Classless Inter-Domain Routing (CIDR)

What is CIDR?

* CIDR is an IP address allocation method that improves data routing efficiency.
* IP addresses have two parts:
  + Network address – series of numerical digits pointing to the network’s unique identifier.
  + Host address - series of numerical digits indicating the host/individual device identifier.

Why CIDR is used over classful addresses?

* Classful addresses consist of 3 types:
  + Class A – Supports 16,777,214 hosts.
  + Class B – Supports 65,534 hosts.
  + Class C – Supports 254 hosts.
* The issue of these classes is that they become inefficient when the total number hosts exceed the current class it is set to.
  + Simply put, if Class C is set as the scheme and there are 255 hosts that are being allocated, the scheme is changed to Class B. This is not efficient because there are now 65,280 unused IP address spaces.

Implementing CIDR in AWS

In AWS, you can use CIDR notation to whitelist IP addresses in various services like security groups, network ACLs (Access Control Lists), and AWS WAF (Web Application Firewall). Here's how you can use CIDR notation to whitelist IPs in AWS:

A screenshot of a computer

Description automatically generated\

*Ben Merritt, SE2 Spring 2024*

* Security Groups:
  + Go to the AWS Management Console and navigate to the EC2 dashboard.
  + Select "Security Groups" from the navigation pane.
  + Choose the security group you want to modify and click on its ID.
  + In the "Inbound" tab, click "Edit".
  + Add a new rule by specifying the CIDR notation for the IP range you want to whitelist along with the appropriate port/protocol.
  + For example, to allow access from a specific IP address (e.g., 203.0.113.1), you would add an inbound rule with the CIDR notation 203.0.113.1/32.
  + Save the changes.
* Network ACLs:
  + Navigate to the VPC dashboard in the AWS Management Console.
  + Select "Network ACLs" from the navigation pane.
  + Choose the network ACL you want to modify and click on its ID.
  + In the "Inbound Rules" or "Outbound Rules" tab, click "Edit".
  + Add a new rule specifying the CIDR notation for the IP range you want to whitelist along with the appropriate port/protocol.
  + Save the changes.
* AWS WAF:
  + Go to the AWS WAF & Shield dashboard.
  + Select "Web ACLs" from the navigation pane.
  + Choose the Web ACL you want to modify and click on its ID.
  + In the "Rules" tab, click "Add rules".
  + Create a rule specifying the CIDR notation for the IP range you want to whitelist.
  + Save the changes.

Security Groups in AWS

In Amazon Web Services (AWS), security groups are fundamental components of network security that act as virtual firewalls for instances (virtual servers) in a Virtual Private Cloud (VPC). Security groups control inbound and outbound traffic to instances by defining rules that allow or deny traffic based on specified criteria. They operate at the instance level, meaning each instance can be associated with one or more security groups.

Here's how security groups work and how they're used to whitelist IPs:

* Inbound Rules: In a security group, you define inbound rules that control incoming traffic to instances associated with the security group. These rules specify the allowed sources of traffic (e.g., IP addresses, other security groups), as well as the protocols and ports for which traffic is permitted.
* Outbound Rules: Similarly, you define outbound rules that control outgoing traffic from instances associated with the security group. Outbound rules specify the destination addresses, protocols, and ports for outgoing traffic.
* CIDR Notation for IP Whitelisting: To whitelist specific IP addresses or ranges, you use CIDR notation in the security group rules. CIDR notation represents an IP address followed by a forward slash and a number indicating the number of bits in the network portion of the address. For example, 203.0.113.1/32 represents a single IP address, while 203.0.113.0/24 represents a range of IP addresses.
* Example of IP Whitelisting: Suppose you want to allow SSH access to an EC2 instance from a specific IP address (e.g., 203.0.113.1). You would create an inbound rule in the security group associated with the instance, specifying SSH (TCP port 22) as the protocol and 203.0.113.1/32 as the source IP address in CIDR notation.
* Dynamic IP Whitelisting: In cases where IP addresses change frequently, such as for remote workers or dynamic cloud environments, you might use security group rules with broader CIDR ranges or update the rules dynamically through automation or AWS services like AWS Lambda.

By configuring security group rules with CIDR notation, you can effectively whitelist specific IP addresses or ranges and control access to your AWS resources based on your security requirements. It's essential to regularly review and update security group configurations to maintain a secure environment.