AWS Egress-Only Internet Gateway (EIGW)

An **Egress-Only Internet Gateway (EIGW)** is an AWS-managed service designed to ensure that resources with IPv6 addresses in a private subnet can access the internet while remaining private and protected from unsolicited inbound traffic. This is particularly important because, unlike IPv4, IPv6 addresses are public by default, meaning instances with IPv6 addressing could potentially be reachable from the internet. The EIGW acts as a safeguard, enabling outbound-only internet connectivity for IPv6-enabled resources, such as downloading updates or communicating with external services, without exposing these resources to inbound traffic.

To use an EIGW, you must create and attach it to a VPC, then update the route table of the private subnet to direct all IPv6 internet-bound traffic (::/0) through the EIGW. This setup ensures that your private instances can access the internet securely while maintaining their privacy. Unlike a standard Internet Gateway, the EIGW explicitly prevents inbound connections, making it a critical component for securing IPv6-enabled architectures. For the AWS Solutions Architect Associate exam, understanding the purpose and configuration of an EIGW demonstrates your ability to design secure and efficient VPC architectures that accommodate the unique characteristics of IPv6.

The **Egress-Only Internet Gateway (EIGW)** does not replace the **Internet Gateway (IGW)**; they serve different purposes and are often used together in specific scenarios depending on the networking requirements of your AWS environment:

1. **Internet Gateway (IGW):**
    - Allows both **inbound** and **outbound** internet traffic for resources in a VPC.
    - Supports IPv4 and IPv6 traffic.
    - Commonly used for public-facing resources, such as web servers, that need to both receive and send internet traffic.
2. **Egress-Only Internet Gateway (EIGW):**
    - Allows **outbound-only** internet access for **IPv6** traffic.
    - Blocks any unsolicited **inbound** internet traffic to ensure resources remain private.
    - Specifically designed to address the challenge of IPv6 addresses being publicly routable by default.

When to Use Each Gateway

- Use an **Internet Gateway (IGW)** for resources that need bidirectional internet access (e.g., public-facing applications).
- Use an **Egress-Only Internet Gateway (EIGW)** for private resources with IPv6 addresses that only need outbound internet access (e.g., downloading patches or accessing external APIs) without exposing them to inbound connections.

Both gateways can coexist in the same VPC, serving different subnets or use cases. For example, a VPC can have an IGW for public-facing instances in a public subnet and an EIGW for private instances with IPv6 addresses in a private subnet.