring works on a source, filter, and target flow, where the source is the ENI attached to a supported EC2 instance where traffic inspection is desired. The filter specifies what traffic to mirror based on the source/destination port and address, protocol, direction, and traffic actions that will be sent to the target. The target is the ENI attached to another EC2 instance within AWS, typically some type of network inspection system.

Please consult the AWS pricing calculator on the "Network Analysis" tab for guidance as this cost will vary depending on region and contract.

For VPC Traffic Mirroring, the target could be a dedicated instance, Network Load Balancer (NLB), or Gateway Load Balancer (GWLB). Mirroring to a dedicated instance is helpful for ad-hoc troubleshooting and other on-demand use cases, but does not scale in large distributed cloud environments that require centralized ownership of a highly available security visibility stack. While both NLBs and GWLBs centralize monitoring sensors, NLB requires peering connections with each source VPC. In a highly scaled-out environment, peering a large number of VPCs or connecting them via a Transit Gateway can be challenging.

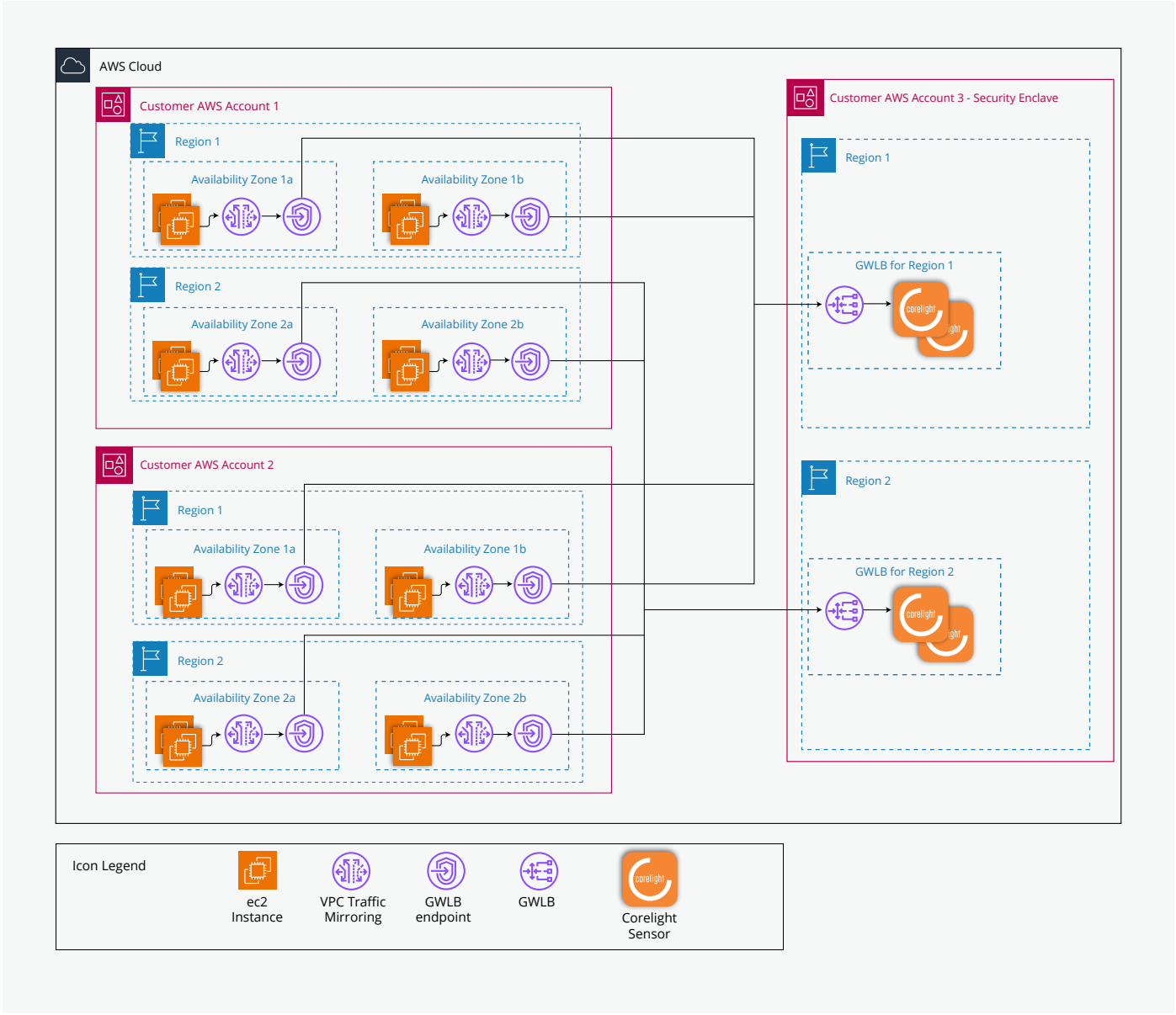


This diagram shows how a GWLBe can also be a target of VPC Traffic Mirroring, which allows mirror sessions to send data to network sensors hosted in other accounts, even by security providers such as Corelight.

AWS GATEWAY LOAD BALANCERS (GWLB)

AWS's Gateway Load Balancers can send data across VPC boundaries without VPC peering. By using a GWLB in concert with a GWLB endpoint (GWLBe), customers can send data via the endpoints to a GWLB outside of the primary account by pairing the two together.

There are some potential cost considerations to take into account when using GWLB/GWLBe. Traffic that is kept in the same AWS region and Availability Zone (AZ) does not incur any network traffic charges from AWS, even across multiple accounts. When using a GWLB within a region with AZ affinity (e.g., where the LB is tied to multiple AZs), you will incur no additional network charges if a GLWBe is used per AZ. Please see the AWS data transfer cost page for more detailed information.



This diagram illustrates an architecture where traffic within an AZ is sent to a matching Corelight Sensor residing in either a separate AWS account or VPC security enclave. The GWLB has AZ affinity; e.g., when created, it is tied to the AZs where the GWLBe will reside. This would be repeated across all AWS accounts and AZs where traffic inspection is desired.

GWLBe encapsulates the original IP traffic plus the VPC Traffic Mirror session VXLAN encapsulation with a GENEVE header and forwards it to the appliance VPC GWLB over UDP port 6081. When the Corelight Sensor receives traffic as the target of the GWLB, it will strip both the GENEVE header and the VXLAN header and process the de-encapsulated traffic.

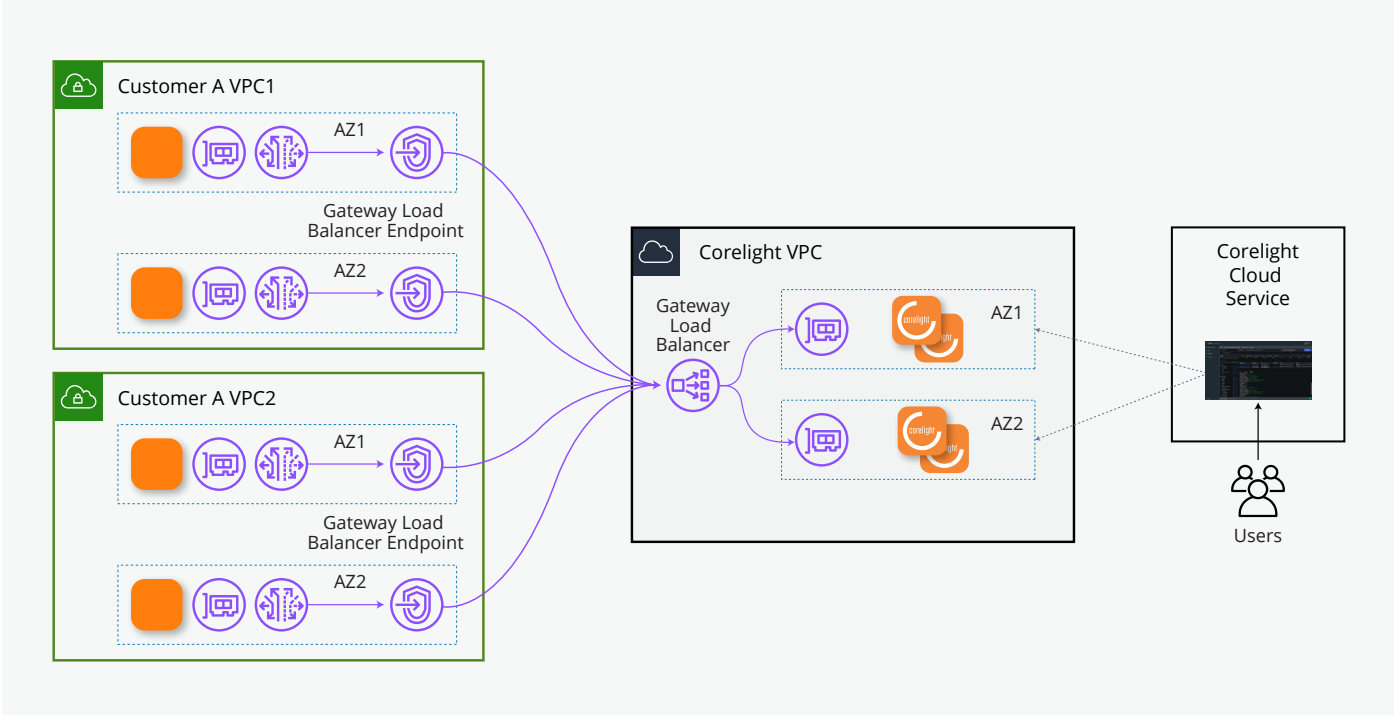
Corelight Sensors may be deployed as either Customer Hosted or Cloud Sensor SaaS, which is Corelight hosted.

CORELIGHT SENSOR DEPLOYMENT (CUSTOMER HOSTED)

For a Customer-Hosted deployment, we recommend that you use a centralized VPC for network traffic inspection. Your security team would manage and administer the security enclave VPC containing the Corelight Sensors behind a GWLB. Corelight Sensors can be managed via Infrastructure as Code (IaC) tools or by Corelight Fleet Manager.

Auto-scaling Corelight Sensors behind GWLB via an auto-scaling group creates an elastically scalable sensor group that can expand and contract based on network traffic demand. GWLB retains AZ affinity, meaning that each AZ's traffic remains in the same AZ without incurring inter-AZ transit charges. GWLBe is deployed in each AZ where traffic is mirrored.

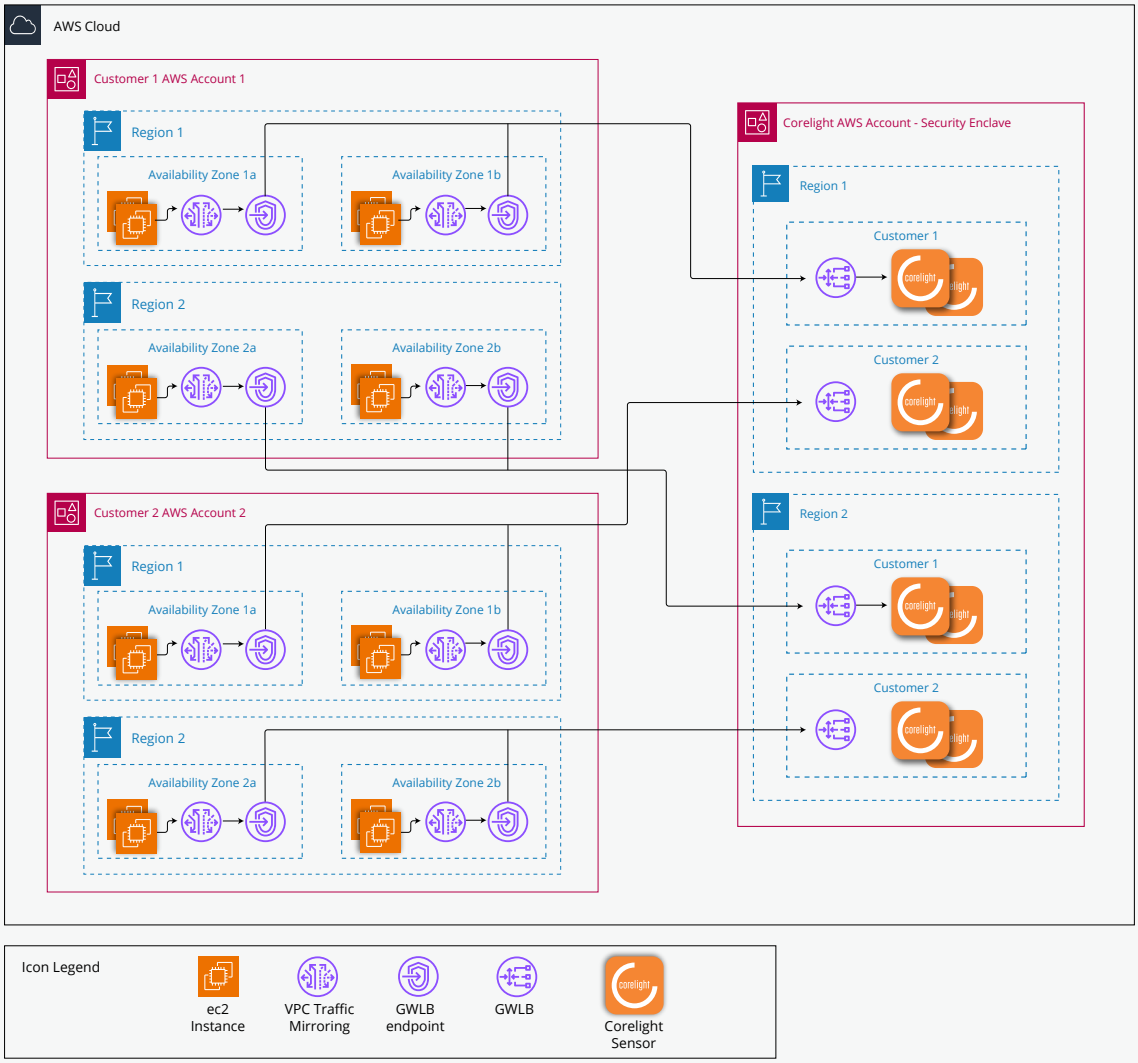
When creating an elastically scalable group of sensors, one can follow the AWS ELB guide.



This diagram shows a high-level overview of how the Corelight-hosted sensor model would work using GWLB fed by GWLBe.

Specific roles are required to create a VPC Traffic Mirror session. This role would need to be tied to any user or automation that creates the Traffic Mirror sessions.

You can monitor mirrored traffic using Amazon CloudWatch, which collects information from network interfaces that are part of a Traffic Mirror session and creates readable, near real-time metrics. This information can be used to monitor and troubleshoot Traffic Mirroring sessions.



This diagram illustrates an architecture where traffic within an AZ is sent to a matching Corelight Sensor residing in a Corelight AWS account within that same region. Each customer has an entirely segmented sensor and GWLB that feeds its data within each region where mirroring is needed. The number of sensors deployed in each AZ for a customer will scale with the load coming into the GWLB and an autoscaling group.

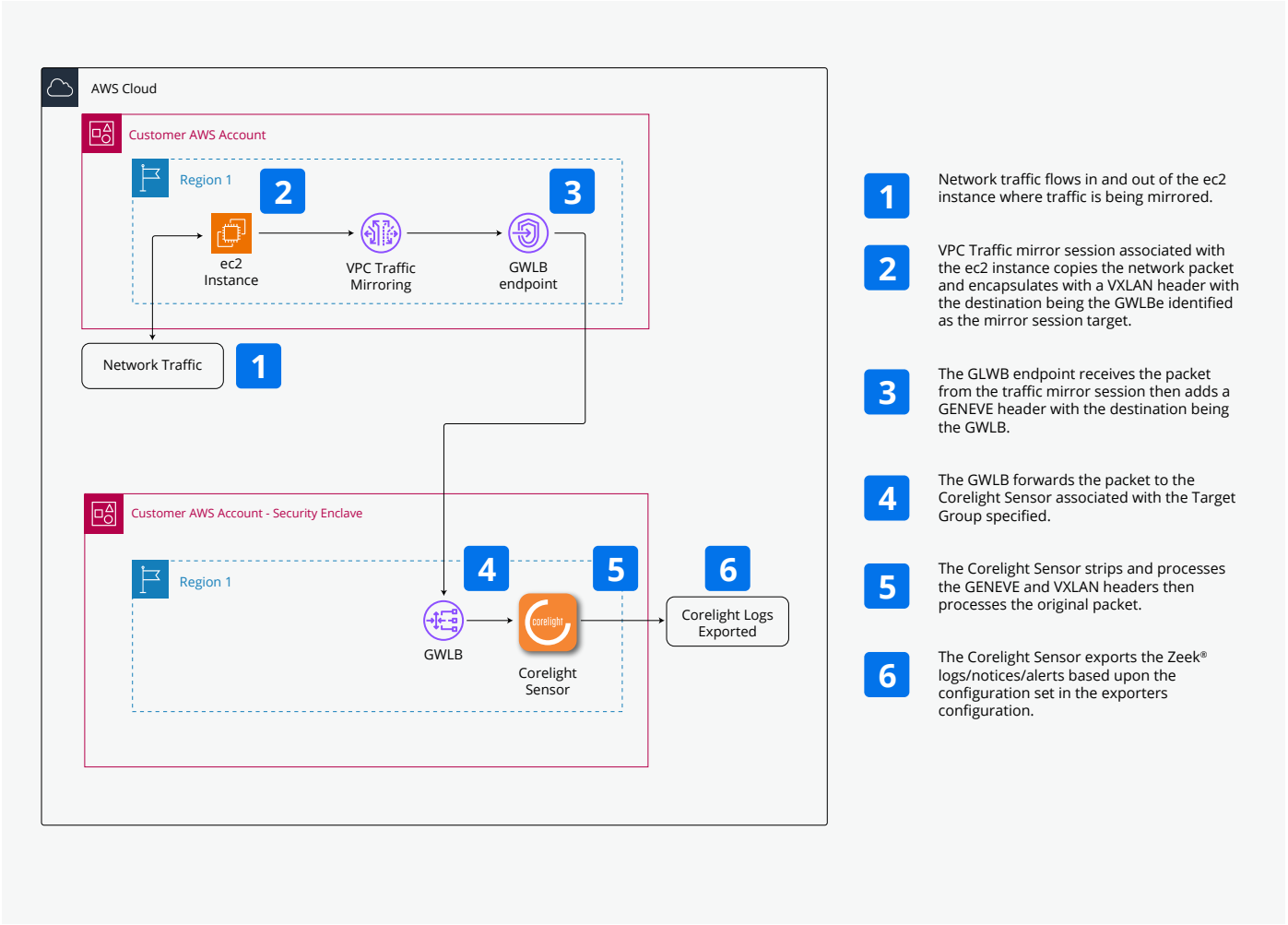
Once the Corelight Sensor analyzes the traffic, it can be exported to multiple destinations. These exports can be configured using the Fleet Manager or Corelight config.

CORELIGHT CLOUD SENSOR SAAS DEPLOYMENT (CORELIGHT HOSTED)

When utilizing Corelight Cloud Sensor SaaS, the sensors are deployed in Corelight's VPC. Corelight assumes the cost of running, deploying, and maintaining the sensors instead of the customer. For the Cloud Sensor SaaS option, data exported from your AWS environment to the ultimate destination is also removed from customer costs. Corelight only supports the use of GWLBe in the customer AWS account to a GWLB in a Corelight AWS account for Cloud Sensor SaaS.

DATA FLOW

In the diagram below, you'll see how data would flow from an EC2 instance to the Corelight Sensor and out to an external log collection source, such as a SIEM.



SUMMARY

As with any system architecture, there are varying ways to achieve the desired result. Each deployment of Corelight Cloud Sensors will be different for each customer — with costs, manageability, and visibility coming into play. The utilization of AWS VPC Traffic Mirroring along with GWLB capabilities to feed Corelight Sensors will provide surgical and elastic network visibility across the AWS compute infrastructure.

To learn more about the Corelight, request a demo at **https://corelight.com/contact**

Corelight provides security teams with network evidence so they can protect the world's most critical organizations and companies. On-prem and in the cloud, our open Network Detection and Response Platform enhances visibility and analytics, leading to faster investigations and expanded threat hunting. Corelight's global customers include Fortune 500 companies, major government agencies, and large research universities. Based in San Francisco, Corelight is an open-core security company founded by the creators of Zeek®, the widely-used network security technology.

info@corelight.com | 888-547-9497