	UNIVERSIDAD AUTONOMA DE OCCIDENTE		
	FACULTAD DE INGENIERIA *DEPARTAMENTO DE AUTOMATICA Y ELECTRONICA*	FIREWALL	
	ESTUDIANTES:	Fecha:	*Valoración*

PRACTICA FIREWALLD

Objetivos

- Aprender a instalar, administrar y configurar FirewallD, un controlador fronted para iptables
- Configurar el firewall de un servidor de acuerdo a requerimientos de seguridad dados

PARTE 1

Se recomienda primero estudiar los comandos de las diapositivas de clase.

Para esta parte puede seguir los tutoriales de YouTube en:

https://www.youtube.com/watch?v=bE8a8j0ExPc&t=252s
https://www.youtube.com/watch?v=If9Lgu1gZ84

Ejercicio

Implementar el caso de estudio "Permitir que el firewall se comporte como NAT" de las diapositivas de clase, de acuerdo a la siguiente topología:

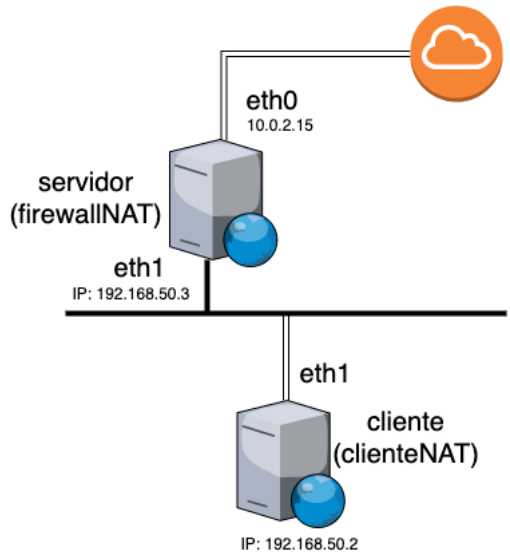

Figura 1. Configuración de Firewall en Vagrant + VirtualBox + Centos para ejercicio NAT

Para esta parte usar un Vagrantfile como este (el mismo de las practicas anteriores):

```
Vagrant.configure("2") do |config|
```

```
  config.vm.define :cliente do |cliente|
    cliente.vm.box = "bento/centos-7.9"
    cliente.vm.network :private_network, ip: "192.168.50.2"
    cliente.vm.hostname = "cliente"
  end

  config.vm.define :servidor do |servidor|
    servidor.vm.box = "bento/centos-7.9"
    servidor.vm.network :private_network, ip: "192.168.50.3"
    servidor.vm.hostname = "servidor"
  end
end
```

RECOMENDACIÓN: Para los comandos siguientes no haga uso de copy+paste. En lugar de eso digite los comandos.

- Antes de iniciar la configuración del firewall es posible que necesite detener el Network Manager

```
service NetworkManager stop
chkconfig NetworkManager off
```

- Para permitir el reenvió de paquetes se debe modificar el archivo /etc/sysctl.conf se debe añadir en el servidor (fiewallNAT):

```
net.ipv4.ip_forward = 1
```

Para comprobar, ejecutar el comando

```
sysctl -p
```

- Definir Zonas en el servidor:

Zona internal, para la interfaz que va con la red privada eth1

Zona public, para la interfaz que va con la red publica eth0

La interfaz eth0 debe quedar configurada en la zona publica, mientras que la eth1 en la zona dmz. Verifique si en su caso particular es necesario agregar o borrar interfaces.

Primero verifique las zonas activas con:

```
firewall-cmd --get-active-zones
```

Luego agruegue o remueva según sea necesario. En mi caso específico tuve que hacer lo siguiente:

```
firewall-cmd  --zone=public --remove-interface=eth1
firewall-cmd  --zone=internal --add-interface=eth1
```

El comando

```
firewall-cmd --get-active-zones
```

Debe mostrar algo como lo siguiente

```
internal
         interfaces: eth1
public
         interfaces: eth0
```

- Definir reglas del NAT (estas son reglas directas (iptables) sobre el firewall)

```
firewall-cmd --direct --add-rule ipv4 nat POSTROUTING 0 -o
eth0 -j MASQUERADE

firewall-cmd --direct --add-rule ipv4 filter FORWARD 0 -i
eth1 -o eth0 -j ACCEPT

firewall-cmd --direct --add-rule ipv4 filter FORWARD 0 -i
eth0 -o eth1 -m state --state RELATED,ESTABLISHED -j ACCEPT
```

Verificar las reglas con

```
[root@servidor ~]# firewall-cmd --direct --get-all-rules
```

- Añadir servicios a las zonas

```
firewall-cmd --zone=public --add-service=http
firewall-cmd --zone=public --add-service=https
firewall-cmd --zone=public --add-service=dns

firewall-cmd --zone=internal --add-service=http
firewall-cmd --zone=internal --add-service=https
firewall-cmd --zone=internal --add-service=dns
```

- Puerta de Enlace en Cliente

Configurar la puerta de enlace de los equipos de la red interna. La puerta de enlace será la dirección del firewall.

Agregar a /etc/sysconfig/network

```
GATEWAY=192.168.50.3
```

- Reiniciar el servicio de network

```
service network restart
```

- Verificación del Gateway desde cliente

```
[root@cliente ~]# netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         192.168.50.3    0.0.0.0         UG        0 0          0 eth1
10.0.2.0        0.0.0.0         255.255.255.0   U         0 0          0 eth0
169.254.0.0     0.0.0.0         255.255.0.0     U         0 0          0 eth0
169.254.0.0     0.0.0.0         255.255.0.0     U         0 0          0 eth1
192.168.50.0    0.0.0.0         255.255.255.0   U         0 0          0 eth1
```

Si les aparecen dos rutas de salida (las que empiezan por 0.0.0.0) pueden borrar la que sale por eth0 con un comando como:

sudo route del -net 0.0.0.0 gw 10.0.2.2 netmask 0.0.0.0 dev eth0

- Ping desde cliente a través de eth1

```
ping –I eth1 8.8.8.8
```

PARTE 2

Topología

En la siguiente topología se muestra como podría usar FirewallD para asignar reglas básicas para un servicio de http

- Configure un box en Vagrant con dos interfaces de red como se muestra en la figura (Ver Vagrantfile abajo).

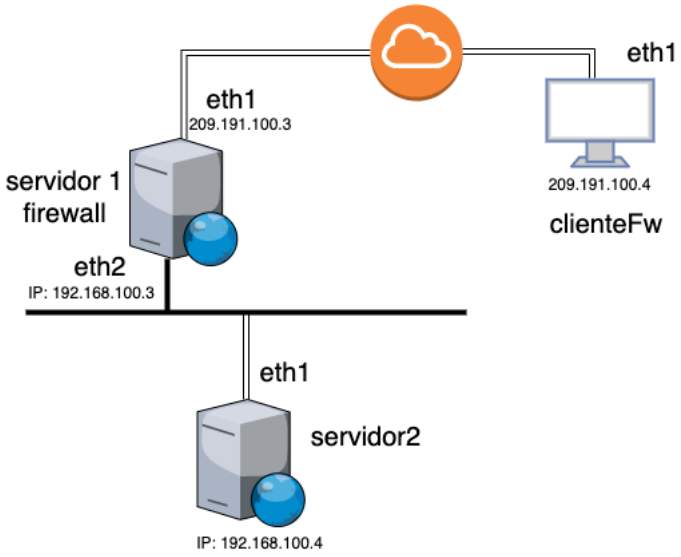

Figura 2. Configuracion de Firewall en Vagrant + VirtualBox + Centos

Para esta parte, configure un Vagrantfile como el siguiente

```
Vagrant.configure("2") do |config|
  config.vm.define :clienteFw do |clienteFw|
    clienteFw.vm.box = "bento/centos-7.9"
    clienteFw.vm.network :private_network, ip: "209.191.100.2"
    clienteFw.vm.hostname = "clienteFw"
  end

  config.vm.define :firewall do |firewall|
    firewall.vm.box = "bento/centos-7.9"
    firewall.vm.network :private_network, ip: "209.191.100.3"
    firewall.vm.network :private_network, ip: "192.168.100.3"
    firewall.vm.hostname = "firewall"
  end

  config.vm.define :servidor2 do |servidor2|
    servidor2.vm.box = "bento/centos-7.9"
    servidor2.vm.network :private_network, ip: "192.168.100.4"
    servidor2.vm.hostname = "servidor2"
  end

end
```

RECOMENDACIÓN: Para los comandos siguientes no haga uso de copy+paste. En lugar de eso digite los comandos.

- Antes de iniciar la configuración del firewall es posible que necesite detener el Network Manager

```
service NetworkManager stop
chkconfig NetworkManager off
```

- Verifique las interfaces asociadas a la zona dmz

```
firewall-cmd --zone=dmz --list-all
```

En mi caso, la salida es:

```
dmz (active)
  target: default
  icmp-block-inversion: no
  interfaces: eth1 eth2
  sources:
  services: ssh
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

CONFIGURAR ZONA DMZ

ASIGNAR ZONA *dmz* A *eth1*

- Asigne la zona dmz como la zona default para eth1. Esta zona solo permite SSH e ICMP.

```
sudo firewall-cmd --set-default-zone=dmz
```

CONFIGURAR INTERFACES

- En este caso se necesita remover (ver si usted necesita removerla) la interfaz eth2 de la zona dmz

```
sudo firewall-cmd --zone=dmz --remove-interface=eth2 --
permanent
```

- De ser necesario agregue la interfaz eth1 (solo si aun no esta agregada). El comando para hacerlo se muestra a continuación

```
sudo firewall-cmd --zone=dmz --add-interface=eth1 –-permanent
```

AGREGAR SERVICIOS

- Agregue los servicios http, y https a la zona dmz

```
firewall-cmd --zone=dmz --add-service=http --permanent
firewall-cmd --zone=dmz --add-service=https --permanent
```

RECARGAR REGLAS

- Recargue la configuración permanente a runtime

```
sudo firewall-cmd --reload
```

- Si corre el comando `firewall-cmd --zone=dmz --list-all`, esta deberia ser la salida:

```
dmz (default)
       interfaces: eth1
       sources:
       services: http https ssh
       ports:
       masquerade: no
       forward-ports:
       icmp-blocks:
       rich rules:
```

De este resultado podemos concluir lo siguiente:

a. La zona dmz es nuestra zona por defecto, la cual aplica a la interfaz eth1, para todas las fuentes de red y puertos.
b. El trafico de entrada http (puerto 80), HTTPS (puerto 443) y SSH (puerto 22) es permitido
c. Ya que no hay restricciones acerca de la versión de IP, esto aplica tanto para IPV4 como para IPV6.
d. Enmascaramiento, y reenvío de puertos no son permitidos.
e. Ya que no tenemos bloques ICMP el trafico ICMP es permitido por completo.

f. Todo el tráfico de salida es permitido

CONFIGURAR ZONA INTERNAL

CONFIGURAR INTERFACES

- Agregar la interfaz eth2 a la zona internal

```
firewall-cmd --zone=internal --add-interface=eth2 --permanent
```

RECARGAR REGLAS

- Recargue la configuración permanente a runtime

```
sudo firewall-cmd --reload
```

- **La zona internal debe lucir como sigue**

```
firewall-cmd --zone=internal --list-all
internal (active)
  target: default
  icmp-block-inversion: no
  interfaces: eth2
  sources:
  services: ssh mdns samba-client dhcpv6-client
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

- Para ver laz zonas activas ejecute

```
firewall-cmd --get-active-zones
dmz
  interfaces: eth1
internal
  interfaces: eth2
```

Ejercicio

1. Basándose en la topología mostrada en la Figura 2, realizar las siguientes configuraciones:

a. Verifique que en el **servidor1 (firewall)** estén instalado el servicio http
b. En el **servidor 1 (firewall)** permita el tráfico entrante hacia http
c. Configure un **servidor 2** corriendo un servicio web seguro
d. Redireccione las peticiones https entrantes al **servidor 1 (firewall)** para que sean atendidas por el **servidor 2**
e. El **servidor 1 (interfaz eth1)** no debería aceptar pings (Deniegue el protocolo ICMP)

HINT:

- Para el punto de redirección, recuerde agregar el enmascaramiento:

```
sudo firewall-cmd --zone=dmz --add-masquerade
sudo firewall-cmd --zone=internal --add-masquerade
```

  En este punto también debe agregar la regla de reenvío (es necesario solamente para la zona dmz)

- Para probar que la redirección funcione, intente abrir la pagina principal del servidor web seguro instalado en servidor 1 (firewall). Si esta bien configurado, deberá redirigirlo hacia la pagina principal del servidor 2.
- Puede usar el comando firewall-cmd --get-icmptypes para ver los mensajes icmps soportados.
- Que comandos se usan para bloquear icmps?
- Que tipos de icmps debe bloquear?
- Probar los pings desde el clienteFw