CLOUD COMPUTING APPLICATIONS

VPC: Virtual Private Cloud

Prof. Reza Farivar

Virtual Private Clouds

- Most Cloud Providers have some sort of network virtualization solution
  - Arguably the most fundamental building block
  - Amazon Virtual Private Cloud (VPC)
  - Microsoft Azure Virtual Network (VNet)
  - Google Virtual Private Cloud (VPC)
  - Oracle Virtual Cloud Networks
- They somewhat differ in detail, but the concepts are general
- In this lesson we will focus on Amazon VPC
  - Geared towards Cloud Architecture

Solving a Fundamental Problem

- Allow many different users have their own private network in the cloud
- Isolate different customers' network packets from each other
- Solution: VPC

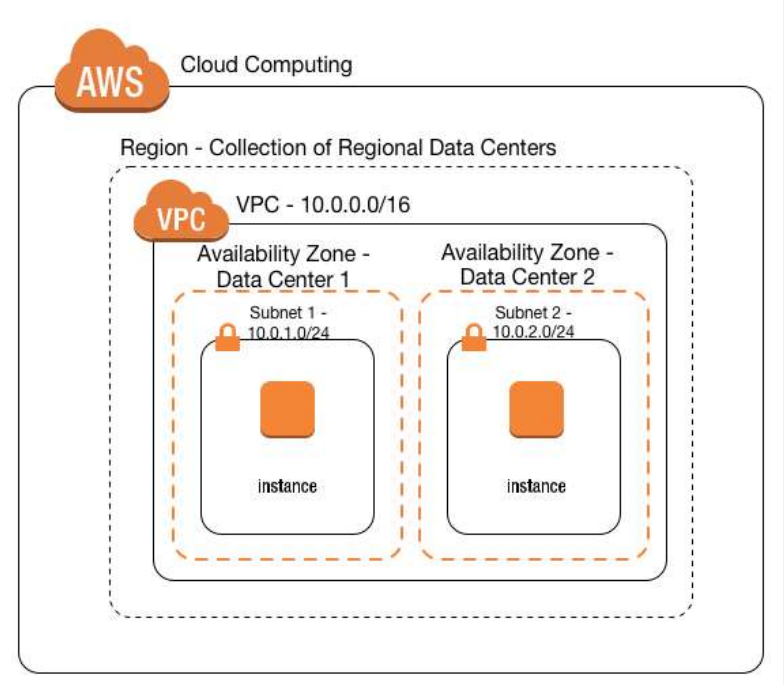
VPCs and Subnets

- You have your “own” network in the cloud
  - VPC
  - In AWS, a VPC is associated with a region, e.g. us-east-1
  - You can have more than one VPC, even in the same region
    - Default 5 quota
  - The IP address range of all the nodes in this VPC can be defined with a CIDR
- Your VPC is subdivided into logically separate segments
  - Subnet
  - Each subnet get a smaller CIDR range
  - Each subnet is associated with one Availability Zone
- You can then launch instances (EC2, RDS, etc.) in a subnet

VPCs, Subnets and Availability Zones

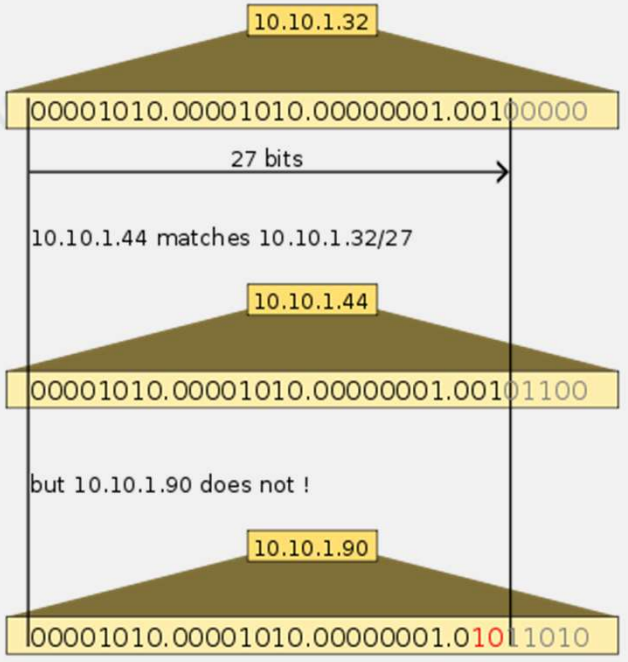
The main routing table, associated with the VPC, has the following route:

Destination	Target
10.0.0.0/16	local



Background Knowledge: CIDR

- CIDR: Classless Inter-Domain Routing
- A method of allocating IP address ranges
- In IPV4, each IP address is a 32 bit value
  - 4 bytes
  - 192.168.0.1
- CIDR notation:
  - 100.101.102.103/24
  - Take the mask (24 bits)
  - Keep the upper 24 bits the same
  - The lower bits can change ➔ range
  - 100.101.102.0 … 100.101.102.255
- IPV6, each address is 128 bits:
  - the IPv6 block *2001:db8::/48* represents the block of IPv6 addresses from *2001:db8:0:0:0:0:0:0* to *2001:db8:0:ffff:ffff:ffff:ffff:ffff*.
  - Note that in IPV6 notation, each segment is written in hex



RFC 1918: Address Allocation for Private Internets

- The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private internets
- 10.0.0.0/8
  - 10.0.0.0 - 10.255.255.255
  - Number of addresses: 16,777,216
- 172.16.0.0/12
  - 172.16.0.0 - 172.31.255.255
  - Number of addresses: 1,048,576
- 192.168.0.0/16
  - 192.168.0.0 - 192.168.255.255
  - Number of addresses: 16,777,216
- Why? Because it is guaranteed no other server on the public internet has an IP address in these ranges
- Routing rules do not conflict

RFC 1918 and AWS VPC

- When you create a VPC, you must specify an IPv4 CIDR block for the VPC
- The allowed block size is between a /16 netmask (65,536 IP addresses) and /28 netmask (16 IP addresses)
  - Note that RFC 1918 would allow for 16 million distinct IP addresses in the 10.0.0.0/8, but Amazon would at most accept a /16 netmask in a VPC or subnet

RFC 1918 range	Example AWS VPC CIDR block
10.0.0.0 - 10.255.255.255 (10/8 prefix)	Your VPC must be /16 or smaller, for example, 10.0.0.0/16.
172.16.0.0 - 172.31.255.255 (172.16/12 prefix)	Your VPC must be /16 or smaller, for example, 172.31.0.0/16.
192.168.0.0 - 192.168.255.255 (192.168/16 prefix)	Your VPC can be smaller, for example 192.168.0.0/20.

Reserved IP Adresses

- The first four IP addresses and the last IP address in each subnet CIDR block are not available for you to use, and cannot be assigned to an instance; E.g. for 10.0.0.0/24:
  - 10.0.0.0: Network address
  - 10.0.0.1: The VPC router
  - 10.0.0.2: The IP address of the DNS server is the base of the VPC network range plus two
  - 10.0.0.3: Reserved for future use
  - 10.0.0.255: Network broadcast address
    - AWS does NOT support broadcast in a VPC, therefore this address is reserved