**VPC**

Q. What are the components of Amazon VPC?

Amazon VPC comprises a variety of objects that will be familiar to customers with existing networks:

* A Virtual Private Cloud: A logically isolated virtual network in the AWS cloud. You define a VPC’s IP address space from ranges you select.
* Subnet: A segment of a VPC’s IP address range where you can place groups of isolated resources.
* Internet Gateway: The Amazon VPC side of a connection to the public Internet.
* NAT Gateway: A highly available, managed Network Address Translation (NAT) service for your resources in a private subnet to access the Internet.
* Virtual private gateway: The Amazon VPC side of a VPN connection.
* Peering Connection: A peering connection enables you to route traffic via private IP addresses between two peered VPCs.
* VPC Endpoints: Enables private connectivity to services hosted in AWS, from within your VPC without using an Internet Gateway, VPN, Network Address Translation (NAT) devices, or firewall proxies.
* Egress-only Internet Gateway: A stateful gateway to provide egress only access for IPv6 traffic from the VPC to the Internet.

The four options are:

1. Amazon VPC with a single public subnet only
2. Amazon VPC with public and private subnets
3. Amazon VPC with public and private subnets and AWS Site-to-Site VPN access
4. Amazon VPC with a private subnet only and AWS Site-to-Site VPN access

Q. How do instances in a VPC access the Internet?

You can use public IP addresses, including Elastic IP addresses (EIPs), to give instances in the VPC the ability to both directly communicate outbound to the Internet and to receive unsolicited inbound traffic from the Internet (e.g., web servers). You can also use the solutions in the next question.

Q. How do instances without public IP addresses access the Internet

Instances without public IP addresses can access the Internet in one of two ways:

1. Instances without public IP addresses can route their traffic through a NAT gateway or a NAT instance to access the Internet. These instances use the public IP address of the NAT gateway or NAT instance to traverse the Internet. The NAT gateway or NAT instance allows outbound communication but doesn’t allow machines on the Internet to initiate a connection to the privately addressed instances.
2. For VPCs with a hardware VPN connection or Direct Connect connection, instances can route their Internet traffic down the virtual private gateway to your existing datacenter. From there, it can access the Internet via your existing egress points and network security/monitoring devices.

Q. Can I connect to my VPC using a software VPN?

Yes. You may use a third-party software VPN to create a site to site or remote access VPN connection with your VPC via the Internet gateway.

Q. Does traffic go over the internet when two instances communicate using public IP addresses?

Traffic between two EC2 instances in the same AWS Region stays within the AWS network, even when it goes over public IP addresses.

Traffic between EC2 instances in different AWS Regions stays within the AWS network, if there is an Inter-Region VPC Peering connection between the VPCs where the two instances reside.

Traffic between EC2 instances in different AWS Regions where there is no Inter-Region VPC Peering connection between the VPCs where these instances reside, is not guaranteed to stay within the AWS network.

Q. How does an AWS Site-to-Site VPN connection work with Amazon VPC?

An AWS Site-to-Site VPN connection connects your VPC to your datacenter. Amazon supports Internet Protocol Security (IPSec) VPN connections. Data transferred between your VPC and datacenter routes over an encrypted VPN connection to help maintain the confidentiality and integrity of data in transit. An internet gateway is not required to establish an AWS Site-to-Site VPN connection.

Q. What IP address ranges are assigned to a default Amazon VPC?

Default VPCs are assigned a CIDR range of 172.31.0.0/16. Default subnets within a default VPC are assigned /20 netblocks within the VPC CIDR range.

Q. Can I use my public IPv4 addresses in VPC and access them over the Internet?

Yes, you can bring your public IPv4 addresses into AWS VPC and statically allocate them to subnets and EC2 instances. To access these addresses over the Internet, you will have to advertise them to the Internet from your on-premises network. You will also have to route the traffic over these addresses between your VPC and on-premises network using AWS DX or AWS VPN connection. You can route the traffic from your VPC using the Virtual Private Gateway. Similarly, you can route the traffic from your on-premises network back to your VPC using your routers.

Q. Can I change the size of a VPC?

Yes. You can expand your existing VPC by adding four (4) secondary IPv4 IP ranges (CIDRs) to your VPC. You can shrink your VPC by deleting the secondary CIDR blocks you have added to your VPC. You cannot however change the size of the IPv6 address range of your VPC.

Q. How many subnets can I create per VPC?

Currently you can create 200 subnets per VPC. If you would like to create more, please [submit a case at the support center](https://aws.amazon.com/contact-us/vpc-request/).

Q. Can I use all the IP addresses that I assign to a subnet?

No. Amazon reserves the first four (4) IP addresses and the last one (1) IP address of every subnet for IP networking purposes.

Q. Can I assign multiple IP addresses to an instance?

Yes. You can assign one or more secondary private IP addresses to an Elastic Network Interface or an EC2 instance in Amazon VPC. The number of secondary private IP addresses you can assign depends on the instance type. See [EC2 User Guide](http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/concepts.html) for more information on the number of secondary private IP addresses that can be assigned per instance type.

Q. Can I specify which subnet will use which gateway as its default?

Yes. You may create a default route for each subnet. The default route can direct traffic to egress the VPC via the Internet gateway, the virtual private gateway, or the NAT gateway.

Q. How do I secure Amazon EC2 instances running within my VPC?

Amazon EC2 security groups can be used to help secure instances within an Amazon VPC. Security groups in a VPC enable you to specify both inbound and outbound network traffic that is allowed to or from each Amazon EC2 instance. Traffic which is not explicitly allowed to or from an instance is automatically denied.

In addition to security groups, network traffic entering and exiting each subnet can be allowed or denied via network Access Control Lists (ACLs).

Q. What are the differences between security groups in a VPC and network ACLs in a VPC?

Security groups in a VPC specify which traffic is allowed to or from an Amazon EC2 instance. Network ACLs operate at the subnet level and evaluate traffic entering and exiting a subnet. Network ACLs can be used to set both Allow and Deny rules. Network ACLs do not filter traffic between instances in the same subnet. In addition, network ACLs perform stateless filtering while security groups perform stateful filtering.

Q. Can Amazon EC2 instances within a VPC communicate with Amazon EC2 instances not within a VPC?

Yes. If an Internet gateway has been configured, Amazon VPC traffic bound for Amazon EC2 instances not within a VPC traverses the Internet gateway and then enters the public AWS network to reach the EC2 instance. If an Internet gateway has not been configured, or if the instance is in a subnet configured to route through the virtual private gateway, the traffic traverses the VPN connection, egresses from your datacenter, and then re-enters the public AWS network.

Q. Can Amazon EC2 instances within a VPC in one region communicate with Amazon EC2 instances within a VPC in another region?

Yes. Instances in one region can communicate with each other using Inter-Region VPC Peering, public IP addresses, NAT gateway, NAT instances, VPN Connections or Direct Connect connections.

Q. Can Amazon EC2 instances within a VPC communicate with Amazon S3?

Yes. There are multiple options for your resources within a VPC to communicate with Amazon S3. You can use VPC Endpoint for S3, which makes sure all traffic remains within Amazon's network and enables you to apply additional access policies to your Amazon S3 traffic. You can use an Internet gateway to enable Internet access from your VPC and instances in the VPC can communicate with Amazon S3. You can also make all traffic to Amazon S3 traverse the Direct Connect or VPN connection, egress from your datacenter, and then re-enter the public AWS network.

Q. Can I monitor the network traffic in my VPC?

Yes. You can use Amazon VPC traffic mirroring and Amazon VPC flow logs features to monitor the network traffic in your Amazon VPC.

Q. How do DNS translations work with Inter-Region VPC Peering?

By default, a query for a public hostname of an instance in a peered VPC in a different region will resolve to a public IP address. Route 53 private DNS can be used to resolve to a private IP address with Inter-Region VPC Peering.

Q. Can I reference security groups across an Inter-Region VPC Peering connection?

No. Security groups cannot be referenced across an Inter-Region VPC Peering connection.

Q. Does Inter-Region VPC Peering support with IPv6?

Yes. Inter-Region VPC Peering supports IPv6.

Q. Can Inter-Region VPC Peering be used with EC2-Classic Link?

No. Inter-Region VPC Peering cannot be used with EC2-ClassicLink.

Q. How many VPCs, subnets, Elastic IP addresses, and internet gateways can I create?

You can have:

* Five Amazon VPCs per AWS account per region
* Two hundred subnets per Amazon VPC
* Five Amazon VPC Elastic IP addresses per AWS account per region
* One internet gateway per Amazon VPC

By default you can create up to 5 VPCs per region.

* **VPC Endpoints:**Enables private connectivity to services hosted in AWS, from within your VPC without using an an Internet Gateway, VPN, Network Address Translation (NAT) devices, or firewall proxies.
* **Egress-only Internet Gateway:** A stateful gateway to provide egress only access for IPv6 traffic from the VPC to the Internet.
* **Peering Connection:** A peering connection enables you to route traffic via private IP addresses between two peered VPCs.
* If a subnet doesn’t have a route to the internet gateway, but has its traffic routed to a virtual private gateway for a VPN connection, the subnet is known as a**VPN-only subnet.**

New subnets are always associated with the default route table.

The first 4 and last 1 IP addresses in a subnet are reserved.

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

You cannot have multiple Internet Gateways in a VPC.