UNIVERSIDAD NACIONAL DEL COMAHUE

Centro Regional Zona Atlántica

Tecnicatura Universitaria en Administración de Sistemas y Software Libre

Redes de datos

Trabajo Práctico Nro: 5 – Firewall en GNU/Linux **Maidana Maximiliano**

Objetivo

Experimentar las reglas de filtrado usando iptables.

Recursos

Para la realización del trabajo sobre el simulador, serán necesarios:

- *2 clientes alpine con cliente lynx* (*un navegador web en modo texto)* y *nmap.*
- 1 Servidor *Web* (*nginx*) al que se le instala *iptables*.
- 1 *switch* ethernet.

Preparación del laboratorio

El cliente *alpine con cliente lynx* y *nmap* puede ser creado con un Dockerfile (imagen *cliente*) y se la utilizará para las PCs.

El servidor Web se obtendrá a partir de la imagen oficial de *nginx* en *dockerhub* sobre la que se instalarán los paquetes necesarios, creando la imagen a aplicar.

Para ello, en un directorio vacío, crear un archivo *Dockerfile* con el siguiente contenido (textual):

```
FROM nginx
ENV DEBIAN_FRONTEND noninteractive
ENV TERM linux
RUN apt-get update && apt-get install -y iptables iproute2 iputils-ping &&  rm -rf /var/cache/apt/*
EXPOSE 80
CMD nginx -g 'daemon off;'
```

Una vez guardado el archivo y sin cambiar de directorio, desde la línea de comandos ejecutar (no omitir el punto final):

```
ubuntu@curza:~/docker$ docker build -t servidor .
```

Ahora existe una imagen de nombre *servidor* a utilizar como en el laboratorio anterior.

Para el cliente Alpine con lynx y nmap, en otro directorio se puede hacer un Dockerfile:

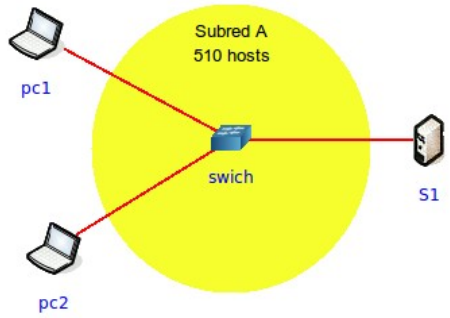
```
FROM alpine:latest
LABEL Alpine, lynx y nmap
RUN apk add --update lynx nmap && rm -rf /var/cache/apk/*
```

Y luego ejecutar:

```
ubuntu@curza:~/docker-alpine$ docker build -t servidor .
```

Actividades

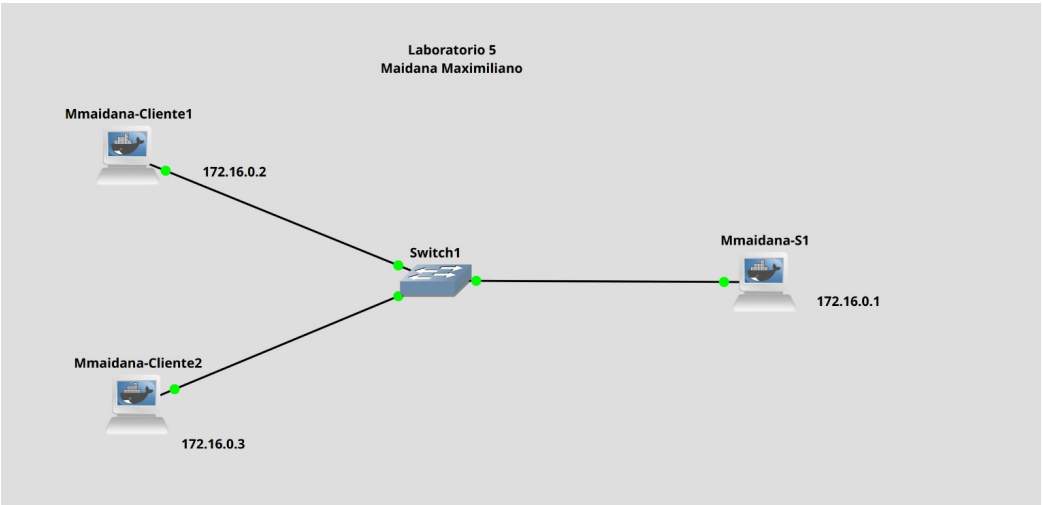
1 Crear la topología indicada en la figura mediante el emulador GNS3.



2 Consignar un rango de direcciones IP para la red que contenga un máximo de 510 hosts. Use para ello cualquiera de los rangos de IP privadas que lo permitan.

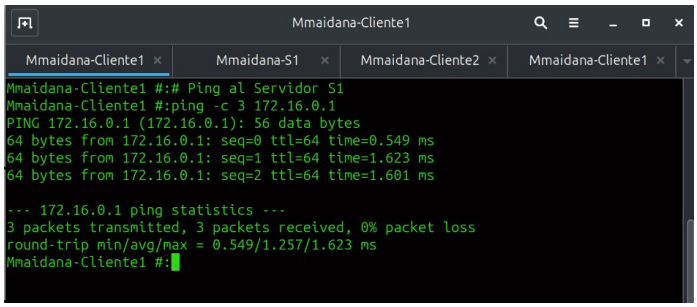
3 Asignar direcciones IP dentro del rango para el servidor S1 y las computadoras pc1 y pc2.

Captura de topologia dentro de la red 172.16.0.0/23

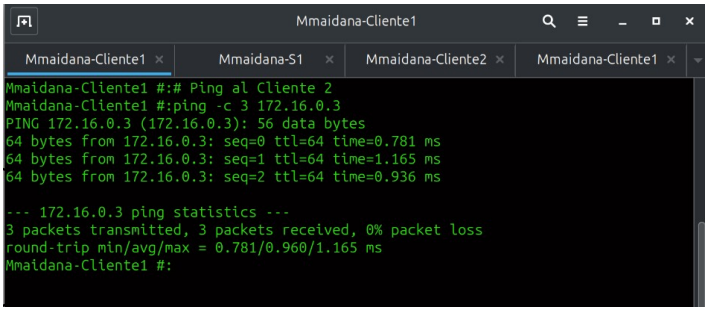


4 Iniciar la simulación y comprobar la conectividad entre los equipos.

Captura de Pantalla desde Mmaidana-Cliente 1

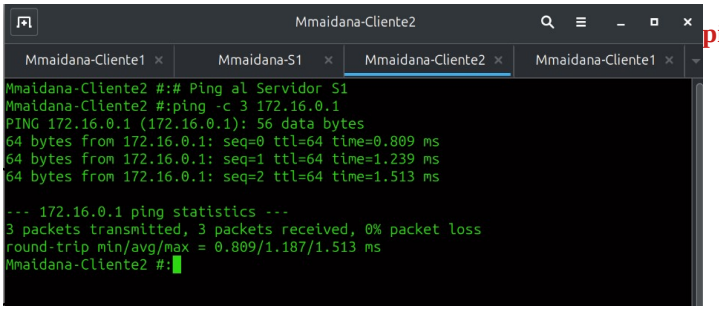


ping al servidor

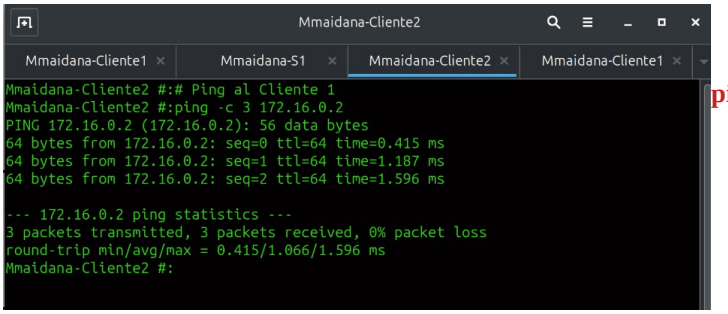


ping a Cliente2

Captura de Pantalla desde Mmaidana-Cliente 2

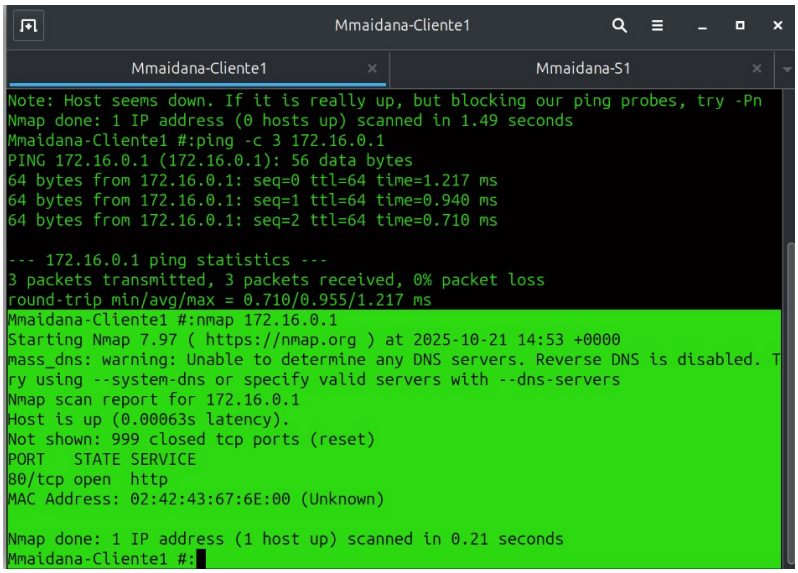


ping al servidor



ping a Cliente1

5 Verificar qué puertos están abiertos en el servidor usando nmap desde una PC cliente (hacer una captura de pantalla).

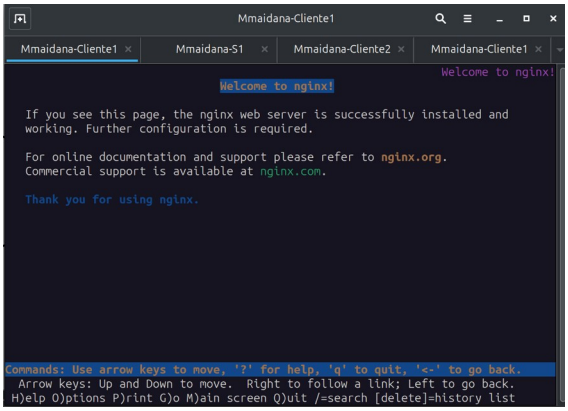


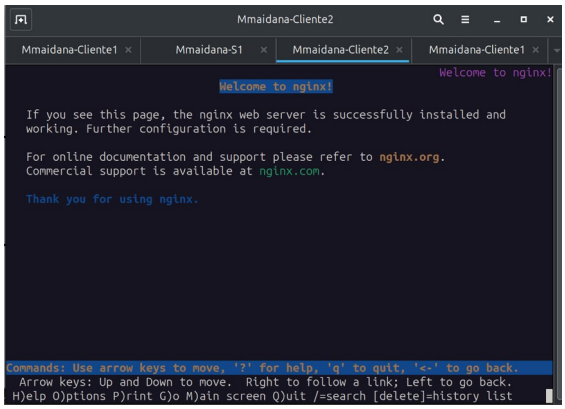
6 Establecer una configuración apropiada para un Firewall en el servidor S1 que cumpla las siguientes condiciones (utilizar la consola auxiliar):

6.1 Como política por defecto, eliminar todo tráfico entrante no permitido explícitamente.

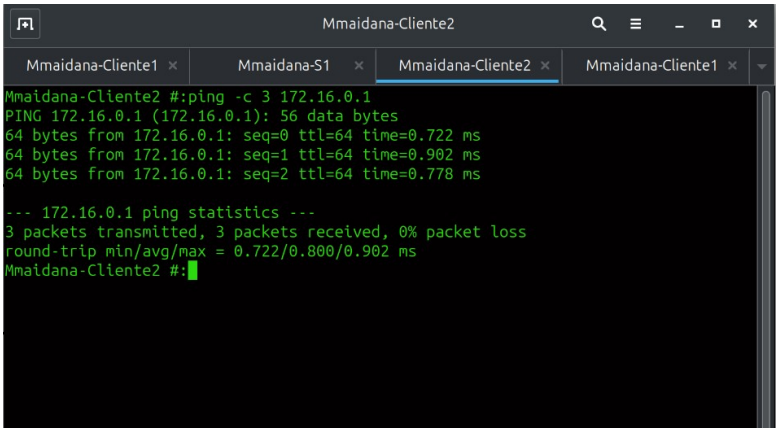
6.2 **Permitir**:

6.2.1 Solicitudes al puerto 80 hacia el servidor, provenientes desde los hosts de la subred.

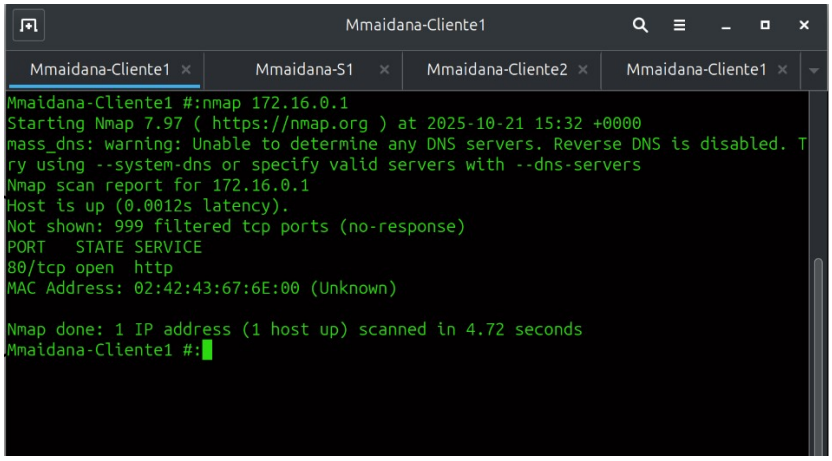




6.2.2 Que el servidor responda solicitudes de ping solo desde el host pc2.



6.2.3 Comprobar nuevamente los puertos en el servidor desde cada una de las PCs y comentar.

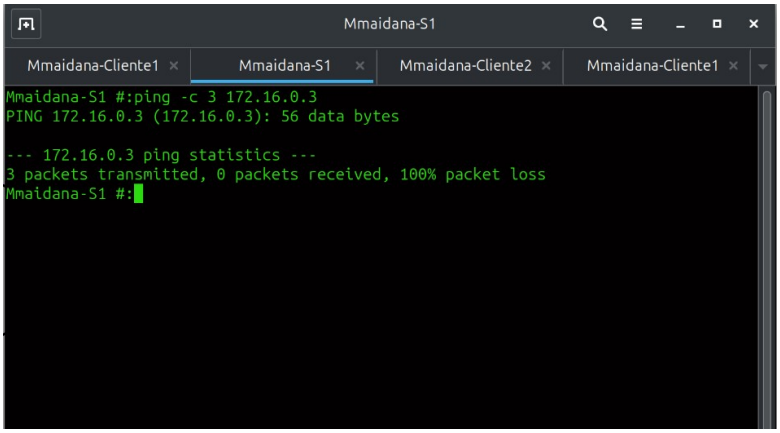


Esto demuestra que firewall está funcionando a la perfección:

1. **80/tcp open http: está funcionando.**
2. **999 filtered tcp ports: nmap ya no ve los puertos como closed (cerrados), sino como filtered (filtrados), porque el firewall simplemente descarta los paquetes.**

6.3 **Denegar**:

6.3.1 Hacer ping desde el servidor hacia el host pc2.



6.3.2 Según el punto 6.2.2 asegurarse de que el pc1 no puede hacer ping al servidor