



Asignatura:

Sistemas Operativos III

Tema:

HOWTO Y VIDEO (FIREWALL)

Participante:

Santiago M. Duval Contreras

Matricula:

2015-3246

Facilitador:

José Doñe

Fecha:

4/5/2020

HOW-TO? | Administrando el Firewall en ClearOS.

HOW-TO? | Administrando el Firewall en ClearOS.

En este documento veremos los pasos requerido para trabajar con el firewall y hacer NAT en ClearOS en Oracle VirtualBox.

Link a demostración audiovisual: <https://youtu.be/7F3-Puwq6i4>

Requerimientos:

Tener instalado el programa VirtualBox y tener el OS de ClearOS instalado con los requisitos de hardware virtual que sean requeridos.

Firewall

Paso 1- Instalar el firewall utilizando la cli.

Descargamos e instalamos el firewall utilizando el comando **yum install firewalld**.

Paso 2 – Iniciar el servicio de firewalld.

Utilizamos el comando **systemctl start firewalld** para iniciar el servicio.

```
[root@cosserver ~]# systemctl status firewalld
■ firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset: enabled)
   Active: active (running) since Sat 2020-03-28 22:57:44 AST; 7min ago
     Docs: man:firewalld(1)
   Main PID: 7988 (firewalld)
   CGroup: /system.slice/firewalld.service
```

Pruebas de Firewalld

- Bloquear Redes: **firewall-cmd --direct --add-rule ipv4 filter INPUT 0 -s 192.168.1.50/24 -j DROP**
- Desbloquear Redes: **firewall-cmd --direct --remove-rule ipv4 filter INPUT 0 -s 192.168.1.50/24 -j DROP**
- Bloquear PC a través de la MAC: **firewall-cmd --zone=work --add-source=00:00:00:00:00:00 firewall-cmd --zone=work --add-rich-rule='rule source mac=00:00:00:00:00:00 drop'**
- Desbloquear PC a través de la MAC después de que haya sido bloqueada: **firewall-cmd --zone=work --remove-rich-rule='rule source mac=00:00:00:00:00:00 drop'**
- Anadir puertos: **firewall-cmd --permanent --zone=public --add-port="port"/tcp**
- Remover puertos: **firewall-cmd --permanent --zone=public --remove-port="port"/tcp**
- Anadir servicios: **firewall-cmd --permanent --zone=public --add-service= "service name"**

HOW-TO? | Administrando el Firewall en ClearOS.

- Remover servicios: **firewall-cmd --permanent --zone=public --remove-service="service name"**
- Ejemplo, bloquear el servicio de ssh para una computadora en la red: **firewall-cmd --direct --add-rule ipv4 filter INPUT 1 -m tcp --source "ip client/24" tcp --deport 22 -j REJECT.**
- Remover regla: **firewall-cmd --direct --remove-rule ipv4 filter INPUT 1 -m tcp --source "ip client/24" tcp --deport 22 -j REJECT.**

Iptables

Paso 1- Instalar iptables utilizando la cli.

Descargamos e instalamos iptables utilizando el comando **yum install iptables-devel.**

Pruebas de Iptables

- Bloquear Redes: **iptables -I INPUT -s [Red] -j DROP**
- Desbloquear Redes: **iptables -D INPUT -s [Red] -j DROP**
- Bloquear PC a través de la MAC: **iptables -I INPUT -m --mac-source [mac] -j DROP**
- Desbloquear PC a través de la MAC después de que haya sido bloqueada: **iptables -D INPUT -m --mac-source [mac] -j DROP**
- Bloquear Puertos: **iptables -I INPUT -p [protocolo] --destination-port 23 -d [ip a la que queremos restringir el uso de puerto] -j DROP**
- Desbloquear Puertos: **iptables -D INPUT -p [protocolo] --destination-port 23 -d [ip a la que queremos conceder el uso de puerto] -j DROP**

Configurando una conexión NAT

Tenemos que tener habilitada una nic de red externa y una nic de red interna. Esto lo podemos verificar con el comando **ip -r.**

Paso 1 - Utilizar nano para editar el archivo que se encuentra en la ruta **/etc/sysctl.conf** y añadimos la siguiente línea de texto **net.ipv4.ip_forward=1**

Paso 2 - Remover la nic interna de la zona publica y moverla a la zona privada con los comandos: **> firewall-cmd --zone=public --remove-interface=enp0s3 ; firewall-cmd --zone=internal --add-interface=enp0s3.**

Paso 3 – Agregar las siguientes reglas para enrutar la nic interna.

- **firewall-cmd --direct --add-rule ipv4 nat POSTROUTING 0 -o [interface externa] -j MASQUERADE.**
- **firewall-cmd --direct --add-rule ipv4 filter FORWARD 0 -i [interfaz externa] -o [interfaz interna] -j ACCEPT**
- **firewall-cmd --direct --add-rule ipv4 filter FORWARD 0 -I [interfaz interna] -o [interfaz externa] -m state --state RELATED,ESTABLISHED -j ACCEPT**