



VPC Overview



Ryan Kroonenburg
AWS COMMUNITY HERO & ALEXA CHAMPION
FOUNDER OF A CLOUD GURU

Udemy

Think of a VPC as a virtual data centre in the cloud.



Rewind 5s

44 ...

What Is A VPC?



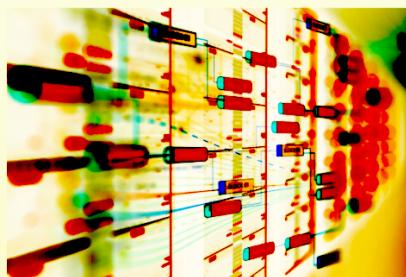
Amazon Virtual Private Cloud (Amazon VPC) lets you provision a logically isolated section of the Amazon Web Services (AWS) Cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways.



What Is A VPC?

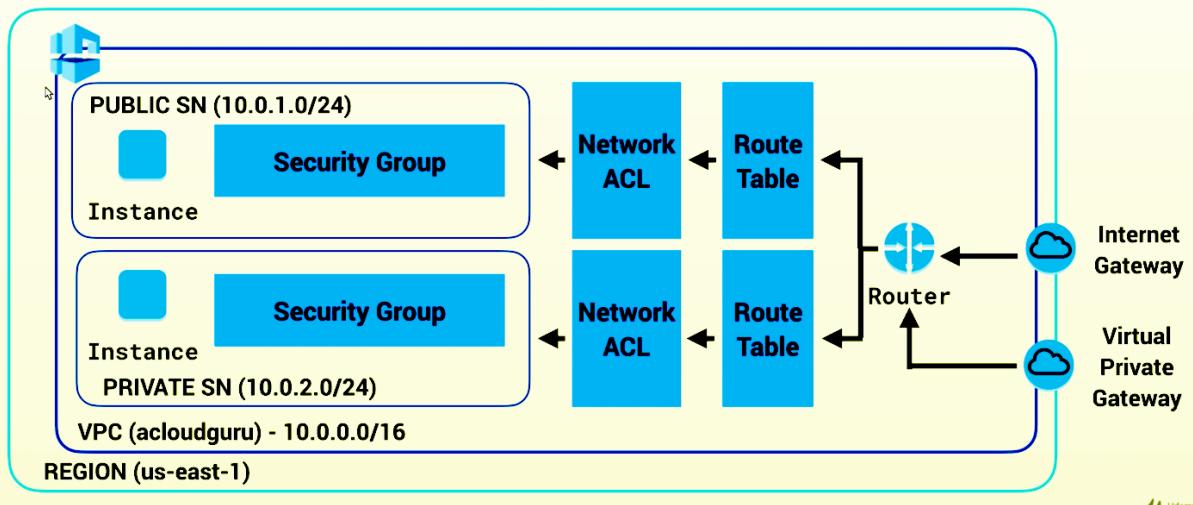


You can easily customize the network configuration for your Amazon Virtual Private Cloud. For example, you can create a public-facing subnet for your webservers that has access to the Internet, and place your backend systems such as databases or application servers in a private-facing subnet with no Internet access. You can leverage multiple layers of security, including security groups and network access control lists, to help control access to Amazon EC2 instances in each subnet.



What Is A VPC?

Additionally, you can create a Hardware Virtual Private Network (VPN) connection between your corporate datacenter and your VPC and leverage the AWS cloud as an extension of your corporate datacenter.

**What Is A VPC?****VPC with Public & Private Subnet(s)**

- 10.0.0.0 - 10.255.255.255 (10/8 prefix)
- 172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
- 192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

CIDR.xyz

AN INTERACTIVE IP ADDRESS AND CIDR RANGE VISUALIZER

CIDR is a notation for describing blocks of IP addresses and is used heavily in various networking configurations. IP addresses contain 4 octets, each consisting of 8 bits giving values between 0 and 255. The decimal value that comes after the slash is the number of bits consisting of the routing prefix. This in turn can be translated into a netmask, and also designates how many available addresses are in the block.

10 . 0 . 0 . 0 / 16

 0 0 0 0 1 0 1 0

255.255.0.0
NETMASK

10.0.0.1
FIRST IP

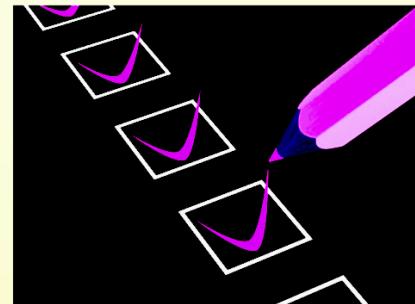
10.0.255.254
LAST IP

65,536
COUNT

Created by [Yuval Adam](#). Source available on [Github](#).

What can we do with a VPC?

- Launch instances into a subnet of your choosing
- Assign custom IP address ranges in each subnet
- Configure route tables between subnets
- Create internet gateway and attach it to our VPC
- Much better security control over your AWS resources
- Instance security groups
- Subnet network access control lists (ACLs)

**Default VPC vs Custom VPC**

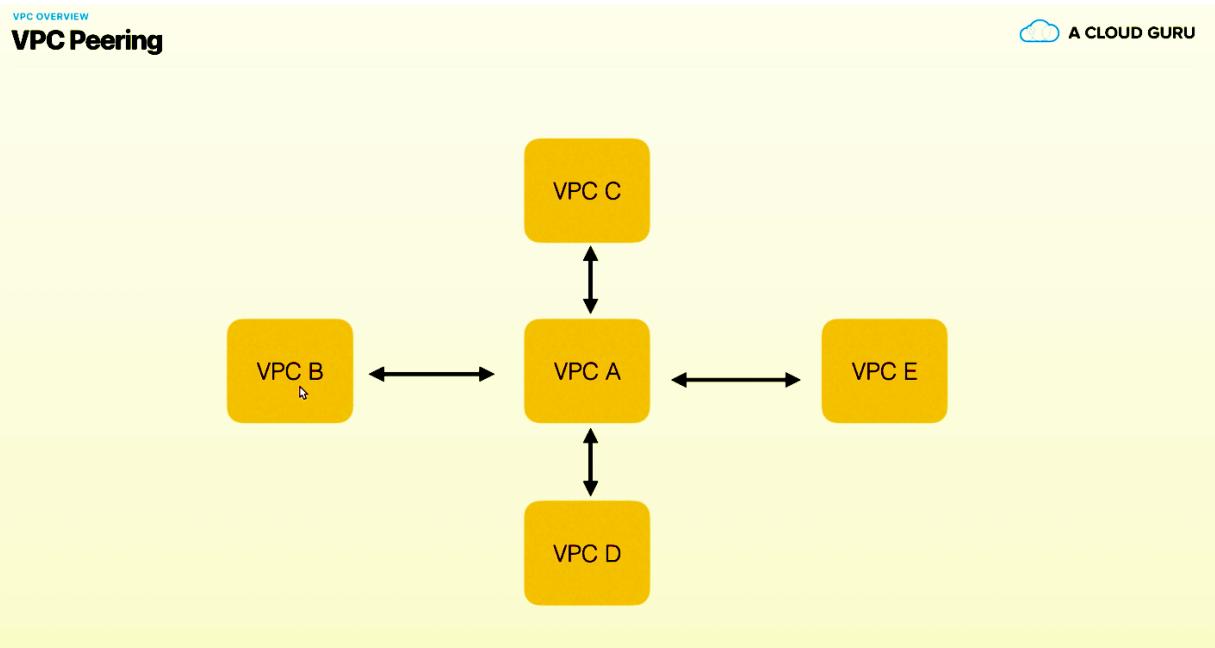
- Default VPC is user friendly, allowing you to immediately deploy instances.
- All Subnets in default VPC have a route out to the internet.
- Each EC2 instance has both a public and private IP address.

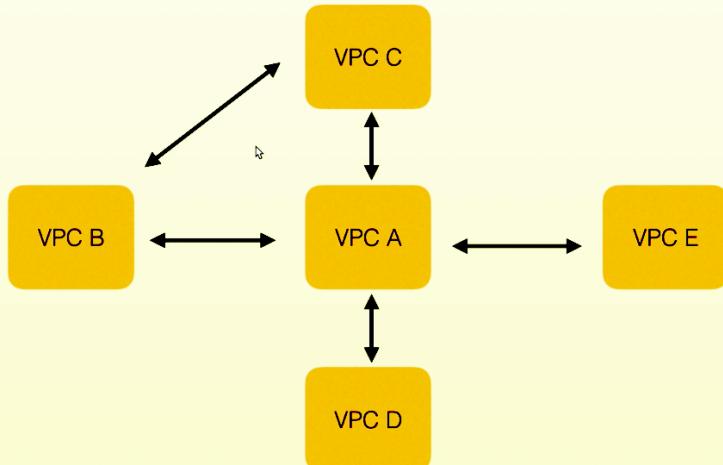
**VPC**

VPC Peering

- Allows you to connect one VPC with another via a direct network route using private IP addresses.
- Instances behave as if they were on the same private network
- You can peer VPC's with other AWS accounts as well as with other VPCs in the same account.
- Peering is in a star configuration: ie 1 central VPC peers with 4 others.
NO TRANSITIVE PEERING!!!
- You can peer between regions.

VPC ←→ VPC



**Remember the following;**

- Think of a VPC as a logical datacenter in AWS.
- Consists of IGWs (Or Virtual Private Gateways), Route Tables, Network Access Control Lists, Subnets, and Security Groups
- 1 Subnet = 1 Availability Zone
- Security Groups are Stateful; Network Access Control Lists are Stateless
- NO TRANSITIVE PEERING



Create Your Own Custom VPC Part 1- LAB



Ryan Kroonenburg
AWS COMMUNITY HERO & ALEXA CHAMPION
FOUNDER OF A CLOUD GURU

Udemy

VPC OVERVIEW

What Is A VPC?



VPC with Public & Private Subnet(s)



Security Group

Network ACL

Route Table

Router

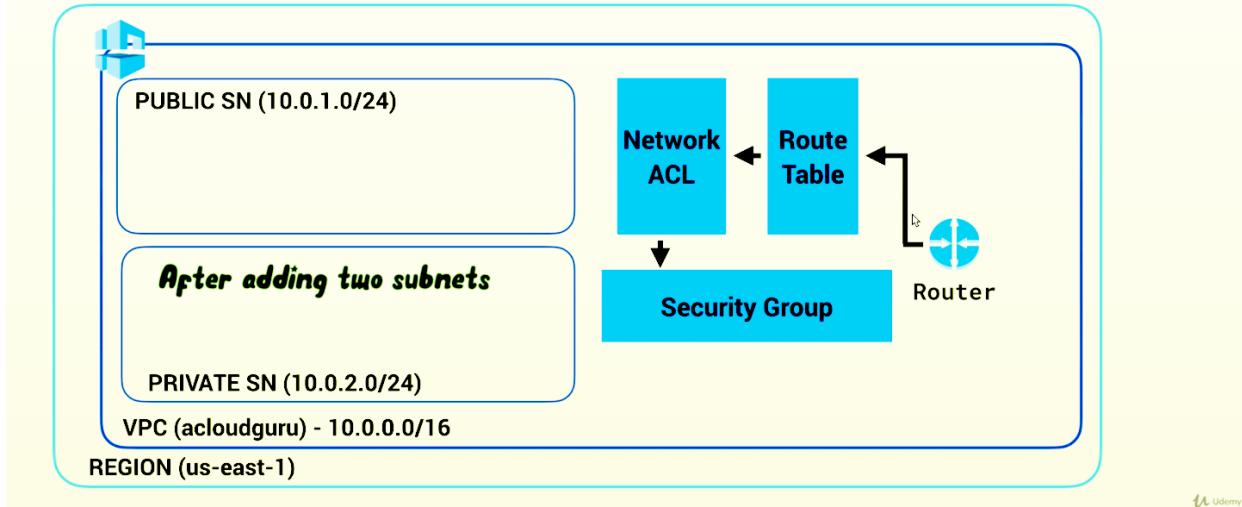
What VPC looks like right after being created in AWS

VPC (acloudguru) - 10.0.0.0/16

REGION (us-east-1)

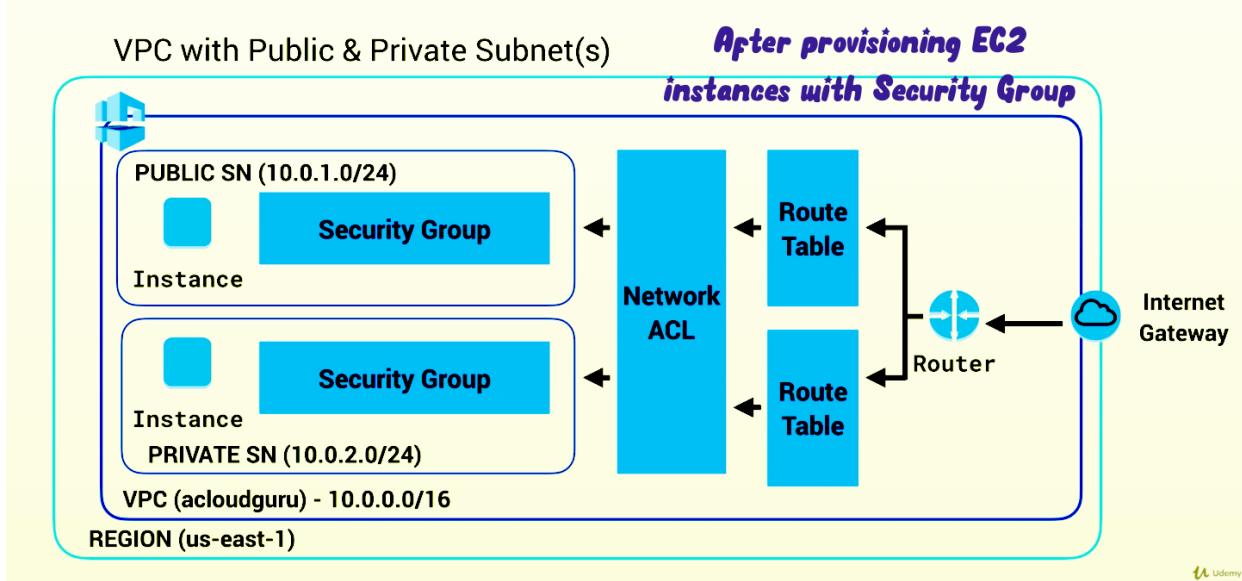
Udemy

VPC with Public & Private Subnet(s)



VPC with Public & Private Subnet(s)

After provisioning EC2 instances with Security Group



Remember the following;

- When you create a VPC a default Route Table, Network Access Control List (NACL) and a default Security Group.
- It won't create any subnets, nor will it create a default internet gateway.
- US-East-1A in your AWS account can be a completely different availability zone to US-East-1A in another AWS account. The AZ's are randomized.
- Amazon always reserve 5 IP addresses within your subnets.
- You can only have 1 Internet Gateway per VPC.
- Security Groups can't span VPCs.