Use a public subnet for resources that must be connected to the internet, and a private subnet for resources that won't be connected to the internet.

A *security group* acts as a virtual firewall for your instance to control inbound and outbound traffic. When you launch an instance in a VPC, you can assign up to five security groups to the instance. Security groups act at the instance level, not the subnet level. Therefore, each instance in a subnet in your VPC could be assigned to a different set of security groups. If you don't specify a particular group at launch time, the instance is automatically assigned to the default security group for the VPC.

* You can specify allow rules, but not deny rules.
* You can specify separate rules for inbound and outbound traffic.
* When you create a security group, it has no inbound rules. Therefore, no inbound traffic originating from another host to your instance is allowed until you add inbound rules to the security group.
* By default, a security group includes an outbound rule that allows all outbound traffic. You can remove the rule and add outbound rules that allow specific outbound traffic only. If your security group has no outbound rules, no outbound traffic originating from your instance is allowed.
* Security groups are stateful — if you send a request from your instance, the response traffic for that request is allowed to flow in regardless of inbound security group rules. Responses to allowed inbound traffic are allowed to flow out, regardless of outbound rules.
* Instances associated with a security group can't talk to each other unless you add rules allowing it (exception: the default security group has these rules by default).
* Security groups are associated with network interfaces. After you launch an instance, you can change the security groups associated with the instance, which changes the security groups associated with the primary network interface (eth0). You can also change the security groups associated with any other network interface. For more information about network interfaces, see [Elastic Network Interfaces](http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html).

You can create up to 500 security groups per VPC.

You can add up to 50 rules to a security group.

You can assign up to 5 security groups to a network interface.

5 default limit of vpcs in one region

200 default limit acls in one network vpc

20 default limit rules for one acl

The following are the basic things that you need to know about network ACLs:

* Your VPC automatically comes with a modifiable default network ACL. By default, it allows all inbound and outbound IPv4 traffic and, if applicable, IPv6 traffic.
* You can create a custom network ACL and associate it with a subnet. By default, each custom network ACL denies all inbound and outbound traffic until you add rules.
* Each subnet in your VPC must be associated with a network ACL. If you don't explicitly associate a subnet with a network ACL, the subnet is automatically associated with the default network ACL.
* You can associate a network ACL with multiple subnets; however, a subnet can be associated with only one network ACL at a time. When you associate a network ACL with a subnet, the previous association is removed.
* A network ACL contains a numbered list of rules that we evaluate in order, starting with the lowest numbered rule, to determine whether traffic is allowed in or out of any subnet associated with the network ACL. The highest number that you can use for a rule is 32766. We recommend that you start by creating rules in increments (for example, increments of 10 or 100) so that you can insert new rules where you need to later on.
* A network ACL has separate inbound and outbound rules, and each rule can either allow or deny traffic.
* Network ACLs are stateless; responses to allowed inbound traffic are subject to the rules for outbound traffic (and vice versa).

You can create a flow log for a VPC, a subnet, or a network interface. If you create a flow log for a subnet or VPC, each network interface in the VPC or subnet is monitored.

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them privately. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, with a VPC in another AWS account, or with a VPC in a different AWS Region.

A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network. Endpoints are virtual devices. They are horizontally scaled, redundant, and highly available VPC components that allow communication between instances in your VPC and services without imposing availability risks or bandwidth constraints on your network traffic There are two types of VPC endpoints: interface endpoints and gateway endpoints. Create the type of VPC endpoint required by the supported service.

You can create your own application in your VPC and configure it as an AWS PrivateLink-powered service (referred to as an endpoint service). Other AWS principals can create a connection from their VPC to your endpoint service using an[interface VPC endpoint](https://docs.aws.amazon.com/vpc/latest/userguide/vpce-interface.html). You are the service provider, and the AWS principals that create connections to your service are service consumers.

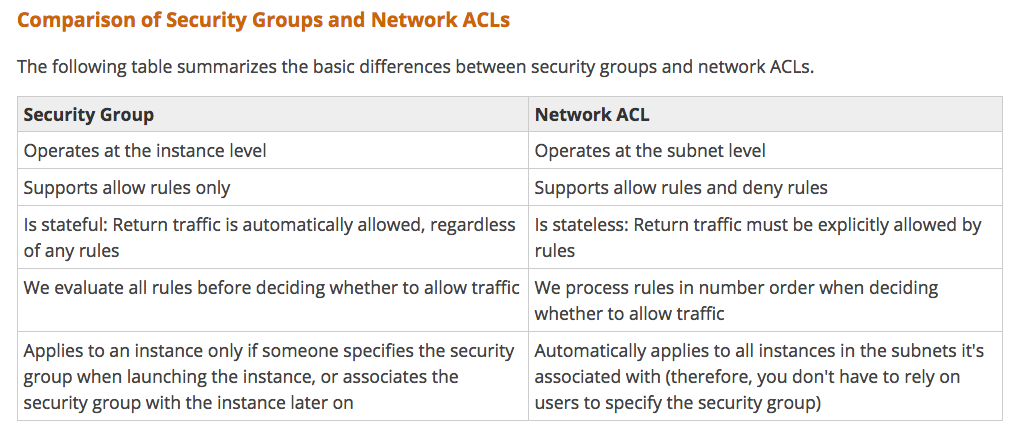
A NAT device forwards traffic from the instances in the private subnet to the Internet or other AWS services, and then sends the response back to the instances. When traffic goes to the Internet, the source IPv4 address is replaced with the NAT device’s address and similarly, when the response traffic goes to those instances, the NAT device translates the address back to those instances’ private IPv4 addresses. NAT devices are not supported for IPv6 traffic—use an egress-only Internet gateway instead. AWS offers two kinds of NAT devices—a *NAT gateway* or a *NAT instance*. We recommend NAT gateways, as they provide better availability and bandwidth over NAT instances. The NAT Gateway service is also a managed service that does not require your administration efforts. A NAT instance is launched from a NAT AMI. You can choose to use a NAT instance for special purposes.

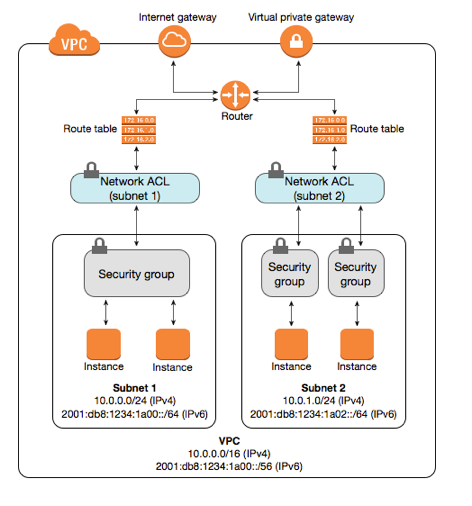
An internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between instances in your VPC and the internet. An internet gateway serves two purposes: to provide a target in your VPC route tables for internet-routable traffic, and to perform network address translation (NAT) for instances that have been assigned public IPv4 addresses.An internet gateway supports IPv4 and IPv6 traffic.

**Enabling Internet Access**

To enable access to or from the internet for instances in a VPC subnet, you must do the following:

* Attach an internet gateway to your VPC.
* Ensure that your subnet's route table points to the internet gateway.
* Ensure that instances in your subnet have a globally unique IP address (public IPv4 address, Elastic IP address, or IPv6 address).
* Ensure that your network access control and security group rules allow the relevant traffic to flow to and from your instance.





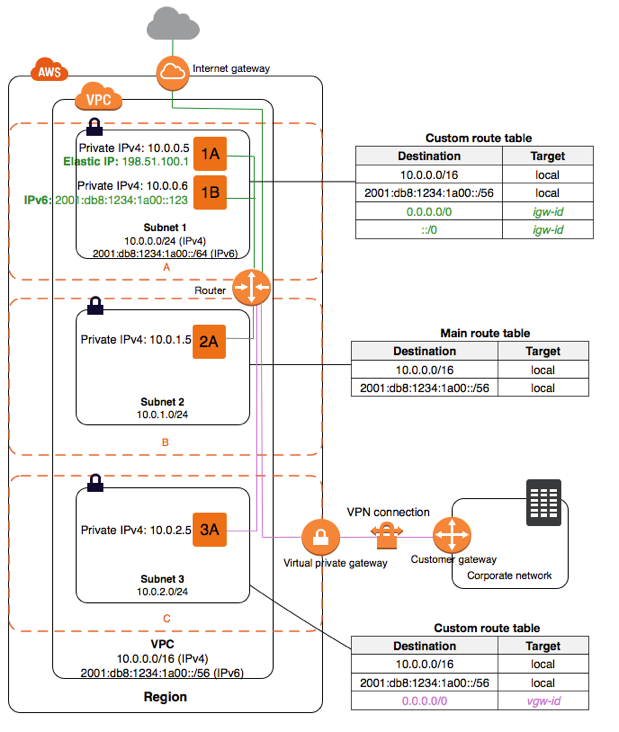
An Elastic IP address is a static, public IPv4 address designed for dynamic cloud computing. You can associate an Elastic IP address with any instance or network interface for any VPC in your account. With an Elastic IP address, you can mask the failure of an instance by rapidly remapping the address to another instance in your VPC. Note that the advantage of associating the Elastic IP address with the network interface instead of directly with the instance is that you can move all the attributes of the network interface from one instance to another in a single step. We currently do not support Elastic IP addresses for IPv6.

Private IPv4 addresses (also referred to as *private IP addresses* in this topic) are not reachable over the Internet, and can be used for communication between the instances in your VPC. When you launch an instance into a VPC, a primary private IP address from the IPv4 address range of the subnet is assigned to the default network interface (eth0) of the instance.  Each instance is also given a private (internal) DNS hostname that resolves to the private IP address of the instance.

You can use AWS Identity and Access Management (IAM) to allow other users, services, and applications to use your Amazon VPC resources without sharing your security credentials.

AWS Direct Connect is a cloud service solution that makes it easy to establish a dedicated network connection from your premises to AWS. Using AWS Direct Connect, you can establish private connectivity between AWS and your datacenter, office, or colocation environment, which in many cases can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.

A VPC spans all the Availability Zones in the region. After creating a VPC, you can add one or more subnets in each Availability Zone.



You may have only one Internet Gateway per VPC.

When you create a custom VPC, a default Security Group, Access control List, and Route Table are created automaticaly. You must create your own subnets, Internet Gateway, and NAT Gateway (if you need one.)

VPC Flow Logs can be created at the VPC, subnet, and network interface levels.

An IGW is provided by default in a default VPC, but not in a manually created VPC. A Public IP address is needed, and of the options provided an EIP is the best option.

An Application Load Balancer must be deployed into at least two subnets.

In contrast to a NAT gateway, traffic between your VPC and the other service does not leave the Amazon network when using VPC endpoints.

By default, new subnets in a custom VPC can communicate with each other across Availability Zones.

Each subnet must reside entirely within one Availability Zone and cannot span zones.