

# Network Firewalls & AWS Security Groups

Tejas Parikh ([t.parikh@northeastern.edu](mailto:t.parikh@northeastern.edu))

CSYE 6225  
Northeastern University

# What is Firewall?

- A firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules.
- A firewall typically establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet, that is assumed not to be secure or trusted.

# Firewall Categories

Firewalls are often categorized as either network firewalls or host-based firewalls.

1. Network firewalls filter traffic between two or more networks; they are either software appliances running on general purpose hardware, or hardware-based firewall computer appliances.
2. Host-based firewalls provide a layer of software on one host that controls network traffic in and out of that single machine.

# Types of Firewall

- Firewalls also vary in type depending on where communication originates, where it is intercepted, and the state of communication being traced.
- The two types of firewall are
  1. packet filtering firewalls
  2. application-level firewalls

# Packet Filtering Firewalls

Packet filtering firewalls operate at a relatively low level of the TCP/IP protocol stack, not allowing packets to pass through the firewall unless they match the established rule set.

# Application Level Firewalls

- Application-layer firewalls work on the application level of the TCP/IP stack (i.e., all browser traffic, or all telnet or FTP traffic), and may intercept all packets traveling to or from an application.
- Application firewalls function by determining whether a process should accept any given connection.
- Application firewalls accomplish their function by hooking into socket calls to filter the connections between the application layer and the lower layers of the OSI model.
- Application firewalls work much like a packet filter but application filters apply filtering rules (allow/block) on a per process basis instead of filtering connections on a per port basis.

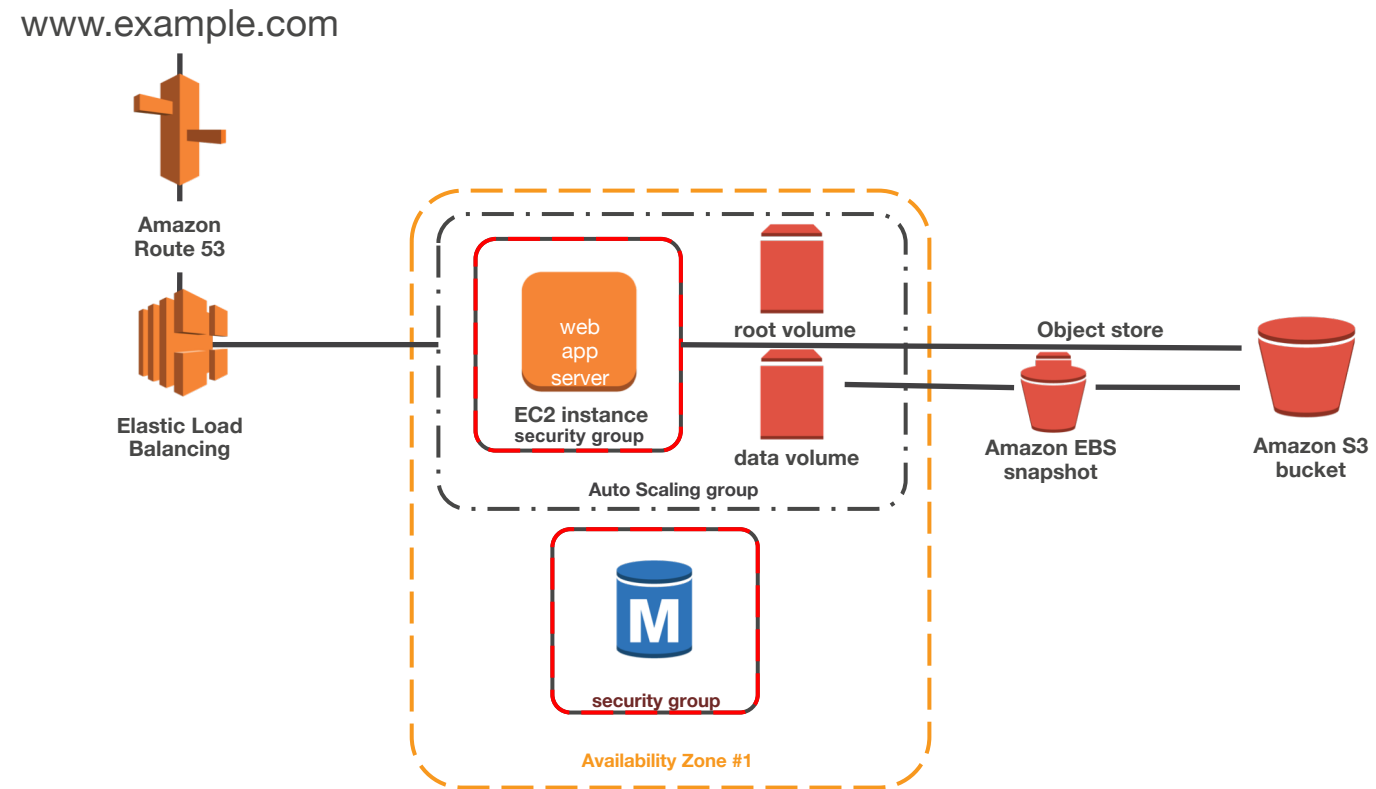
# AWS EC2 Security Groups

- A EC2 security group acts as a virtual firewall that controls the traffic for one or more instances.
- When you launch an instance, you associate one or more security groups with the instance.
- You add rules to each security group that allow traffic to or from its associated instances.
- You can modify the rules for a security group at any time; the new rules are automatically applied to all instances that are associated with the security group.
- When we decide whether to allow traffic to reach an instance, we evaluate all the rules from all the security groups that are associated with the instance.

# AWS RDS Security Groups

- RDS Security groups control the access that traffic has in and out of a DB instance.
- Each DB security group rule enables a specific source to access a DB instance that is associated with that DB security group.
- The source can be a range of addresses (e.g., 203.0.113.0/24), or an EC2 security group.
- When you specify an EC2 security group as the source, you allow incoming traffic from all EC2 instances that use that EC2 security group.
- Note that DB security group rules apply to inbound traffic only; outbound traffic is NOT currently permitted for DB instances.





# Additional Resources

<https://fall2019.csye6225.cloud/>