## Control traffic to subnets using Network ACLs

A network access control list (ACL) is an **optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets**. You might set up network ACLs with rules **like your security groups** to add an additional layer of security to your VPC.

## ENIs (Elastic Network Interfaces)

Essentially, ENIs are virtual network cards you can attach to your EC2 instances. They are used to enable network connectivity for your instances and having more than one of them connected to your instance allows it to communicate on two different subnets.

You are already using them if you are running an EC2.

The default interface, eth0, is attached to an ENI that was created when you launched the instance and is used to handle all traffic sent and received from the instance.

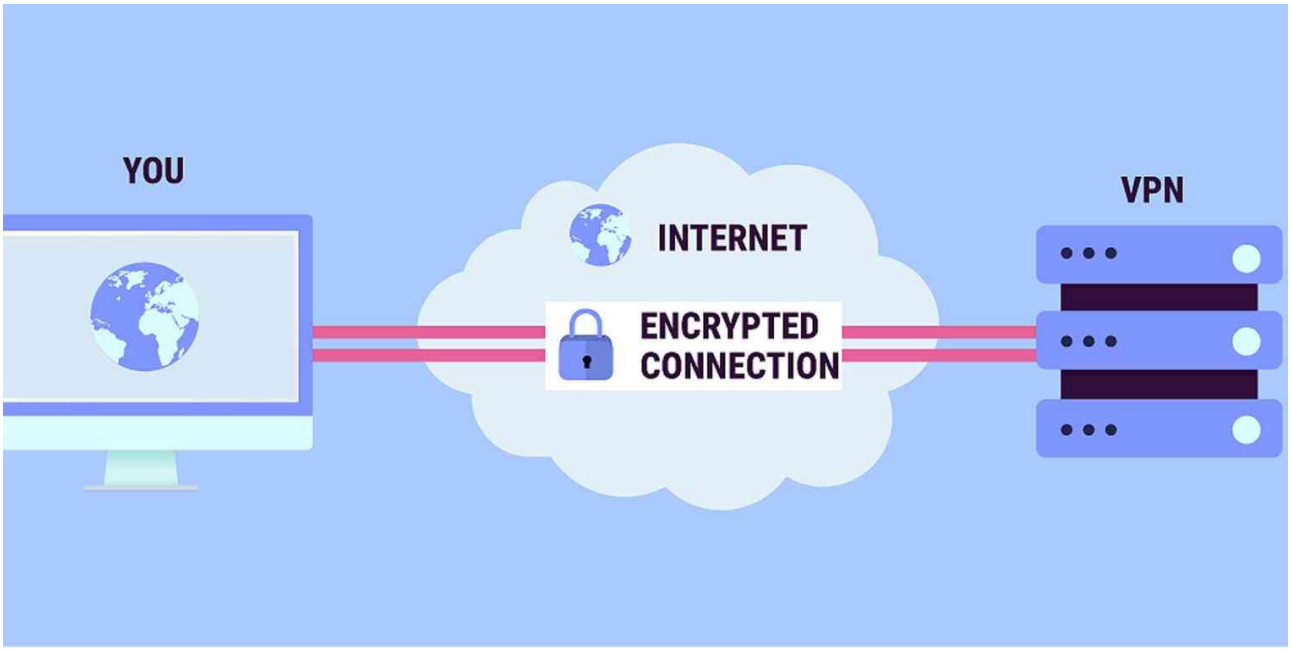
You are not limited to just one network interface though and attaching a secondary network interface allows you to connect your EC2 instance to two networks at once, which can be very useful when designing your network architecture.

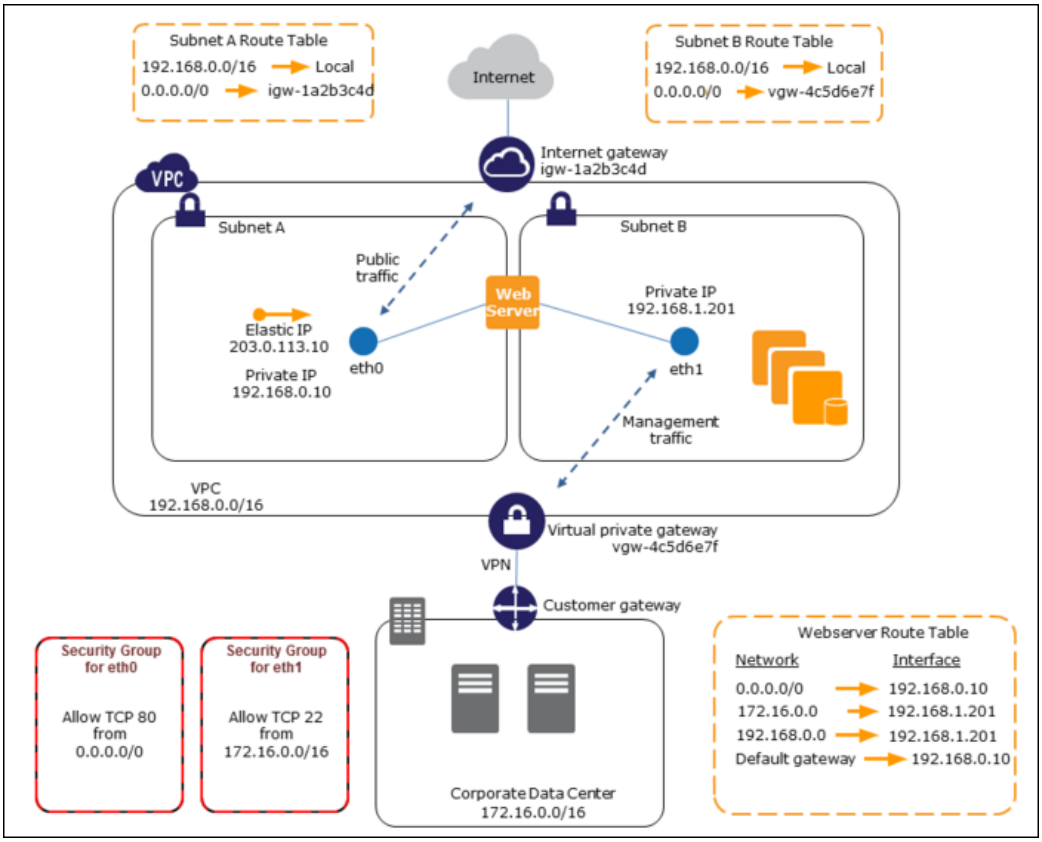
You can use them to host load balancers, proxy servers, and NAT servers on an EC2 instance, routing traffic from one subnet to another.

A common use case for ENIs is the creation of management networks. This allows you to have public-facing applications like web servers in a public subnet but lock down SSH access down to a private subnet on a secondary network interface. In this scenario, you would connect using a VPN to the private management subnet, then administrate your servers as usual.

The configuration for this scenario includes a virtual private cloud (VPC) with a public subnet and a private subnet, and a virtual private gateway to enable communication with your own network over an IPsec VPN tunnel. We recommend this scenario if you want to extend your network into the cloud and also directly access the internet from your VPC. This scenario enables you to run a multi-tiered application with a scalable web front end in a public subnet, and to house your data in a private subnet that is connected to your network by an **IPsec AWS Site-to-Site VPN connection.**

A VPN establishes a secure, encrypted connection between your computer and the internet, providing a private tunnel for your data and communications while you use public networks.






ENIs is allowing this web server instance to access networks from two different subnets.

An Elastic IP address is a public IPv4 address, which is reachable from the internet. If your instance does not have a public IPv4 address, you can associate an Elastic IP address with your instance to enable communication with the internet. For example, this allows you to connect to your instance from your local computer.