En primer lugar, procedemos a abrir la cuarta placa de red, configurándose para que opere en la red interna. A esta conexión la designamos con el nombre "Firewall". A continuación, encendemos las máquinas y asignamos a cada una una dirección IP, máscara de red y gateway estáticos, asegurándonos de que todas pertenezcan al mismo rango. Esta configuración facilitará la comunicación entre ellas mediante la función de Ping.

* DC:
* Dirección IP: 192.168.2.201
* Máscara de Red: 255.255.255.0
* Puerto de Enlace: 192.168.2.254
* Nodo 1:
* Dirección IP: 192.168.2.131
* Máscara de Red: 255.255.255.0
* Puerto de Enlace: 192.168.2.254
* Nodo 2:
* Dirección IP: 192.168.2.132
* Máscara de Red: 255.255.255.0
* Puerto de Enlace: 192.168.2.254
* CentOS 9:
* Dirección IP: 192.168.2.133"

Aplicaremos 3 reglas en los puertos: 433 - 3306 - 22.

Puerto 22:

Comando: iptables -D input -i enp0s10 -p tcp --dport 22 -j ACCEPT:

El comando `iptables -D input -i enp0s10 -p tcp --dport 22 -j ACCEPT` se utiliza para eliminar una regla de filtrado de paquetes en el firewall. Esta regla específica permite el tráfico TCP entrante en el puerto 22 a través de la interfaz de red enp0s10. Al eliminar esta regla, se revoca la autorización para que los paquetes que cumplen con estos criterios sean aceptados, lo que implica que futuros intentos de conexión a través de SSH en el puerto 22 a través de la interfaz enp0s10 serán bloqueados según las reglas predeterminadas o las reglas subsiguientes en la cadena INPUT de iptables.

Comando: iptables -A input -i enp0s10 -p tcp --dport 22 -j DROP

Esta regla de iptables bloquea el tráfico TCP entrante al puerto 22 (usado para SSH) en la interfaz de red enp0s10. Utiliza la acción "DROP" para descartar los paquetes que cumplen con los criterios (protocolo TCP, puerto 22, enp0s10).

Puerto 3306:

Comando: iptables -A INPUT -i enp0s10 -p tcp --dport 3306 -j DROP

Esta regla bloquea el tráfico TCP entrante al puerto 3306, utilizado típicamente para conexiones a servidores MySQL. Al emplear la acción "DROP", se restringe el acceso a la base de datos MySQL a través de la interfaz de red enp0s10, fortaleciendo la seguridad del servidor.

Puerto 433:

Comando: iptables -A INPUT -i enp0s10 -p tcp --dport 443 -j DROP

Esta regla bloquea el tráfico TCP entrante al puerto 443, que es comúnmente utilizado para conexiones HTTPS seguras. Al usar la acción "DROP", se impide el acceso a servicios web seguros a través de la interfaz de red enp0s10, brindando un control adicional sobre la seguridad.



