Aclient must knowthe IP address of a virtual machine in the cloud to be able to connect to it. TheDomain

Name Service (DNS) is used to map human-friendly names of computer systems to IP addresses in the

Internet or in private networks. DNS is a hierarchical distributed database and plays a role reminiscent

of a phone book on the Internet. In late 2010 Amazon announced a DNS service called Route 53 to

route users to AWS services and to infrastructure outside of AWS. A network of DNS servers is scattered

across the globe, which enables customers to gain reliable access to AWS and place strict controls over

who can manage their DNS system by allowing integration with AWS Identity and AccessManagement

(IAM).

For several reasons, including security and the ability of the infrastructure to scale up, the IP addresses

of instances visible to the outside world are mapped internally to private IP addresses. A virtual machine

running under Amazon’s EC2 has several IP addresses:

1. EC2 Private IP Address. The internal address of an instance; it is only used for routing within the

EC2 cloud.

2. EC2 Public IP Address. Network traffic originating outside the AWS network must use either the

public IP address or the elastic IP address of the instance. The public IP address is translated using

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.

3. 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 the cloud user to mask instance or availability zone failures by programmatically remapping

public IP addresses to any instance associated with the user’s account. This allows fast recovery after

a system failure. For example, rather than waiting for a cloud maintenance team to reconfigure or

replace the failing host or waiting for DNS to propagate the new public IP to all of the customers

of a Web service hosted by EC2, the Web service provider can remap the elastic IP address to a

replacement instance. Amazon charges a fee for unallocated Elastic IP addresses.

Amazon Web Services use security groups to control access to users’ virtual machines. A virtual

machine instance belongs to one and only one security group, which can only be defined before the

instance is launched. Once an instance is running, the security group the instance belongs to cannot be

changed. However, more than one instance can belong to a single security group.

Security group rules control inbound traffic to the instance and have no effect on outbound traffic from

the instance. The inbound traffic to an instance, either from outside the cloud or from other instances

running on the cloud, is blocked unless a rule stating otherwise is added to the security group of the

instance. For example, assume a client running on instance A in the security group  A is to connect to

a server on instance B listening on TCP port P, where B is in security group  B. A new rule must be added to security group  B to allow connections to port P; to accept responses from server B, a new

rule must be added to security group  A.

The following steps allow the user to add a security rule:

1. Sign in to the AWS Management Console at http://aws.amazon.com using your email

address and password and select EC2 service.

2. Use the EC2 Request Instance Wizard to specify the instance type, whether it should be monitored,

and specify a key/value pair for the instance to help organize and search (see Figures 11.6

and 11.7).

3. Provide a name for the key pair. Then on the left-side panel, choose Security Groups under Network

& Security, select the desired security group, and click on the Inbound tab to enter the desired rule

(see Figure 11.6).

To allocate an Elastic IP address, use the Elastic IPs tab of the Network & Security left-side panel.

On Linux or Unix systems the port numbers below 1,024 can only be assigned by the root. The

plain ASCII file called services maps friendly textual names for Internet services to their assigned port

numbers and protocol types, as in the following example:

netstat 15/tcp

ftp 21/udp

ssh 22/tcp

telnet 23/tcp

http 80/tcp