Chapter 11 – Cloud Application Development
Contents

- Motivation.
- Connecting clients to instances through firewalls.
Motivation

Some of the questions of interest to application developers:

- How easy is it to use the cloud?
- How knowledgeable should an application developer be about networking and security?
- How easy is it to port an existing application to the cloud?
- How easy is it to develop a new cloud application?

The answers are different for the three cloud delivery models:

- SaaS applications are designed for the end-users and are accessed over the Web; familiar with the API of a particular application is necessary.
- PaaS provides a set of tools and services designed to facilitate application coding and deploying.
- IaaS provides the hardware and the software for servers, storage, networks, including operating systems and storage management software; the IaaS model poses the most challenges.
A pyramid model of cloud computing paradigms; the infrastructure provides the basic resources, the platform adds an environment to facilitate the use of these resources, while software allows direct access to services.
Connecting clients to instances through firewalls

- A firewall → a software system based on a set of rules for filtering network traffic; its function is to protect a computer in a local area network from unauthorized access.

- Firewalls
  - First generation → operated below the transport layer, and discarded packets based on the information in the headers of physical, data link, and network layer protocols.
  - Second generation → operate at the transport layer and maintain the state of all connections passing through them and opened the possibility of denial of service attacks.
  - Third generation → understand widely-used application layer protocols such as FTP, HTTP, TELNET, SSH, and DNS. These firewalls examine the header of application layer protocols and support intrusion detection systems (IDS).
Firewalls screen incoming and sometimes outgoing traffic. The first obstacle encountered by the inbound or outbound traffic is a router firewall, the next one is the firewall provided by the host operating system; sometimes, the antivirus software provides a third line of defense.
Connecting to a AWS instance

- A client must know the IP address of a virtual machine in the cloud, to be able to connect to it.

- A virtual machine running under EC2 has several IP addresses:
  - EC2 **private** IP address → the internal address of an instance; it is only used for routing within the EC2 cloud.
  - EC2 **public** IP address → network traffic originating outside the AWS network must use the public IP address or the elastic IP address of the instance. The public IP address is translated using the Network Address Translation (NAT) to the private IP address when an instance is launched and it is valid until the instance is terminated. Traffic to the public address is forwarded to the private IP address of the instance.
  - EC2 **elastic** IP address → the IP address allocated to an AWS account and used by traffic originated outside AWS. NAT is used to map an elastic IP address to the private IP address. Elastic IP addresses allow a cloud user to mask instance or availability zone failures by programmatically re-mapping a public IP addresses to any instance associated with the user’s account.