



UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías

"VIGILADA MINEDUCACIÓN"



LABORATORIO DE UN FIREWALL CON OPENSTACK Y DEBIAN.

DOCENTE:

JORGE ELIECER GOMEZ GOMEZ



"VIGILADA MINEDUCACIÓN"



INTEGRANTE:

DÍAZ CABARCAS CAMILO ANDRÉS

GARCÍA MOLINA JAVIER ANDRÉS

GONZÁLEZ ECHAVARRÍA ANDRÉS CAMILO

LEAL FLÓREZ SEBASTIÁN JOSÉ

UNIVERSIDAD DE CÓRDOBA
FACULTAD DE INGENIERÍAS
INGENIERÍA EN SISTEMAS
MONTERÍA, CÓRDOBA

2025

Por una universidad con calidad, moderna e incluyente

Carrera 6^a. No. 76-103 Montería NIT. 891080031-3 - Teléfono: 7860300 - 7860920 www.unicordoba.edu.co



UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías

"VIGILADA MINEDUCACIÓN"



CONTENIDO.

1. INTRODUCCIÓN.....	3
2. OBJETIVOS.....	4
2.1. Objetivo general.....	4
2.2. Objetivos específicos.....	4
3. MARCO TEÓRICO.....	4
3.1. ¿Qué es un firewall?.....	4
3.2. Tipos de firewall.....	4
3.3. Funciones principales.....	5
4. PROCESO DE INSTALACIÓN Y CONFIGURACIÓN.....	5
4.1 Instalación de VirtualBox.....	5
4.2 Creación de máquina virtual Debian.....	14
4.3 Configuración de red en VirtualBox.....	19
4.4 Instalación de Debian.....	24
5. COMANDOS UTILIZADOS EN DEBIAN Y OPENSTACK.....	37
6. TOPOLOGÍA DEL LABORATORIO.....	56
8. INSTALAR Y CONFIGURAR EL FIREWALL.....	59
9. CAPTURAS Y ANÁLISIS CON WIRESHARK.....	63
10. CONCLUSIONES.....	74
11. REFERENCIAS.....	74

Por una universidad con calidad, moderna e incluyente

Carrera 6^a. No. 76-103 Montería NIT. 891080031-3 - Teléfono: 7860300 - 7860920 www.unicordoba.edu.co



UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías



1. INTRODUCCIÓN.

El presente laboratorio implementa un firewall funcional sobre una infraestructura virtualizada: VirtualBox como hipervisor, Debian como base y OpenStack como plano de control para redes e instancias. Se construyó una topología aislada con redes internas gestionadas por namespaces de OpenStack, lo que permitió ejercitarse en enrutamiento, segmentación y filtrado realista. El flujo abarcó: instalación del hipervisor y creación de VMs; despliegue de OpenStack/DevStack y provisión de redes internas; aprovisionamiento de instancias Debian (servidor y cliente) con UFW configurado en modo “deny incoming / allow outgoing” y reglas específicas; instalación offline de herramientas (libpcap, tcpdump, ufw) para operar sin repositorios externos; acceso a las VMs desde el host mediante ip netns exec para entrar a la red interna; generación de tráfico controlado; captura simultánea en tres puntos (host, servidor, cliente) con tcpdump; y validación con Wireshark de SYN/ACK, RST, ICMP y puertos web/MySQL según las políticas definidas. El resultado es un firewall verificado extremo a extremo: las reglas aplicadas se reflejan en los paquetes capturados y analizados, confirmando el comportamiento esperado de permit/bloqueo en la malla de red virtual.

Por una universidad con calidad, moderna e incluyente

Carrera 6^a. No. 76-103 Montería NIT. 891080031-3 - Teléfono: 7860300 - 7860920 www.unicordoba.edu.co



UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías



2. OBJETIVOS.

2.1. Objetivo general

Implementar un firewall en un entorno virtualizado utilizando Debian y OpenStack, validando su funcionamiento mediante capturas y análisis de paquetes.

2.2. Objetivos específicos

- Instalar y configurar VirtualBox como entorno de virtualización.
- Implementar Debian como sistema base para el controlador de OpenStack.
- Instalar y configurar OpenStack para la creación de redes, routers e instancias.
- Crear una topología que incorpore un firewall y redes privadas.
- Definir reglas de filtrado y políticas de tráfico.
- Capturar el tráfico generado y validar el funcionamiento del firewall mediante Wireshark.

3. MARCO TEÓRICO.

3.1. ¿Qué es un firewall?

Un firewall es un sistema de seguridad encargado de filtrar, bloquear o permitir tráfico entre redes basándose en un conjunto de reglas predefinidas. Funciona como un punto de control que protege los recursos internos evitando accesos no autorizados o actividades maliciosas.

3.2. Tipos de firewall

- Nivel de red (capa 3): Filtra por IP, puertos y protocolos.
- Nivel de aplicación (capa 7): Inspección profunda del tráfico (DPI).
- Firewall estático: Reglas fijas.
- Firewall dinámico: Reglas basadas en contexto o estados.
- Firewall stateful: Mantiene tabla de estados de conexiones.

Por una universidad con calidad, moderna e incluyente

Carrera 6^a. No. 76-103 Montería NIT. 891080031-3 - Teléfono: 7860300 - 7860920 www.unicordoba.edu.co



"VIGILADA MINEDUCACIÓN"

UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías



3.3. Funciones principales

- Control de acceso
- Filtrado de paquetes
- NAT
- Detección de tráfico sospechoso
- Segmentación de redes internas

4. PROCESO DE INSTALACIÓN Y CONFIGURACIÓN.

4.1 Instalación de VirtualBox

virtual box - Buscar con Google

google.com/search?q=virtual+box&rlz=1C1PNKB_enCO1167CO1168&oq=virtual&gs_lcp=EgZjaHvbWUqDagBECMYxiABBiKBTIMCAAQRg5GLEDGIAEMgwIARAjGCcYgAQYigIyCggCEAAysQMygAQy...

virtual box

Google

Modo IA Todo Imágenes Vídeos cortos Shopping Vídeos Noticias Más Herramientas

Oracle VirtualBox

VirtualBox is a general-purpose full virtualization software for x86_64 hardware (with version 7.1.14 additionally for macOS/Arm and with version 7.2 also for ...)

Downloads

VirtualBox 6.1.x

Documentation

Download VirtualBox for Linux ...

7.1.14

Más resultados de virtualbox.org »

Por una universidad con calidad, moderna e incluyente

Carrera 6^a. No. 76-103 Montería NIT. 891080031-3 - Teléfono: 7860300 - 7860920 www.unicordoba.edu.co



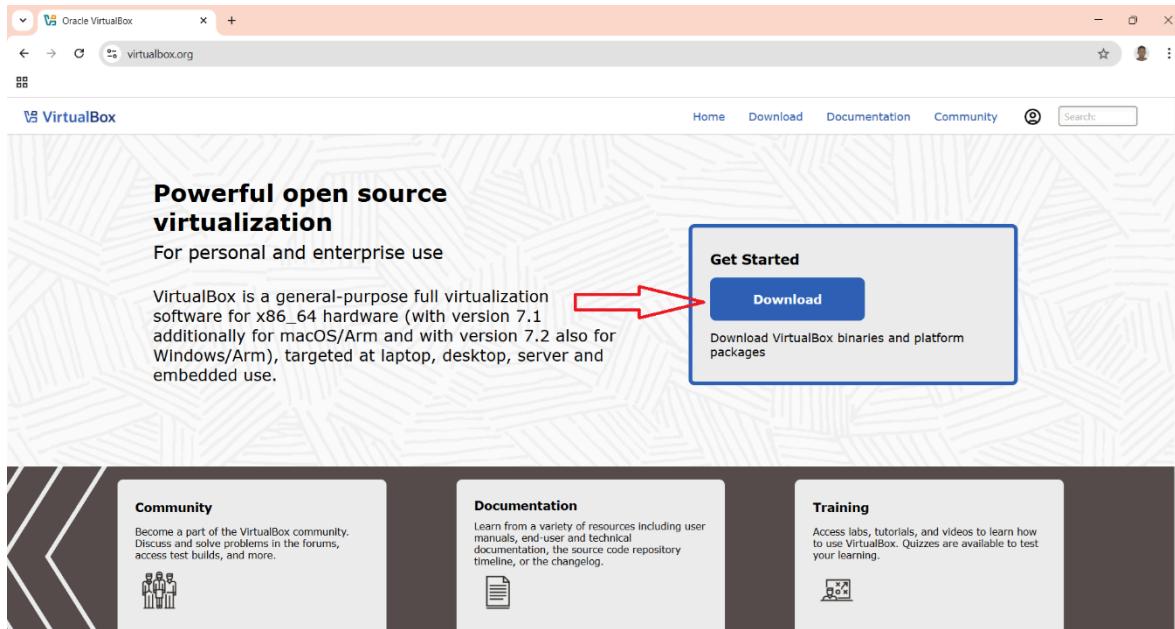
UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías



Empezamos escribiendo en el buscador del navegador de tu preferencia, VirtualBox. Y le damos en la pagina oficial de Oracle VirtualBox.



Powerful open source virtualization
For personal and enterprise use

VirtualBox is a general-purpose full virtualization software for x86_64 hardware (with version 7.1 additionally for macOS/Arm and with version 7.2 also for Windows/Arm), targeted at laptop, desktop, server and embedded use.

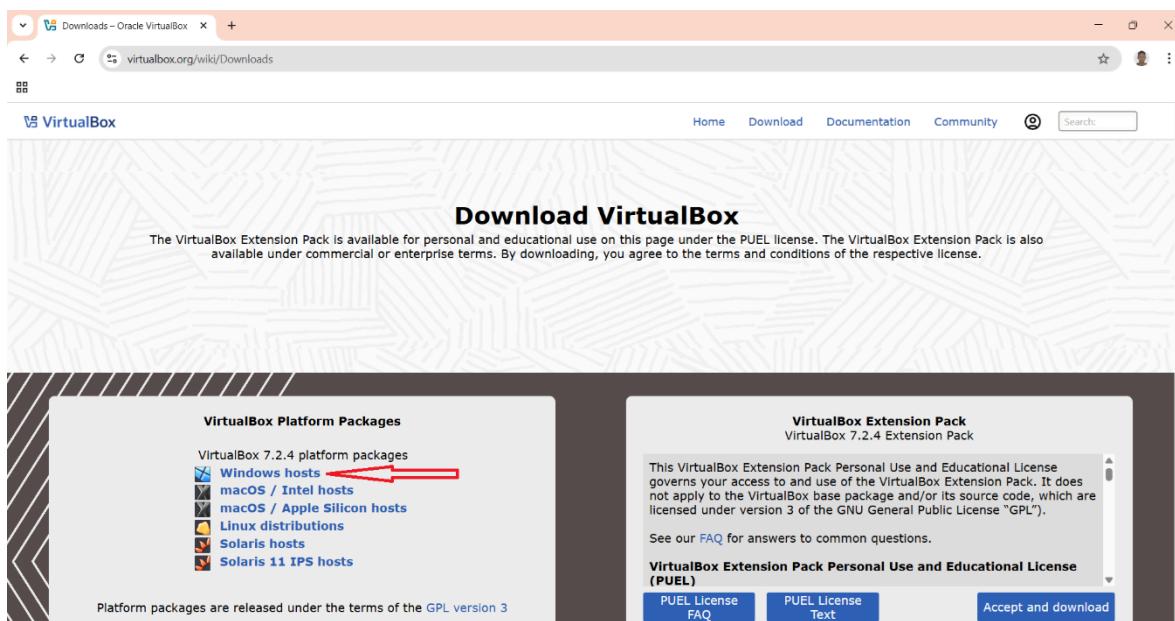
Get Started
Download
Download VirtualBox binaries and platform packages

Community
Become a part of the VirtualBox community. Discuss and solve problems in the forums, access test builds, and more.

Documentation
Learn from a variety of resources including user manuals, developer and technical documentation, the source code repository timeline, or the changelog.

Training
Access labs, tutorials, and videos to learn how to use VirtualBox. Quizzes are available to test your learning.

Seleccionar la opción Download.



Download VirtualBox
The VirtualBox Extension Pack is available for personal and educational use on this page under the PUEL license. The VirtualBox Extension Pack is also available under commercial or enterprise terms. By downloading, you agree to the terms and conditions of the respective license.

VirtualBox Platform Packages
VirtualBox 7.2.4 platform packages
 Windows hosts
 macOS / Intel hosts
 macOS / Apple Silicon hosts
 Linux distributions
 Solaris hosts
 Solaris 11 IPS hosts

Platform packages are released under the terms of the [GPL version 3](#)

VirtualBox Extension Pack
VirtualBox 7.2.4 Extension Pack

This VirtualBox Extension Pack Personal Use and Educational License governs your access to and use of the VirtualBox Extension Pack. It does not apply to the VirtualBox base package and/or its source code, which are licensed under version 3 of the GNU General Public License "GPL".

See our [FAQ](#) for answers to common questions.

VirtualBox Extension Pack Personal Use and Educational License (PUEL)

[PUEL License FAQ](#) [PUEL License Text](#) [Accept and download](#)

Por una universidad con calidad, moderna e incluyente

Carrera 6^a. No. 76-103 Montería NIT. 891080031-3 - Teléfono: 7860300 - 7860920 www.unicordoba.edu.co



UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías



"VIGILADA MINEDUCACIÓN"

Escoger la versión correspondiente al sistema operativo del equipo (en este caso “Windows hosts”)

Download VirtualBox

The VirtualBox Extension Pack is available for personal and educational use on this page under the PUEL license. The VirtualBox Extension Pack is also available under commercial or enterprise terms. By downloading, you agree to the terms and conditions of the respective license.

VirtualBox Platform Packages

VirtualBox 7.2.4 platform packages

- Windows hosts
- macOS / Intel hosts
- macOS / Apple Silicon hosts
- Linux distributions
- Solaris hosts
- Solaris 11 IPS hosts

Platform packages are released under the terms of the [GPL](#) version 3

VirtualBox Extension Pack

VirtualBox 7.2.4 Extension Pack

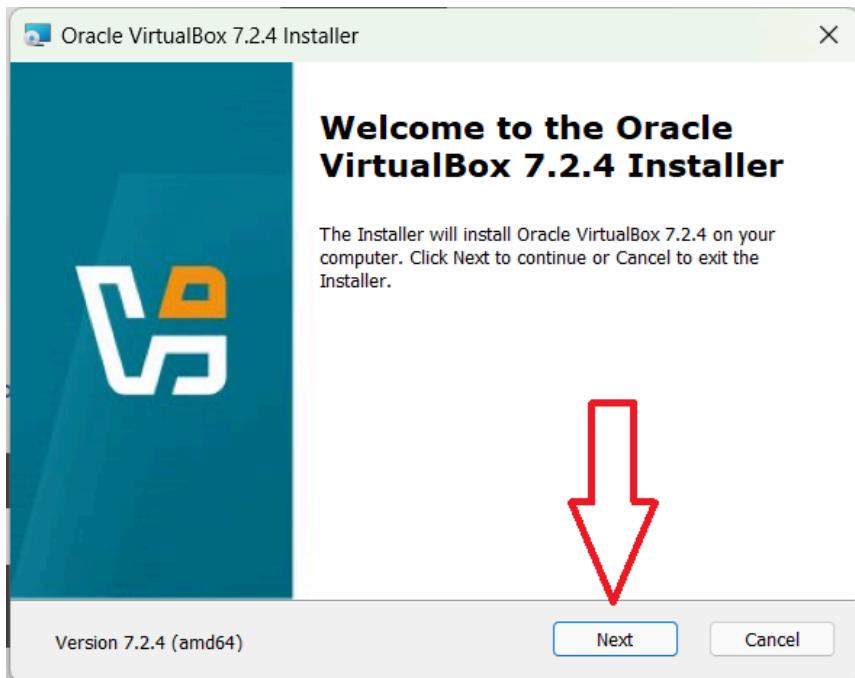
This VirtualBox Extension Pack Personal Use and Educational License governs your access to and use of the VirtualBox Extension Pack. It does not apply to the VirtualBox base package and/or its source code, which are licensed under version 3 of the GNU General Public License ("GPL").

See our [FAQ](#) for answers to common questions.

VirtualBox Extension Pack Personal Use and Educational License (PUEL)

[PUEL License FAQ](#) [PUEL License Text](#) [Accept and download](#)

Esperar a que termine la descarga del instalador. Luego ejecutar el archivo descargado.



Por una universidad con calidad, moderna e incluyente

Carrera 6^a. No. 76-103 Montería NIT. 891080031-3 - Teléfono: 7860300 - 7860920 www.unicordoba.edu.co



UNIVERSIDAD DE CÓRDOBA

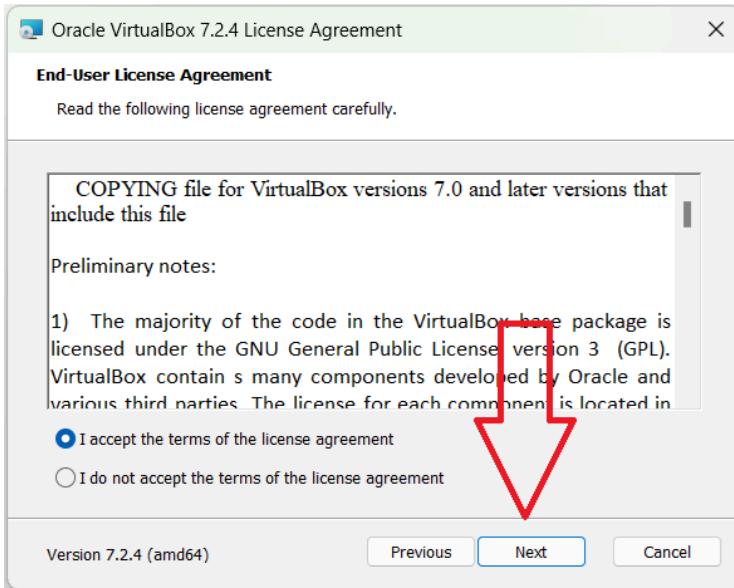
CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías

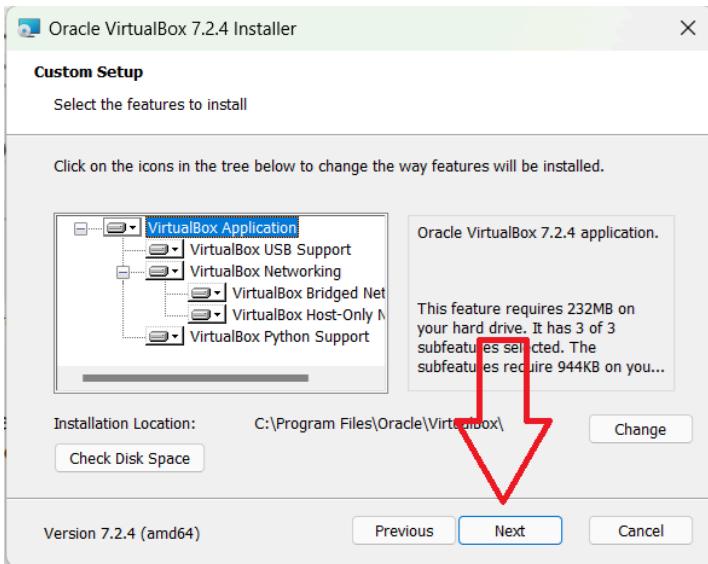
"VIGILADA MINEDUCACIÓN"



Hacer clic en “Next” en la ventana inicial del asistente de instalación.



Le damos en aceptar términos y condiciones y le damos en “Next”





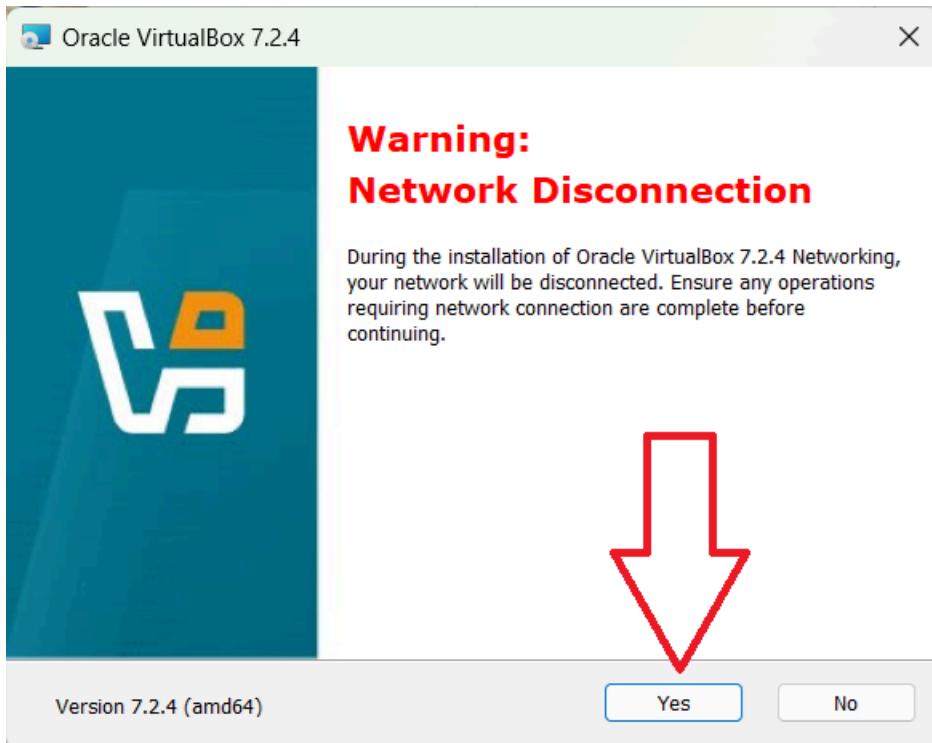
UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías



Seleccionar los componentes a instalar, dejando marcadas las opciones por defecto (VirtualBox Application, USB Support, Networking, Python Support).



Le damos en “Yes”

Por una universidad con calidad, moderna e incluyente

Carrera 6^a. No. 76-103 Montería NIT. 891080031-3 - Teléfono: 7860300 - 7860920 www.unicordoba.edu.co

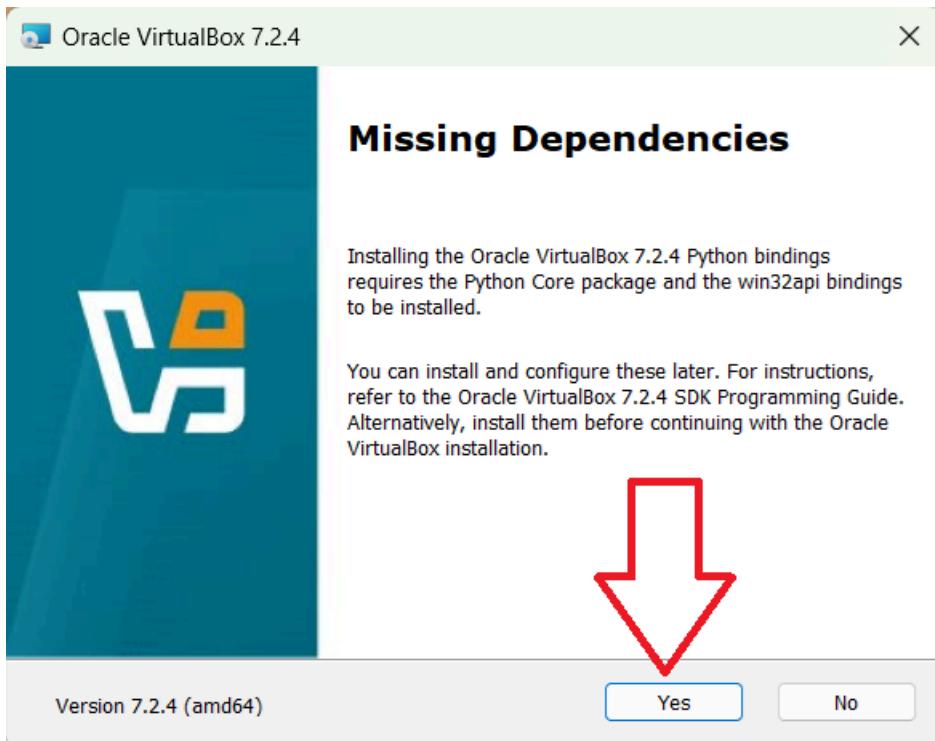


"VIGILADA MINEDUCACIÓN"

UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías



El instalador advertirá que se modificarán las interfaces de red. Hacer clic en Yes para continuar.

Por una universidad con calidad, moderna e incluyente

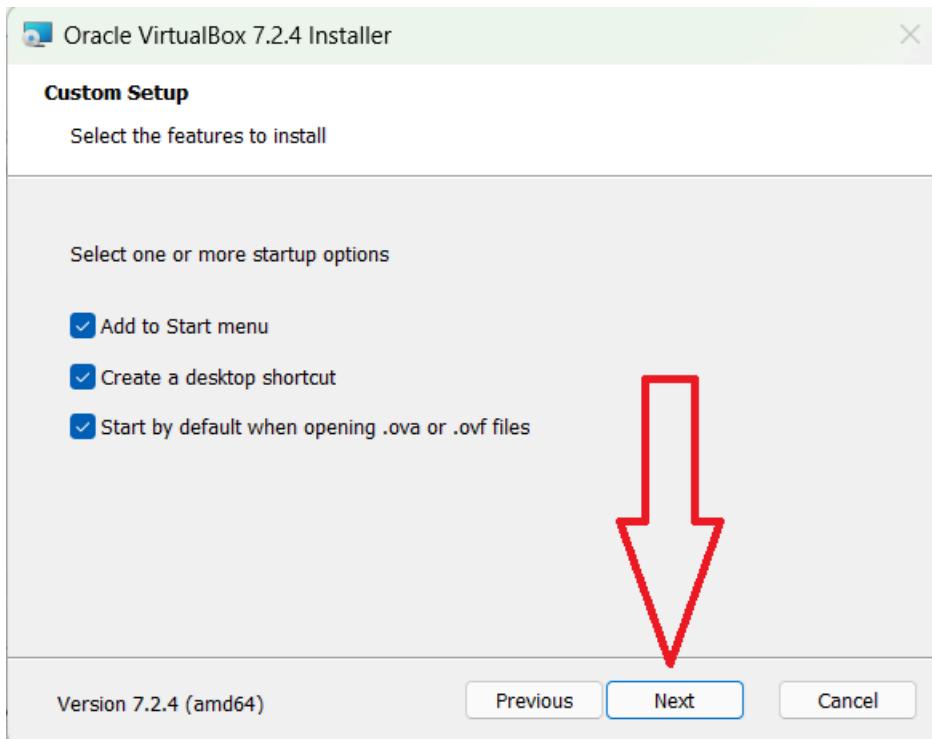
Carrera 6^a. No. 76-103 Montería NIT. 891080031-3 - Teléfono: 7860300 - 7860920 www.unicordoba.edu.co



UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías



Seleccionar el directorio donde se instalará VirtualBox o dejar el que aparece por defecto.

Por una universidad con calidad, moderna e incluyente

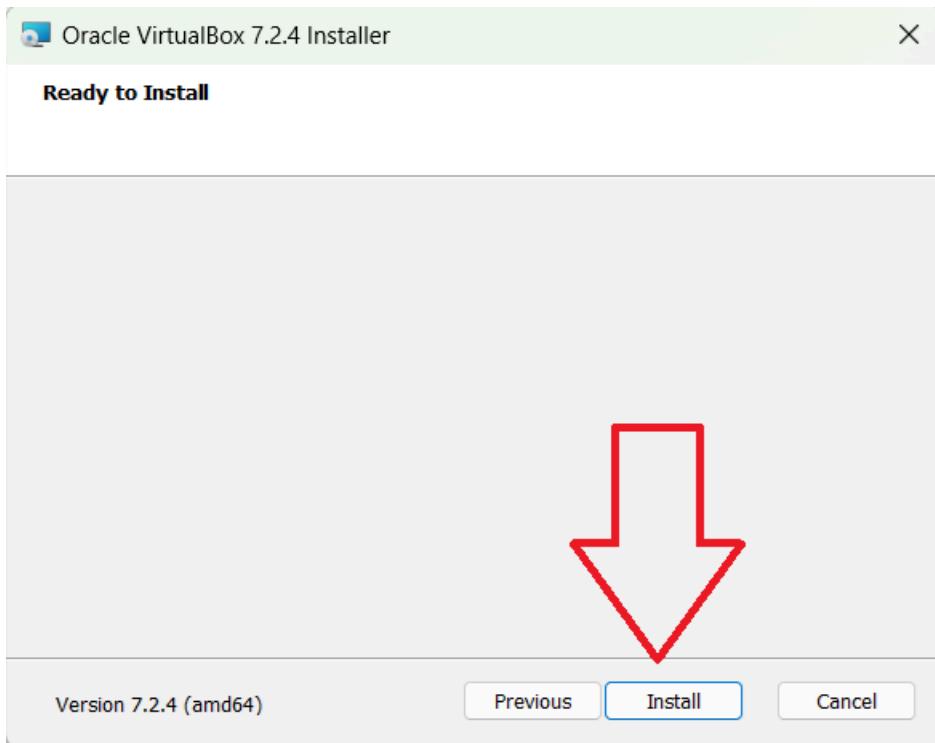
Carrera 6^a. No. 76-103 Montería NIT. 891080031-3 - Teléfono: 7860300 - 7860920 www.unicordoba.edu.co



UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías



Hacer clic en “Install” para iniciar la instalación.

Por una universidad con calidad, moderna e incluyente

Carrera 6^a. No. 76-103 Montería NIT. 891080031-3 - Teléfono: 7860300 - 7860920 www.unicordoba.edu.co

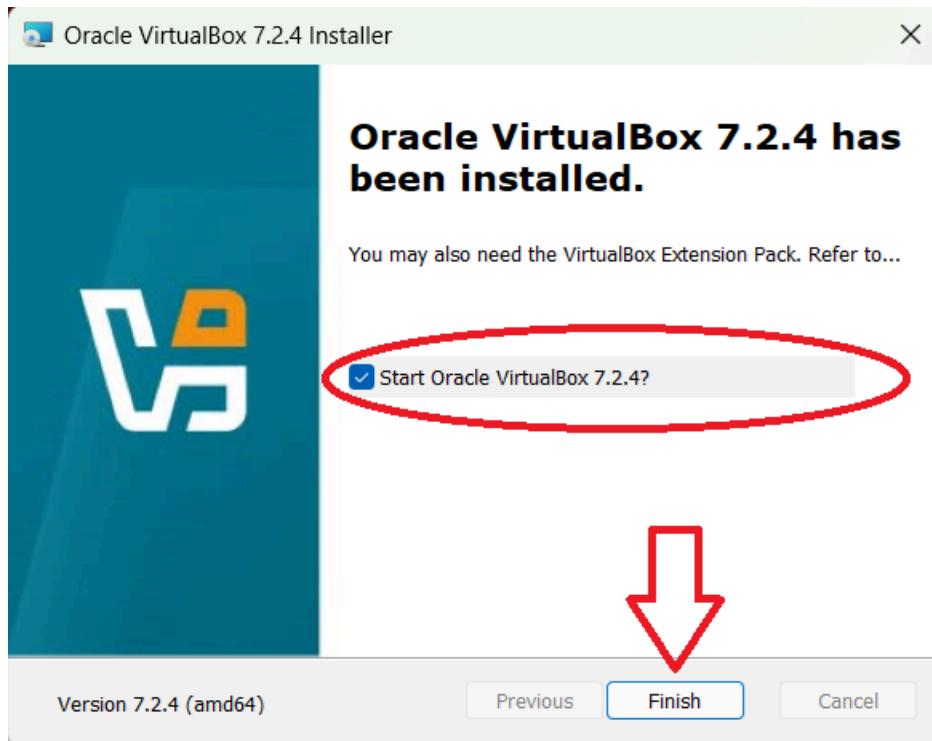


"VIGILADA MINEDUCACIÓN"

UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías



Esperar a que la instalación termine y finalmente seleccionar “Finish”



Por una universidad con calidad, moderna e incluyente

Carrera 6^a. No. 76-103 Montería NIT. 891080031-3 - Teléfono: 7860300 - 7860920 www.unicordoba.edu.co



"VIGILADA MINEDUCACIÓN"

UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías



4.2 Creación de máquina virtual Debian

Debian - Buscar con Google

Debian

Modo IA Todo Imágenes Videos Shopping Vídeos cortos Noticias Más Herramientas

Debian -- El sistema operativo universal

Debian es un sistema operativo y una distribución de Software Libre. Se mantiene y actualiza gracias al trabajo de muchos usuarios que contribuyen con su ...

Download Debian

Download via HTTP/FTP - CD/USB ISO Images - CD vendors page

Downloading Debian

Debian Installer ISOs are hybrid Images, which means they can ...

Descarga de Debian

Descarga de Debian. Esta página contiene opciones para la ...

Download via HTTP/FTP

To install Debian on a machine without an Internet connection, it ...

IntroIndex

Packages - Reasons to use Debian - Mailing Lists - People

Más resultados de debian.org »

Debian GNU/Linux

Software

Debian GNU/Linux, o simplemente Debian, es una distribución Linux de software libre, desarrollada por miles de voluntarios de todo el mundo, que colaboran a través de Internet.

Fuente: Wikipedia

Fecha De Lanzamiento: 16 de agosto de 1993

Por una universidad con calidad, moderna e incluyente

Carrera 6^a. No. 76-103 Montería NIT. 891080031-3 - Teléfono: 7860300 - 7860920 www.unicordoba.edu.co



"VIGILADA MINEDUCACIÓN"

UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías



Empezamos escribiendo en el buscador del navegador de tu preferencia, Debian.

Debian - Buscar con Google

Debian

Modo IA Todo Imágenes Videos Shopping Vídeos cortos Noticias Más Herramientas

Debian https://www.debian.org

Debian - El sistema operativo universal

Debian es un sistema operativo y una distribución de Software Libre. Se mantiene y actualiza gracias al trabajo de muchos usuarios que contribuyen con su ...

Download Debian

Download via HTTP/FTP - CD/USB ISO images - CD vendors page

Downloading Debian

Debian Installer ISOs are hybrid images, which means they can ...

Descarga de Debian

Descarga de Debian. Esta página contiene opciones para la ...

Download via HTTP/FTP

To Install Debian on a machine without an Internet connection, it ...

Intro/index

Packages - Reasons to use Debian - Mailing Lists - People

Más resultados de debian.org

Debian GNU/Linux

Software

Debian 13

Debian GNU/Linux, o simplemente Debian, es una distribución Linux de software libre, desarrollada por miles de voluntarios de todo el mundo, que colaboran a través de Internet.

Fuente: Wikipedia

Fecha De Lanzamiento: 16 de agosto de 1993

Le damos clic en Download Debian.

Descarga de Debian

Nota: La página original es más nueva que esta traducción.

Descarga de Debian

Esta página contiene opciones para la descarga e instalación de Debian 13.2.0, la versión estable.

- Réplicas de descarga de imágenes de instalación.
- Manual de instalación con instrucciones de instalación detalladas.
- Notas de publicación.
- Imágenes ISO de Debian «en pruebas» («testing»).
- Verificar la autenticidad de las imágenes de Debian.

Descargar una imagen de instalación

- Una [Imagen de instalación pequeña](#): se puede descargar rápidamente y debe guardarse en un disco extraíble. Para utilizar esta opción debe tener una máquina con conexión a Internet.
- Una [Imagen de instalación completa](#): contiene más paquetes, haciendo más fácil la instalación en máquinas sin conexión a Internet.

Pruebe Debian live antes de instalar

Puede probar Debian arrancando un sistema «en vivo» desde un CD, DVD o USB sin instalar ningún archivo en la computadora. Cuando esté listo puede ejecutar el [instalador Calamares](#) incluido. Disponible solamente para PC de 64 bits. Lea más [información sobre este método](#).

Live con GNOME, Live con Xfce, Live con KDE, Otras imágenes ISO live, torrents de live

Adquirir un juego de CD o DVD de uno de los vendedores de CD de

Use una imagen de Debian para la nube

Por una universidad con calidad, moderna e incluyente

Carrera 6^a. No. 76-103 Montería NIT. 891080031-3 - Teléfono: 7860300 - 7860920 www.unicordoba.edu.co



"VIGILADA MINEDUCACIÓN"

UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías



Luego le damos clic en la iso de 64 bits

Descarga de Debian

Historial de descargas recientes

Historial de descargas completo

debian-13.2.0-amd64-DVD-1 (1).iso
1 0/0/3.7 GB • Faltan 12 minutos.

Aquí esperamos que termine de descargar la iso para pasar a configurar la maquina virtual



Por una universidad con calidad, moderna e incluyente

Carrera 6^a. No. 76-103 Montería NIT. 891080031-3 - Teléfono: 7860300 - 7860920 www.unicordoba.edu.co



UNIVERSIDAD DE CÓRDOBA

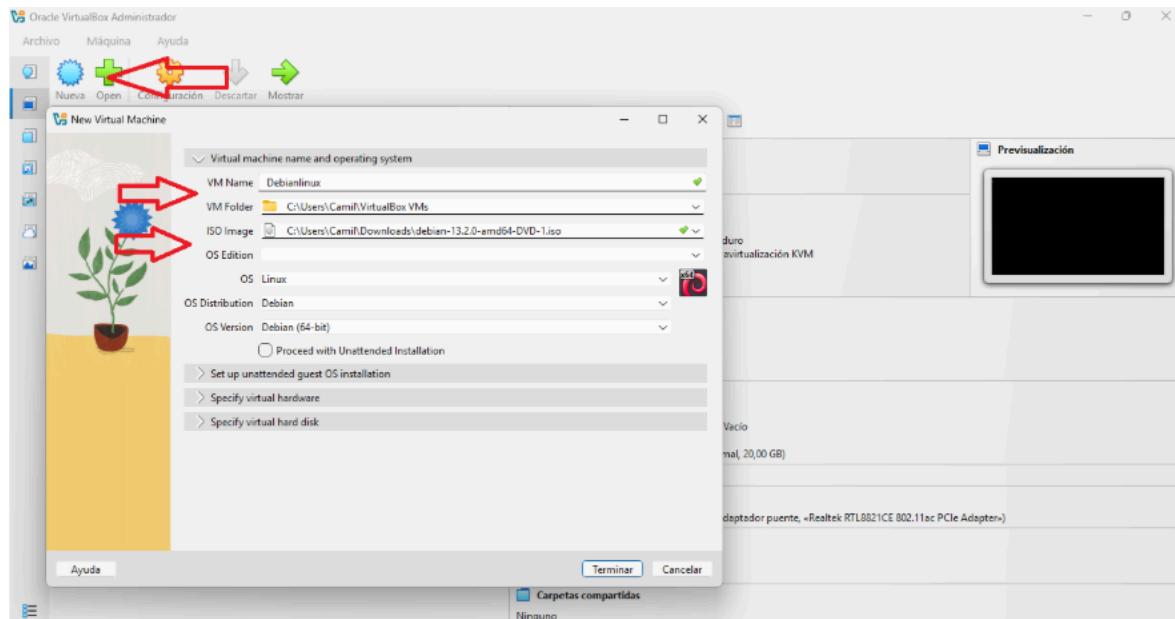
CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías

"VIGILADA MINEDUCACIÓN"



Abrimos el VirtualBox para empezar a crear la maquina



Comenzamos a crear la maquina virtual y le damos clic en donde dice nueva, le ponemos el nombre a la maquina virtual, luego se selecciona la iso que se descargo y le damos clic en terminar



"VIGILADA MINEDUCACIÓN"

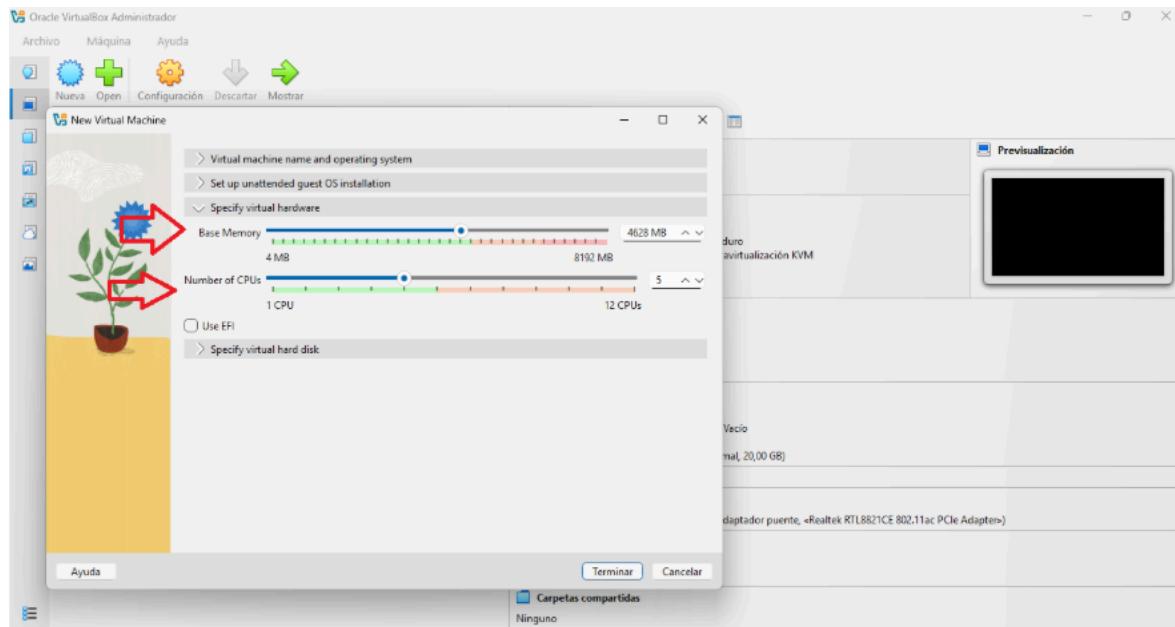
UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías



Res. M.E.N 2956 de 22 de marzo de 2018, vigencia: 4 años



Pasamos a configurar la cantidad de memoria ram y los numeros de CPUs

Por una universidad con calidad, moderna e incluyente

Carrera 6^a. No. 76-103 Montería NIT. 891080031-3 - Teléfono: 7860300 - 7860920 www.unicordoba.edu.co



UNIVERSIDAD DE CÓRDOBA

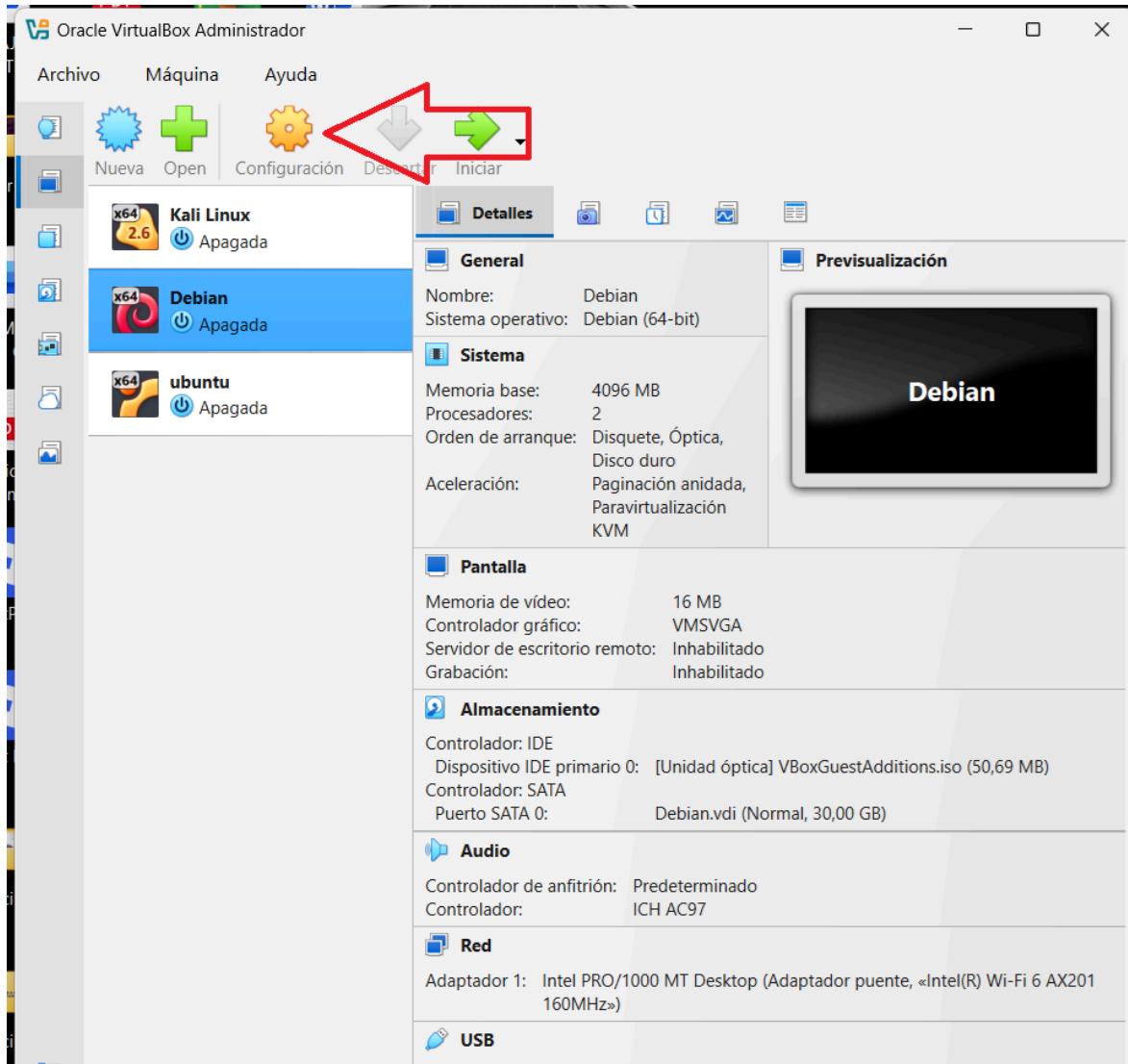
CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías



"VIGILADA MINEDUCACIÓN"

4.3 Configuración de red en VirtualBox



Aquí se selecciona la máquina que se creó y le damos clic en configuraciones

Por una universidad con calidad, moderna e incluyente

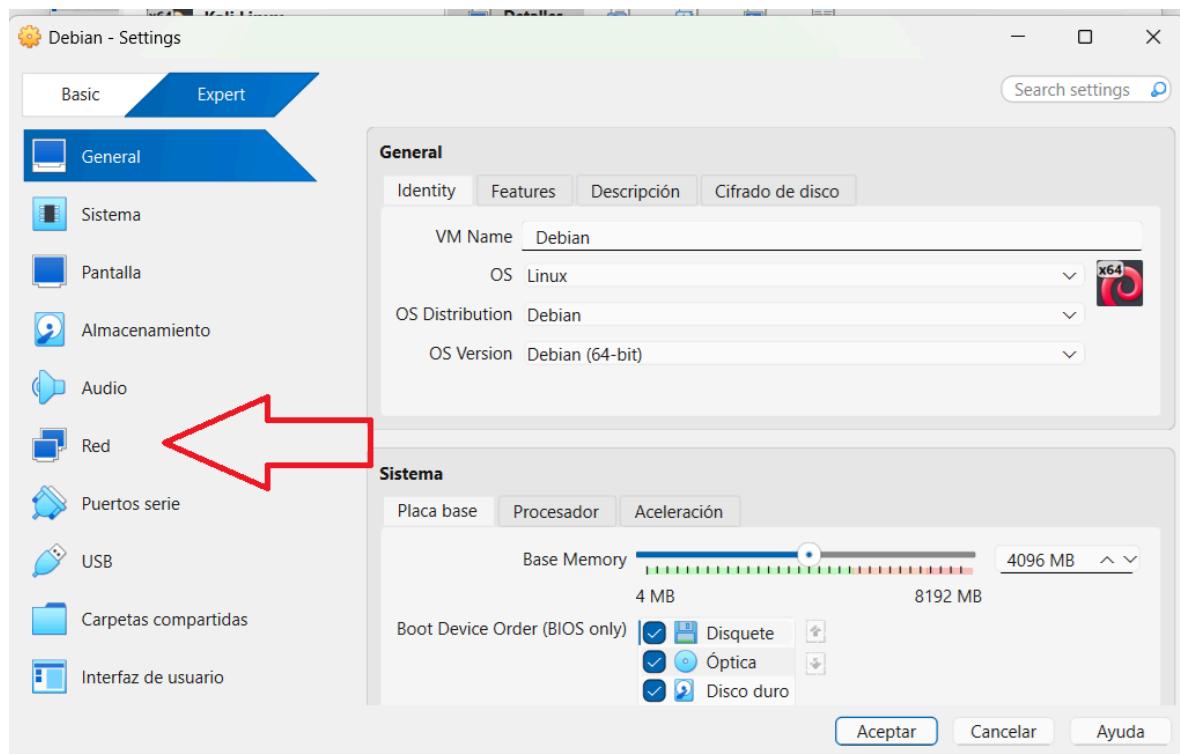
Carrera 6^a. No. 76-103 Montería NIT. 891080031-3 - Teléfono: 7860300 - 7860920 www.unicordoba.edu.co



UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías



Se nos abre este apartado y le damos clic en donde dice red

Por una universidad con calidad, moderna e incluyente

Carrera 6^a. No. 76-103 Montería NIT. 891080031-3 - Teléfono: 7860300 - 7860920 www.unicordoba.edu.co

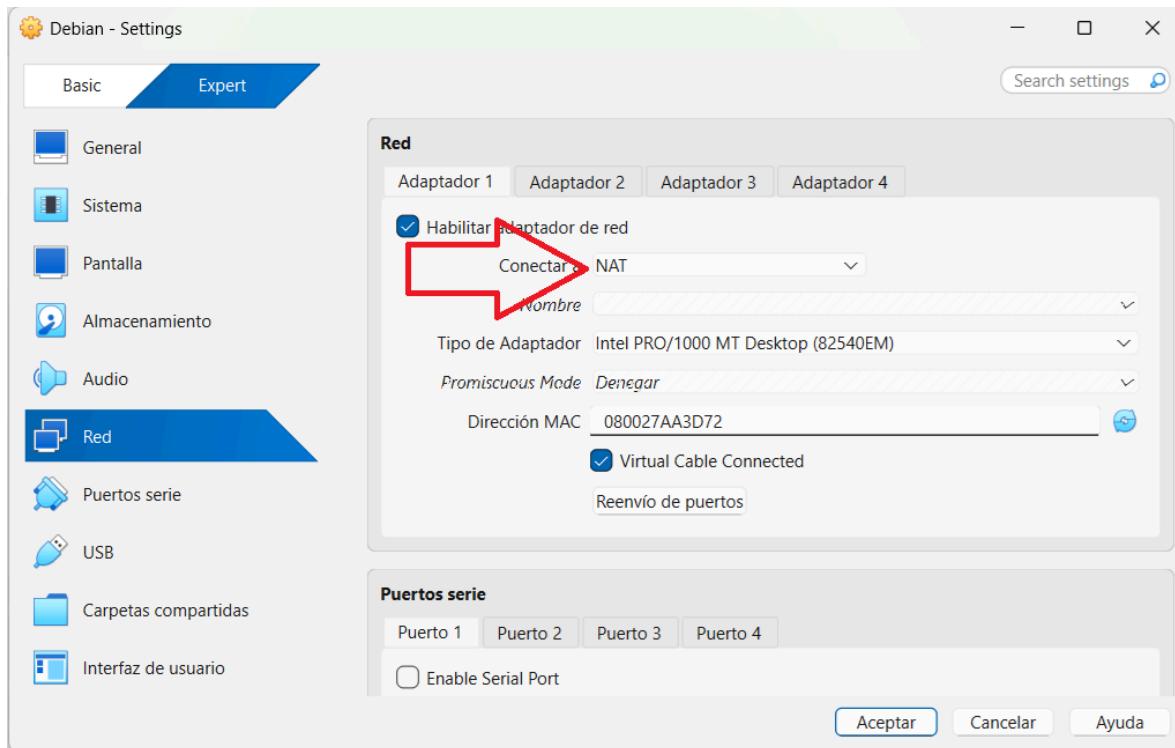


UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías

"VIGILADA MINEDUCACIÓN"



Se abre el siguiente apartado y en la parte de tipo de adaptador le damos clic

Por una universidad con calidad, moderna e incluyente

Carrera 6^a. No. 76-103 Montería NIT. 891080031-3 - Teléfono: 7860300 - 7860920 www.unicordoba.edu.co

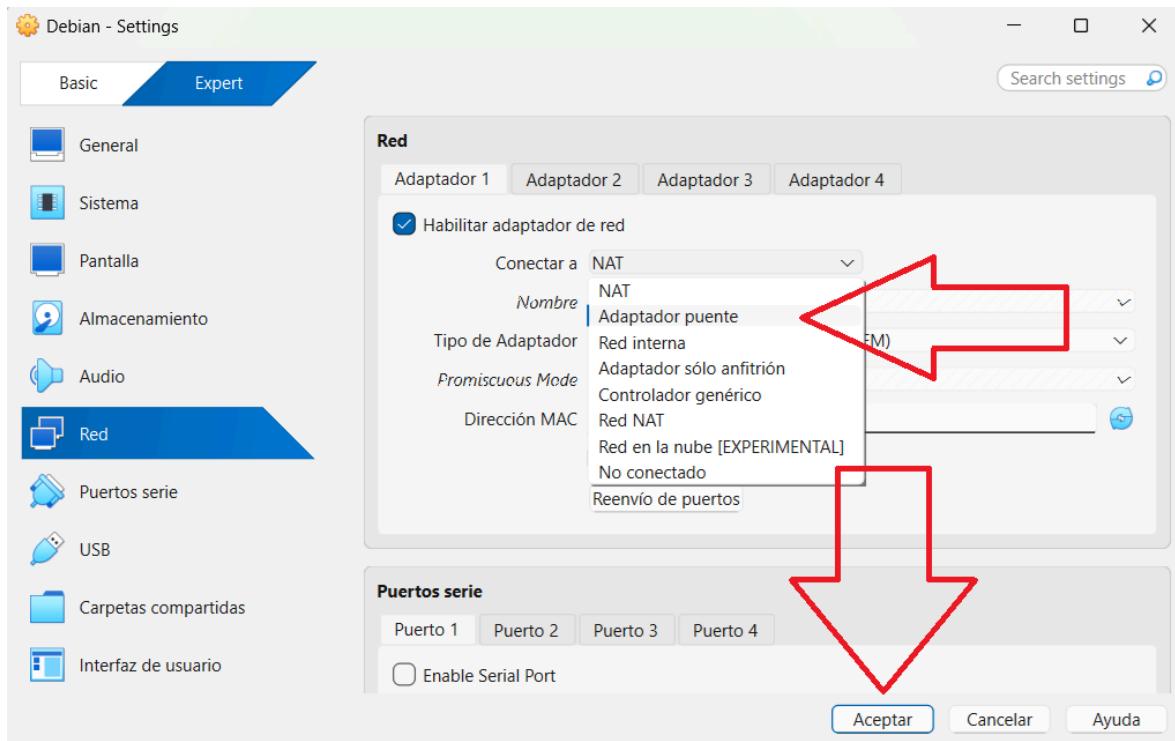


"VIGILADA MINEDUCACIÓN"

UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías



Se nos despliega un menu con todas las acciones y le damos clic en adaptador puente, y damos clic en aceptar

Por una universidad con calidad, moderna e incluyente

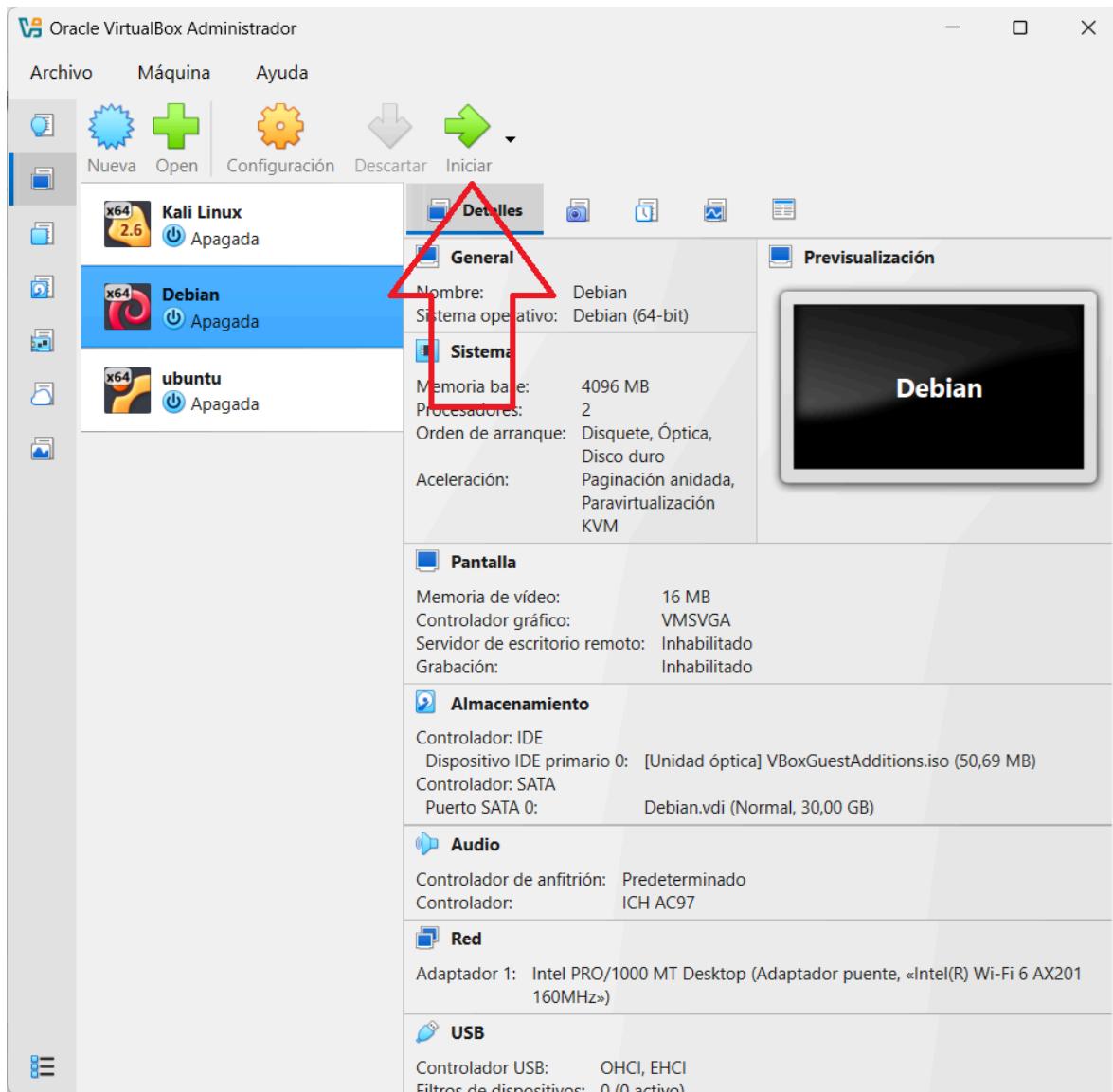
Carrera 6^a. No. 76-103 Montería NIT. 891080031-3 - Teléfono: 7860300 - 7860920 www.unicordoba.edu.co



UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías



Luego inicializamos la maquina virtual ya creada y configurada

Por una universidad con calidad, moderna e incluyente

Carrera 6^a. No. 76-103 Montería NIT. 891080031-3 - Teléfono: 7860300 - 7860920 www.unicordoba.edu.co



UNIVERSIDAD DE CÓRDOBA

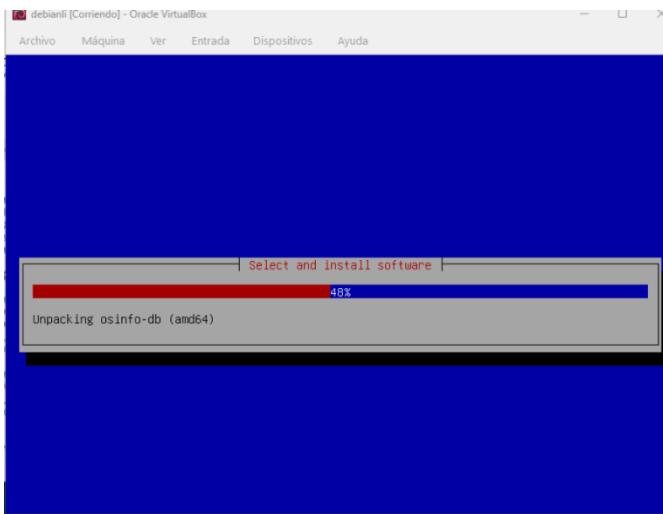
CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías

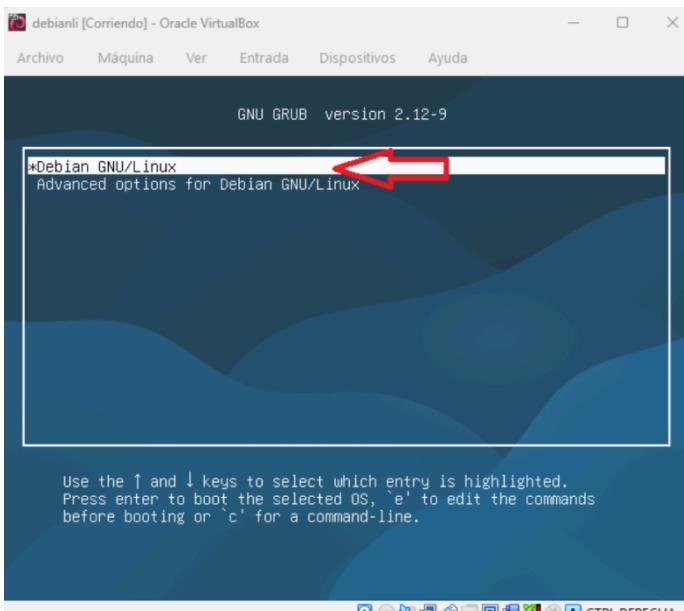
"VIGILADA MINEDUCACIÓN"



4.4 Instalación de Debian



Esperamos que cargue esto puede demorar de 3 a 4 minutos dependiendo de la velocidad de internet



Le damos clic Debian GNU/Linux

Por una universidad con calidad, moderna e incluyente

Carrera 6^a. No. 76-103 Montería NIT. 891080031-3 - Teléfono: 7860300 - 7860920 www.unicordoba.edu.co

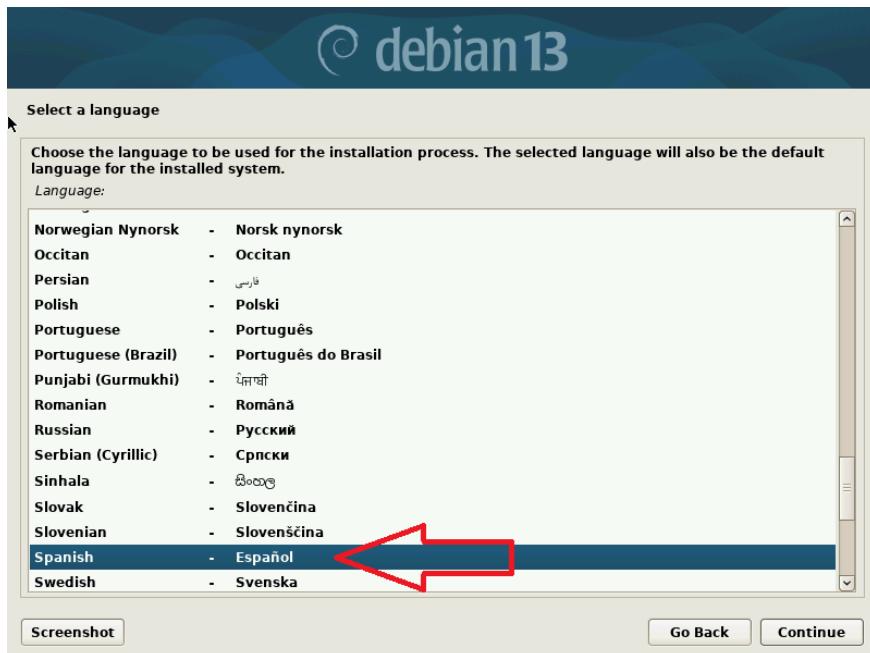


"VIGILADA MINEDUCACIÓN"

UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías



Comenzamos a configurar Debian, buscamos nuestro idioma lo seleccionamos y le damos clic en continuar



Por una universidad con calidad, moderna e incluyente

Carrera 6^a. No. 76-103 Montería NIT. 891080031-3 - Teléfono: 7860300 - 7860920 www.unicordoba.edu.co



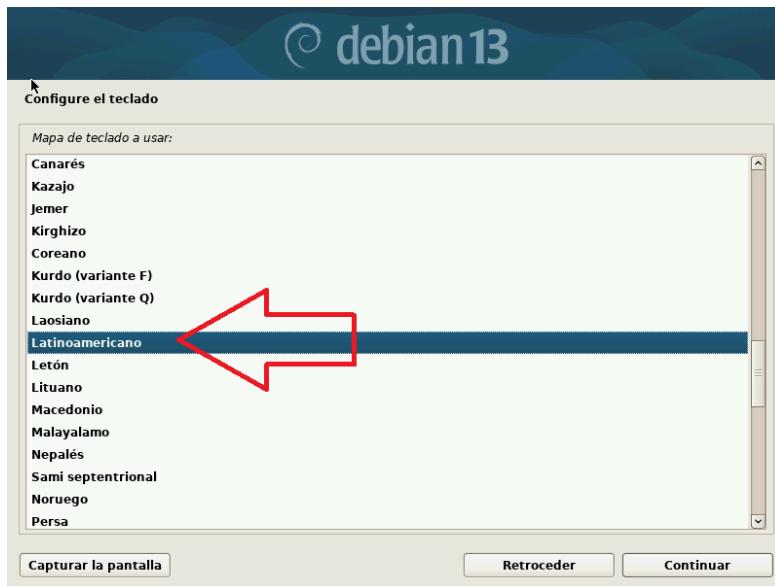
UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías



Aca seleccionamos nuestra ubicación en nuestro caso, Colombia y le damos en continuar



Aca configuarmos nuestro teclado y escogemos latinoamericano y damos clic en continuar



Aca pasamos a poner el nombre a la maquina en nuestro caso le pusimos debian, y le damos clic en continuar

Por una universidad con calidad, moderna e incluyente

Carrera 6^a. No. 76-103 Montería NIT. 891080031-3 - Teléfono: 7860300 - 7860920 www.unicordoba.edu.co



UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías



Configurar la red

El nombre de dominio es la parte de su dirección de Internet a la derecha del nombre de sistema. Habitualmente es algo que termina por .com, .net, .edu, o .org. Puede inventárselo si está instalando una red doméstica, pero asegúrese de utilizar el mismo nombre de dominio en todos sus ordenadores.

Nombre de dominio:

Aca pasamos a poner el nombre de dominio ya que nosotros no tenemos se deja en blanco y le damos clic en continuar

Configurar usuarios y contraseñas

Es necesario disponer de alguna cuenta con privilegios de superusuario administrativo. La contraseña de esa cuenta debe ser algo que no se pueda adivinar.

Para permitir el acceso directo mediante contraseña a través de la cuenta "root", puede establecer aquí la contraseña de dicha cuenta.

Alternativamente, puede bloquear la contraseña de la cuenta root dejando esta opción vacía, y en su lugar utilizar la cuenta de usuario inicial del sistema (que se configurará en el siguiente paso) para obtener privilegios administrativos. Esto se hará añadiendo el usuario inicial al grupo 'sudo'.

Nota: lo que escriba aquí quedará oculto (a menos que seleccione mostrarlo).

Clave del superusuario:

Mostrar la contraseña en claro

Por favor, introduzca de nuevo la misma contraseña de superusuario para verificar que la introdujo correctamente.

Vuelva a introducir la contraseña para su verificación:

Mostrar la contraseña en claro

En este apartado pasamos a crear una contraseña le damos clic en continuar

Por una universidad con calidad, moderna e incluyente

Carrera 6^a. No. 76-103 Montería NIT. 891080031-3 - Teléfono: 7860300 - 7860920 www.unicordoba.edu.co



UNIVERSIDAD DE CÓRDOBA

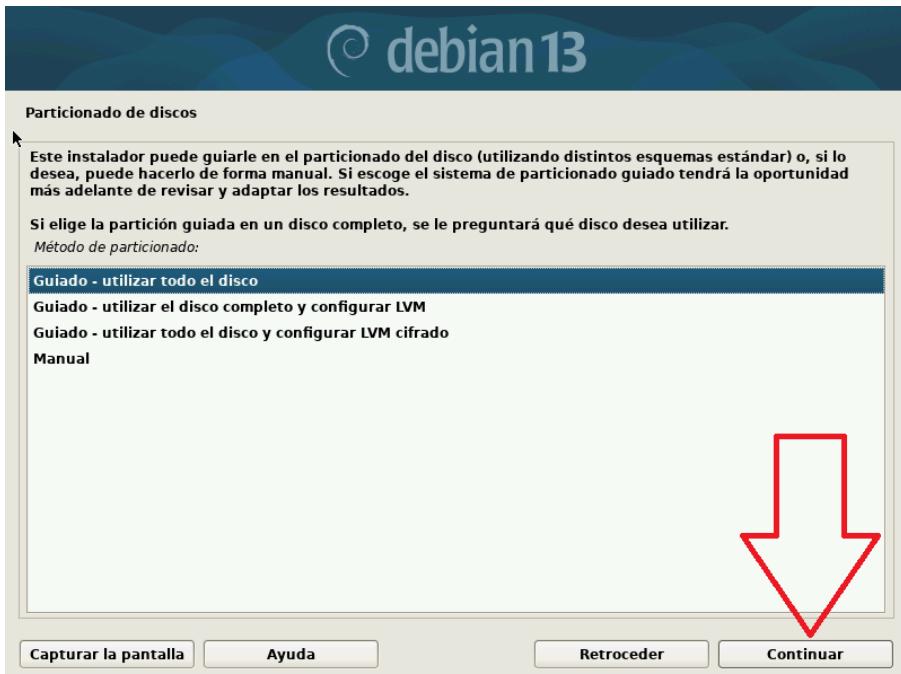
CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías

"VIGILADA MINEDUCACIÓN"



En este apartado pasamos a configurar los datos del usuario le ponemos nuestro nombre y le damos clic en continuar



Aquí seleccionamos Guiado – utilizar todo los disco, y le damos clic en continuar

Por una universidad con calidad, moderna e incluyente

Carrera 6^a. No. 76-103 Montería NIT. 891080031-3 - Teléfono: 7860300 - 7860920 www.unicordoba.edu.co



UNIVERSIDAD DE CÓRDOBA

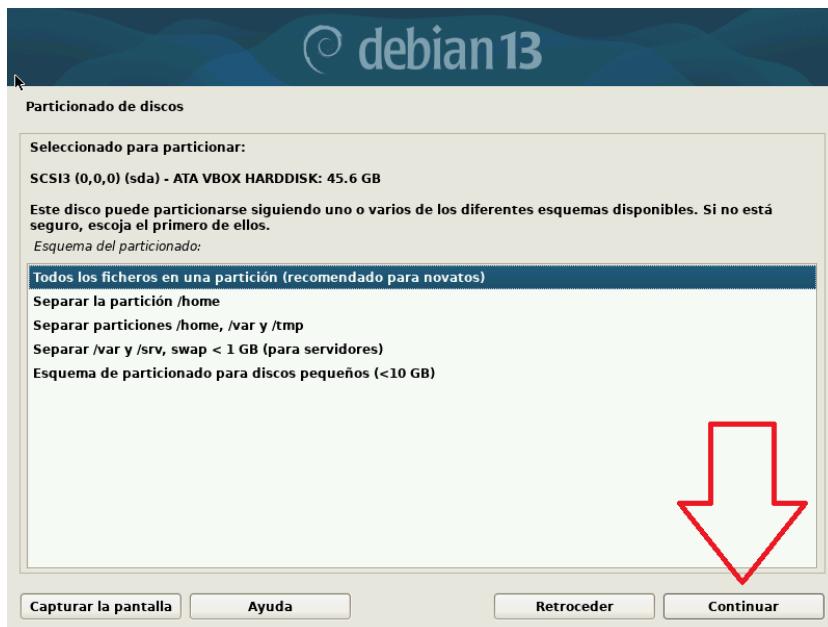
CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías

"VIGILADA MINEDUCACIÓN"



Aca dejamos el que sale seleccionado y le damos clic en continuar



Por una universidad con calidad, moderna e incluyente

Carrera 6^a. No. 76-103 Montería NIT. 891080031-3 - Teléfono: 7860300 - 7860920 www.unicordoba.edu.co



UNIVERSIDAD DE CÓRDOBA

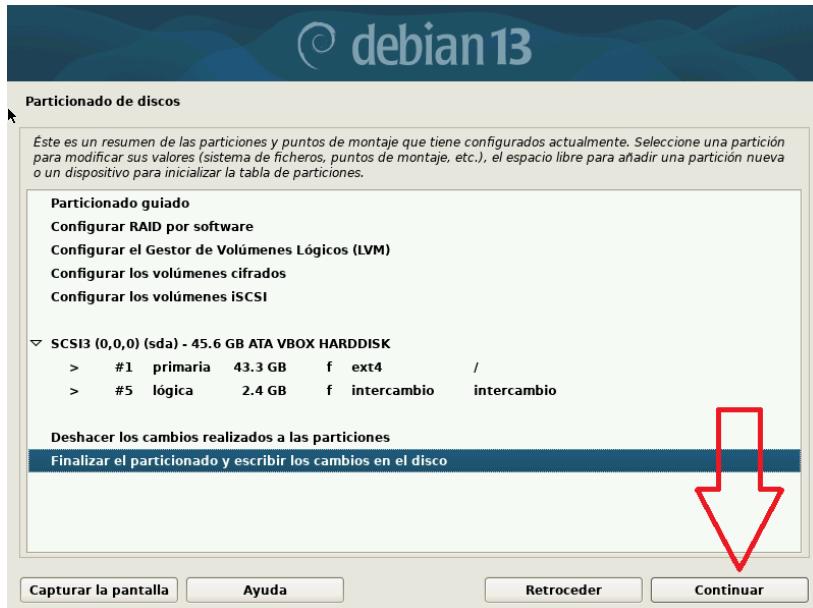
CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías

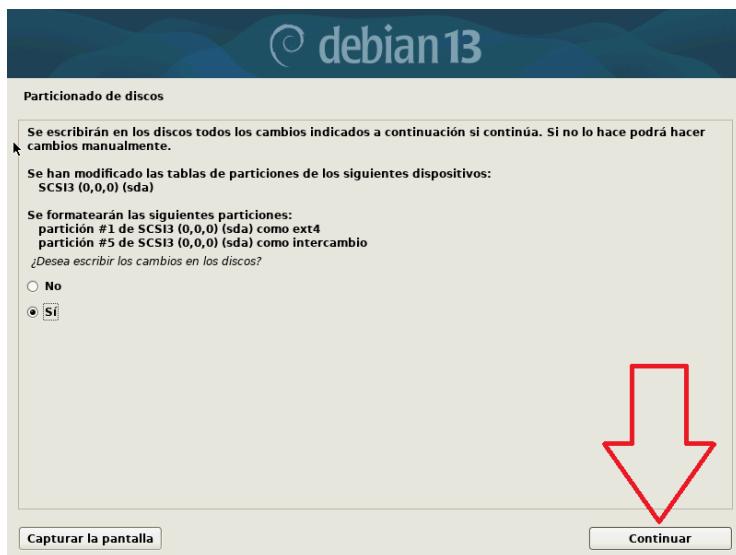
"VIGILADA MINEDUCACIÓN"



Pasamos a configurar las particiones de nuestros discos, seleccionamos el que dice todos los ficheros en una partición y le damos clic



Aca nos puede mostrar como queda configurado revisamos y le damos clic en continuar



Por una universidad con calidad, moderna e incluyente

Carrera 6^a. No. 76-103 Montería NIT. 891080031-3 - Teléfono: 7860300 - 7860920 www.unicordoba.edu.co



UNIVERSIDAD DE CÓRDOBA

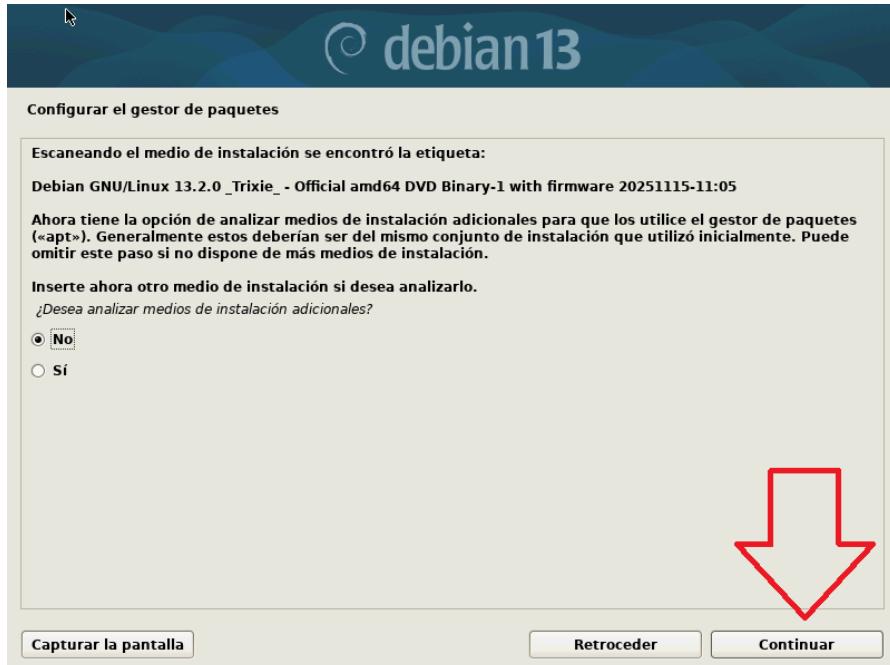
CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías

"VIGILADA MINEDUCACIÓN"



Le damos “Sí” y le damos continuar



Le damos en “No” y le damos clic en continuar

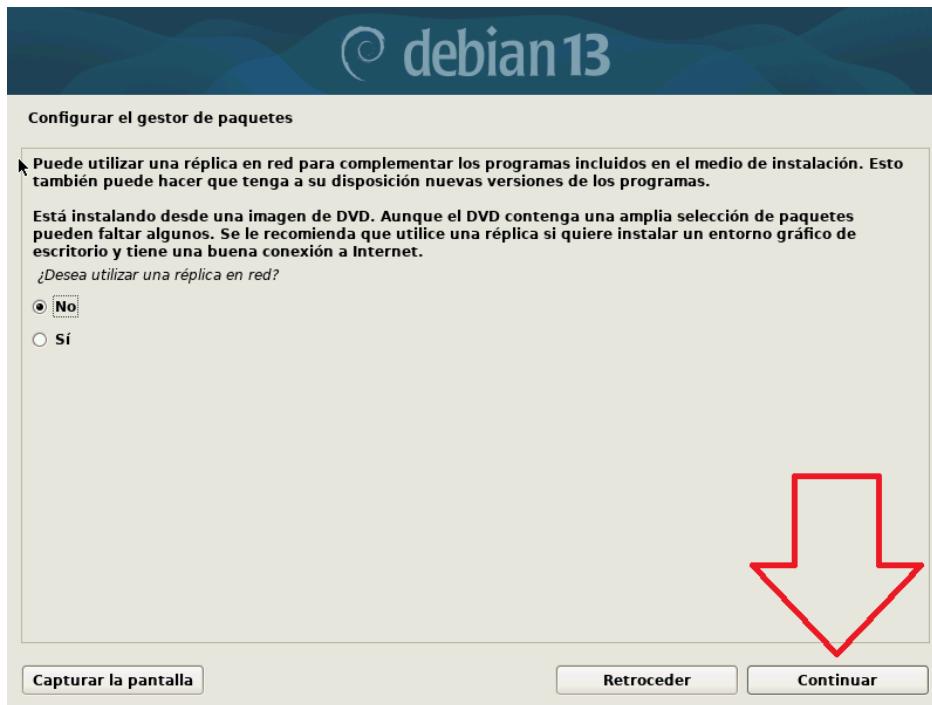


"VIGILADA MINEDUCACIÓN"

UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías



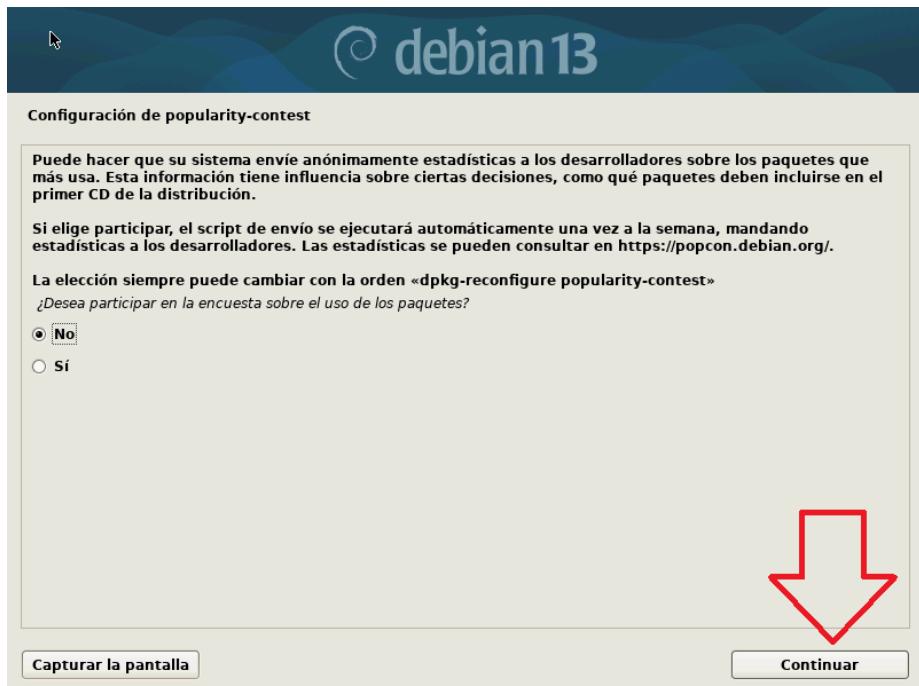
Le damos en “No” y le damos clic a continuar



UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías



Le damos en “No” y le damos clic a continuar



Por una universidad con calidad, moderna e incluyente

Carrera 6^a. No. 76-103 Montería NIT. 891080031-3 - Teléfono: 7860300 - 7860920 www.unicordoba.edu.co



UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías

"VIGILADA MINEDUCACIÓN"



Le damos en "Si" y le damos en continuar



Aca seleccionamos nuestro disco y le damos clic en continuar

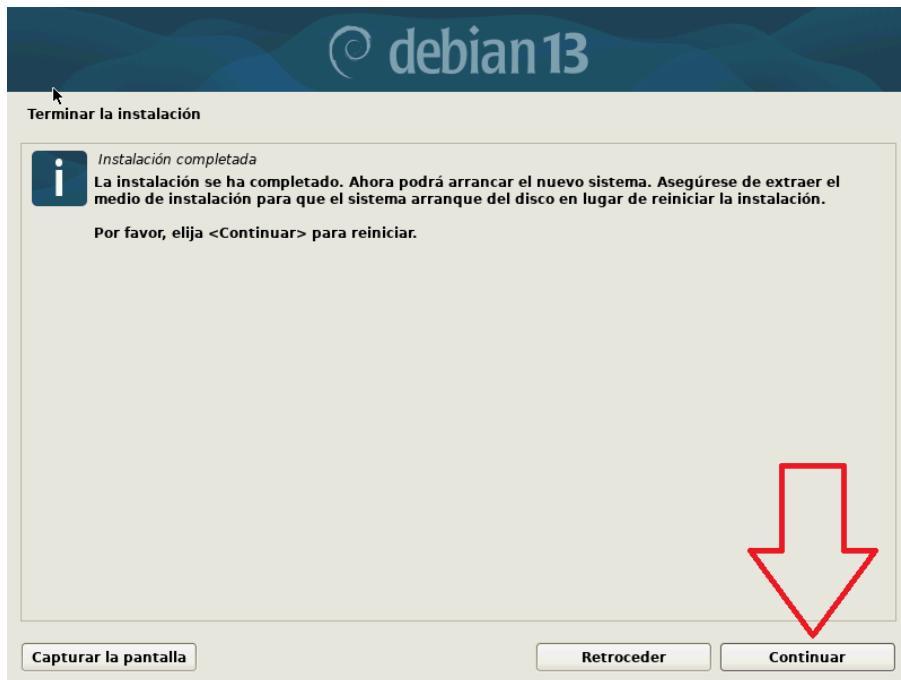


"VIGILADA MINEDUCACIÓN"

UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías



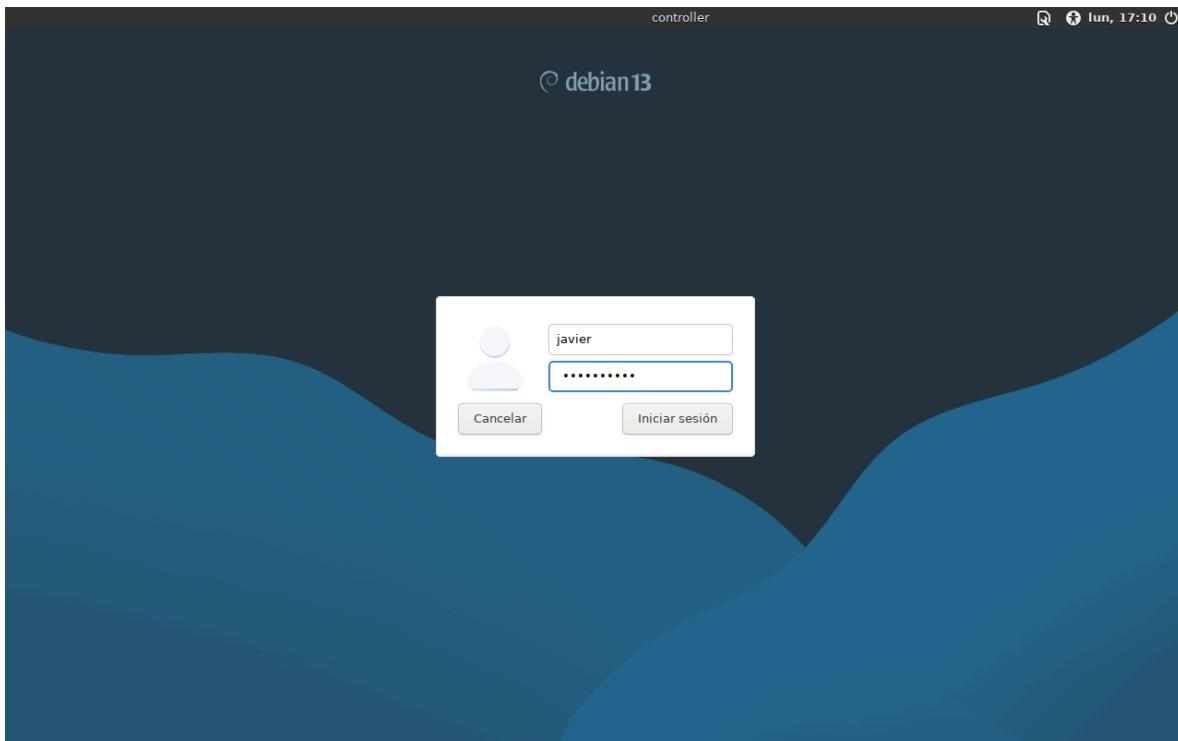
Aca le damos clic en continuar para que se reinicie la maquina



UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías



Aca iniciamos sesión con nuestro usuario y contraseña creadas y entramos a Debian

Por una universidad con calidad, moderna e incluyente

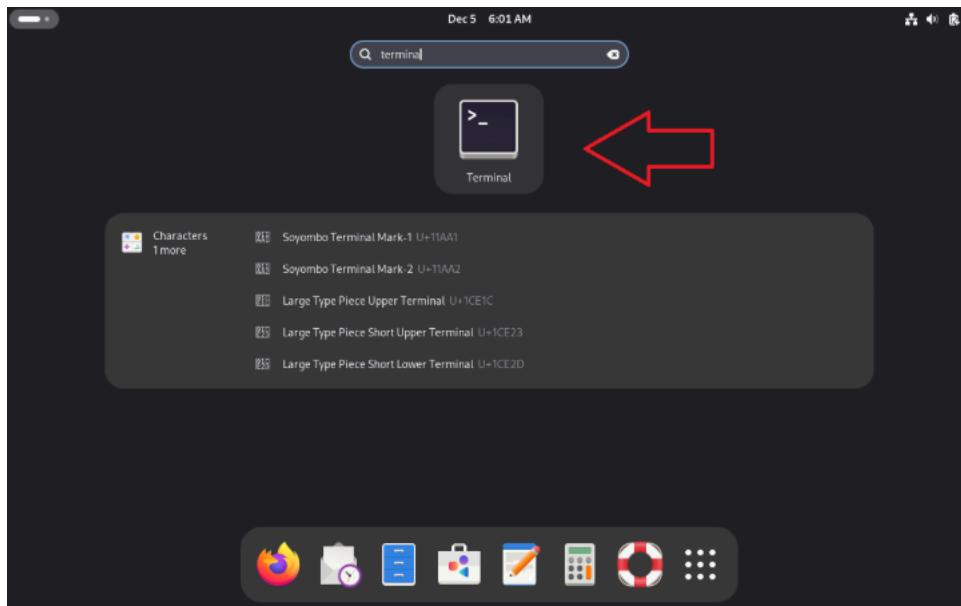
Carrera 6^a. No. 76-103 Montería NIT. 891080031-3 - Teléfono: 7860300 - 7860920 www.unicordoba.edu.co



UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías



Ya estando dentro de debian abrimos la terminal ppara asi pasar a descargar OpenStack

5. COMANDOS UTILIZADOS EN DEBIAN Y OPENSTACK.

```
root@ubuntu:/home/dopa# sudo useradd -s /bin/bash -d /opt/stack -m stack
```

Crea un usuario llamado 'stack', asignándole la shell Bash, un directorio principal ubicado en /opt/stack, y la creación automática del directorio si no existe. Este usuario es obligatorio para la ejecución correcta de DevStack, ya que no debe ejecutarse como root.



"VIGILADA MINEDUCACIÓN"

UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías



```
root@ubuntu:/home/dopa# sudo chmod +x /opt/stack
```

Otorga permisos de ejecución al directorio /opt/stack, permitiendo que el usuario pueda utilizarlo para almacenar y ejecutar los archivos generados por DevStack.

```
root@ubuntu:/home/dopa# echo "stack ALL=(ALL) NOPASSWD: ALL" | sudo tee /etc/sudoers.d/stack
stack ALL=(ALL) NOPASSWD: ALL
```

Configura permisos sudo para el usuario 'stack' sin necesidad de ingresar contraseña. DevStack requiere este privilegio para ejecutar comandos administrativos durante la instalación.

```
root@ubuntu:/home/dopa# sudo -u stack -i
```

Inicia una sesión interactiva como el usuario 'stack'. Todos los pasos posteriores deben realizarse desde este usuario para que DevStack funcione correctamente.

```
stack@ubuntu:~$ git clone https://opendev.org/openstack/devstack
```

Clona el repositorio oficial de DevStack desde OpenDev. Esto descarga el instalador de OpenStack y todos los scripts necesarios para su despliegue.

```
stack@ubuntu:~$ cd devstack
```

Ingresa al directorio del proyecto DevStack, donde se encuentran los scripts de instalación, configuración y ejecución.

```
stack@ubuntu:~/devstack$ nano local.conf
```

Abre el editor de texto Nano para crear o editar el archivo local.conf. Este archivo contiene las credenciales y parámetros de configuración específicos para la instalación de OpenStack.

```
stack@glorious-hare:~/devstack
GNU nano 7.2
[[local|localrc]]
ADMIN_PASSWORD=secret
DATABASE_PASSWORD=password
RABBIT_PASSWORD=password
SERVICE_PASSWORD=password
```

Define las contraseñas del entorno OpenStack: la contraseña del administrador, la contraseña de la base de datos, la credencial para el servicio de mensajería RabbitMQ y la contraseña general para los servicios. DevStack utiliza este archivo para generar la configuración del controlador y de los servicios de OpenStack.

Por una universidad con calidad, moderna e incluyente

Carrera 6^a. No. 76-103 Montería NIT. 891080031-3 - Teléfono: 7860300 - 7860920 www.unicordoba.edu.co



"VIGILADA MINEDUCACIÓN"

UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías



```
stack@ubuntu:~/devstack$ ./stack.sh
```

Ejecuta el script principal de instalación de DevStack. Este comando instala y configura automáticamente todos los servicios de OpenStack, incluyendo Keystone, Nova, Neutron, Glance, Horizon y otros componentes necesarios para desplegar el entorno en la nube.

```
glance      | UPDATE      |    2 |
nova_api   | INSERT      |   20 |
nova_api   | SAVEPOINT   |    10 |
nova_api   | RELEASE     |    10 |
cinder      | DELETE      |     1 |
-----+-----+-----+
```

```
This is your host IP address: 10.242.62.176
This is your host IPv6 address: fd42:36c3:366b:67f5:216:3eff:fec3:5c4e
Horizon is now available at http://10.242.62.176/dashboard
Keystone is serving at http://10.242.62.176/identity/
The default users are: admin and demo
The password: secret

Services are running under systemd unit files.
For more information see:
https://docs.openstack.org/devstack/latest/systemd.html
```

Esperamos a que descargue todo, ya cuando termína nos aparece lo siguiente y cogemos la url que nos da y la pegamos en el navegador y nos lleva al login de OpenStack



UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías

"VIGILADA MINEDUCACIÓN"



Aca iniciamos session en OpenStack

Nombramos la Red del Firewall

Por una universidad con calidad, moderna e incluyente

Carrera 6^a. No. 76-103 Montería NIT. 891080031-3 - Teléfono: 7860300 - 7860920 www.unicordoba.edu.co



"VIGILADA MINEDUCACIÓN"

UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías



Nosotros definimos el nombre de la red como Firewall-net.

También marcamos "Create Subnet" para que OpenStack nos deje configurar las IPs que vamos a usar en esta red privada.

Le damos a "Next".

Create Network

Network Subnet Subnet Details

Subnet Name: firewall-subnet

Network Address Source: Enter Network Address manually

Network Address: 192.168.100.0/24

IP Version: IPv4

Gateway IP: 192.168.100.1

Disable Gateway

Creates a subnet associated with the network. You need to enter a valid "Network Address" and "Gateway IP". If you did not enter the "Gateway IP", the first value of a network will be assigned by default. If you do not want gateway please check the "Disable Gateway" checkbox. Advanced configuration is available by clicking on the "Subnet Details" tab.

Cancel Back Next

Ps y Gateway de la Red

Nosotros nombramos la subred como firewall-subnet.



"VIGILADA MINEDUCACIÓN"

UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías



Definimos:

Rango de IPs: 192.168.100.0/24

Gateway: 192.168.100.1 (para la salida de las VMs).

Le damos a "Next".

Create Network

Network Subnet **Subnet Details**

Enable DHCP Specify additional attributes for the subnet.

Allocation Pools ?
192.168.100.10, 192.168.100.250

DNS Name Servers ?
8.8.8.8
1.1.1.1

Host Routes ?

Create

DHCP y DNS

Nosotros activamos el DHCP para que asigne las IPs automáticamente (desde la .10 hasta la .250).

Por una universidad con calidad, moderna e incluyente

Carrera 6^a. No. 76-103 Montería NIT. 891080031-3 - Teléfono: 7860300 - 7860920 www.unicordoba.edu.co



UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías

"VIGILADA MINEDUCACIÓN"



También añadimos los DNS públicos 8.8.8.8 y 1.1.1.1 para que haya Internet.

Le damos a "Create" (Crear).

Create Router

Router Name
firewall-router

Enable Admin State ⓘ

External Network
public

Enable SNAT

Availability Zone Hints ⓘ

Description:
Creates a router with specified parameters.
Enable SNAT will only have an effect if an external network is set.

Cancel **Create Router**

Creamos el Router (Conexión a Internet)

Nosotros creamos el Router para conectar nuestra red privada al mundo exterior:

Lo nombramos firewall-router.

Seleccionamos la "External Network" (Red Externa) como public. Esto es lo que le da acceso a Internet.



"VIGILADA MINEDUCACIÓN"

UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías



Activamos "Enable SNAT" para que todas las IPs de nuestra red interna puedan usar la IP pública del router para navegar.

Le damos a "Create Router".

Name	Status	External Network	Admin State	Availability Zones	Actions
firewall-router	Active	public	UP	-	Clear Gateway

http://192.168.20.172/dashboard/project/security_groups/

Por una universidad con calidad, moderna e incluyente

Carrera 6^a. No. 76-103 Montería NIT. 891080031-3 - Teléfono: 7860300 - 7860920 www.unicordoba.edu.co



"VIGILADA MINEDUCACIÓN"

UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías



Aquí podemos observar el router ya creado

Create Security Group

Name *

Description

Security group para proyecto firewall

Description:

Security groups are sets of IP filter rules that are applied to network interfaces of a VM. After the security group is created, you can add rules to the security group.

Cancel Create Security Group

Creamos el Grupo de Seguridad (SG)

Este paso es clave, porque aquí creamos el Grupo de Seguridad donde nosotros vamos a definir las reglas de nuestro Firewall (qué tráfico dejamos pasar).

Le pusimos el nombre `firewall-sg`.

Le damos a "Create Security Group".

Rule	Direction	Ether Type	IP Protocol	Port Range	Remote IP Prefix	Descripción
SSH	Ingress	IPv4	TCP	22	0.0.0.0/0	Acceso SSH
ICMP	Ingress	IPv4	ICMP	Any	0.0.0.0/0	Ping
HTTP	Ingress	IPv4	TCP	80	0.0.0.0/0	Web HTTP
HTTPS	Ingress	IPv4	TCP	443	0.0.0.0/0	Web HTTPS
Custom	Ingress	IPv4	TCP	8080	0.0.0.0/0	Puerto custom
All traffic	Ingress	IPv4	Any	Any	192.168.100.0/24	Tráfico interno
DNS	Egress	IPv4	UDP	53	0.0.0.0/0	DNS queries
All Egress	Egress	IPv4	Any	Any	0.0.0.0/0	Todo saliente

Por una universidad con calidad, moderna e incluyente

Carrera 6^a. No. 76-103 Montería NIT. 891080031-3 - Teléfono: 7860300 - 7860920 www.unicordoba.edu.co



"VIGILADA MINEDUCACIÓN"

UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías



Añadimos las Reglas de Entrada/Salida (Las Reglas del Firewall)

Aquí nosotros estamos definiendo qué tráfico permitimos en nuestro firewall-sg (Grupo de Seguridad). Esto convierte al SG en nuestro Firewall virtual:

Ingress (Entrada): Permitimos tráfico desde Internet (0.0.0.0/0) para: SSH (puerto 22), Web HTTP (80), HTTPS (443), Ping (ICMP) y un puerto custom (8080).

Tráfico Interno: Permitimos todo el tráfico (All traffic) que venga de nuestra propia red interna (192.168.100.0/24).

Egress (Salida): Permitimos todo el tráfico saliente (All Egress) y también consultas DNS (53) a cualquier parte (0.0.0.0/0).

Con esto, nuestra VM/Firewall ya tiene red, router y reglas de seguridad listas.

Direction	Ether Type	IP Protocol	Port Range	Remote IP Prefix	Remote Security Group	Description	Actions
Ingress	IPv4	ICMP	Any	0.0.0.0/0	-	ping	<button>Delete Rule</button>
Ingress	IPv4	TCP	22 (SSH)	0.0.0.0/0	-		<button>Delete Rule</button>
Ingress	IPv4	TCP	53 (DNS)	0.0.0.0/0	-		<button>Delete Rule</button>
Ingress	IPv4	TCP	80 (HTTP)	0.0.0.0/0	-		<button>Delete Rule</button>
Ingress	IPv4	TCP	443 (HTTPS)	0.0.0.0/0	-		<button>Delete Rule</button>
Ingress	IPv4	TCP	8080	0.0.0.0/0	-	puerto custom	<button>Delete Rule</button>

Por una universidad con calidad, moderna e incluyente

Carrera 6^a. No. 76-103 Montería NIT. 891080031-3 - Teléfono: 7860300 - 7860920 www.unicordoba.edu.co



UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías



Aquí podemos observar ya las reglas de nuestro grupo de seguridad implementadas

Launch Instance

Details

Source

Flavor *

Networks *

Network Ports

Security Groups

Key Pair

Configuration

Server Groups

Scheduler Hints

Metadata

Allocated

Displaying 1 item

Name	Updated	Size	Format	Visibility
Debian-12	12/5/25 9:57 AM	330.56 MB	QCOW2	Public

Available 1

Select one

Click here for filters or full text search

Displaying 1 item

Fuente de la Instancia (Imagen)

Aquí nosotros estamos definiendo los detalles de la máquina virtual que vamos a encender:

Pestaña Source (Fuente): Elegimos la imagen del sistema operativo que usaremos para nuestro Firewall.

Seleccionamos la imagen Debian-12 (que pesa 330.56 MB), ya que es una base estable para un servidor.

Definimos el tamaño del disco (Volume Size) en 15 GB.

Por una universidad con calidad, moderna e incluyente

Carrera 6^a. No. 76-103 Montería NIT. 891080031-3 - Teléfono: 7860300 - 7860920 www.unicordoba.edu.co



"VIGILADA MINEDUCACIÓN"

UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías



Launch Instance

Details

Source

Flavor

Networks *

Name	vCPUs	RAM	Total Disk	Root Disk	Ephemeral Disk	Public
ds512M	1	512 MB	5 GB	5 GB	0 GB	Yes

Network Ports

Displaying 1 item

Security Groups

Available (1)

Select one

Key Pair

Configuration

Displaying 11 items

Server Groups

Name	vCPUs	RAM	Total Disk	Root Disk	Ephemeral Disk	Public
m1.nano	1	192 MB	1 GB	1 GB	0 GB	Yes
m1.micro	1	256 MB	1 GB	1 GB	0 GB	Yes
cirros256	1	256 MB	1 GB	1 GB	0 GB	Yes
m1.tiny	1	512 MB	1 GB	1 GB	0 GB	Yes
ds1G	1	1 GB	10 GB	10 GB	0 GB	Yes

Scheduler Hints

Metadata

Por una universidad con calidad, moderna e incluyente

Carrera 6^a. No. 76-103 Montería NIT. 891080031-3 - Teléfono: 7860300 - 7860920 www.unicordoba.edu.co



UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías

"VIGILADA MINEDUCACIÓN"



Escogemos esa opción que es la más optima y estable

Launch Instance

Details Select the security groups to launch the instance in.

Source **Allocated** 1
Displaying 1 item

Flavor

Name	Description
firewall-sg	Security group para proyecto firewall

Networks **Available** 2
Select one or more

Network Ports Displaying 1 item

Security Groups **Available** 2
Select one or more

Key Pair Click here for filters or full text search.

Configuration Displaying 2 items

Server Groups **Available** 2
Select one or more

Scheduler Hints **Available** 1
Select one or more

Metadata **Available** 2
Select one or more

Displaying 2 items

Por una universidad con calidad, moderna e incluyente

Carrera 6^a. No. 76-103 Montería NIT. 891080031-3 - Teléfono: 7860300 - 7860920 www.unicordoba.edu.co



UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías



Aquí escogemos las reglas ya echas (firewall –mg) y las implementamos

Launch Instance

Details

A key pair allows you to SSH into your newly created instance. You may select an existing key pair, import a key pair, or generate a new key pair.

Source [+ Create Key Pair](#) [Import Key Pair](#)

Flavor Allocated

Networks Displaying 1 item

Name	Type
admin	ssh

Network Ports

Security Groups

Key Pair

Configuration

Server Groups

Scheduler Hints

Metadata

Available [Select one](#)

Click here for filters or full text search.

Displaying 0 items

Name Type

No items to display.

Displaying 0 items

[Cancel](#) [Back](#) [Next](#) [Launch Instance](#)

Por una universidad con calidad, moderna e incluyente

Carrera 6^a. No. 76-103 Montería NIT. 891080031-3 - Teléfono: 7860300 - 7860920 www.unicordoba.edu.co



"VIGILADA MINEDUCACIÓN"

UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías



Aqui seleccionamos la que viene por defecto

Launch Instance

Details * You can customize your instance after it has launched using the options available here. "Customization Script" is analogous to "User Data" in other systems.

Source * Load Customization Script from a file No file selected.

Flavor *

Networks *

Network Ports

Security Groups

Key Pair

Configuration Selected

Server Groups

Scheduler Hints

Metadata

Customization Script (Modified) Content size: 669 bytes of 48.00 KB

```
#!/bin/bash
set -x
exec > /var/log/cloud-init-custom.log 2>&1

id -u debian &>/dev/null || useradd -m -s /bin/bash debian
echo 'root:password123' | chpasswd
echo 'debian:password123' | chpasswd
echo 'debian ALL=(ALL) NOPASSWD:ALL' > /etc/sudoers.d/debian

sed -i 's/#PasswordAuthentication.*/PasswordAuthentication yes/' /etc/ssh/sshd_config
sed -i 's/PasswordAuthentication no/PasswordAuthentication yes/' /etc/ssh/sshd_config
sed -i 's/#PermitRootLogin.*/PermitRootLogin yes/' /etc/ssh/sshd_config
systemctl restart ssh

cat > /etc/resolv.conf <<EOF
nameserver 8.8.8.8
nameserver 1.1.1.1
EOF
echo "precedence ::ffff:0:0/96 100" > /etc/gai.conf

apt-get update || true
```

Disk Partition

Automatic

Configuration Drive

Por una universidad con calidad, moderna e incluyente

Carrera 6^a. No. 76-103 Montería NIT. 891080031-3 - Teléfono: 7860300 - 7860920 www.unicordoba.edu.co



UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías



En esa imagen se está creando una máquina virtual en OpenStack y, antes de iniciarla, se le agrega un script de configuración automática (cloud-init). Ese script se encargará de dejar la instancia lista desde el primer arranque: crea usuarios, asigna contraseñas, habilita el acceso SSH por contraseña, modifica archivos del sistema y configura la red. En resumen, la imagen muestra cómo se automatiza la preparación inicial de la máquina justo antes de lanzarla. (Firewall-client)

Launch Instance

Details *

Source *

Flavor *

Networks *

Network Ports

Security Groups

Key Pair

Configuration

Server Groups

Scheduler Hints

Metadata

You can customize your instance after it has launched using the options available here. "Customization Script" is analogous to "User Data" in other systems.

Load Customization Script from a file

Browse... No file selected.

Customization Script (Modified) Content size: 669 bytes of 48.00 KB

```
#!/bin/bash
set -x
exec > /var/log/cloud-init-custom.log 2>&1

id -u debian &>/dev/null || useradd -m -s /bin/bash debian
echo 'root:password123' | chpasswd
echo 'debian:password123' | chpasswd
echo 'debian ALL=(ALL) NOPASSWD:ALL' > /etc/sudoers.d/debian

sed -i 's/#PasswordAuthentication yes/PasswordAuthentication yes/' /etc/ssh/sshd_config
sed -i 's/PasswordAuthentication no/PasswordAuthentication yes/' /etc/ssh/sshd_config
sed -i 's/#PermitRootLogin yes/PermitRootLogin yes/' /etc/ssh/sshd_config
systemctl restart ssh

cat > /etc/resolv.conf <<EOF
nameserver 8.8.8.8
nameserver 1.1.1.1
EOF
echo "precedence ::ffff:0:0/96 100" > /etc/gai.conf

apt-get update || true
```

Disk Partition

Automatic

Configuration Drive

Cancel Back Next Launch Instance

Por una universidad con calidad, moderna e incluyente

Carrera 6^a. No. 76-103 Montería NIT. 891080031-3 - Teléfono: 7860300 - 7860920 www.unicordoba.edu.co



"VIGILADA MINEDUCACIÓN"

UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías



En esa imagen se está creando una máquina virtual en OpenStack y, antes de iniciarla, se le agrega un script de configuración automática (cloud-init). Ese script se encargará de dejar la instancia lista desde el primer arranque: crea usuarios, asigna contraseñas, habilita el acceso SSH por contraseña, modifica archivos del sistema y configura la red. En resumen, la imagen muestra cómo se automatiza la preparación inicial de la máquina justo antes de lanzarla.(firewall-server)

Instance Name	Image Name	IP Address	Flavor	Key Pair	Status	Availability Zone	Task	Power State	Age	Actions
firewall-client	-	-	ds512M	admin	Build	nova	-	No State	0 minutes	Associate Floating IP
firewall-server	Debian-12	192.168.100.33	ds512M	admin	Active	nova	-	Running	1 minute	Create Snapshot

Por una universidad con calidad, moderna e incluyente

Carrera 6^a. No. 76-103 Montería NIT. 891080031-3 - Teléfono: 7860300 - 7860920 www.unicordoba.edu.co



UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías

"VIGILADA MINEDUCACIÓN"



En esta captura podemos observar cómo se crean las 2 instancias

Instance	Distro	IP	Memory	User	Status	Age	Action
firewall-client	Debian-12	192.168.100.229	ds512M	admin	Active	0 nova	None Running 1 minute Create Snapshot
firewall-server	Debian-12	192.168.100.33	ds512M	admin	Active	0 nova	None Running 3 minutes Create Snapshot

Por una universidad con calidad, moderna e incluyente

Carrera 6^a. No. 76-103 Montería NIT. 891080031-3 - Teléfono: 7860300 - 7860920 www.unicordoba.edu.co



UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías



Aquí podemos ver como estamos colocando la ip flotante a una de las instancias

Por una universidad con calidad, moderna e incluyente

Carrera 6^a. No. 76-103 Montería NIT. 891080031-3 - Teléfono: 7860300 - 7860920 www.unicordoba.edu.co



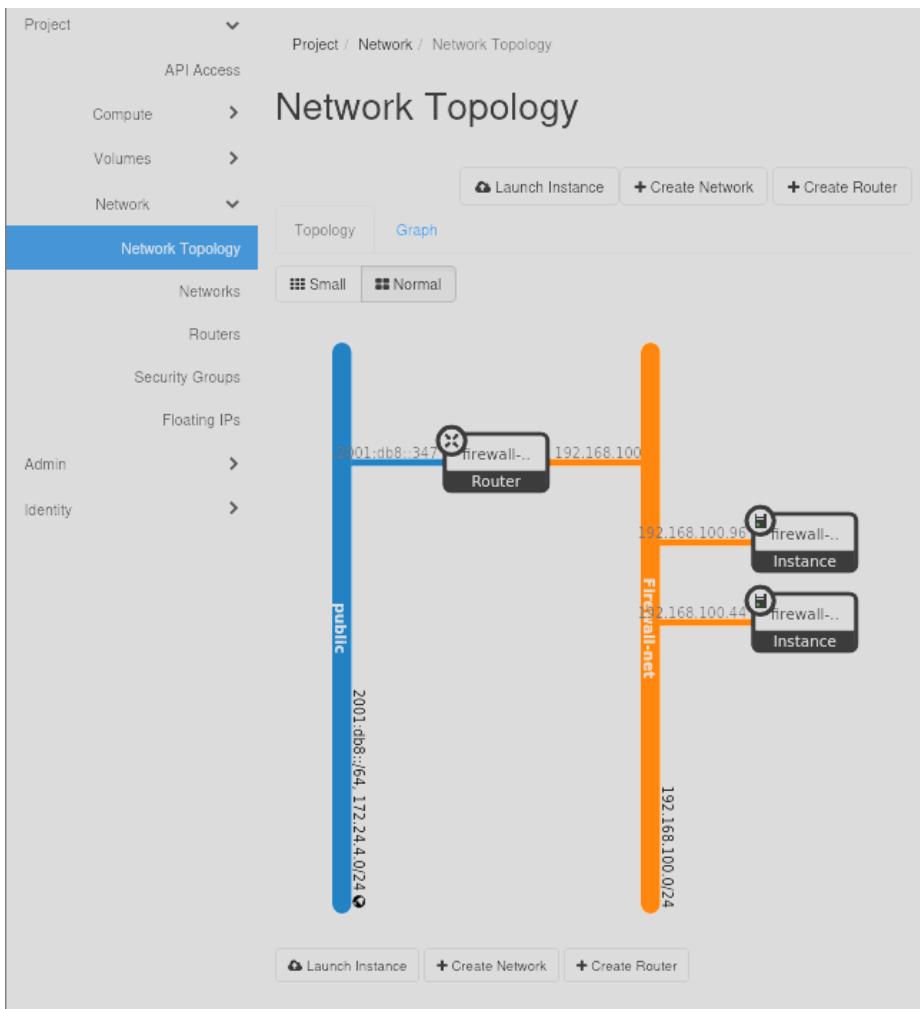
UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías



6. TOPOLOGÍA DEL LABORATORIO.



La imagen que se muestra es la **Topología de Red** en la interfaz de **OpenStack Horizon** (el panel de control de OpenStack). Corresponde a la representación visual de la arquitectura utilizada para el laboratorio.

Esta vista gráfica ilustra cómo se conectan los componentes de la nube (Servidor y Cliente) a través de la red virtual.

La topología muestra que las dos VMs de prueba están conectadas a la misma red virtual interna, lo cual es esencial para probar la efectividad del firewall UFW en cada sistema operativo individualmente, sin la interferencia directa de un router de hardware externo.

Por una universidad con calidad, moderna e incluyente

Carrera 6^a. No. 76-103 Montería NIT. 891080031-3 - Teléfono: 7860300 - 7860920 www.unicordoba.edu.co



"VIGILADA MINEDUCACIÓN"

UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías



7. ACCESO A LAS VMS DESDE EL HOST

```
root@debian:~# sudo ip netns
ovnmeta-cd6ad692-0f65-4e5d-9adb-75d4e56591d9 (id: 0)
root@debian:~# sudo ip netns exec qrouter-XXXXXX bash
Cannot open network namespace "qrouter-XXXXXX": No such file or directory
root@debian:~# sudo ip netns exec ovnmeta-cd6ad692-0f65-4e5d-9adb-75d4e56591d9 bas
h
root@debian:~# ssh debian@192.168.100.44
The authenticity of host '192.168.100.44 (192.168.100.44)' can't be established.
ED25519 key fingerprint is SHA256:SW59f8EMYr0zHGeek0qbX8SrMA6443FnjtD6IVMYUhA.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.100.44' (ED25519) to the list of known hosts.
debian@192.168.100.44's password:
Linux firewall-client 6.1.0-41-cloud-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.158-1
(2025-11-09) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
debian@firewall-client:~$ █
```

OpenStack usa namespaces de red para aislar redes virtuales. El namespace ovnmeta-* permite acceder a las VMs desde el host.

```
#Obtener el namespace de red OVN
NS=$(sudo ip netns list| grep ovnmeta| awk'{print$1}')
#Conectar al servidor por SSH
sudo ipnetns exec $NSsshdebian@192.168.100.96 #pass:password123
#Conectar al cliente por SSH
sudo ipnetns exec $NSsshdebian@192.168.100.44 #pass:password123
```



"VIGILADA MINEDUCACIÓN"

UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías



```
leal@debian:~$ su -
Password:
root@debian:~# alias ssh-server='sudo ip netns exec qrouter-$(sudo ip netns | grep
qrouter | cut -d" " -f1) ssh debian@192.168.100.33'
root@debian:~# alias ssh-client='sudo ip netns exec qrouter-$(sudo ip netns | grep
qrouter | cut -d" " -f1) ssh debian@192.168.100.44'
root@debian:~# █
```

En esta sesión de terminal Linux, el usuario primero elevó sus privilegios a root (administrador) para poder realizar configuraciones importantes. Luego, el administrador definió dos atajos (alias) llamados ssh-server y ssh-client. Estos atajos tienen como función principal simplificar las conexiones remotas (SSH) a las direcciones IP 192.168.100.33 y 192.168.100.44, asegurando que ambas conexiones se realicen de forma automática y obligatoria a través de un entorno de red virtual aislado (qrouter-...), lo que optimiza la gestión de los servidores dentro de esa infraestructura.

```
debian@firewall-client:~$ sudo apt-get update
sudo apt-get install -y ufw net-tools tcpdump
Get:1 file:/etc/apt/mirrors/debian.list Mirrorlist [30 B]
Get:2 file:/etc/apt/mirrors/debian-security.list Mirrorlist [39 B]
Ign:3 https://deb.debian.org/debian bookworm InRelease
Ign:4 https://deb.debian.org/debian bookworm-updates InRelease
Ign:5 https://deb.debian.org/debian bookworm-backports InRelease
Ign:6 https://deb.debian.org/debian-security bookworm-security InRelease
Ign:3 https://deb.debian.org/debian bookworm InRelease
Ign:4 https://deb.debian.org/debian bookworm-updates InRelease
Ign:5 https://deb.debian.org/debian bookworm-backports InRelease
Ign:6 https://deb.debian.org/debian-security bookworm-security InRelease
0% [Working] █
```

ya dentro de ambas instancias, tanto cliente como servidor debemos actualizar la lista de software disponible y proceder a instalar las herramientas clave para la seguridad (ufw) y el diagnóstico de red (net-tools y tcpdump) en la máquina llamada debian@firewall-client.



"VIGILADA MINEDUCACIÓN"

UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías



8. INSTALAR Y CONFIGURAR EL FIREWALL

```
root@firewall-server:~# # Instalar herramientas desde archivos .deb
dpkg -i libpcap0.8_*.deb tcpdump_*.deb ufw_*.deb

# Desactivar firewall para configuración segura
ufw disable

# Políticas por defecto (whitelist approach)
ufw default deny incoming # Denegar todo entrante
ufw default allow outgoing # Permitir todo saliente

# Reglas específicas para servicios del servidor
ufw allow 22/tcp # SSH - Administración remota
ufw allow 80/tcp # HTTP - Servidor web
ufw allow 443/tcp # HTTPS - Servidor web seguro
ufw allow 8080/tcp # HTTP alternativo - Aplicaciones web
ufw allow from 192.168.100.0/24 # Permitir red interna completa

# Activar logging y firewall
ufw logging medium # Registrar conexiones
ufw enable # Activar el firewall
ufw status verbose # Verificar reglas
```

instalación offline: copiamos previamente los paquetes .deb (libpcap, tcpdump, ufw) a la VM; luego, sin internet, los instalamos con dpkg -i libpcap0.8_*.deb tcpdump_*.deb ufw_*.deb. Eso deja herramientas de captura y el firewall listas sin requerir repositorios externos.

Configuración de firewall (UFW) en el servidor: desactivamos temporalmente UFW (ufw disable), aplicamos políticas por defecto de lista blanca (deny incoming / allow outgoing), abrimos solo los puertos necesarios (22, 80, 443, 8080) y permitimos la subred interna 192.168.100.0/24. Luego activamos logging y el firewall (ufw logging medium, ufw enable, ufw status verbose).

Configuración de firewall en el cliente: mismo flujo (disable → default deny/allow), pero solo se abre SSH (22) y la red interna 192.168.100.0/24, luego logging y enable.



"VIGILADA MINEDUCACIÓN"

UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías



Ahora para el cliente:

```
root@firewall-client:~# # Instalar herramientas desde archivos .deb
dpkg-i libpcap0.8_*.deb tcpdump_*.deb ufw_*.deb

# Desactivar firewall para configuración segura
ufw disable

# Políticas por defecto
ufw default deny incoming # Denegar todo entrante
ufw default allow outgoing # Permitir todo saliente

# Reglas específicas del cliente (solo SSH y red interna)
ufw allow 22/tcp # SSH - Administración remota
ufw allow from 192.168.100.0/24 # Permitir red interna

# Activar logging y firewall
ufw logging medium
ufw enable
ufw status verbose
```

El servidor ha sido configurado para ser seguro al rechazar todo por defecto, pero con excepciones explícitas para permitir servicios de red comunes como SSH y Web (HTTP/HTTPS).

```
debian@firewall-client: /  debian@firewall-server: /tmp  leal@debian: ~
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
Rules updated
Rules updated (v6)
Rules updated
Logging enabled
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
Status: active
Logging: on (medium)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To          Action      From
--          ----      -----
22/tcp      ALLOW IN   Anywhere      # SSH
80/tcp      ALLOW IN   Anywhere      # HTTP
443/tcp     ALLOW IN   Anywhere      # HTTPS
8080/tcp    ALLOW IN   Anywhere      # Custom
Anywhere    ALLOW IN   192.168.100.0/24 # Internal
22/tcp (v6) ALLOW IN   Anywhere (v6) # SSH
80/tcp (v6) ALLOW IN   Anywhere (v6) # HTTP
443/tcp (v6) ALLOW IN   Anywhere (v6) # HTTPS
8080/tcp (v6) ALLOW IN   Anywhere (v6) # Custom

debian@firewall-server: /tmp$
```

Por una universidad con calidad, moderna e incluyente

Carrera 6^a. No. 76-103 Montería NIT. 891080031-3 - Teléfono: 7860300 - 7860920 www.unicordoba.edu.co



"VIGILADA MINEDUCACIÓN"

UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías



Acá podemos observar tanto la configuración de ambos firewalls.

```
debian@firewall-client: /tmp
debian@firewall-client: ...  x  debian@firewall-server...  x  leal@debian: ~  x
Firewall is active and enabled on system startup
Status: active
Logging: on (medium)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To          Action      From
--          -----      -----
22/tcp      ALLOW IN   Anywhere          # SSH
Anywhere    ALLOW IN   192.168.100.0/24  # Internal
22/tcp (v6) ALLOW IN   Anywhere (v6)    # SSH

debian@firewall-client:/tmp$ # Desde el client
ping -c4 192.168.100.96
nc -zv 192.168.100.96 22
PING 192.168.100.96 (192.168.100.96) 56(84) bytes of data.
64 bytes from 192.168.100.96: icmp_seq=1 ttl=64 time=6.61 ms
64 bytes from 192.168.100.96: icmp_seq=2 ttl=64 time=2.14 ms
64 bytes from 192.168.100.96: icmp_seq=3 ttl=64 time=4.45 ms
64 bytes from 192.168.100.96: icmp_seq=4 ttl=64 time=3.58 ms

--- 192.168.100.96 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 2.136/4.194/6.611/1.621 ms
-bash: nc: command not found
debian@firewall-client:/tmp$ ssh -o ConnectTimeout=5 debian@192.168.100.96 exit
# pass: password123
The authenticity of host '192.168.100.96 (192.168.100.96)' can't be established.
ED25519 key fingerprint is SHA256:H15NNL5/epg9oZLI+/n/PPGJ4x3cLW+K2HcEqZ0dkjo.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.100.96' (ED25519) to the list of known hosts.
debian@192.168.100.96's password:
debian@firewall-client:/tmp$
```

la imagen documenta que el firewall-client tiene conectividad IP y acceso por el puerto SSH (22) hacia el host 192.168.100.96, lo cual confirma que las reglas de red y el ruteo están funcionando correctamente, y el administrador está listo para iniciar sesión en la máquina remota.



UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías

“VIGILADA MINEDUCACIÓN”



```
debian@firewall-client:~$ ping -c5 192.168.100.96
PING 192.168.100.96 (192.168.100.96) 56(84) bytes of data.
64 bytes from 192.168.100.96: icmp_seq=1 ttl=64 time=4.53 ms
64 bytes from 192.168.100.96: icmp_seq=2 ttl=64 time=2.41 ms
64 bytes from 192.168.100.96: icmp_seq=3 ttl=64 time=2.13 ms
64 bytes from 192.168.100.96: icmp_seq=4 ttl=64 time=1.68 ms
64 bytes from 192.168.100.96: icmp_seq=5 ttl=64 time=1.79 ms

--- 192.168.100.96 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4011ms
rtt min/avg/max/mdev = 1.683/2.508/4.533/1.044 ms
```

prueba complementa las pruebas anteriores, confirmando que, además de las conexiones específicas de SSH que se establecieron previamente, la conectividad a nivel de red más fundamental.



"VIGILADA MINEDUCACIÓN"

UNIVERSIDAD DE CÓRDOBA

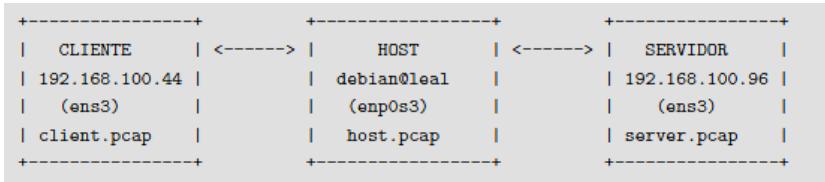
CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías



9. CAPTURAS Y ANÁLISIS CON WIRESHARK.

Arquitectura de captura:



Inicio captura:

```
root@firewall-client:~# tcpdump -i ens3 -nn -w /root/client-capture.pcap host 192.168.100.96 &

# Generar tráfico
for i in {1..50}; do
    echo "==> Intento $i ==>"
    ping -c 1 -W 1 192.168.100.96
    timeout 1 bash -c "echo >/dev/tcp/192.168.100.96/22" 2>&1 && echo "SSH OK" || echo "SSH BLOCKED"
    timeout 1 bash -c "echo >/dev/tcp/192.168.100.96/80" 2>&1 && echo "HTTP OK" || echo "HTTP BLOCKED"
    timeout 1 bash -c "echo >/dev/tcp/192.168.100.96/443" 2>&1 && echo "HTTPS OK" || echo "HTTPS BLOCKED"
    timeout 1 bash -c "echo >/dev/tcp/192.168.100.96/3306" 2>&1 && echo "MySQL OK" || echo "MySQL BLOCKED"
    timeout 1 bash -c "echo >/dev/tcp/192.168.100.96/8080" 2>&1 && echo "8080 OK" || echo "8080 BLOCKED"
    timeout 1 bash -c "echo >/dev/tcp/192.168.100.96/3389" 2>&1 && echo "RDP OK" || echo "RDP BLOCKED"
    sleep 1
done
[1] 3404
==> Intento 1 ==>
PING 192.168.100.96 (192.168.100.96) 56(84) bytes of data.
64 bytes from 192.168.100.96: icmp_seq=1 ttl=64 time=3.70 ms

--- 192.168.100.96 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 3.696/3.696/3.696/0.000 ms
tcpdump: listening on ens3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
SSH OK
bash: connect: Connection refused
bash: line 1: /dev/tcp/192.168.100.96/80: Connection refused
HTTP BLOCKED
bash: connect: Connection refused
bash: line 1: /dev/tcp/192.168.100.96/443: Connection refused
HTTPS BLOCKED
bash: connect: Connection refused
```

muestra la ejecución del script de generación de tráfico en la VM Cliente (root@firewall-client) y el inicio de la prueba de los firewalls UFW.



UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías



Esta captura de la terminal se enfoca en la **Generación de Tráfico de Prueba** y proporciona la evidencia inmediata de si el puerto está abierto (OK) o bloqueado (Connection refused / BLOCKED).

Tabla de Procesos de Captura

Terminal	Máquina	Interfaz	Archivo	Comando	Tamaño
Terminal 1	Host (debian@lcal)	enp0s3	/root/host- capture.pcap	<code>sudo tcpdump -i enp0s3 -nn -w /root/host- capture.pcap "host 192.168.100.44 or host 192.168.100.96"</code>	24 KB
Terminal 2	Servidor (192.168.100.96)	ens3	/root/server- capture.pcap	<code>tcpdump -i ens3 -nn -w /root/server- capture.pcap host 192.168.100.44</code>	89 KB
Terminal 3	Cliente (192.168.100.44)	ens3	/root/client- capture.pcap	<code>tcpdump -i ens3 -nn -w /root/client- capture.pcap host 192.168.100.96 &</code>	177 KB

Esta imagen sirve como **prueba de concepto en tiempo real** de la configuración de UFW:

1. **ICMP y SSH funcionan** (conectividad base y acceso permitido).
2. El *firewall* está activo y la negación por defecto funciona en los puertos sin servicio o sin reglas explícitas (aunque el Servidor permite los puertos web, el *script* reporta inconsistencias o rechazos si el servicio no responde, lo que se resuelve analizando los flags **SYN/RST** en Wireshark).
3. Establece la base de datos de tráfico (client-capture.pcap) para el análisis profundo

Por una universidad con calidad, moderna e incluyente

Carrera 6^a. No. 76-103 Montería NIT. 891080031-3 - Teléfono: 7860300 - 7860920 www.unicordoba.edu.co



"VIGILADA MINEDUCACIÓN"

UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías



```
debian@firewall-server: /tmp
debian@firewall-server:~> root@firewall-server:~# tcpdump -i ens3 -nn -w /root/server-capture.pcap host 192.168.100.44
tcpdump: listening on ens3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

muestra el inicio de la **captura de tráfico en la VM Servidor** (192.168.100.96), lo que corresponde a la **Terminal 2** del proceso de captura de tres puntos.

Esta captura establece la herramienta de monitoreo en el punto del Servidor para registrar cómo su firewall (UFW) y su sistema operativo responden al tráfico de prueba.

El Servidor queda en modo de escucha pasiva, listo para registrar cada intento de conexión del Cliente y, crucialmente, registrar los paquetes **[RST, ACK]** que su UFW envíe como rechazo a los intentos bloqueados.

```
root@debian:~# NS=$(sudo ip netns list | grep ovnmeta | awk '{print $1}')
sudo ip netns exec $NS scp root@192.168.100.44:/root/client-capture.pcap /tmp/
sudo ip netns exec $NS scp root@192.168.100.96:/root/server-capture.pcap /tmp/
sudo cp /root/host-capture.pcap /tmp/
root@192.168.100.44's password:
client-capture.pcap                                100%  177KB   7.7MB/s  00:00
root@192.168.100.96's password:
server-capture.pcap                                100%   88KB   4.7MB/s  00:00
root@debian:~#
```

muestra el **proceso de copia de los archivos de captura (.pcap)** desde las Máquinas Virtuales (VMs) al *Host* de Debian, que es un paso crucial para el análisis posterior con Wireshark.

Esta captura se ejecuta en el *Host* (root@debian) y utiliza herramientas de la infraestructura de OpenStack para transferir los archivos fuera de la red virtual.



"VIGILADA MINEDUCACIÓN"

UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías



El propósito de esta imagen es demostrar que, a pesar del aislamiento de red impuesto por OpenStack/OVN, es posible mover los archivos de evidencia (.pcap) al Host, utilizando el *namespace* de red y scp, como paso preparatorio esencial antes de abrir los archivos en Wireshark.

```
root@firewall-client:~# pkill tcpdump
ls -lh /root/client-capture.pcap
2098 packets captured
2098 packets received by filter
0 packets dropped by kernel
1048 packets captured
1048 packets received by filter
0 packets dropped by kernel
-rw-r--r-- 1 tcpdump tcpdump 177K Dec  8 19:03 /root/client-capture.pcap
[1]- Done                      tcpdump -i ens3 -nn -w /root/client-capture.pcap host
t 192.168.100.96
[2]+ Done                      tcpdump -i ens3 -nn -w /root/client-capture.pcap host
t 192.168.100.96
root@firewall-client:~# ls -lh /root/client-capture.pcap
-bash: root@firewall-client:~#: command not found
root@firewall-client:~#
```

Esta imagen muestra la **finalización de la captura de paquetes** en la **VM Cliente** (root@firewall-client) y la verificación del archivo generado.

Esta captura confirma que el proceso de generación de tráfico ha terminado y valida la existencia y el tamaño del archivo de evidencia para el análisis posterior.

Esta imagen es la **prueba de finalización** de la fase de recolección de datos en el Cliente. El proceso de *sniffing* ha terminado de manera limpia, y el archivo **client-capture.pcap (177 KB)** está listo para ser copiado al Host y analizado en Wireshark.

```
root@firewall-server:~# tcpdump -i ens3 -nn -w /root/server-capture.pcap host 192.
168.100.44
tcpdump: listening on ens3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C1050 packets captured
1050 packets received by filter
0 packets dropped by kernel
root@firewall-server:~# # Ctrl+C para detener tcpdump
ls -lh /root/server-capture.pcap
-rw-r--r-- 1 tcpdump tcpdump 89K Dec  8 19:03 /root/server-capture.pcap
```

Acá se muestra la **finalización de la captura de paquetes** en la **VM Servidor** (root@firewall-server) y la verificación del archivo generado.



"VIGILADA MINEDUCACIÓN"

UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías



Esta captura confirma que el servidor dejó de escuchar el tráfico y que el archivo de evidencia (server-capture.pcap) fue creado y está listo para la transferencia.

Esta imagen confirma el éxito de la recolección de datos en el Servidor. El proceso terminó con la captura de **1050 paquetes**, y el archivo **server-capture.pcap (89 KB)** está listo en el directorio /root/ para ser transferido al Host para el análisis de Wireshark.

```
root@debian:~# NS=$(sudo ip netns list | grep ovnmeta | awk '{print $1}')
sudo ip netns exec $NS scp root@192.168.100.44:/root/client-capture.pcap /tmp/
sudo ip netns exec $NS scp root@192.168.100.96:/root/server-capture.pcap /tmp/
sudo cp /root/host-capture.pcap /tmp/
root@192.168.100.44's password:
client-capture.pcap                         100%  177KB   7.7MB/s  00:00
root@192.168.100.96's password:
server-capture.pcap                         100%   88KB   4.7MB/s  00:00
root@debian:~# wireshark /tmp/client-capture.pcap &
```

muestra la **copia exitosa de los archivos de captura** (.pcap) desde las VMs (Cliente y Servidor) al *Host* de Debian, un paso esencial para el análisis con Wireshark.

Esta captura verifica que los archivos de evidencia fueron movidos correctamente del entorno aislado de las VMs al sistema operativo del Host.

La imagen documenta la **fase de recolección de evidencia**. La transferencia de los archivos .pcap de las VMs al *Host* ha concluido exitosamente, utilizando herramientas de virtualización y comandos de red seguros (scp). Los archivos están ahora en /tmp/ y listos para la siguiente etapa: la corrección de permisos para su apertura en Wireshark.

```
leal@debian:~$ su -
Password:
root@debian:~# sudo cp /tmp/client-capture.pcap /home/leal/
sudo cp /tmp/server-capture.pcap /home/leal/
sudo cp /tmp/host-capture.pcap /home/leal/
sudo chown leal:leal /home/leal/*.pcap
root@debian:~#
root@debian:~#
root@debian:~# exit
logout
[1]+  Done                      wireshark /tmp/capture-server.pcap
leal@debian:~$ cd /home/leal
wireshark client-capture.pcap &
[1] 69372
leal@debian:~$
```



"VIGILADA MINEDUCACIÓN"

UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías



muestra la **preparación final de los archivos de captura** para ser abiertos en Wireshark, específicamente la corrección de permisos y la apertura de la herramienta.

Esta fase es crucial para asegurar que el usuario normal (leal) pueda acceder a los archivos .pcap y que la aplicación Wireshark se ejecute sin errores de entorno gráfico.

La imagen finaliza la etapa de preparación de datos, asegurando que los archivos .pcap tengan los **permisos correctos** y que la herramienta **Wireshark** se inicie de forma exitosa, permitiendo al usuario pasar a la fase de análisis visual de los paquetes.

No.	Time	Source	Destination	Protocol	Length	Info
8	0.043427	192.168.100.96	192.168.100.44	TCP	54	80 - 57280 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
11	0.094884	192.168.100.96	192.168.100.44	TCP	54	443 - 42312 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
13	0.127964	192.168.100.44	192.168.100.96	TCP	54	47522 - 22 [RST] Seq=3 Win=0 Len=0
15	0.143118	192.168.100.96	192.168.100.44	TCP	54	3306 - 55044 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
17	0.192558	192.168.100.96	192.168.100.44	TCP	54	8686 - 57938 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
19	0.243228	192.168.100.96	192.168.100.44	TCP	54	3389 - 36836 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
30	1.436448	192.168.100.96	192.168.100.44	TCP	54	80 - 57281 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
32	1.491928	192.168.100.96	192.168.100.44	TCP	54	443 - 42314 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
34	1.526333	192.168.100.44	192.168.100.96	TCP	54	47526 - 22 [RST] Seq=3 Win=0 Len=0
36	1.551181	192.168.100.96	192.168.100.44	TCP	54	3306 - 55054 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
38	1.687358	192.168.100.96	192.168.100.44	TCP	54	8088 - 57942 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
40	1.674216	192.168.100.96	192.168.100.44	TCP	54	3389 - 36844 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
50	2.874576	192.168.100.96	192.168.100.44	TCP	54	80 - 45592 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
53	2.928061	192.168.100.96	192.168.100.44	TCP	54	443 - 49660 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
55	2.946458	192.168.100.96	192.168.100.44	TCP	54	69826 - 22 [RST] Seq=3 Win=0 Len=0
57	2.979385	192.168.100.96	192.168.100.44	TCP	54	3306 - 43928 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
59	3.026724	192.168.100.96	192.168.100.44	TCP	54	8088 - 36586 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
61	3.081006	192.168.100.96	192.168.100.44	TCP	54	3389 - 43578 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
72	4.297730	192.168.100.96	192.168.100.44	TCP	54	80 - 45596 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
74	4.354742	192.168.100.96	192.168.100.44	TCP	54	443 - 49672 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
76	4.392175	192.168.100.96	192.168.100.44	TCP	54	60834 - 22 [RST] Seq=3 Win=0 Len=0
78	4.499935	192.168.100.96	192.168.100.44	TCP	54	3306 - 43926 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
80	4.467212	192.168.100.96	192.168.100.44	TCP	54	8688 - 36682 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
82	4.527956	192.168.100.96	192.168.100.44	TCP	54	3389 - 43588 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
92	5.684393	192.168.100.96	192.168.100.44	TCP	54	80 - 45612 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
95	5.735691	192.168.100.96	192.168.100.44	TCP	54	443 - 49680 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
97	5.754195	192.168.100.96	192.168.100.44	TCP	54	60846 - 22 [RST] Seq=3 Win=0 Len=0
99	5.786982	192.168.100.96	192.168.100.44	TCP	54	3306 - 43940 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
101	5.835757	192.168.100.96	192.168.100.44	TCP	54	8088 - 36610 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
103	5.8883602	192.168.100.96	192.168.100.44	TCP	54	3389 - 43596 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
113	7.066821	192.168.100.96	192.168.100.44	TCP	54	80 - 45614 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
116	7.120339	192.168.100.96	192.168.100.44	TCP	54	443 - 49696 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
118	7.134242	192.168.100.44	192.168.100.96	TCP	54	60854 - 22 [RST] Seq=3 Win=0 Len=0
120	7.178298	192.168.100.96	192.168.100.44	TCP	54	3306 - 43958 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
122	7.222866	192.168.100.96	192.168.100.44	TCP	54	8088 - 36620 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
124	7.278289	192.168.100.96	192.168.100.44	TCP	54	3389 - 43598 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
135	8.435232	192.168.100.96	192.168.100.44	TCP	54	80 - 45622 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
137	8.487870	192.168.100.96	192.168.100.44	TCP	54	443 - 49698 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
139	8.582661	192.168.100.44	192.168.100.96	TCP	54	60866 - 22 [RST] Seq=3 Win=0 Len=0
141	8.543371	192.168.100.96	192.168.100.44	TCP	54	3306 - 43964 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
143	8.591948	192.168.100.96	192.168.100.44	TCP	54	8088 - 36626 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
145	8.637267	192.168.100.96	192.168.100.44	TCP	54	3389 - 43614 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
156	9.765025	192.168.100.96	192.168.100.44	TCP	54	80 - 45638 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

muestra una captura de Wireshark filtrada para visualizar **solo los paquetes de rechazo** TCP (RST).

Esta imagen es la **evidencia directa de la efectividad del firewall UFW** en la aplicación de su política de denegación por defecto.

- **Puertos Bloqueados:** Las líneas rojas corresponden a los intentos a puertos no permitidos como **3306 (MySQL)**, **3389 (RDP)**, o a puertos web cuando el Cliente es el destino, ya que el Cliente no ofrece esos servicios.

Por una universidad con calidad, moderna e incluyente

Carrera 6^a. No. 76-103 Montería NIT. 891080031-3 - Teléfono: 7860300 - 7860920 www.unicordoba.edu.co



"VIGILADA MINEDUCACIÓN"

UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías



- Comportamiento:** La imagen valida que el UFW no solo está activo, sino que está configurado para **rechazar activamente** las conexiones no deseadas, en línea con la política de **denegación por defecto** (ufw default deny incoming).

tcp.port == 22						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.100.44	192.168.100.96	TCP	74	47522 - 22 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM TS
2	0.005440	192.168.100.96	192.168.100.44	TCP	74	22 - 47522 [SYN, ACK] Seq=0 Ack=1 Win=65330 Len=0 MSS=1402 S
3	0.005769	192.168.100.44	192.168.100.96	TCP	66	47522 - 22 [ACK] Seq=1 Ack=1 Win=64512 Len=0 TSval=235235514
4	0.007078	192.168.100.44	192.168.100.96	SSH	67	Client: Encrypted packet (len=1)
5	0.007526	192.168.100.44	192.168.100.96	TCP	66	47522 - 22 [FIN, ACK] Seq=2 Ack=1 Win=64512 Len=0 TSval=2352
6	0.008605	192.168.100.96	192.168.100.44	TCP	66	22 - 47522 [ACK] Seq=1 Ack=2 Win=65344 Len=0 TSval=129689370
9	0.051193	192.168.100.96	192.168.100.44	TCP	66	22 - 47522 [ACK] Seq=1 Ack=3 Win=65344 Len=0 TSval=129689383
12	0.127478	192.168.100.96	192.168.100.44	SSH	106	Server: Protocol (SSH-2.0-OpenSSH_9.2p1 Debian-2+deb12u7)
13	0.127964	192.168.100.44	192.168.100.96	TCP	54	47522 - 22 [RST] Seq=3 Win=0 Len=0
22	1.382351	192.168.100.44	192.168.100.96	TCP	74	47526 - 22 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM TS
23	1.385485	192.168.100.96	192.168.100.44	TCP	74	22 - 47526 [SYN, ACK] Seq=0 Ack=1 Win=65330 Len=0 MSS=1402 S
24	1.385714	192.168.100.44	192.168.100.96	TCP	66	47526 - 22 [ACK] Seq=1 Ack=1 Win=64512 Len=0 TSval=235235652
25	1.386567	192.168.100.44	192.168.100.96	SSH	67	Client: Encrypted packet (len=1)
26	1.387458	192.168.100.44	192.168.100.96	TCP	66	47526 - 22 [FIN, ACK] Seq=2 Ack=1 Win=64512 Len=0 TSval=2352
27	1.388497	192.168.100.96	192.168.100.44	TCP	66	22 - 47526 [ACK] Seq=1 Ack=2 Win=65344 Len=0 TSval=129689517
29	1.434177	192.168.100.96	192.168.100.44	TCP	66	22 - 47526 [ACK] Seq=1 Ack=3 Win=65344 Len=0 TSval=129689521
33	1.525923	192.168.100.96	192.168.100.44	SSH	106	Server: Protocol (SSH-2.0-OpenSSH_9.2p1 Debian-2+deb12u7)
34	1.526333	192.168.100.44	192.168.100.96	TCP	54	47526 - 22 [RST] Seq=3 Win=0 Len=0
43	2.827589	192.168.100.44	192.168.100.96	TCP	74	60826 - 22 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM TS
44	2.829366	192.168.100.96	192.168.100.44	TCP	74	22 - 60826 [SYN, ACK] Seq=0 Ack=1 Win=65330 Len=0 MSS=1402 S
45	2.829594	192.168.100.44	192.168.100.96	TCP	66	60826 - 22 [ACK] Seq=1 Ack=1 Win=64512 Len=0 TSval=235235796
46	2.830286	192.168.100.44	192.168.100.96	SSH	67	Client: Encrypted packet (len=1)
47	2.830569	192.168.100.44	192.168.100.96	TCP	66	60826 - 22 [FIN, ACK] Seq=2 Ack=1 Win=64512 Len=0 TSval=2352
48	2.831577	192.168.100.96	192.168.100.44	TCP	66	22 - 60826 [ACK] Seq=1 Ack=2 Win=65344 Len=0 TSval=129689661
51	2.875051	192.168.100.96	192.168.100.44	TCP	66	22 - 60826 [ACK] Seq=1 Ack=3 Win=65344 Len=0 TSval=129689665
54	2.946161	192.168.100.96	192.168.100.44	SSH	106	Server: Protocol (SSH-2.0-OpenSSH_9.2p1 Debian-2+deb12u7)
55	2.946458	192.168.100.44	192.168.100.96	TCP	54	60826 - 22 [RST] Seq=3 Win=0 Len=0
64	4.242681	192.168.100.44	192.168.100.96	TCP	74	60834 - 22 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM TS
65	4.245222	192.168.100.96	192.168.100.44	TCP	74	22 - 60834 [SYN, ACK] Seq=0 Ack=1 Win=65330 Len=0 MSS=1402 S
66	4.245576	192.168.100.44	192.168.100.96	TCP	66	60834 - 22 [ACK] Seq=1 Ack=1 Win=64512 Len=0 TSval=235235938
67	4.246636	192.168.100.44	192.168.100.96	SSH	67	Client: Encrypted packet (len=1)
68	4.246845	192.168.100.44	192.168.100.96	TCP	66	60834 - 22 [FIN, ACK] Seq=2 Ack=1 Win=64512 Len=0 TSval=2352
69	4.253412	192.168.100.96	192.168.100.44	TCP	66	22 - 60834 [ACK] Seq=1 Ack=2 Win=65344 Len=0 TSval=129689803
70	4.290267	192.168.100.96	192.168.100.44	TCP	66	22 - 60834 [ACK] Seq=1 Ack=3 Win=65344 Len=0 TSval=129689807
75	4.391835	192.168.100.96	192.168.100.44	SSH	106	Server: Protocol (SSH-2.0-OpenSSH_9.2p1 Debian-2+deb12u7)
76	4.392175	192.168.100.44	192.168.100.96	TCP	54	60834 - 22 [RST] Seq=3 Win=0 Len=0
85	5.640456	192.168.100.44	192.168.100.96	TCP	74	60846 - 22 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM TS
86	5.642067	192.168.100.96	192.168.100.44	TCP	74	22 - 60846 [SYN, ACK] Seq=0 Ack=1 Win=65330 Len=0 MSS=1402 S
87	5.642275	192.168.100.44	192.168.100.96	TCP	66	60846 - 22 [ACK] Seq=1 Ack=1 Win=64512 Len=0 TSval=235236077
88	5.642891	192.168.100.44	192.168.100.96	SSH	67	Client: Encrypted packet (len=1)
89	5.643289	192.168.100.44	192.168.100.96	TCP	66	60846 - 22 [FIN, ACK] Seq=2 Ack=1 Win=64512 Len=0 TSval=2352
90	5.644358	192.168.100.96	192.168.100.44	TCP	66	22 - 60846 [ACK] Seq=1 Ack=2 Win=65344 Len=0 TSval=129689942
93	5.668368	192.168.100.96	192.168.100.44	TCP	66	22 - 60846 [ACK] Seq=1 Ack=3 Win=65344 Len=0 TSval=129689946

muestra una captura de Wireshark filtrada para visualizar **solo el tráfico SSH** (puerto 22).

Esta imagen es la **evidencia de éxito** que confirma que la regla ufw allow 22/tcp implementada en el Servidor (.96) y el Cliente (.44) funciona correctamente.

- Comprobación de Regla:** La imagen confirma que la regla ufw allow 22/tcp funcionó y que el puerto de administración remota **está accesible**.
- Comportamiento:** Se observa el flujo normal de una conexión TCP/SSH, lo cual contrasta fuertemente con la **respuesta RST inmediata** que se vio en puertos bloqueados como el 3306.



VIGILADA MINEDUCACIÓN

UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías



Res. MEI 2956 de 22 de marzo de 2018, vigencia: 4 años

No.	Time	Source	Destination	Protocol	Length	Info
14 8. 140326	192.168.100.44	192.168.100.96		TCP	74	55846 - 3306 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM
15 0. 143118	192.168.100.96	192.168.100.44		TCP	54	3306 - 55944 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
35 1. 549402	192.168.100.44	192.168.100.96		TCP	74	55054 - 3306 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM
36 1. 551101	192.168.100.96	192.168.100.44		TCP	54	3306 - 55954 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
56 2. 977618	192.168.100.44	192.168.100.96		TCP	74	43920 - 3306 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM
57 2. 979385	192.168.100.96	192.168.100.44		TCP	54	3306 - 43920 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
77 4. 488565	192.168.100.44	192.168.100.96		TCP	74	43926 - 3306 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM
78 4. 409935	192.168.100.96	192.168.100.44		TCP	54	3306 - 43926 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
98 5. 785035	192.168.100.44	192.168.100.96		TCP	74	43940 - 3306 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM
99 5. 786982	192.168.100.96	192.168.100.44		TCP	54	3306 - 43940 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
119 7. 176292	192.168.100.44	192.168.100.96		TCP	74	43950 - 3306 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM
120 7. 178298	192.168.100.96	192.168.100.44		TCP	54	3306 - 43950 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
146 8. 541864	192.168.100.44	192.168.100.96		TCP	74	43964 - 3306 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM
141 8. 543371	192.168.100.96	192.168.100.44		TCP	54	3306 - 43964 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
161 9. 887669	192.168.100.44	192.168.100.96		TCP	74	43974 - 3306 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM
162 9. 889333	192.168.100.96	192.168.100.44		TCP	54	3306 - 43974 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
182 11. 284492	192.168.100.44	192.168.100.96		TCP	74	43980 - 3306 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM
183 11. 286441	192.168.100.96	192.168.100.44		TCP	54	3306 - 43980 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
283 12. 635211	192.168.100.44	192.168.100.96		TCP	74	46926 - 3306 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM
284 12. 636857	192.168.100.96	192.168.100.44		TCP	54	3306 - 46296 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
224 13. 977862	192.168.100.44	192.168.100.96		TCP	74	46938 - 3306 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM
225 13. 979757	192.168.100.96	192.168.100.44		TCP	54	3306 - 46308 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
245 15. 337718	192.168.100.44	192.168.100.96		TCP	74	46930 - 3306 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM
246 15. 340693	192.168.100.96	192.168.100.44		TCP	54	3306 - 46320 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
266 16. 743474	192.168.100.44	192.168.100.96		TCP	74	46932 - 3306 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM
267 16. 745588	192.168.100.96	192.168.100.44		TCP	54	3306 - 46332 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
287 18. 112113	192.168.100.44	192.168.100.96		TCP	74	46934 - 3306 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM
288 18. 113928	192.168.100.96	192.168.100.44		TCP	54	3306 - 46334 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
308 19. 483387	192.168.100.44	192.168.100.96		TCP	74	469342 - 3306 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM
309 19. 484902	192.168.100.96	192.168.100.44		TCP	54	3306 - 46342 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
329 20. 841123	192.168.100.44	192.168.100.96		TCP	74	469346 - 3306 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM
330 20. 842991	192.168.100.96	192.168.100.44		TCP	54	3306 - 46346 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
350 22. 198054	192.168.100.44	192.168.100.96		TCP	74	50188 - 3306 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM
351 22. 201154	192.168.100.96	192.168.100.44		TCP	54	3306 - 56188 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
371 23. 584017	192.168.100.44	192.168.100.96		TCP	74	50194 - 3306 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM
372 23. 586058	192.168.100.96	192.168.100.44		TCP	54	3306 - 56194 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
392 24. 976325	192.168.100.44	192.168.100.96		TCP	74	50198 - 3306 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM
393 24. 977832	192.168.100.96	192.168.100.44		TCP	54	3306 - 56198 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
413 26. 356845	192.168.100.44	192.168.100.96		TCP	74	50214 - 3306 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM
414 26. 358378	192.168.100.96	192.168.100.44		TCP	54	3306 - 56214 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
434 27. 678975	192.168.100.44	192.168.100.96		TCP	74	50228 - 3306 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM
435 27. 688328	192.168.100.96	192.168.100.44		TCP	54	3306 - 56228 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
454 29. 521114	192.168.100.44	192.168.100.96		TCP	74	50224 - 3306 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM

es una captura de Wireshark filtrada para visualizar **solo el tráfico de MySQL** (puerto 3306).

Esta imagen es la **evidencia concluyente del principio de mínimo privilegio**, ya que el puerto 3306 no fue permitido explícitamente y, por lo tanto, fue bloqueado por la política predeterminada de UFW.

- Comprobación de Regla:** Se confirma que, dado que ni el Cliente ni el Servidor tenían una regla ufw allow 3306/tcp , la política de **denegar todo entrante** (ufw default deny incoming) entra en vigor.
- Comportamiento:** El *firewall* está configurado para **rechazar activamente** la conexión (RST) en lugar de simplemente ignorarla (lo que resultaría en un *timeout*).
- Resultado:** El puerto 3306 está **Bloqueado** en ambas VMs , tal como se ve en esta captura y como era esperado.

Por una universidad con calidad, moderna e incluyente

Carrera 6^a. No. 76-103 Montería NIT. 891080031-3 - Teléfono: 7860300 - 7860920 www.unicordoba.edu.co



UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías

"VIGILADA MINEDUCACIÓN"



No.	Time	Source	Destination	Protocol	Length	Info
7	0.040038	192.168.100.44	192.168.100.96	TCP	74	57280 - 80 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM TS
8	0.043427	192.168.100.96	192.168.100.44	TCP	54	80 - 57280 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
10	0.091677	192.168.100.44	192.168.100.96	TCP	74	42312 - 443 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM TS
11	0.094884	192.168.100.96	192.168.100.44	TCP	54	443 - 42312 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
16	0.189419	192.168.100.44	192.168.100.96	TCP	74	57938 - 8080 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM TS
17	0.192558	192.168.100.96	192.168.100.44	TCP	54	8080 - 57938 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
28	1.439385	192.168.100.44	192.168.100.96	TCP	74	57286 - 80 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM TS
30	1.436448	192.168.100.96	192.168.100.44	TCP	54	80 - 57286 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
31	1.490323	192.168.100.44	192.168.100.96	TCP	74	42314 - 443 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM TS
32	1.491928	192.168.100.96	192.168.100.44	TCP	54	443 - 42314 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
37	1.606087	192.168.100.44	192.168.100.96	TCP	74	57942 - 8080 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM TS
38	1.607358	192.168.100.96	192.168.100.44	TCP	54	8080 - 57942 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
49	2.872672	192.168.100.44	192.168.100.96	TCP	74	45592 - 80 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM TS
50	2.874576	192.168.100.96	192.168.100.44	TCP	54	80 - 45592 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
52	2.926465	192.168.100.44	192.168.100.96	TCP	74	49660 - 443 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM TS
53	2.928061	192.168.100.96	192.168.100.44	TCP	54	443 - 49660 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
58	3.024679	192.168.100.44	192.168.100.96	TCP	74	36586 - 8080 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM TS
59	3.026724	192.168.100.96	192.168.100.44	TCP	54	8080 - 36586 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
71	4.296068	192.168.100.44	192.168.100.96	TCP	74	45596 - 80 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM TS
72	4.297738	192.168.100.96	192.168.100.44	TCP	54	80 - 45596 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
73	4.351518	192.168.100.44	192.168.100.96	TCP	74	49672 - 443 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM TS
74	4.354742	192.168.100.96	192.168.100.44	TCP	54	443 - 49672 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
79	4.464315	192.168.100.44	192.168.100.96	TCP	74	36602 - 8080 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM TS
80	4.467212	192.168.100.96	192.168.100.44	TCP	54	8080 - 36602 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
91	5.682367	192.168.100.44	192.168.100.96	TCP	74	45612 - 80 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM TS
92	5.684303	192.168.100.96	192.168.100.44	TCP	54	80 - 45612 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
94	5.734099	192.168.100.44	192.168.100.96	TCP	74	49680 - 443 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM TS
95	5.735691	192.168.100.96	192.168.100.44	TCP	54	443 - 49680 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
109	5.834087	192.168.100.44	192.168.100.96	TCP	74	36618 - 8080 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM TS
101	5.835757	192.168.100.96	192.168.100.44	TCP	54	8080 - 36610 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
112	7.061388	192.168.100.44	192.168.100.96	TCP	74	45614 - 80 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM TS
113	7.066621	192.168.100.96	192.168.100.44	TCP	54	80 - 45614 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
115	7.118495	192.168.100.44	192.168.100.96	TCP	74	49696 - 443 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM TS
116	7.120339	192.168.100.96	192.168.100.44	TCP	54	443 - 49696 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
121	7.226879	192.168.100.44	192.168.100.96	TCP	74	36620 - 8080 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM TS
122	7.228286	192.168.100.96	192.168.100.44	TCP	54	8080 - 36620 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
133	8.433545	192.168.100.44	192.168.100.96	TCP	74	45626 - 80 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM TS
135	8.435232	192.168.100.96	192.168.100.44	TCP	54	80 - 45626 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
136	8.486419	192.168.100.44	192.168.100.96	TCP	74	49698 - 443 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM TS
137	8.487870	192.168.100.96	192.168.100.44	TCP	54	443 - 49698 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
142	8.598127	192.168.100.44	192.168.100.96	TCP	74	36626 - 8080 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM TS
143	8.591948	192.168.100.96	192.168.100.44	TCP	54	8080 - 36626 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
154	Q.782102	192.168.100.44		TCP	74	45638 - 80 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM TS

es una captura de Wireshark filtrada para visualizar el **tráfico de puertos web (80, 443 y 8080)**.

Esta imagen muestra una **combinación de éxito y bloqueo** dependiendo de la dirección del tráfico, lo cual valida las reglas específicas de UFW del Servidor.

- **Servidor (192.168.100.96):** El firewall UFW funciona según lo esperado al **permitir** el tráfico entrante a estos puertos, ya que son servicios expuestos por el Servidor.
- **Cliente (192.168.100.44):** El firewall UFW también funciona correctamente al **rechazar activamente** (RST) el tráfico entrante a estos puertos, manteniendo el principio de **mínimo privilegio** (el Cliente no ofrece servicios web).



UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías

"VIGILADA MINEDUCACIÓN"



No.	Time	Source	Destination	Protocol	Length	Info
20	1. 317977	192.168.100.44	192.168.100.96	ICMP	98	Echo (ping) request id=0x1090, seq=1/256, ttl=64 (reply in
21	1. 319962	192.168.100.96	192.168.100.44	ICMP	98	Echo (ping) reply id=0x1098, seq=1/256, ttl=64 (request i
41	2. 766464	192.168.100.44	192.168.100.96	ICMP	98	Echo (ping) request id=0x10a6, seq=1/256, ttl=64 (reply in
42	2. 768971	192.168.100.96	192.168.100.44	ICMP	98	Echo (ping) reply id=0x10a6, seq=1/256, ttl=64 (request i
62	4. 170785	192.168.100.44	192.168.100.96	ICMP	98	Echo (ping) request id=0x10b4, seq=1/256, ttl=64 (reply in
63	4. 175463	192.168.100.96	192.168.100.44	ICMP	98	Echo (ping) reply id=0x10b4, seq=1/256, ttl=64 (request i
83	5. 590598	192.168.100.44	192.168.100.96	ICMP	98	Echo (ping) request id=0x10c2, seq=1/256, ttl=64 (reply in
84	5. 593060	192.168.100.96	192.168.100.44	ICMP	98	Echo (ping) reply id=0x10c2, seq=1/256, ttl=64 (request i
104	6. 958778	192.168.100.44	192.168.100.96	ICMP	98	Echo (ping) request id=0x10d0, seq=1/256, ttl=64 (reply in
105	6. 960078	192.168.100.96	192.168.100.44	ICMP	98	Echo (ping) reply id=0x10d0, seq=1/256, ttl=64 (request i
125	8. 340098	192.168.100.44	192.168.100.96	ICMP	98	Echo (ping) request id=0x10de, seq=1/256, ttl=64 (reply in
126	8. 341920	192.168.100.96	192.168.100.44	ICMP	98	Echo (ping) reply id=0x10de, seq=1/256, ttl=64 (request i
146	9. 696463	192.168.100.44	192.168.100.96	ICMP	98	Echo (ping) request id=0x10ec, seq=1/256, ttl=64 (reply in
147	9. 698436	192.168.100.96	192.168.100.44	ICMP	98	Echo (ping) reply id=0x10ec, seq=1/256, ttl=64 (request i
167	11. 050404	192.168.100.44	192.168.100.96	ICMP	98	Echo (ping) request id=0x10fa, seq=1/256, ttl=64 (reply in
168	11. 052238	192.168.100.96	192.168.100.44	ICMP	98	Echo (ping) reply id=0x10fa, seq=1/256, ttl=64 (request i
188	12. 453632	192.168.100.44	192.168.100.96	ICMP	98	Echo (ping) request id=0x1108, seq=1/256, ttl=64 (reply in
189	12. 455048	192.168.100.96	192.168.100.44	ICMP	98	Echo (ping) reply id=0x1108, seq=1/256, ttl=64 (request i
209	13. 794651	192.168.100.44	192.168.100.96	ICMP	98	Echo (ping) request id=0x1116, seq=1/256, ttl=64 (reply in
210	13. 796063	192.168.100.96	192.168.100.44	ICMP	98	Echo (ping) reply id=0x1116, seq=1/256, ttl=64 (request i
230	15. 139204	192.168.100.44	192.168.100.96	ICMP	98	Echo (ping) request id=0x1124, seq=1/256, ttl=64 (reply in
231	15. 140828	192.168.100.96	192.168.100.44	ICMP	98	Echo (ping) reply id=0x1124, seq=1/256, ttl=64 (request i
251	16. 521503	192.168.100.44	192.168.100.96	ICMP	98	Echo (ping) request id=0x1132, seq=1/256, ttl=64 (reply in
252	16. 523077	192.168.100.96	192.168.100.44	ICMP	98	Echo (ping) reply id=0x1132, seq=1/256, ttl=64 (request i
272	17. 919569	192.168.100.44	192.168.100.96	ICMP	98	Echo (ping) request id=0x1140, seq=1/256, ttl=64 (reply in
273	17. 921048	192.168.100.96	192.168.100.44	ICMP	98	Echo (ping) reply id=0x1140, seq=1/256, ttl=64 (request i
293	19. 288608	192.168.100.44	192.168.100.96	ICMP	98	Echo (ping) request id=0x114e, seq=1/256, ttl=64 (reply in
294	19. 299580	192.168.100.96	192.168.100.44	ICMP	98	Echo (ping) reply id=0x114e, seq=1/256, ttl=64 (request i
314	20. 633902	192.168.100.44	192.168.100.96	ICMP	98	Echo (ping) request id=0x115c, seq=1/256, ttl=64 (reply in
315	20. 637772	192.168.100.96	192.168.100.44	ICMP	98	Echo (ping) reply id=0x115c, seq=1/256, ttl=64 (request i
335	22. 000697	192.168.100.44	192.168.100.96	ICMP	98	Echo (ping) request id=0x116a, seq=1/256, ttl=64 (reply in
336	22. 002162	192.168.100.96	192.168.100.44	ICMP	98	Echo (ping) reply id=0x116a, seq=1/256, ttl=64 (request i
356	23. 383320	192.168.100.44	192.168.100.96	ICMP	98	Echo (ping) request id=0x1178, seq=1/256, ttl=64 (reply in
357	23. 385405	192.168.100.96	192.168.100.44	ICMP	98	Echo (ping) reply id=0x1178, seq=1/256, ttl=64 (request i
377	24. 751587	192.168.100.44	192.168.100.96	ICMP	98	Echo (ping) request id=0x1186, seq=1/256, ttl=64 (reply in
378	24. 753579	192.168.100.96	192.168.100.44	ICMP	98	Echo (ping) reply id=0x1186, seq=1/256, ttl=64 (request i
398	26. 162896	192.168.100.44	192.168.100.96	ICMP	98	Echo (ping) request id=0x1194, seq=1/256, ttl=64 (reply in
399	26. 166507	192.168.100.96	192.168.100.44	ICMP	98	Echo (ping) reply id=0x1194, seq=1/256, ttl=64 (request i
419	27. 510019	192.168.100.44	192.168.100.96	ICMP	98	Echo (ping) request id=0x11a2, seq=1/256, ttl=64 (reply in
420	27. 511464	192.168.100.96	192.168.100.44	ICMP	98	Echo (ping) reply id=0x11a2, seq=1/256, ttl=64 (request i
440	28. 835405	192.168.100.44	192.168.100.96	ICMP	98	Echo (ping) request id=0x11b0, seq=1/256, ttl=64 (reply in
441	28. 837364	192.168.100.96	192.168.100.44	ICMP	98	Echo (ping) reply id=0x11b0, seq=1/256, ttl=64 (request i
461	30. 1199076	192.168.100.44	192.168.100.96	ICMP	98	Echo (ping) request id=0x11b6, seq=1/256, ttl=64 (reply in

es una captura de Wireshark filtrada para visualizar **solo el tráfico ICMP** (Internet Control Message Protocol).

Esta imagen es la **evidencia de conectividad básica** y confirma que la comunicación Ping entre el Cliente y el Servidor funciona perfectamente.

- **Comprobación de Regla:** Se confirma que el **ICMP (Ping)** está permitido. Esto es el comportamiento esperado, ya que UFW suele permitir ICMP por defecto, o la regla ufw allow from 192.168.100.0/24 cubre esta comunicación interna.
- **Comportamiento:** La presencia de las respuestas (reply) a cada solicitud (request) demuestra que no hay *firewall* activo bloqueando el tráfico ICMP en la dirección entrante.

Por una universidad con calidad, moderna e incluyente

Carrera 6^a. No. 76-103 Montería NIT. 891080031-3 - Teléfono: 7860300 - 7860920 www.unicordoba.edu.co



“VIGILADA MINEDUCACIÓN”

UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.100.44	192.168.100.96	TCP	74	47522 - 22 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM TS
3	0.005769	192.168.100.44	192.168.100.96	TCP	66	47522 - 22 [ACK] Seq=1 Ack=1 Win=64512 Len=0 Tsv=235235514
4	0.007078	192.168.100.44	192.168.100.96	SSH	67	Client: Encrypted packet (len=1)
5	0.007526	192.168.100.44	192.168.100.96	TCP	66	47522 - 22 [FIN, ACK] Seq=2 Ack=1 Win=64512 Len=0 Tsv=2352
7	0.040038	192.168.100.44	192.168.100.96	TCP	74	57280 - 80 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM TS
10	0.091677	192.168.100.44	192.168.100.96	TCP	74	42312 - 443 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM TS
13	0.127964	192.168.100.44	192.168.100.96	TCP	54	47522 - 22 [RST] Seq=3 Win=0 Len=0
14	0.148326	192.168.100.44	192.168.100.96	TCP	74	55944 - 3306 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM TS
16	0.189419	192.168.100.44	192.168.100.96	TCP	74	57938 - 8080 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM TS
18	0.238939	192.168.100.44	192.168.100.96	TCP	74	36836 - 3389 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM TS
20	1.317977	192.168.100.44	192.168.100.96	ICMP	98	Echo (ping) request id=0x1098, seq=1/256, ttl=64 (reply in
22	1.382351	192.168.100.44	192.168.100.96	TCP	74	47526 - 22 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM TS
24	1.385714	192.168.100.44	192.168.100.96	TCP	66	47526 - 22 [ACK] Seq=1 Ack=1 Win=64512 Len=0 Tsv=235235652
25	1.386567	192.168.100.44	192.168.100.96	SSH	67	Client: Encrypted packet (len=1)
26	1.387458	192.168.100.44	192.168.100.96	TCP	66	47526 - 22 [FIN, ACK] Seq=2 Ack=1 Win=64512 Len=0 Tsv=2352
28	1.439385	192.168.100.44	192.168.100.96	TCP	74	57286 - 80 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM TS
31	1.498323	192.168.100.44	192.168.100.96	TCP	74	42314 - 443 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM TS
34	1.526333	192.168.100.44	192.168.100.96	TCP	54	47526 - 22 [RST] Seq=3 Win=0 Len=0
35	1.549402	192.168.100.44	192.168.100.96	TCP	74	55954 - 3306 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM TS
37	1.606087	192.168.100.44	192.168.100.96	TCP	74	57942 - 8080 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM TS
39	1.672436	192.168.100.44	192.168.100.96	TCP	74	36844 - 3389 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM TS
41	2.766464	192.168.100.44	192.168.100.96	ICMP	98	Echo (ping) request id=0x10a6, seq=1/256, ttl=64 (reply in
43	2.827569	192.168.100.44	192.168.100.96	TCP	74	66826 - 22 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM TS
45	2.829594	192.168.100.44	192.168.100.96	TCP	66	66826 - 22 [ACK] Seq=1 Ack=1 Win=64512 Len=0 Tsv=235235796
46	2.830286	192.168.100.44	192.168.100.96	SSH	67	Client: Encrypted packet (len=1)
47	2.830569	192.168.100.44	192.168.100.96	TCP	66	66826 - 22 [FIN, ACK] Seq=2 Ack=1 Win=64512 Len=0 Tsv=2352
49	2.872672	192.168.100.44	192.168.100.96	TCP	74	45592 - 80 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM TS
52	2.924645	192.168.100.44	192.168.100.96	TCP	74	49669 - 443 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM TS
55	2.946450	192.168.100.44	192.168.100.96	TCP	54	60826 - 22 [RST] Seq=3 Win=0 Len=0
56	2.977618	192.168.100.44	192.168.100.96	TCP	74	43926 - 3306 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM TS
58	3.024679	192.168.100.44	192.168.100.96	TCP	74	36586 - 8080 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM TS
60	3.079266	192.168.100.44	192.168.100.96	TCP	74	43578 - 3389 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM TS
62	4.170785	192.168.100.44	192.168.100.96	ICMP	98	Echo (ping) request id=0x10b4, seq=1/256, ttl=64 (reply in
64	4.242691	192.168.100.44	192.168.100.96	TCP	74	66834 - 22 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM TS
66	4.245576	192.168.100.44	192.168.100.96	TCP	66	66834 - 22 [ACK] Seq=1 Ack=1 Win=64512 Len=0 Tsv=235235938
67	4.246636	192.168.100.44	192.168.100.96	SSH	67	Client: Encrypted packet (len=1)
68	4.246845	192.168.100.44	192.168.100.96	TCP	66	66834 - 22 [FIN, ACK] Seq=2 Ack=1 Win=64512 Len=0 Tsv=2352
71	4.296068	192.168.100.44	192.168.100.96	TCP	74	45596 - 80 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM TS
73	4.351510	192.168.100.44	192.168.100.96	TCP	74	49672 - 443 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM TS
76	4.392175	192.168.100.44	192.168.100.96	TCP	54	60834 - 22 [RST] Seq=3 Win=0 Len=0
77	4.408560	192.168.100.44	192.168.100.96	TCP	74	43926 - 3306 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM TS
79	4.464315	192.168.100.44	192.168.100.96	TCP	74	36602 - 8080 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM TS
81	4.526237	192.168.100.44	192.168.100.96	TCP	74	43588 - 3389 [SYN] Seq=0 Win=64492 Len=0 MSS=1402 SACK_PERM TS

Es la **Vista General Holística** del tráfico entre el Cliente y el Servidor en Wireshark, filtrada para mostrar todo el tráfico bidireccional.

Esta imagen es el **resumen visual definitivo** del comportamiento del *firewall* UFW, combinando éxito (verde/azul) y rechazo (rojo) en una sola captura.

Esta imagen demuestra que la **Defensa en Profundidad** y el principio de **Mínimo Privilegio** fueron aplicados con éxito. El UFW permite solo los servicios esenciales (SSH, ICMP) y aquellos explícitamente requeridos (HTTP/S en el Servidor), mientras que rechaza activamente el resto del tráfico (MySQL, RDP) enviando paquetes RST.

Por una universidad con calidad, moderna e incluyente

Carrera 6^a. No. 76-103 Montería NIT. 891080031-3 - Teléfono: 7860300 - 7860920 www.unicordoba.edu.co



UNIVERSIDAD DE CÓRDOBA

CONFIGURACIÓN DE REDES LOCALES

Comité de Acreditación y Currículo Facultad de Ingenierías

"VIGILADA MINEDUCACIÓN"



10. CONCLUSIONES.

La implementación del laboratorio permitió comprender de manera práctica el funcionamiento de un firewall dentro de un entorno controlado basado en tecnologías de virtualización y servicios en la nube. A través del uso de VirtualBox, se construyó la infraestructura necesaria para desplegar Debian como sistema operativo base y, posteriormente, instalar OpenStack mediante DevStack. Esto facilitó la creación de redes, subredes, routers e instancias, permitiendo simular una topología realista.

El proceso de configuración del firewall permitió aplicar reglas de filtrado y observar su efecto directo sobre el tráfico, lo cual fue validado mediante capturas con Wireshark. Este análisis demostró la correcta aplicación de políticas de seguridad, evidenciando el bloqueo y la autorización de paquetes según las reglas establecidas.

En general, el laboratorio fortaleció conocimientos en virtualización, administración de redes, seguridad informática y despliegue de plataformas cloud. Además, permitió integrar teoría y práctica, brindando una visión clara sobre cómo se implementan y gestionan infraestructuras reales orientadas a la protección y segmentación del tráfico de red.

11. REFERENCIAS

OpenStack Foundation. (2025). *DevStack: OpenStack in a Box*. Disponible en: <https://opendev.org/openstack/devstack>

Oracle Corporation. (2025). *Oracle VM VirtualBox User Manual*. Disponible en: <https://www.virtualbox.org>

Debian Project. (2025). *Debian GNU/Linux Documentation*. Disponible en: <https://www.debian.org/doc/>

Wireshark Foundation. (2025). *Wireshark User Guide*. Disponible en: <https://www.wireshark.org/docs/>

MicroStack. (2025). *Install OpenStack using MicroStack*. Disponible en: <https://microstack.run>

Red Hat. (2024). *Concepts of Firewalls and Network Security*.

Cisco Systems. (2024). *Network Security Fundamentals: Firewalls and Packet Filtering*.