https://medium.com/awesome-cloud/aws-vpc-endpoints-overview-intro-getting-started-guide-91ca23b5af8d

AWS — VPC Endpoints Overview

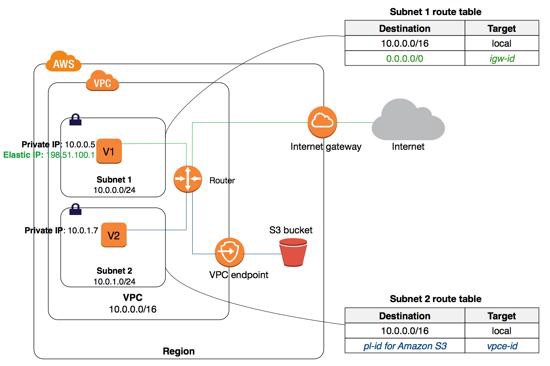
[Ashish Patel](https://iamaashishpatel.medium.com/?source=post_page-----91ca23b5af8d-----------------------------------)

[Ashish Patel](https://iamaashishpatel.medium.com/?source=post_page-----91ca23b5af8d-----------------------------------)

Follow

[Apr 5, 2020](https://medium.com/awesome-cloud/aws-vpc-endpoints-overview-intro-getting-started-guide-91ca23b5af8d?source=post_page-----91ca23b5af8d-----------------------------------) · 3 min read

Introduction to AWS VPC Endpoints — What is VPC Endpoints?



AWS — VPC Endpoints

TL;DR

[VPC endpoint](https://docs.aws.amazon.com/vpc/latest/userguide/vpc-endpoints.html) enables creation of a private connection between VPC to supported AWS services and VPC endpoint services powered by PrivateLink using its private IP address. Traffic between VPC and AWS service does not leave the Amazon network.

There are two types of VPC endpoints:

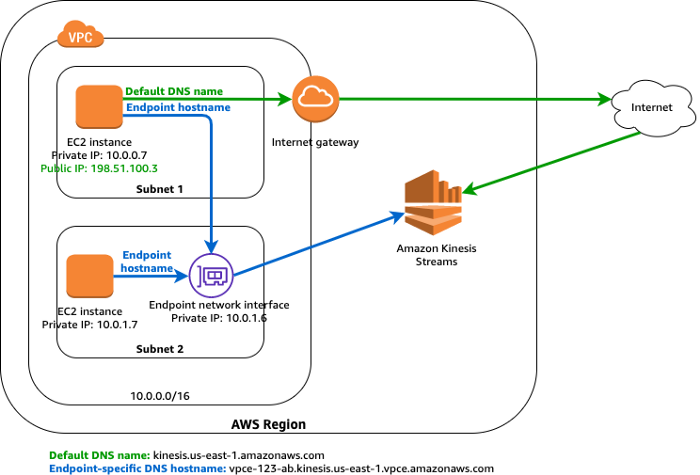
[**Interface endpoint**](https://docs.aws.amazon.com/vpc/latest/userguide/vpce-interface.html)is an elastic network interface (ENI) with a private IP address from the IP address range of user’s subnet that serves as an entry point for traffic destined to a supported service. It enables you to privately access services by using private IP addresses.

[**Gateway endpoint**](https://docs.aws.amazon.com/vpc/latest/userguide/vpce-gateway.html) is a gateway that you specify as a target for a route in your route table for traffic destined to a supported AWS service. Currently supports S3 and DynamoDB services.

VPC Endpoints Key points

1. VPC endpoint enables users to privately connect their VPC to supported AWS services.
2. VPC Endpoint does not require a public IP address, access over the Internet, NAT device, a VPN connection or AWS Direct Connect to communicate with resources in the service.
3. Endpoints are virtual devices, that are horizontally scaled, redundant, and highly available VPC components that allow communication between instances in the VPC.
4. Access to the resources in other services can be controlled by endpoint policies.
5. By default, Endpoint policy, allows full access to the service. Endpoint policies must be written in JSON format.
6. Endpoint policy does not override or replace IAM user policies or service-specific policies (such as S3 bucket policies).

**Interface Endpoints:**



AWS — VPC Endpoints — Interface Endpoints

1. When you create an interface endpoint, AWS generate endpoint-specific DNS hostnames (private) that you can use to communicate with the service. This is optional.
2. Network ACL for the subnet can restrict traffic, and needs to be configured properly.

**Gateway Endpoints:**

1. A route is automatically added to the Route table with a destination that specifies the prefix list of service and the target with the endpoint id.  
   e.g. *A rule with destination s3 service (pl-63a5400a (com.amazonaws.us-east-1.s3, 54.231.0.0/17, 52.216.0.0/15, 3.5.16.0/21, 3.5.0.0/20))* *and a target with this endpoints’ id(e.g.*vpce-0b66ba758a38cef8c*) will be added to the route tables.*
2. Endpoint needs to be associated with the Route table and the route table cannot be modified to remove the route entry. It can only be deleted by removing the Endpoint association with the Route table or when the endpoint is deleted.
3. Security groups needs to be modified to allow Outbound traffic from the VPC to the service that specified in the endpoint. Use the service prefix list ID (e.g. *com.amazonaws.us-east-1.s3)* as the destination in the outbound rule.
4. Multiple endpoints can be created in a single VPC, for multiple services.
5. Multiple endpoints to the same service cannot be specified in a single route table.
6. You can create multiple endpoints in a single VPC for a single service, But *different route tables*used to enforce different access policies from different subnets to the same service.
7. You can modify the endpoint policy that’s attached to your endpoint, and add or remove the route tables that are used by the endpoint.

VPC Endpoints Limitations

1. VPC endpoints support IPv4 traffic only.
2. Endpoints are supported within the same Region only. You cannot create an endpoint between a VPC and a service in a different Region.
3. Endpoints cannot transfer an endpoint from one VPC to another, or from one service to another.

**Interface Endpoints:**

1. For each interface endpoint, you can choose only one subnet per Availability Zone.
2. Each interface endpoint can support a bandwidth of up to 10 Gbps per Availability Zone by default. Additional capacity may be added automatically based on your usage.
3. Interface Endpoint supports TCP traffic only.
4. Endpoints cannot be transferred from one VPC to another, or from one service to another.

**Gateway Endpoints:**

1. Endpoint connections cannot be extended out of a VPC i.e. resources across the VPN connection, VPC peering connection, AWS Direct Connect connection cannot use the endpoint