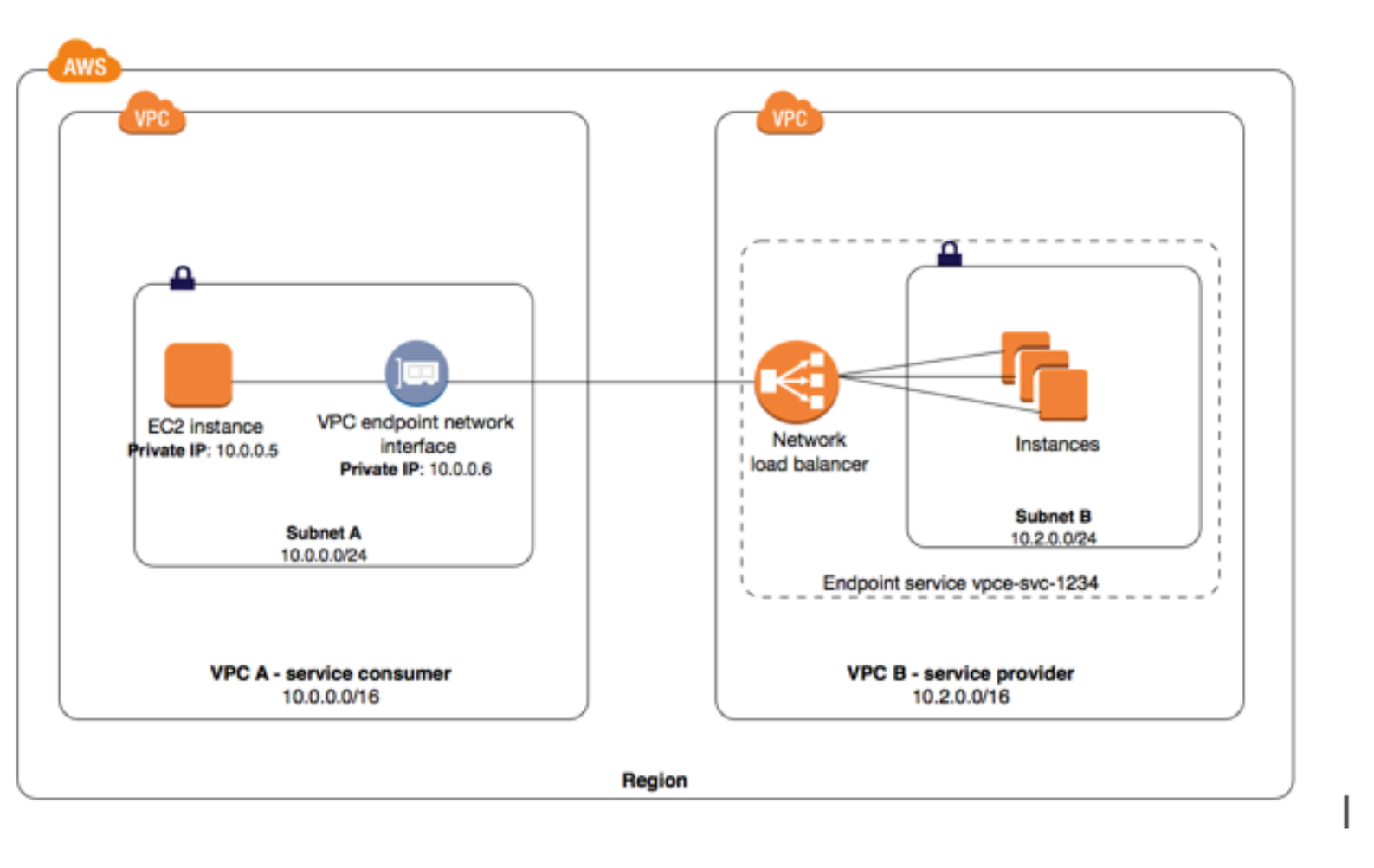
Cloud Network Security 101: AWS VPC Endpoints

Becki Lee | September 12, 2019



Network security is critical to operating in the cloud. There are many different ways you can secure your network, but the best approach is to layer multiple methods. The more layers implemented in your security, the harder it is for malicious actors to access your network.

In a three part blog series, we will focus on several "layers" of practicing defense in depth. This first blog discusses VPC endpoints - what they are, how they work, limitations of using endpoints, and how they can help improve network security.

For the security-minded, Amazon Web Services VPC endpoints present a safer way to allow network resources to connect to other AWS services. Prior to the introduction of endpoints, VPC resources had to go out to the internet to communicate with certain services. This poses a potential security and availability risk, and complicates infrastructure architecture.

Now, VPC endpoints allow traffic to flow between a VPC and other services without ever leaving the Amazon network. This introduces a number of benefits, not the least of which is improved network security.

What is a VPC endpoint?

An endpoint is a network component that connects EC2 instances in a VPC to certain AWS services without requiring public IP addresses. With a VPC endpoint, instances don't need a NAT device, VPN connection, internet gateway, or AWS Direct Connect to communicate with supported services — they can communicate solely within AWS.

There are two types of VPC endpoints:

- Interface endpoints
- Gateway endpoints

Both types keep traffic within the AWS network, but support different services and work in different ways. The destination service dictates which endpoint type you should use — see the AWS documentation for details.

What are AWS VPC interface endpoints?

An interface endpoint is an elastic network interface that allows a private IP address in a subnet to connect VPC resources to a number of AWS services, such as CloudFormation, Elastic Load Balancers (ELBs), SNS, and more.

Interface endpoints also let VPC resources connect to supported AWS Marketplace partner services in addition to endpoint services, which are hosted by AWS customers or partners in their own VPCs.

Traffic from VPC resources to the endpoint network interface is controlled by security group rules. AWS PrivateLink then enables the endpoint to connect the traffic to other services without going over the internet.

AWS charges usage and data processing rates for PrivateLink, so there are additional costs involved with creating and using an interface endpoint.

How do AWS VPC interface endpoints work?

When you choose one or more subnets in a VPC to use your interface endpoint, AWS creates an endpoint network interface in each selected subnet.

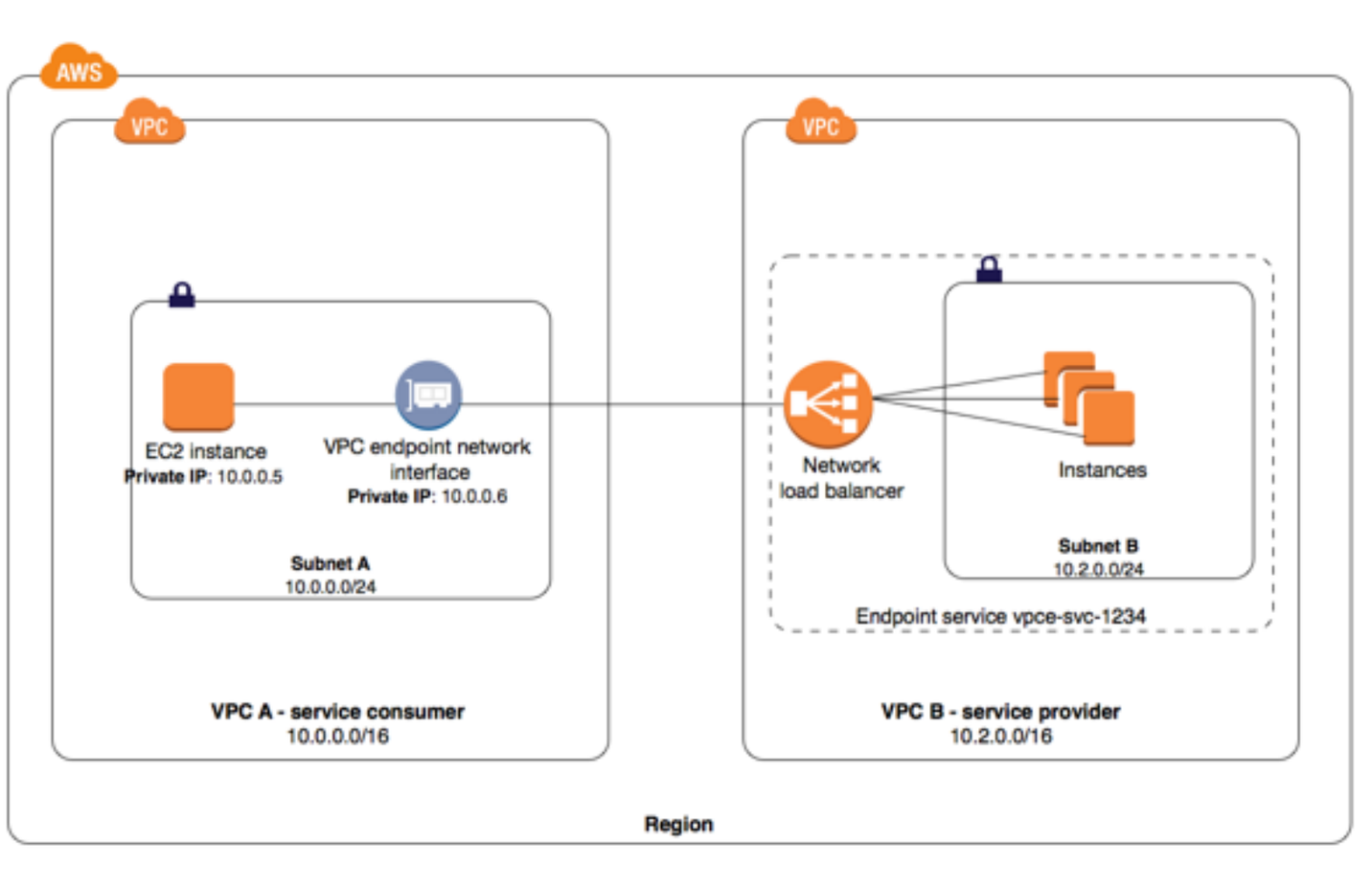
Next, you associate security groups with the endpoint network interface. The security group must have a rule allowing communication between the endpoint network interface and the resources in the VPC that need to connect to the service.

You can then optionally enable private DNS when connecting to the service, which allows requests to use the default DNS hostname instead of endpoint-specific hostnames. Private DNS is enabled by default for AWS and AWS Marketplace services.

Finally, the owner of the service, such as AWS itself or a third party from the Marketplace — known as the **service provider** — either manually or automatically accepts endpoint requests from you, the **service consumer**.

Accepted endpoint requests are then privately connected to the service.

Interface endpoints also allow you to attach an endpoint policy controlling access to the service.



Above, instances in subnet A of VPC A use an interface endpoint to access the services in subnet B. Image from https://docs.aws.amazon.com/vpc/latest/userguide/endpoint-service.html

What are AWS VPS gateway endpoints?

In contrast, a gateway endpoint is a target for a route in a route table to connect VPC resources to S3 or DynamoDB. Traffic is then routed from instances in a subnet to one of these two services.

A VPC may have multiple gateway endpoints to different services in a route table or multiple gateway endpoints to the same service in different route tables, but it may not have multiple gateway endpoints to the same service in the same route table.

Gateway endpoints do not use PrivateLink. Therefore, apart from the standard costs of data transfer and resource use, AWS doesn't charge extra for using gateway endpoints, unlike interface endpoints.

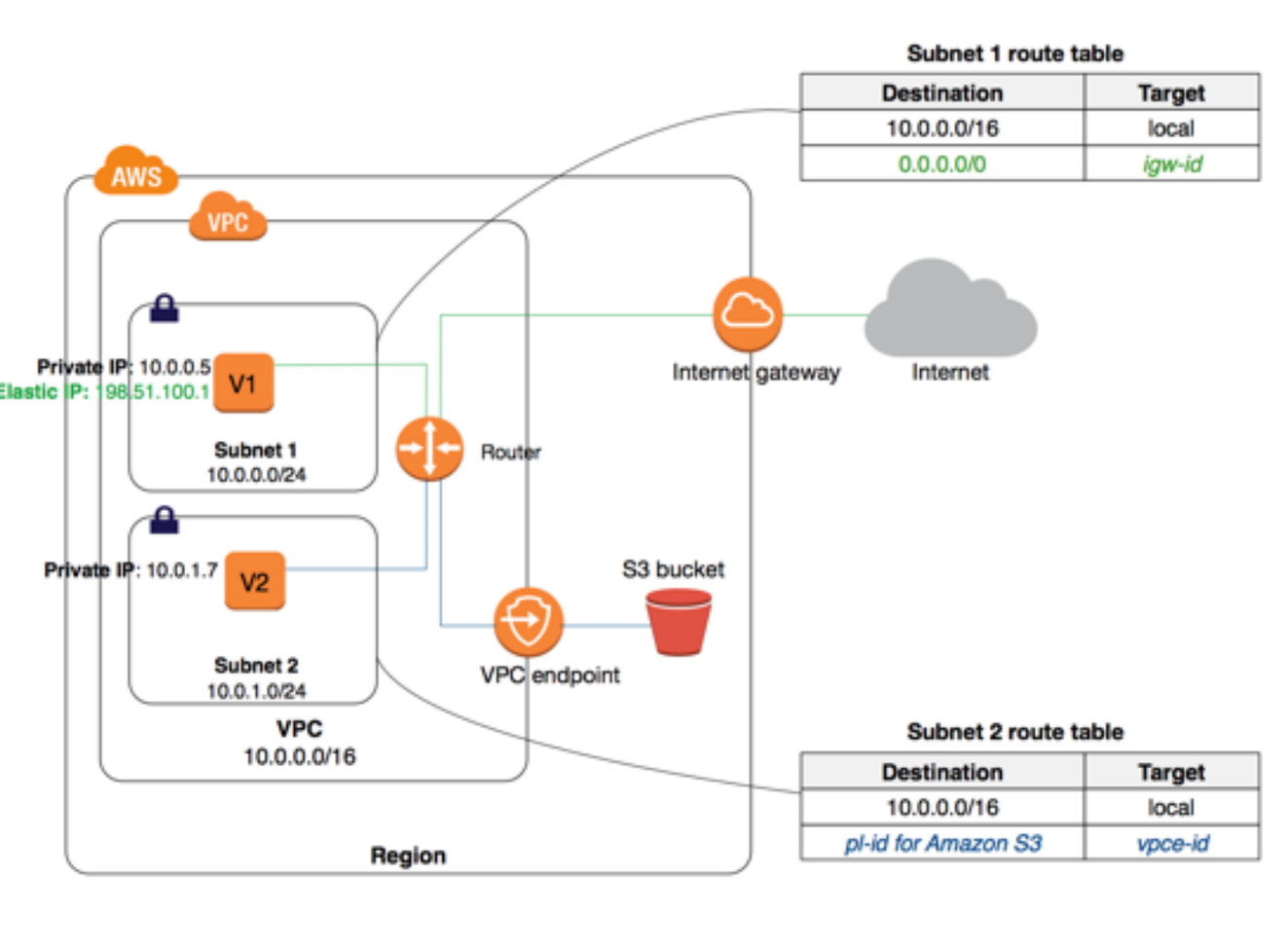
How do AWS VPC gateway endpoints work?

To set up a gateway endpoint, you specify the VPC and the service its resources will connect to. As with interface endpoints, you may specify a policy for the gateway endpoint to control access to the service.

Then, you specify the route table(s) where routes to the service will be created. Each created route has a destination set to the service prefix list ID and a target set to the endpoint ID.

Subnets associated with the route tables are automatically granted access to the endpoint, and traffic from instances in the subnet is routed through the endpoint to the service according to the endpoint policy. The default policy allows full access from any credentialed user or service within the VPC to S3 or DDB resources.

A VPC security group must have a rule allowing outbound traffic from the VPC to the specified service (S3 or DDB) in order for traffic to flow through a gateway endpoint.



Above, instances in subnet 2 can access Amazon S3 through the VPC gateway endpoint. Image from https://docs.aws.amazon.com/vpc/latest/userguide/vpce-gateway.html

VPC endpoints can improve network security

The biggest reason VPC endpoints are beneficial to network security is that there's no need for VPC resources to traverse the internet to reach a particular service. By preventing data from being unnecessarily exposed to the internet, it's easier to secure network traffic and ensure it remains compliant with standards such as PCI or HIPAA that concern sensitive data.

VPC endpoints also simplify infrastructure architecture. For example, you can use an interface endpoint to connect traffic from an instance to a service such as SQS, or you can:

- Configure an internet gateway
- Configure security group or network ACL rules
- Set up route tables
- Risk compromising your sensitive data

You can use a gateway endpoint to connect traffic from a private subnet to a service such as S3, or you can:

- Create a public subnet
- Launch an EC2 instance with an internet gateway or NAT device
- Route traffic to the internet to ultimately connect to S3
- Risk compromising your sensitive data

Additionally, VPC endpoints keep communication within AWS, which prevents availability risks and bandwidth constraints on your network traffic.

The limitations of VPC endpoints

There are a few items worth noting when using VPC endpoints:

- The VPC endpoint and service must be in the same region
- VPC endpoints support IPv4 traffic only
- Endpoints can't be transferred from one VPC or service to another
- S3 bucket policies can be used to control access to buckets from specific gateway endpoints or VPCs
- DynamoDB doesn't support resource-based policies, so access is only controlled through the gateway endpoint and user/role/group IAM policies

For more information on endpoint limitations, see the AWS documentation for interface endpointsand gateway endpoints.

VPC endpoints: Just one part of defense in depth

VPC endpoints are one element of a defense in depth approach to network security. Combined with tightly scoped security group and network ACL rules; IAM user/group/role, resource, and endpoint policies; and other methods of VPC security, you can effectively limit the exposure of critical data to the internet and more effectively secure your network.

To learn more about Fugue and how we can help with your cloud security, please visit fugue.co.

SEARCH

Search

RELATED POSTS

Cloud Network Security 101: AWS Security Groups vs NACLs
September 19, 2019

Securing Microsoft Azure Virtual Networks and Network Security Groups
November 1, 2019

Introducing the Engineer's Handbook on Cloud Security
August 26, 2020

Cloud Network Security 101: Azure Virtual Network Service Endpoints
September 17, 2020

Cloud Network Security 101: Azure Private Link & Private Endpoints
September 25, 2020

Cloud Network Security 101: Azure Service Endpoints vs. Private Endpoints
October 8, 2020

POPULAR CATEGORIES

Security & Compliance | Cloud | AWS | Fugue | cloud security

CATEGORIZED UNDER

cloud security | network security

Featured Posts

Introducing the Engineer's Handbook on Cloud Security
Drew Wright
August 26, 2020

3 Big Amazon S3 Vulnerabilities You May Be Missing
Drew Wright
May 21, 2020

Cloud Security for Newly Distributed Engineering Teams
Drew Wright
March 19, 2020

Company
About
Customers
Press
Events
Careers
Security
Privacy Policy

Product
Login
Pricing
Overview
API
Documentation
Submit a Ticket

Resources
Blog
Cloud Security
Cloud Compliance
Case Studies
Library

Subscribe to our newsletter:
Subscribe

GET DEMO CONTACT US