



Actividad [#3] - [Actividad 3. Firewall]

[Sistemas Operativos II]

Ingeniería en Desarrollo de Software

Tutor: Marco Alonso Rodríguez

Alumno: Alan David López Rojas

Fecha:06/06/2022



Índice

Investigación.....	pág. 3
Capturas de pantalla.....	pág. 7
Conclusión.....	pág. 29
Bibliografía.....	pág. 30



Investigación

¿Cuál es la principal función del firewall?

Un firewall es un elemento de hardware o software utilizado en una red de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de red que haya definido la organización responsable de la red. Su modo de funcionar es indicado por la recomendación RFC 2979, que define las características de comportamiento y requerimientos de interoperabilidad. La ubicación habitual de un cortafuegos es el punto de conexión de la red interna de la organización con la red exterior, que normalmente es Internet; de este modo se protege la red interna de intentos de acceso no autorizados desde Internet, que puedan aprovechar vulnerabilidades de los sistemas de la red interna.

La función principal de un firewall o corta fuego es bloquear cualquier intento de acceso no autorizado a dispositivos internos privados de nuestra red de datos (LAN) desde las conexiones externas de internet comúnmente llamado WAN.

Un firewall o cortafuegos proporciona un modo de filtrar la información que se comunica a través de la conexión de red. Cuando están presentes en un equipo individual, se denomina un firewall personal. Cuando los firewalls están presentes en una red empresarial para la protección de múltiples equipos se denomina Firewall de red.

Los Firewalls permiten o bloquean la comunicación entre equipos basados en reglas. Cada regla define un determinado patrón de tráfico de red y la acción a realizar cuando se detecta. Estas reglas personalizables proporcionan control y fluidez sobre el uso de la red.

Un firewall puede ser un programa software o dispositivo hardware. El sistema operativo Windows o Linux Firewall, son ejemplos de firewalls de software. ZyXEL ZyWALL USG o SonicWall TZ firewall son ejemplos de firewall de hardware

¿Cuáles son los tipos de firewall que existen?

Los Firewall tradicionales son de hardware, es decir, un dispositivo específico instalado en una red para levantar una defensa y proteger a la red del exterior. Son utilizados en entornos profesionales: el administrador de red define una serie de reglas para permitir el acceso y detiene los intentos de conexión no permitidos.

Los Firewall personales son programas que filtran el tráfico que entra y sale de una computadora. Una vez instalados, el usuario debe definir el nivel de seguridad: permite o deniega el acceso de determinados programas a Internet (de forma temporal o definitiva) y autoriza o no los accesos desde el exterior.

Firewalls hardware

Los firewall de hardware se utilizan más en empresas y grandes corporaciones. Normalmente son dispositivos que se colocan entre el router y la conexión telefónica. Como ventajas, podemos destacar que, al ser independientes del PC, no es necesario configurarlos cada vez que reinstalamos el sistema operativo y no consumen recursos del sistema.

Su mayor inconveniente es el mantenimiento, ya que son difíciles de actualizar y de configurar correctamente.

Los firewalls hardware pueden ser adquiridos como un producto independiente pero recientemente los firewalls hardware suelen encontrarse integrados en routers de banda ancha y deberían ser considerados

una parte importante de cara a la configuración de una red, especialmente cuando se usa una conexión de banda ancha.

Los firewalls hardware usan filtrado de paquetes para examinar la cabecera de un paquete y así determinar su origen y su destino. Esta información se compara con un conjunto de reglas predefinidas o creadas por el usuario que determinan si el paquete tiene que ser redirigido o descartado.

Entre los principales fabricantes de firewalls hardware destacan Checkpoint y Cisco.

Firewalls software

Estos programas son los más comunes en los hogares, ya que, aparte de resultar mucho más económicos que el hardware, su instalación y actualización es más sencilla. Eso sí, presentan algunos problemas inherentes a su condición: consumen recursos del PC, algunas veces no se ejecutan correctamente o pueden ocasionar errores de compatibilidad con otro software instalado

Al igual que ocurre con los firewalls hardware, hay un gran número de firewalls software en el mercado. Debido a que el firewall software debe estar siempre ejecutándose en cada ordenador, debería tenerse en cuenta los recursos que necesita para ejecutarse y también es importante comprobar que no haya ninguna incompatibilidad de cara a la elección del firewall software. Un buen firewall software se ejecutará en segundo plano en el sistema y usará sólo una pequeña parte de los recursos del mismo. Es importante monitorizar el firewall software una vez instalado y descargar e instalar las actualizaciones disponibles periódicamente.

Para los usuarios “normales”, la mejor opción de firewalls es un firewall software. Los firewalls software se instalan en el ordenador (como cualquier otro programa) y pueden ser configurados de diversas maneras, permitiendo cierto control sobre su funcionalidad y sus características de protección. Los firewalls software protegen el ordenador ante ataques externos que intentan obtener el control de la máquina o conseguir acceso a la misma y, dependiendo del programa de firewall, puede también proporcionar protección contra los virus, troyanos y gusanos más comunes. Muchos firewalls software tienen controles definidos por el usuario para establecer una compartición segura de archivos e impresoras y para bloquear aplicaciones no seguras e impedir que se ejecuten en el sistema.

¿Cómo funciona un firewall?

Cuando alguien en Internet o en una red intenta conectarse a un equipo, ese intento se conoce como “solicitud no solicitada”. Cuando el equipo recibe una solicitud no solicitada, Firewall bloquea la conexión. Si utiliza un programa, por ejemplo, de mensajería instantánea o un juego de red con varios jugadores, que tiene que recibir información desde Internet o de una red, el servidor de seguridad le pregunta si desea bloquear o desbloquear (permitir) la conexión.

Si elige desbloquear la conexión, Firewall de Windows crea una excepción de modo que el servidor de seguridad no se interpondrá cuando ese programa tenga que recibir información en el futuro.

Qué hace y qué no hace

- Ayuda a evitar que virus y gusanos informáticos lleguen a un equipo.
- Pide el permiso del usuario para bloquear o desbloquear ciertas solicitudes de conexión.
- Crea un registro de seguridad, si desea tener uno, que almacene los intentos correctos y fallidos de conectarse a un equipo. Esto puede ser de utilidad como herramienta de solución de problemas.

- No detecta o deshabilita los virus y gusanos informáticos si ya se encuentran en el equipo. Por ese motivo, debería instalar también software antivirus y mantenerlo actualizado para ayudar a impedir que virus, gusanos y otras amenazas para la seguridad dañen el equipo o lo usen para propagarse.
- No impide que el usuario abra correo electrónico con archivos adjuntos peligrosos. No abra archivos adjuntos de correo electrónico que provenga de remitentes que no conozca. Incluso aunque conozca y confíe en el origen del mensaje, debe actuar con precaución. Si alguien a quien conoce le envía un archivo adjunto en el correo electrónico, observe la línea de asunto cuidadosamente antes de abrirlo. Si la línea de asunto parece un galimatías o no tiene sentido para usted, consulte al remitente antes de abrirlo.
- No impide que el correo no solicitado o spam aparezca en la bandeja de entrada. Sin embargo, algunos programas de correo electrónico pueden servir de ayuda en ese propósito.

¿Qué es UFW y cuál es su función?

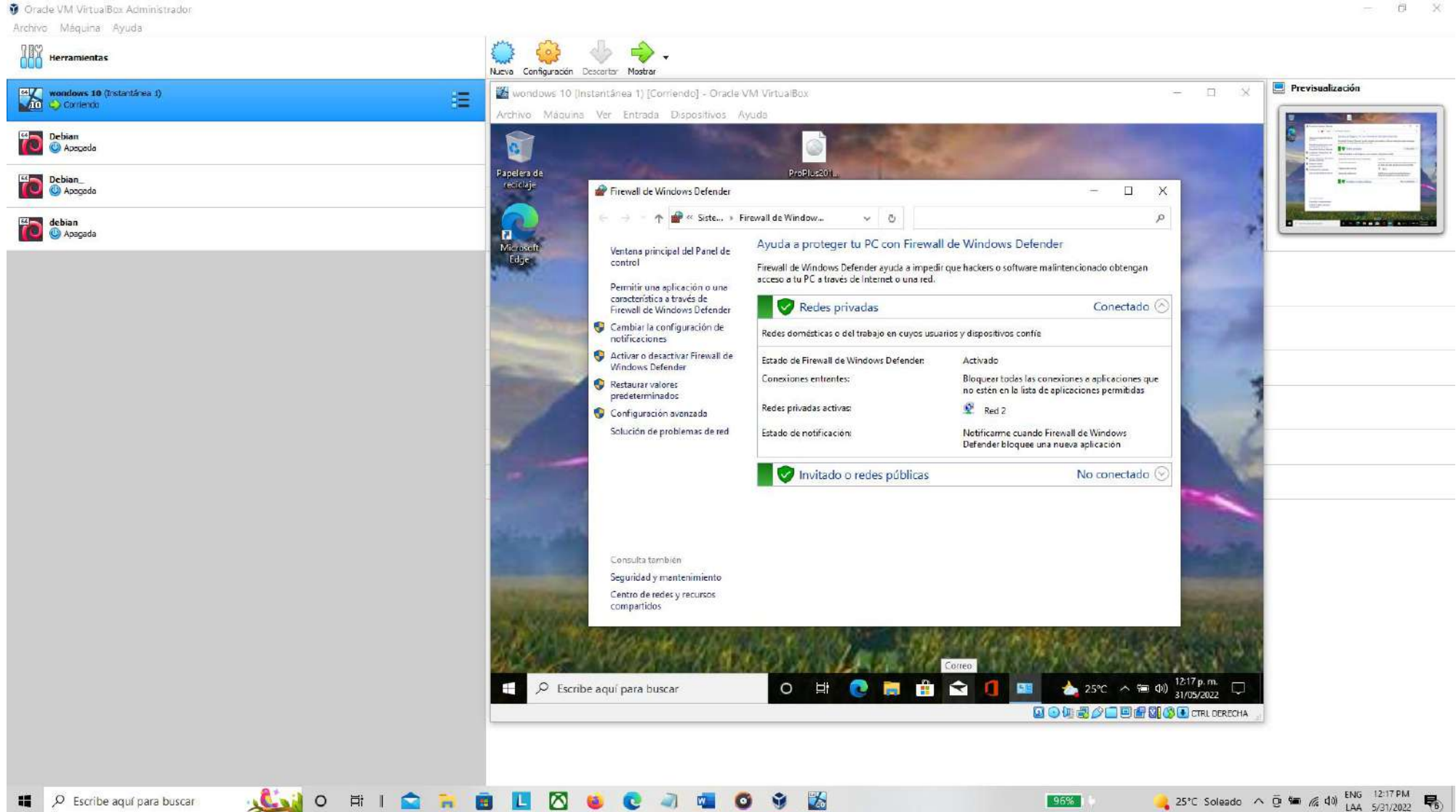
Las siglas "UFW" significan "Uncomplicated Firewall" y hacen referencia a una aplicación que tiene como objetivo establecer reglas en "iptables", las tablas de firewall nativas en Linux. Puesto que iptables tiene una sintaxis relativamente compleja, utilizar UFW para realizar su configuración es una alternativa útil sin escatimar en seguridad.

Este cortafuegos es totalmente gratuito, de código abierto y está escrito en Python. Viene por defecto en Ubuntu desde la versión 8.04 LTS, y muchas distros han decidido añadirlo igualmente por defecto debido a su utilidad.

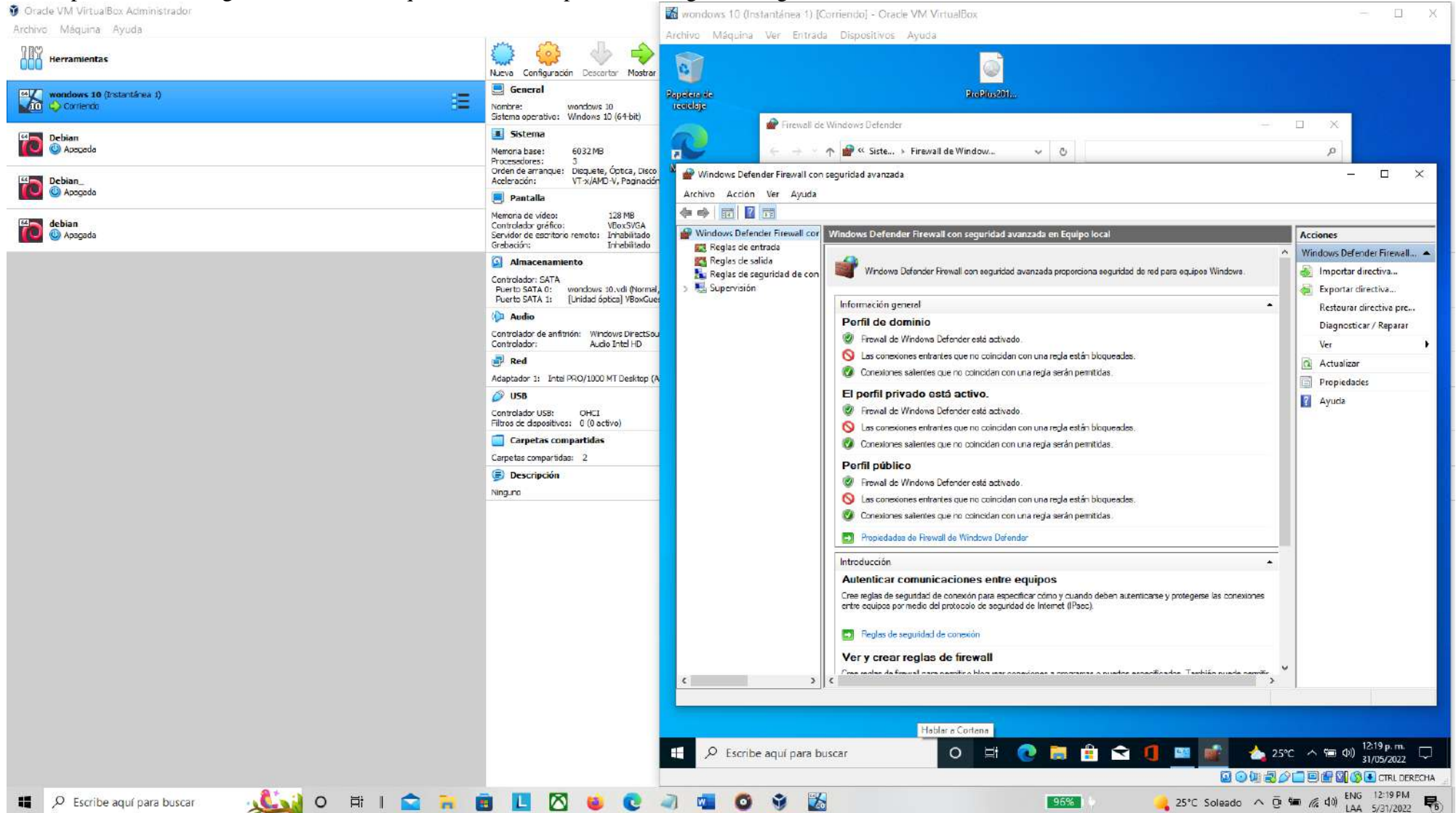
UFW o Uncomplicated Firewall es una interfaz para iptables orientada a simplificar el proceso de configuración de un firewall. Aunque iptables es una herramienta sólida y flexible, puede resultar difícil para los principiantes aprender a usarlo para configurar correctamente un firewall. Si se desea comenzar a proteger la de uso red, UFW puede ser la mejor opción.

Capturas de pantalla Firewall Windows

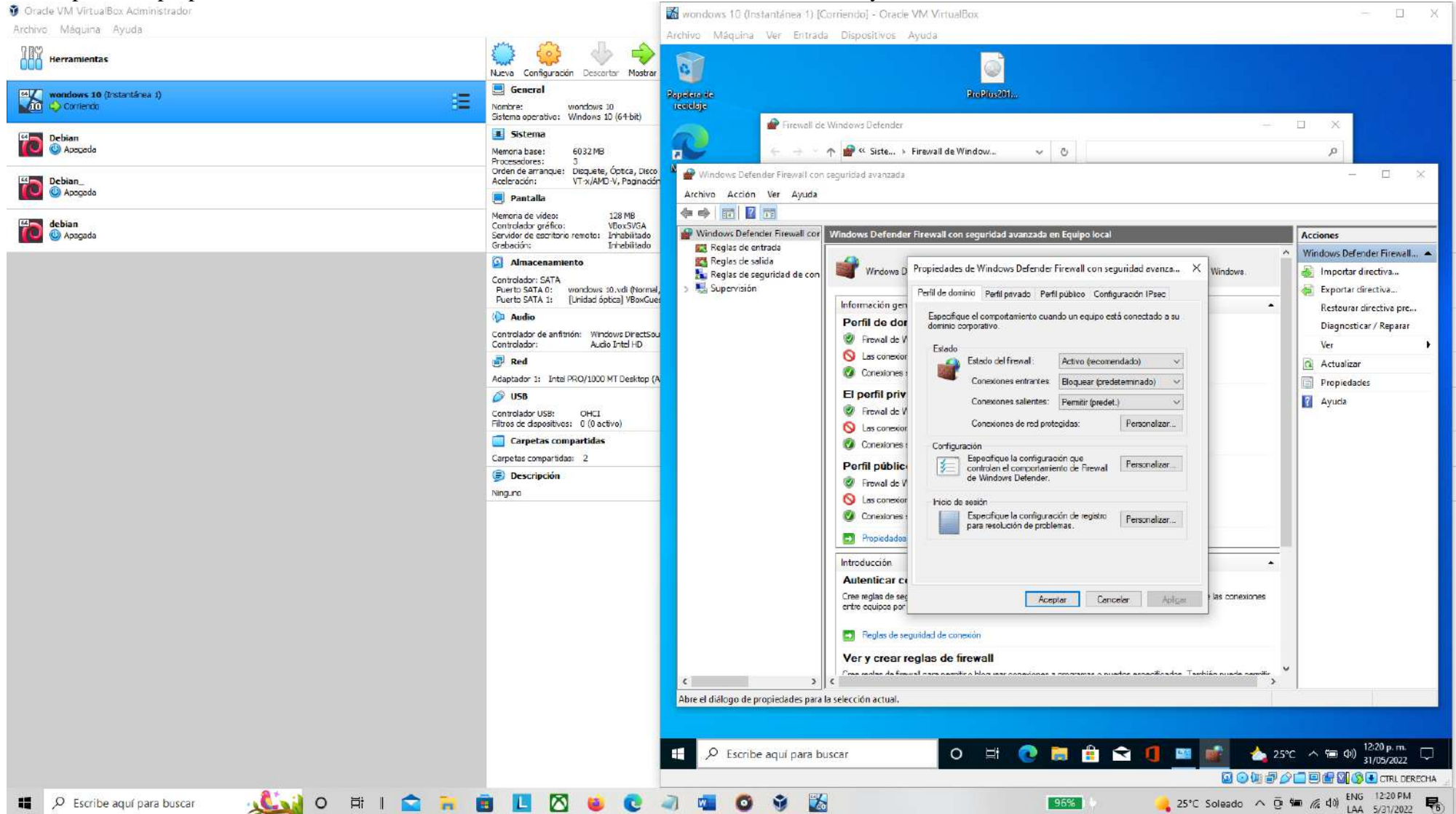
El primer paso fue ingresar a la configuración de Windows y después a firewall de Windows que se muestra enseguida.



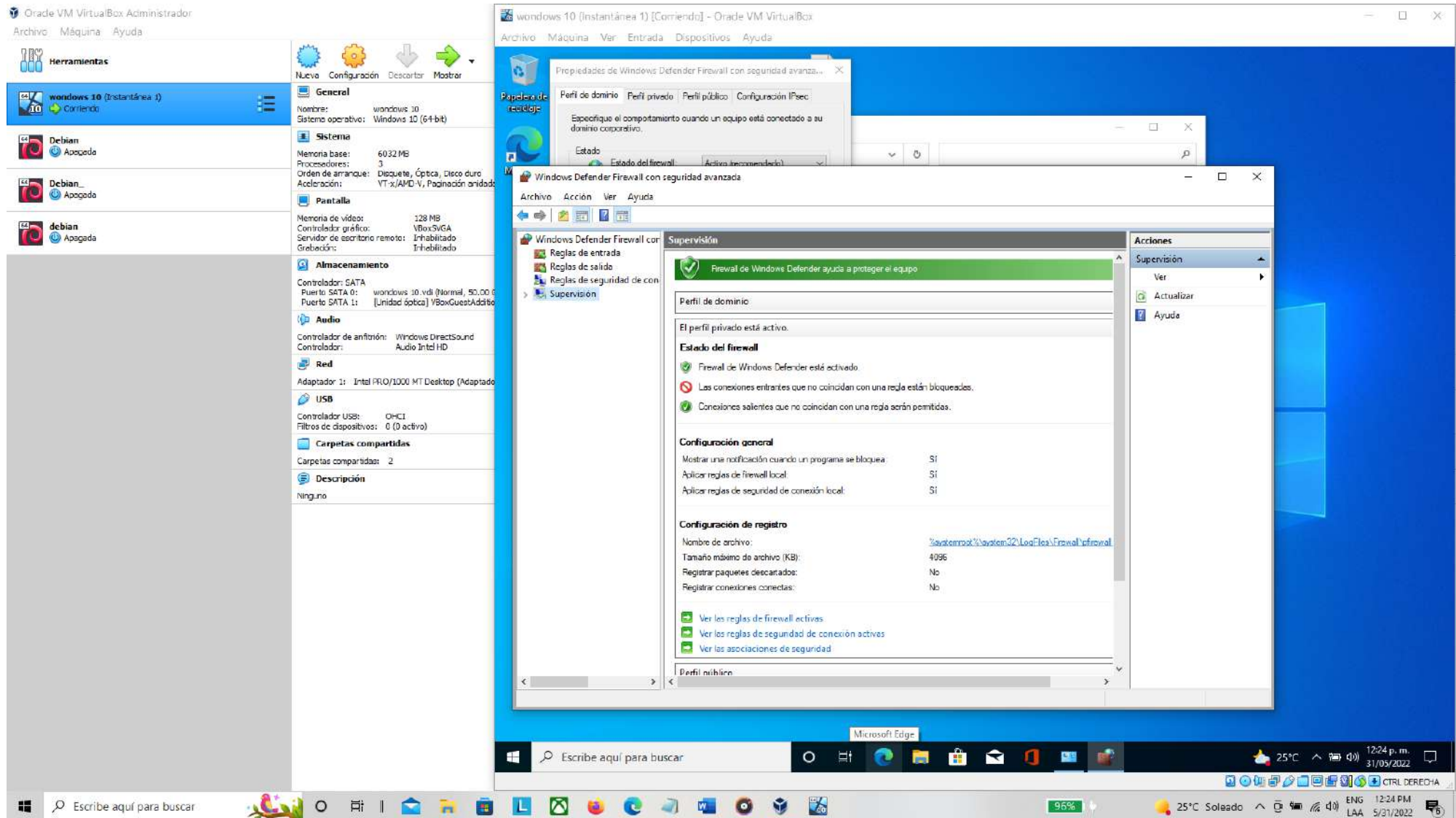
En el apartado de configuración avanzada que muestra las opciones de reglas de seguridad



En la opción de propiedades de Windows defender firewall se muestra el estado del firewall y su funcionamiento en las redes



En la sección de supervisión dentro de las mismas opciones avanzadas se encuentra la lista de las reglas que están registradas en el firewall y si se encuentran activas o inhabilitadas como se muestra en las dos capturas siguientes.



Oracle VM VirtualBox Administrador

Archivo Máquina Ayuda

Herramientas

Nuevo Configuración Descartar Mostrar

windows 10 (Instantánea 1) Corriendo

Debian Apagado

Debian Apagado

debian Apagado

General

Nombre: windows 10
Sistema operativo: Windows 10 (64-bit)

Sistema

Memoria base: 6032 MB
Procesadores: 3
Orden de arranque: Disco duro
Aceleración: VT-x/AMD-V, Paginación anidada

Pantalla

Memoria de vídeo: 128 MB
Controlador gráfico: VBoxSVGA
Servidor de escritorio remoto: I-habilitado
Grabación: I-habilitado

Almacenamiento

Controlador: SATA
Puerto SATA 0: windows 10.vdi (Normal, 50,00 GB)
Puerto SATA 1: [Unidad óptica] VBoxGuestAdditions

Audio

Controlador de sonido: Windows DirectSound
Controlador: Audio Intel HD

Red

Adaptador 1: Intel PRO/1000 MT Desktop (Adaptado)

USB

Controlador USB: OHCI
Filtros de dispositivos: 0 (0 activo)

Carpetas compartidas

Carpetas compartidas: 2

Descripción

Ninguno

windows 10 (Instantánea 1) [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Var Entrada Dispositivos Ayuda

Propiedades de Windows Defender Firewall con seguridad avanzada

Perfil de dominio Perfil privado Perfil público Configuración IPsec

Especifique el comportamiento cuando un equipo está conectado a su dominio corporativo.

Estado Estado del firewall Activo (recomendado)

Windows Defender Firewall con seguridad avanzada

Archivo Acción Ver Ayuda

Windows Defender Firewall con seguridad avanzada

Reglas de entrada

Nombre	Grupo	Perfil	Habilitado	Acción
Microsoft Lync		Privado	Sí	Permit
Microsoft Lync		Privado	Sí	Permit
Microsoft Lync Ucmapi		Privado	Sí	Permit
Microsoft Lync Ucmapi		Privado	Sí	Permit
Microsoft Office Outlook		Privado	Sí	Permit
@FirewallAPI.dll - 80201	@FirewallAPI.dll - 80200	Todo	Sí	Permit
@FirewallAPI.dll - 80206	@FirewallAPI.dll - 80200	Todo	Sí	Permit
Administración de tarjetas inteligentes vi...	Administración de tarjetas i...	Priva...	No	Permit
Administración de tarjetas inteligentes vi...	Administración de tarjetas i...	Dom...	No	Permit
Administración de tarjetas inteligentes vi...	Administración de tarjetas i...	Priva...	No	Permit
Administración de tarjetas inteligentes vi...	Administración de tarjetas i...	Dom...	No	Permit
Administración remota de Firewall de Wi...	Administración remota de F...	Priva...	No	Permit
Administración remota de Firewall de Wi...	Administración remota de F...	Dom...	No	Permit
Administración remota de Firewall de Wi...	Administración remota de F...	Priva...	No	Permit
Administración remota de Firewall de Wi...	Administración remota de F...	Dom...	No	Permit
Administración remota de registro de ev...	Administración remota de t...	Dom...	No	Permit
Administración remota de registro de ev...	Administración remota de t...	Priva...	No	Permit
Administración remota de registro de ev...	Administración remota de t...	Dom...	No	Permit
Administración remota de registro de ev...	Administración remota de t...	Priva...	No	Permit
Administración remota de registro de ev...	Administración remota de t...	Dom...	No	Permit
Administración remota de registro de ev...	Administración remota de t...	Priva...	No	Permit
Administración remota de servicios (NP...	Administración remota de s...	Dom...	No	Permit
Administración remota de servicios (NP...	Administración remota de s...	Priva...	No	Permit
Administración remota de servicios (RPC)	Administración remota de s...	Dom...	No	Permit
Administración remota de servicios (RPC)	Administración remota de s...	Priva...	No	Permit
Administración remota de servicios (RPC)	Administración remota de s...	Priva...	No	Permit
Administración remota de servicios (RPC)	Administración remota de s...	Dom...	No	Permit
Administración remota de tareas progra...	Administración remota de t...	Dom...	No	Permit

Acciones

Reglas de entrada

Nueva regla...

Filtrar por perfil

Filtrar por estado

Filtrar por grupo

Ver

Actualizar

Exportar lista...

Ayuda

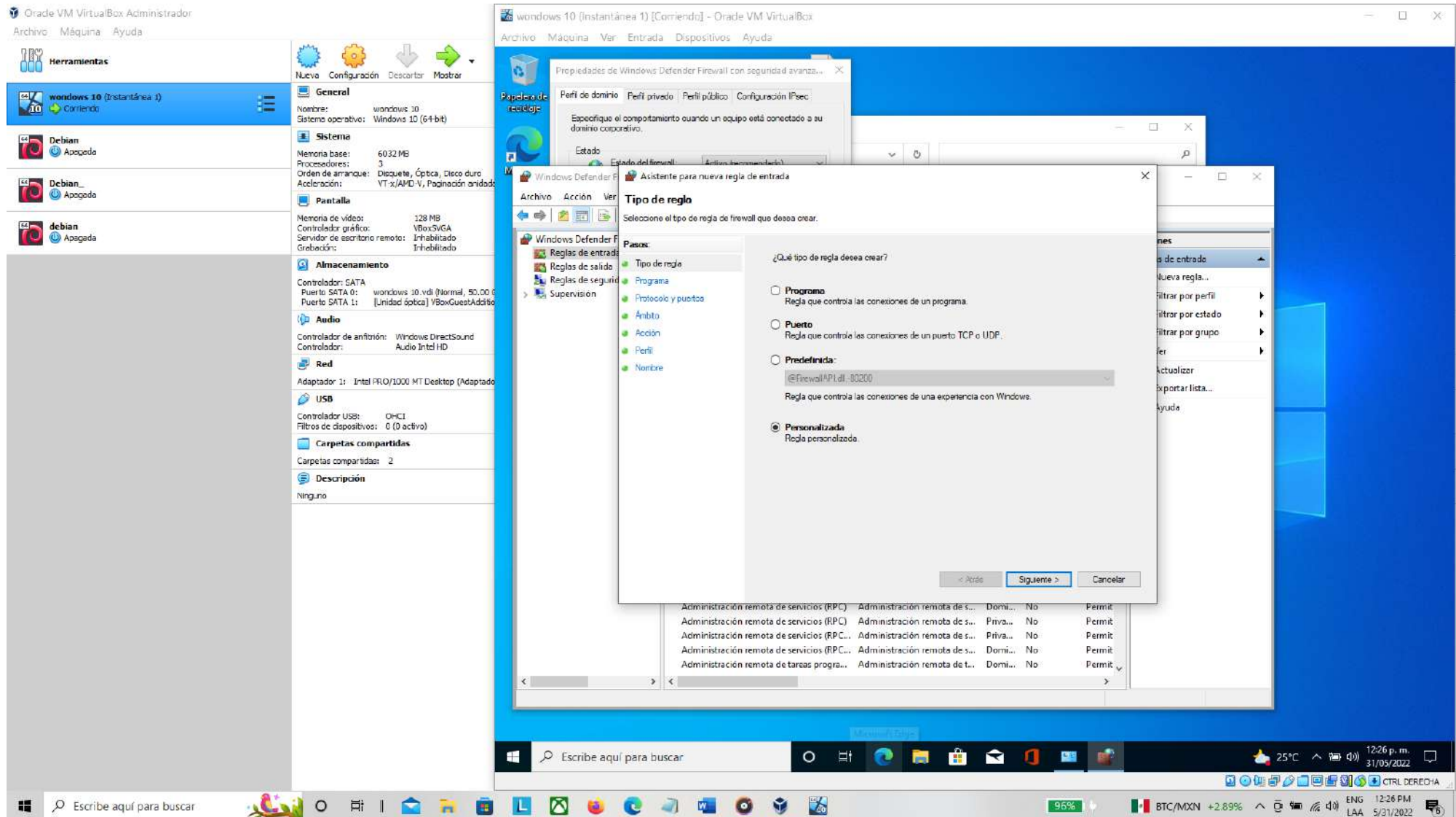
Vista de tareas

Escribe aquí para buscar

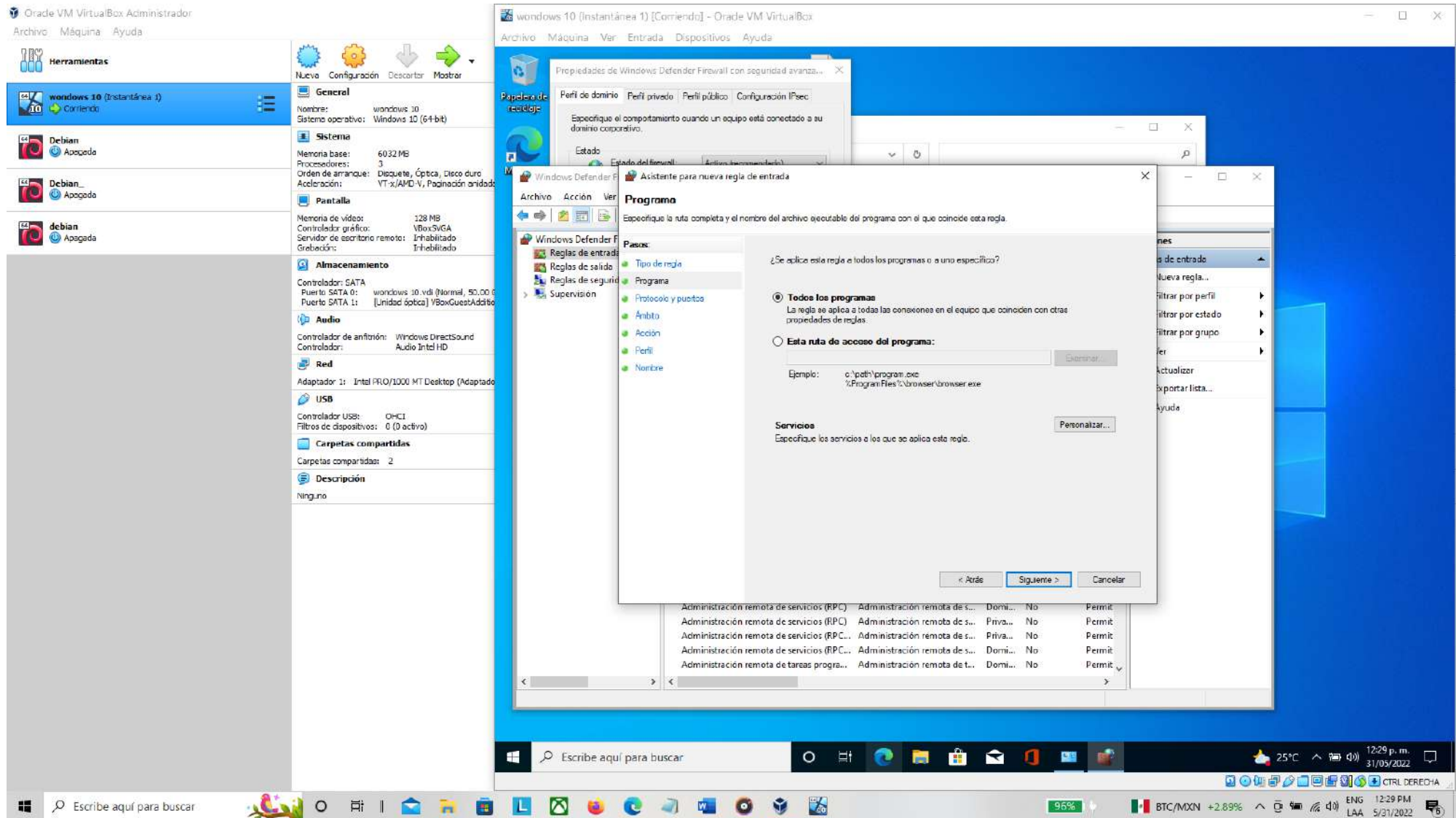
25°C 12:25 p. m. 31/05/2022

ENG LAA 5/31/2022

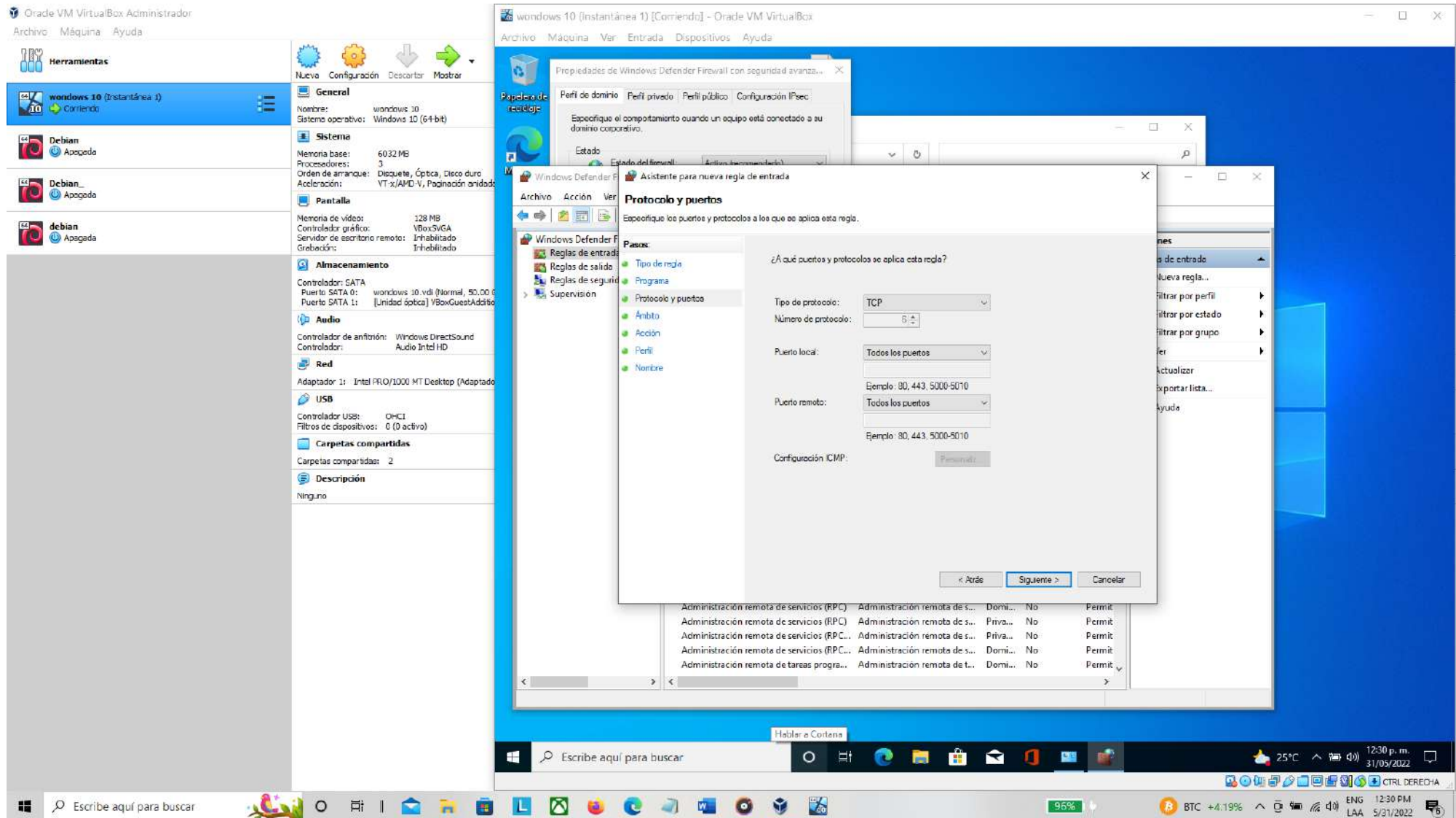
Se va a crear una regla nueva como lo pide la actividad para eso se da clic en la opción “Nueva regla” que esta de lado derecho, y en la siguiente ventana se elige el tipo de regla que se creara, en este caso personalizada.



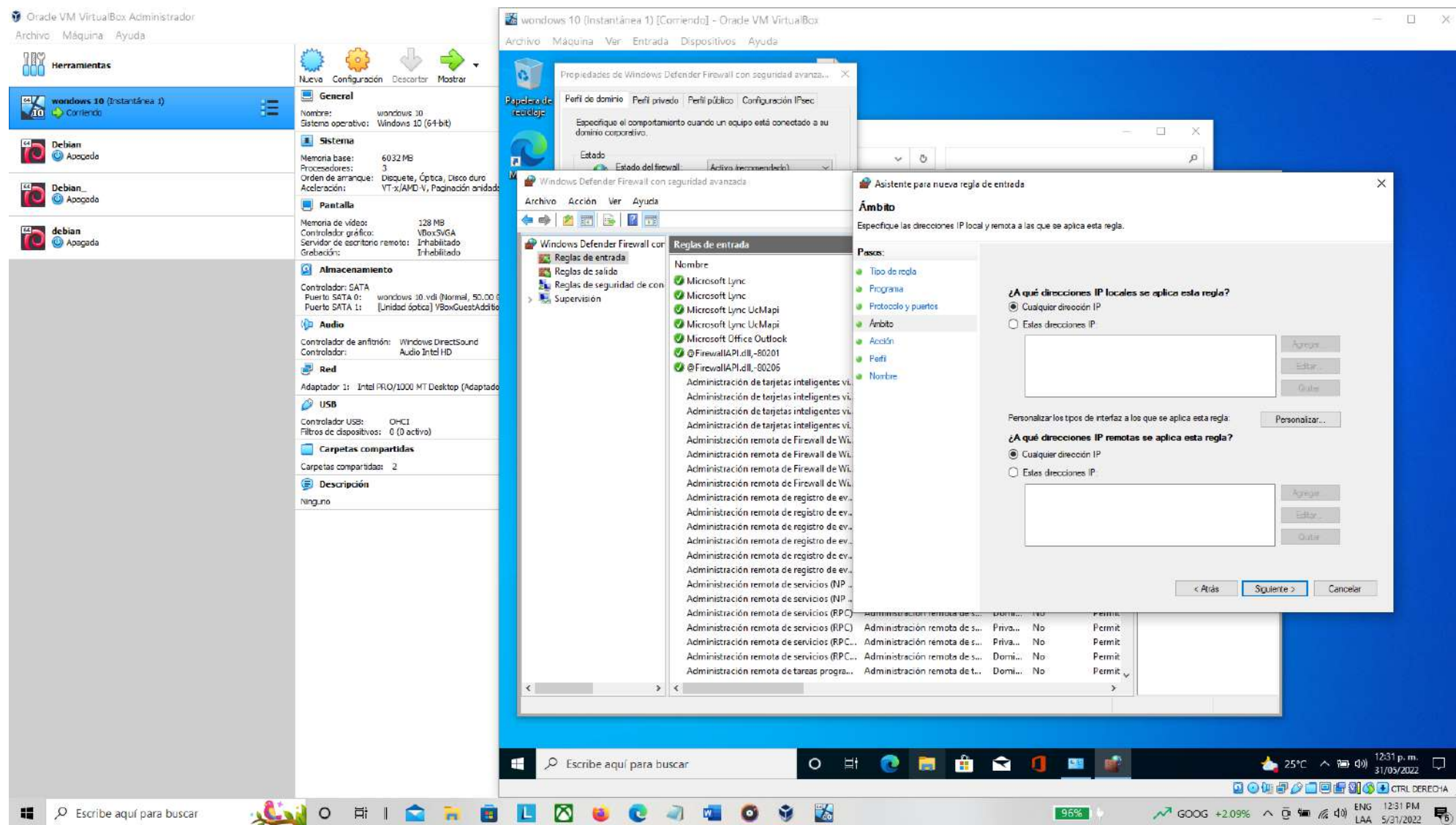
Una vez elegido el tipo de regla a crear la siguiente ventana muestra a que programa o programas se aplicara esta nueva regla, se escoge la opción a todos los programas.



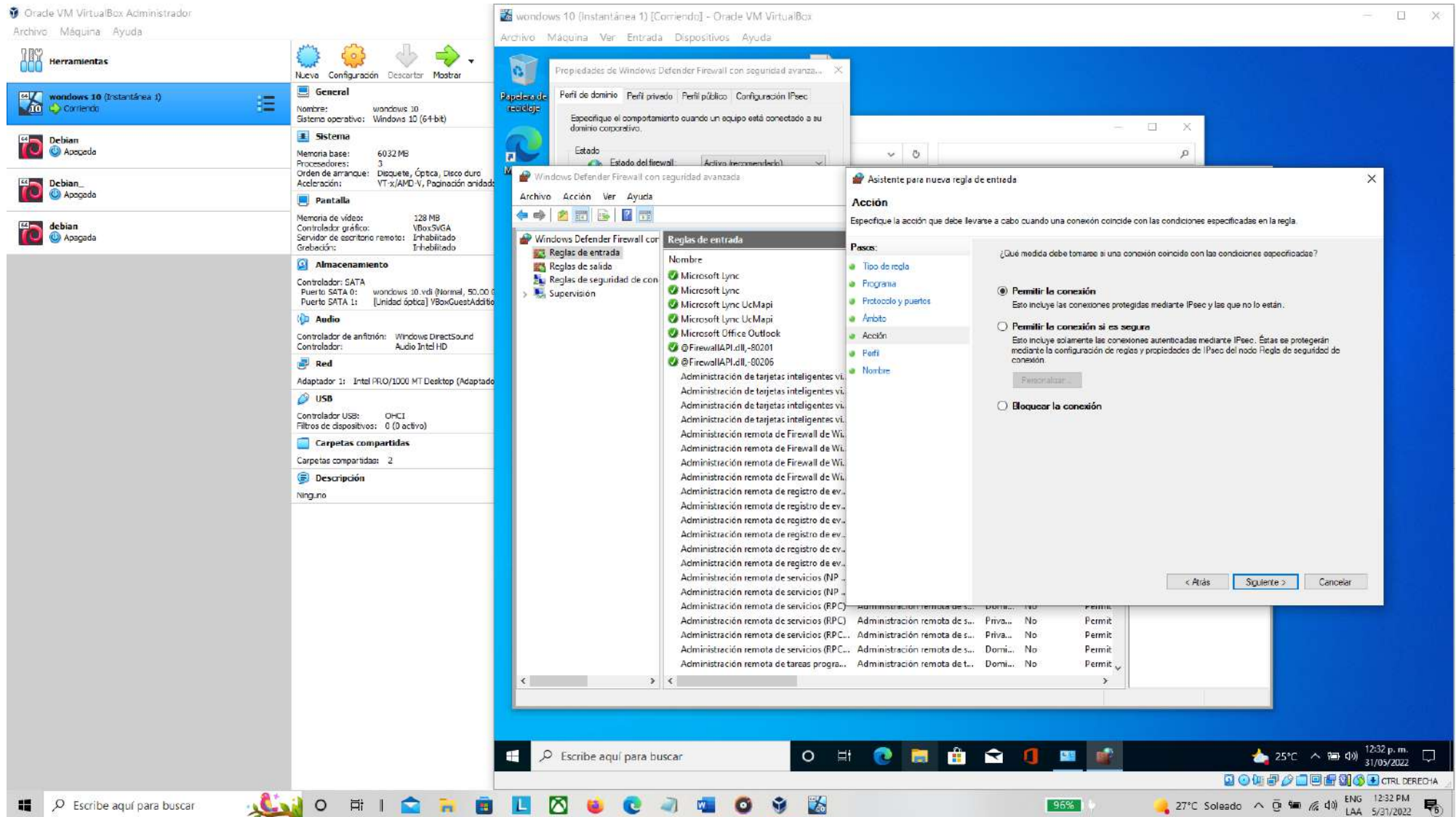
En la siguiente ventana se especificará que tipo de protocolo se aplica a esta regla y que puertos va a restringir, para esta regla se escoge el protocolo TCP y aplicar a todos los puertos.



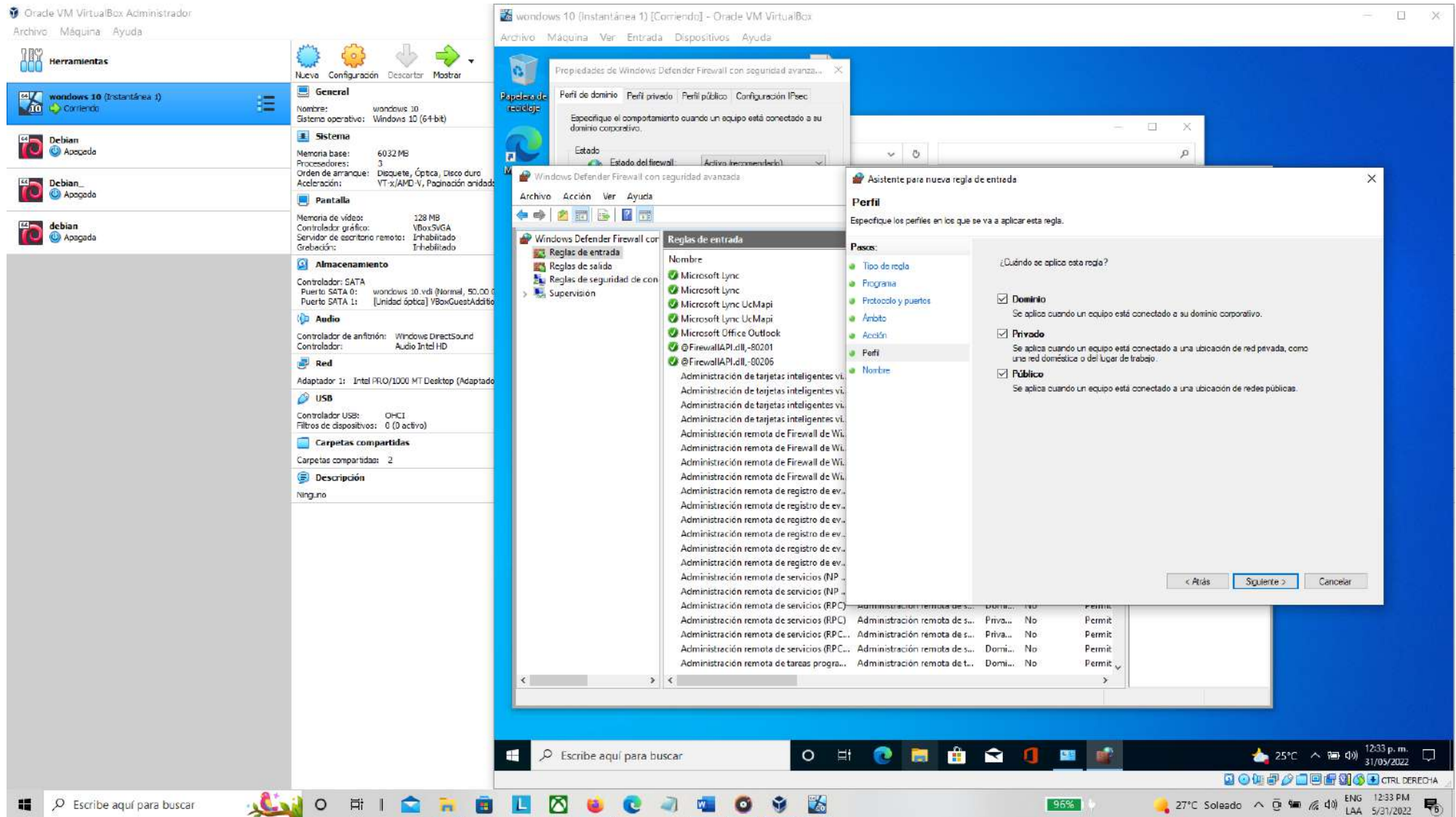
Aquí podemos especificar que la regla se aplica solo al tráfico de red hacia o desde las direcciones IP especificada, se queda en blanco este apartado.



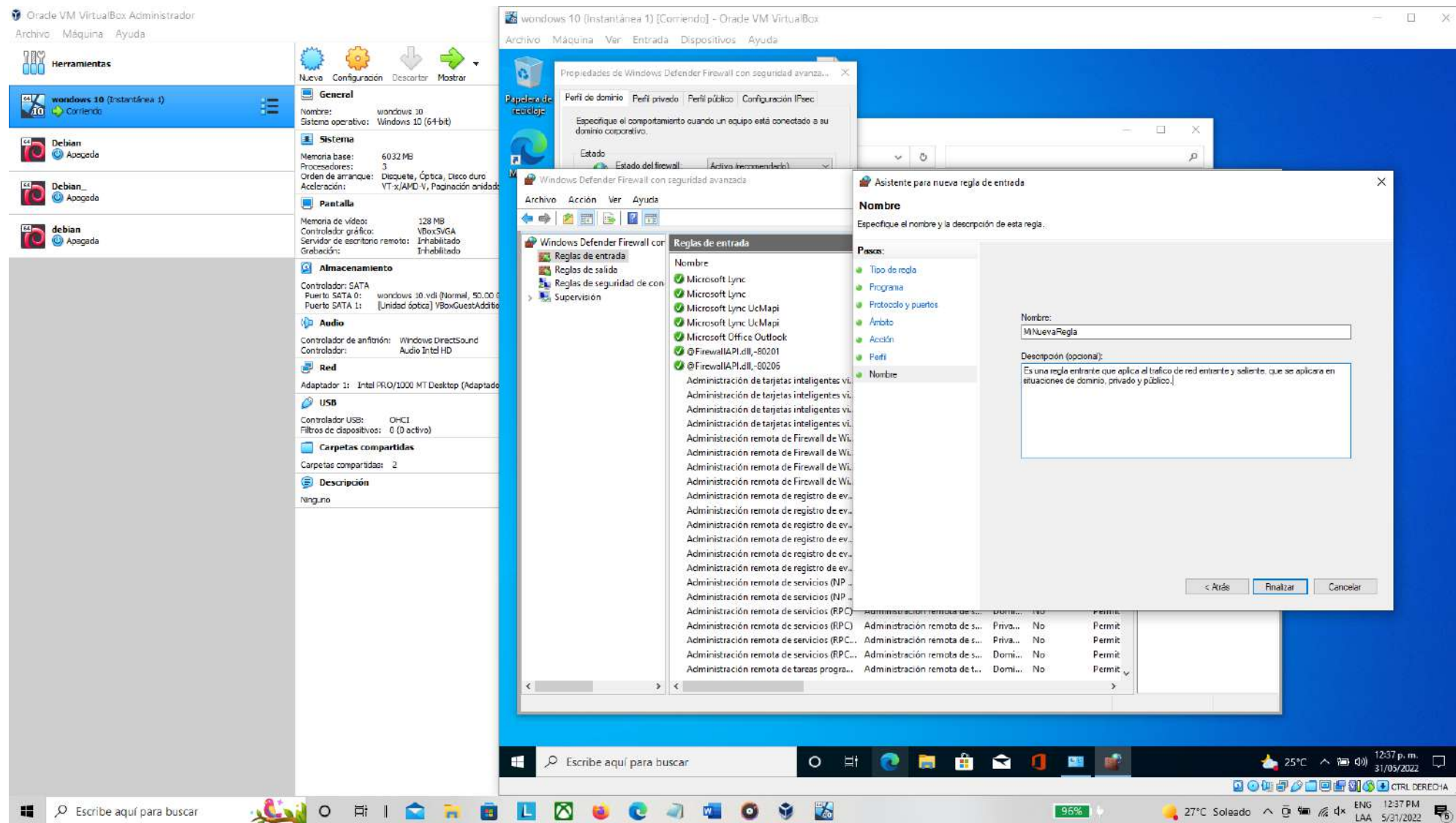
En la ventana de acción se selecciona que tipo de acción se llevara a cabo, para nuestra nueva regla se dejara en permitir la conexión.



En la ventana de perfil se selecciona cuando se aplicara esta nueva regla que será en todos los apartados, cuando la red sea publica, privada y de dominio.



Y finalmente se le da nombre a esta nueva regla “MiNuevaRegla” y una pequeña descripción de que hace para futuras referencias.



Aquí se observa que MiNuevaRegla esta en la lista y esta activa.

Oracle VM VirtualBox Administrador

Archivo Máquina Ayuda

Herramientas

Nuevo Configuración Descartar Mostrar

windows 10 (Instantánea 1) Corriendo

Debian Apagado

Debian Apagado

debian Apagado

General

Nombre: windows 10
Sistema operativo: Windows 10 (64-bit)

Sistema

Memoria base: 6032 MB
Procesadores: 3
Orden de arranque: Disco duro, Óptica, Disco duro
Aceleración: VT-x/AMD-V, Paginación anidada

Pantalla

Memoria de vídeo: 128 MB
Controlador gráfico: VBoxSVGA
Servidor de escritorio remoto: I-habilitado
Grabación: I-habilitado

Almacenamiento

Controlador: SATA
Puerto SATA 0: windows 10.vdi (Normal, 50,00 GB)
Puerto SATA 1: [Unidad óptica] VBoxGuestAdditions.vdi

Audio

Controlador de audio: Windows DirectSound
Controlador: Audio Intel HD

Red

Adaptador 1: Intel PRO/1000 MT Desktop (Adaptado)

USB

Controlador USB: OHCI
Filtros de dispositivos: 0 (0 activo)

Carpetas compartidas

Carpetas compartidas: 2

Descripción

Ninguno

windows 10 (Instantánea 1) [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Var Entrada Dispositivos Ayuda

Propiedades de Windows Defender Firewall con seguridad avanzada

Perfil de dominio Perfil privado Perfil público Configuración IPsec

Especifique el comportamiento cuando un equipo está conectado a su dominio corporativo.

Estado Estado del firewall Activo (recomendado)

Windows Defender Firewall con seguridad avanzada

Archivo Acción Ver Ayuda

Reglas de entrada

Nombre	Grupo	Perfil	Habilitado	Acción
MiNuevaRegla		Todo	Sí	Permit
Microsoft Lync		Privado	Sí	Permit
Microsoft Lync		Privado	Sí	Permit
Microsoft Lync Ucmapi		Privado	Sí	Permit
Microsoft Lync Ucmapi		Privado	Sí	Permit
Microsoft Office Outlook		Privado	Sí	Permit
@FirewallAPI.dll - 80201	@FirewallAPI.dll - 80200	Todo	Sí	Permit
@FirewallAPI.dll - 80206	@FirewallAPI.dll - 80200	Todo	Sí	Permit
Administración de tarjetas inteligentes vi...	Administración de tarjetas i...	Priv...	No	Permit
Administración de tarjetas inteligentes vi...	Administración de tarjetas i...	Dom...	No	Permit
Administración de tarjetas inteligentes vi...	Administración de tarjetas i...	Priv...	No	Permit
Administración de tarjetas inteligentes vi...	Administración de tarjetas i...	Dom...	No	Permit
Administración remota de Firewall de Wi...	Administración remota de F...	Priv...	No	Permit
Administración remota de Firewall de Wi...	Administración remota de F...	Dom...	No	Permit
Administración remota de Firewall de Wi...	Administración remota de F...	Priv...	No	Permit
Administración remota de Firewall de Wi...	Administración remota de F...	Dom...	No	Permit
Administración remota de registro de ev...	Administración remota de r...	Priv...	No	Permit
Administración remota de registro de ev...	Administración remota de r...	Dom...	No	Permit
Administración remota de registro de ev...	Administración remota de r...	Priv...	No	Permit
Administración remota de registro de ev...	Administración remota de r...	Dom...	No	Permit
Administración remota de servicios (NP ...	Administración remota de s...	Dom...	No	Permit
Administración remota de servicios (NP ...	Administración remota de s...	Priv...	No	Permit
Administración remota de servicios (RPC ...	Administración remota de s...	Dom...	No	Permit
Administración remota de servicios (RPC ...	Administración remota de s...	Priv...	No	Permit
Administración remota de servicios (RPC ...	Administración remota de s...	Dom...	No	Permit
Administración remota de servicios (RPC ...	Administración remota de s...	Priv...	No	Permit

Acciones

Reglas de entrada

Nueva regla...

Filtrar por perfil

Filtrar por estado

Filtrar por grupo

Ver

Actualizar

Exportar lista...

Ayuda

MiNuevaRegla

Desactivar regla

Cortar

Copiar

Eliminar

Propiedades

Ayuda

Explorador de archivos

Escribe aquí para buscar

25°C

12:37 p. m.
31/05/2022

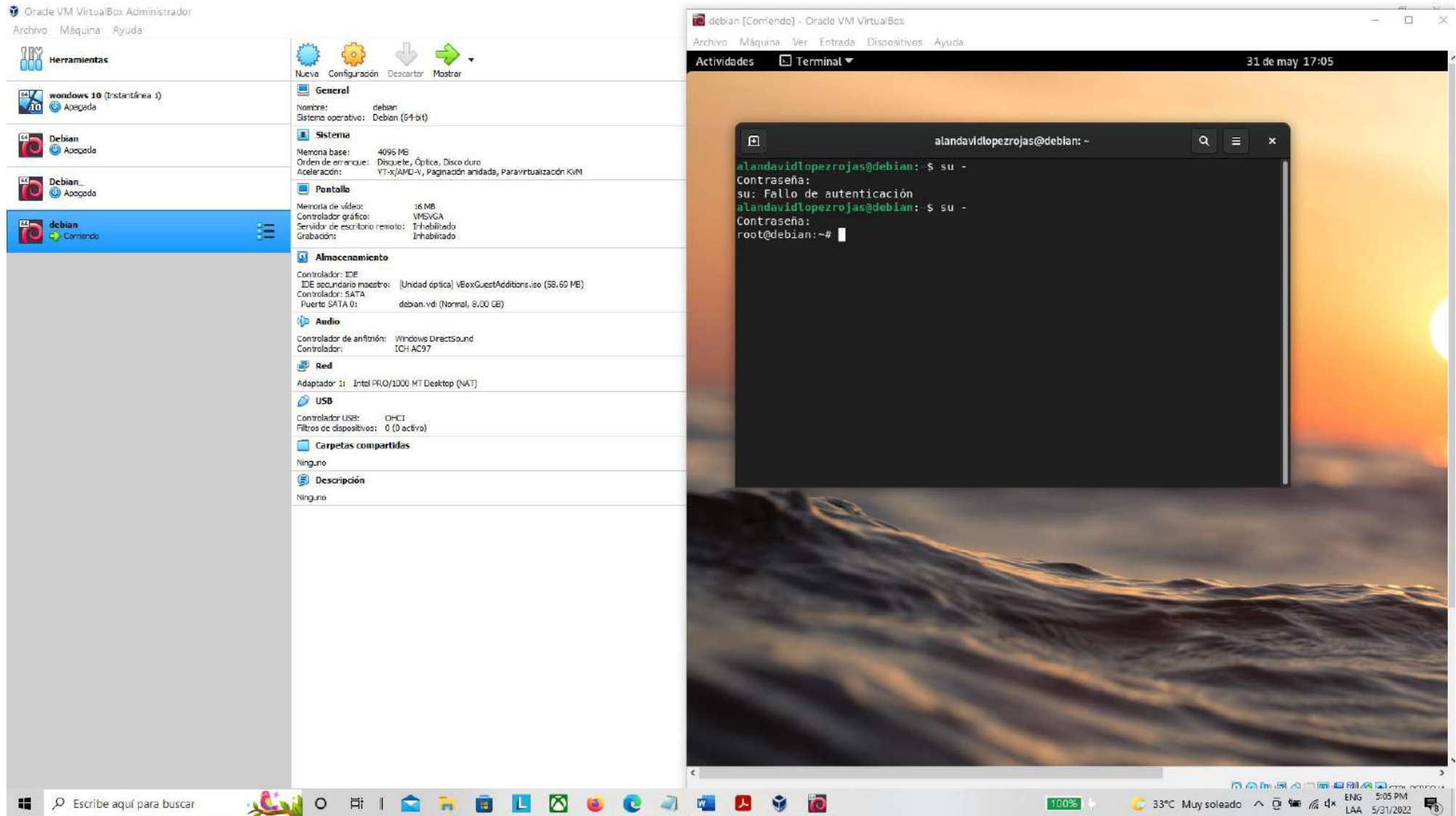
96%

27°C Soleado

ENG 12:37 PM
LAA 5/31/2022

Firewall Debian Linux

A continuación, pasamos a la instalación y configuración del firewall de Debian, el primer paso fue iniciar la máquina virtual con el sistema operativo Debian, ya que no está instalado por default el firewall UFW, hay que instalarlo manualmente, inicio la terminal de comandos, accedo como Super usuario con mi contraseña.



Una vez ingreso como root procedo a escribir el comando “apt-get install ufw” que permite la instalación del firewall ufw en el sistema

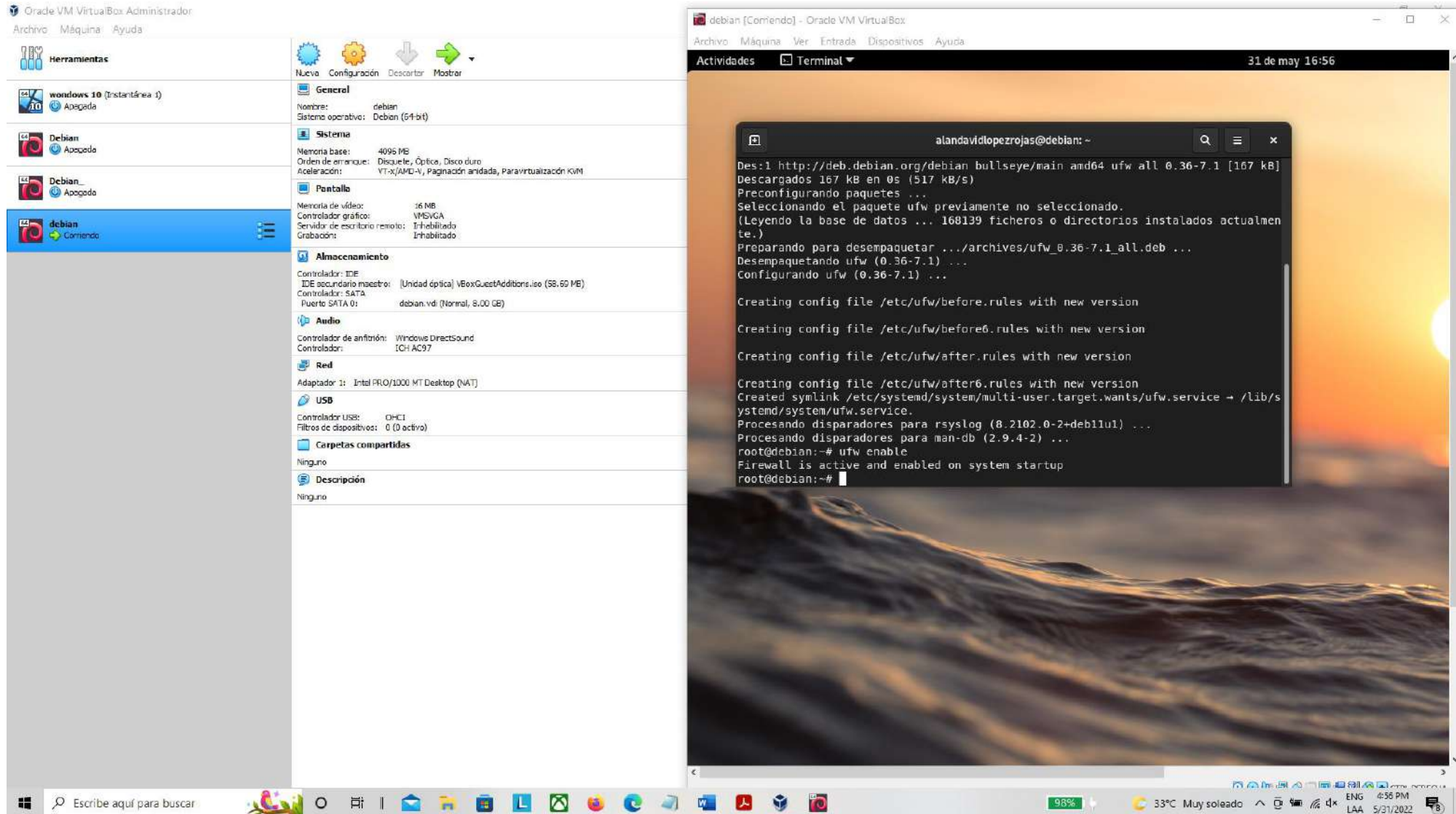
The image shows the Oracle VM VirtualBox Administrator interface. On the left, a list of VMs includes 'wondows 10', 'Debian', and 'debian'. The 'debian' VM is selected and its settings are shown on the right. The settings are categorized into General, Sistema, Pantalla, Almacenamiento, Audio, Red, USB, and Carpetas compartidas. The 'Sistema' tab is active, showing details like Name (debian), OS (Debian 64-bit), Memory (4096 MB), and Acceleration (VT-x/AMD-V, Pánginacón anidada, Paravirtualización KVM).

Overlaid on the VirtualBox window is a terminal window titled 'debian [Comando] - Oracle VM VirtualBox'. The terminal shows the execution of the command 'apt-get install ufw' as root. The output indicates that the package 'ufw' is being installed, including downloading, dependency resolution, and configuration steps. The terminal output is as follows:

```
alandavidlopezrojas@debian: ~  
alandavidlopezrojas@debian:~$ su -  
Contraseña:  
root@debian:~# apt-get install ufw  
Leyendo lista de paquetes... Hecho  
Creando árbol de dependencias... Hecho  
Leyendo la información de estado... Hecho  
Se instalarán los siguientes paquetes NUEVOS:  
  ufw  
0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 0 no actualizados.  
Se necesita descargar 167 kB de archivos.  
Se utilizarán 857 kB de espacio de disco adicional después de esta operación.  
Des:1 http://deb.debian.org/debian bullseye/main amd64 ufw all 0.36-7.1 [167 kB]  
Descargados 167 kB en 0s (517 kB/s)  
Preconfigurando paquetes ...  
Seleccionando el paquete ufw previamente no seleccionado.  
(Leyendo la base de datos ... 168139 ficheros o directorios instalados actualmen  
te.)  
Preparando para desempaquetar .../archives/ufw_0.36-7.1_all.deb ...  
Desempaquetando ufw (0.36-7.1) ...  
Configurando ufw (0.36-7.1) ...  
  
Creating config file /etc/ufw/before.rules with new version  
Creating config file /etc/ufw/before6.rules with new version
```

The bottom of the image shows the host's taskbar with various application icons, a search bar, and system status indicators like battery level (98%), temperature (33°C), and date (5/31/2022).

Una vez instalado hay que activarlo, para esto puse el comando # ufw enable, que lo habilito.



The image shows the Oracle VM VirtualBox Administrator interface on the left and a terminal window on the right. The VirtualBox window displays the configuration for a Debian VM, including general settings, system resources, and hardware configuration. The terminal window shows the execution of the `ufw enable` command, which successfully enables the firewall.

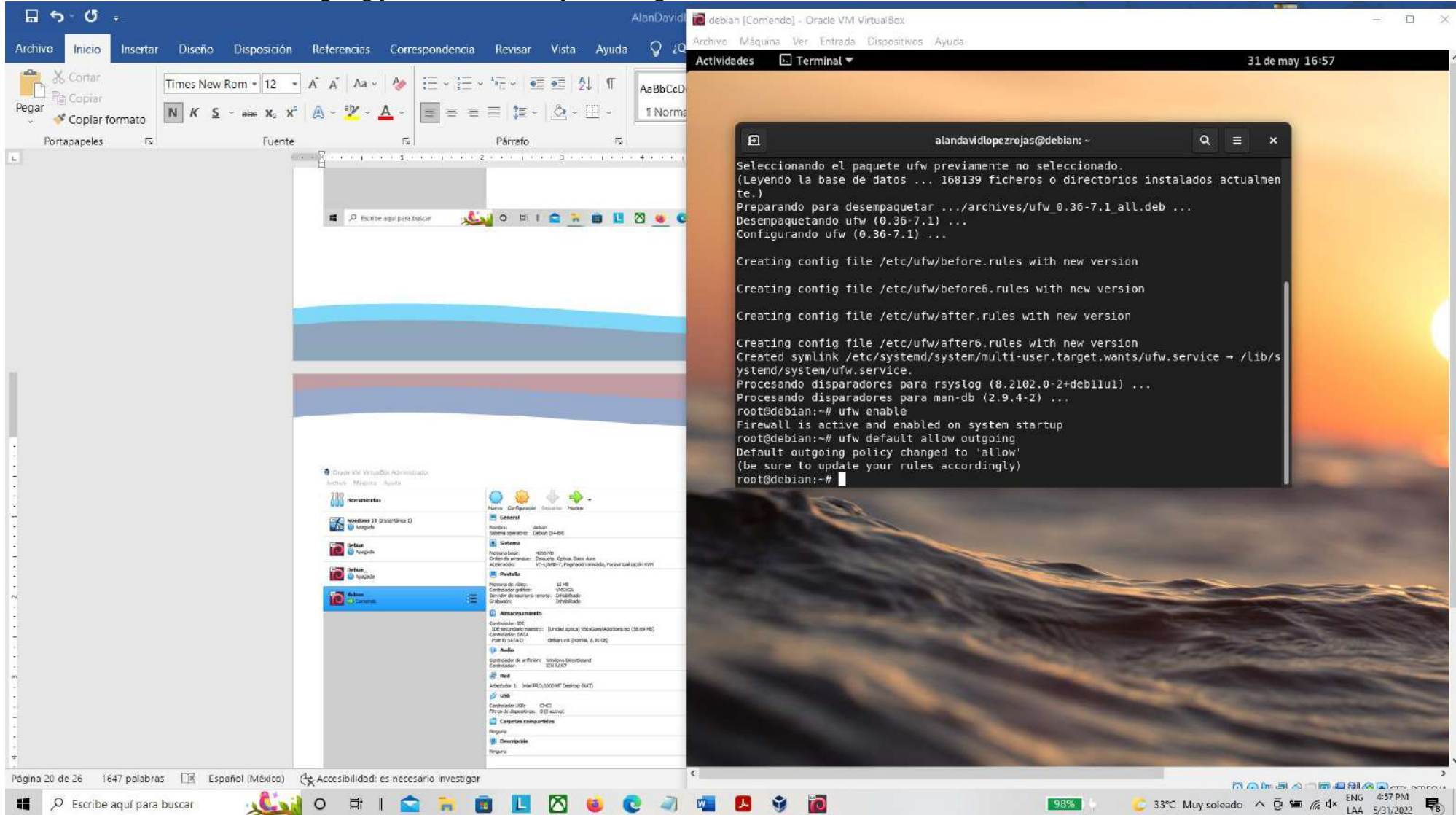
Oracle VM VirtualBox Administrator - VM Configuration:

- Herramientas:** Nueva, Configuración, Descartar, Mostrar
- General:** Nombre: debian, Sistema operativo: Debian (64-bit)
- Sistema:** Memoria base: 4096 MB, Orden de arranque: Disco duro, VT-x/AMD-V: Paginación anidada, Paravirtualización KVM
- Pantalla:** Memoria de vídeo: 32 MB, Controlador gráfico: VMXGPA, Servidor de escritorio remoto: Habilitado, Grabación: Inhabilitado
- Almacenamiento:** Controlador: IDE, IDE secundario maestro: Unidad óptica VBoxGuestAdditions.iso (58,59 MB), Controlador: SATA, Puerto SATA 0: debian.vdi (Normal, 8,00 GB)
- Audio:** Controlador de emulación: Windows DirectSound, Controlador: ICH AC97
- Red:** Adaptador 1: Intel PRO/1000 MT Desktop (NAT)
- USB:** Controlador USB: OHCI, Filtros de dispositivos: 0 (0 activo)
- Carpetas compartidas:** Ninguno
- Descripción:** Ninguno

Terminal Output:

```
alandavidlopezrojas@debian: ~  
Des:1 http://deb.debian.org/debian bullseye/main amd64 ufw all 0.36-7.1 [167 kB]  
Descargados 167 kB en 0s (517 kB/s)  
Preconfigurando paquetes ...  
Seleccionando el paquete ufw previamente no seleccionado.  
(Leyendo la base de datos ... 168139 ficheros o directorios instalados actualmen  
te.)  
Preparando para desempaquetar .../archives/ufw_0.36-7.1_all.deb ...  
Desempaquetando ufw (0.36-7.1) ...  
Configurando ufw (0.36-7.1) ...  
  
Creating config file /etc/ufw/before.rules with new version  
  
Creating config file /etc/ufw/before6.rules with new version  
  
Creating config file /etc/ufw/after.rules with new version  
  
Creating config file /etc/ufw/after6.rules with new version  
Created symlink /etc/systemd/system/multi-user.target.wants/ufw.service → /lib/s  
ystemd/system/ufw.service.  
Procesando disparadores para rsyslog (8.2102.0-2+deb11u1) ...  
Procesando disparadores para man-db (2.9.4-2) ...  
root@debian:~# ufw enable  
Firewall is active and enabled on system startup  
root@debian:~#
```


En este paso voy a utilizar la configuración de bloque y permiso, para los cual bloqueo el tráfico de entrada y permito el tráfico de salida con el siguiente comando: `# ufw default allow outgoing` y `# ufw default deny incoming`.



The screenshot displays a virtual machine environment. On the left, a LibreOffice Writer window is open, showing a blank document with a ruler and various toolbars. The right side of the image features a terminal window titled 'almandavidlopezrojas@debian: ~'. The terminal output shows the installation and configuration of the UFW firewall:

```
Seleccionando el paquete ufw previamente no seleccionado.
(Leyendo la base de datos ... 168139 ficheros o directorios instalados actualmen
te.)
Preparando para desempaquetar .../archives/ufw_0.36-7.1_all.deb ...
Desempaquetando ufw (0.36-7.1) ...
Configurando ufw (0.36-7.1) ...

Creating config file /etc/ufw/before.rules with new version
Creating config file /etc/ufw/before6.rules with new version
Creating config file /etc/ufw/after.rules with new version
Creating config file /etc/ufw/after6.rules with new version
Created symlink /etc/systemd/system/multi-user.target.wants/ufw.service → /lib/s
ystemd/system/ufw.service.
Procesando disparadores para rsyslog (8.2102.0-2+deb11u1) ...
Procesando disparadores para man-db (2.9.4-2) ...
root@debian:~# ufw enable
Firewall is active and enabled on system startup
root@debian:~# ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
root@debian:~#
```

The terminal window also shows the system information for the Debian VM, including hardware details like the CPU, memory, and disk space.

Oracle VM VirtualBox Administrador

Archivo Máquina Ayuda

Herramientas

windows 10 (Instantánea 1)
Apagada

Debian
Apagada

Debian
Apagada

debian
Corriendo

Nueva Configuración Descartar Mostrar

General

Nombre: debian
Sistema operativo: Debian (64-bit)

Sistema

Memoria base: 4096 MB
Orden de arranque: Disco duro
Aceleración: VT-x/AMD-V, Paginación anidada, Paravirtualización KVM

Pantalla

Memoria de vídeo: 16 MB
Controlador gráfico: VMXGA
Servidor de escritorio remoto: Inhabilitado
Grabación: Inhabilitado

Almacenamiento

Controlador: IDE
IDE secundario maestro: [Unidad óptica] VBoxGuestAdditions.iso (58,50 MB)
Controlador: SATA
Puerto SATA 0: debian.vdi (Normal, 8,00 GB)

Audio

Controlador de interfaz: Windows DirectSound
Controlador: ICH AC97

Red

Adaptador 1: Intel PRO/1000 MT Desktop (NAT)

USB

Controlador USB: OHCI
Filtros de dispositivos: 0 (0 activo)

Carpetas compartidas

Ninguno

Descripción

Ninguno

debian [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Actividades Terminal

31 de may 16:58

alandavidlopezrojas@debian: ~

```
Preparando para desempaquetar .../archives/ufw 0.36-7.1_all.deb ...  
Desempaquetando ufw (0.36-7.1) ...  
Configurando ufw (0.36-7.1) ...  
  
Creating config file /etc/ufw/before.rules with new version  
  
Creating config file /etc/ufw/before6.rules with new version  
  
Creating config file /etc/ufw/after.rules with new version  
  
Creating config file /etc/ufw/after6.rules with new version  
Created symlink /etc/systemd/system/multi-user.target.wants/ufw.service → /lib/s  
ystemd/system/ufw.service.  
Procesando disparadores para rsyslog (8.2102.0-2+deb11u1) ...  
Procesando disparadores para man-db (2.9.4-2) ...  
root@debian:~# ufw enable  
Firewall is active and enabled on system startup  
root@debian:~# ufw default allow outgoing  
Default outgoing policy changed to 'allow'  
(be sure to update your rules accordingly)  
root@debian:~# ufw default deny incoming  
Default incoming policy changed to 'deny'  
(be sure to update your rules accordingly)  
root@debian:~#
```

Escribe aquí para buscar

98%

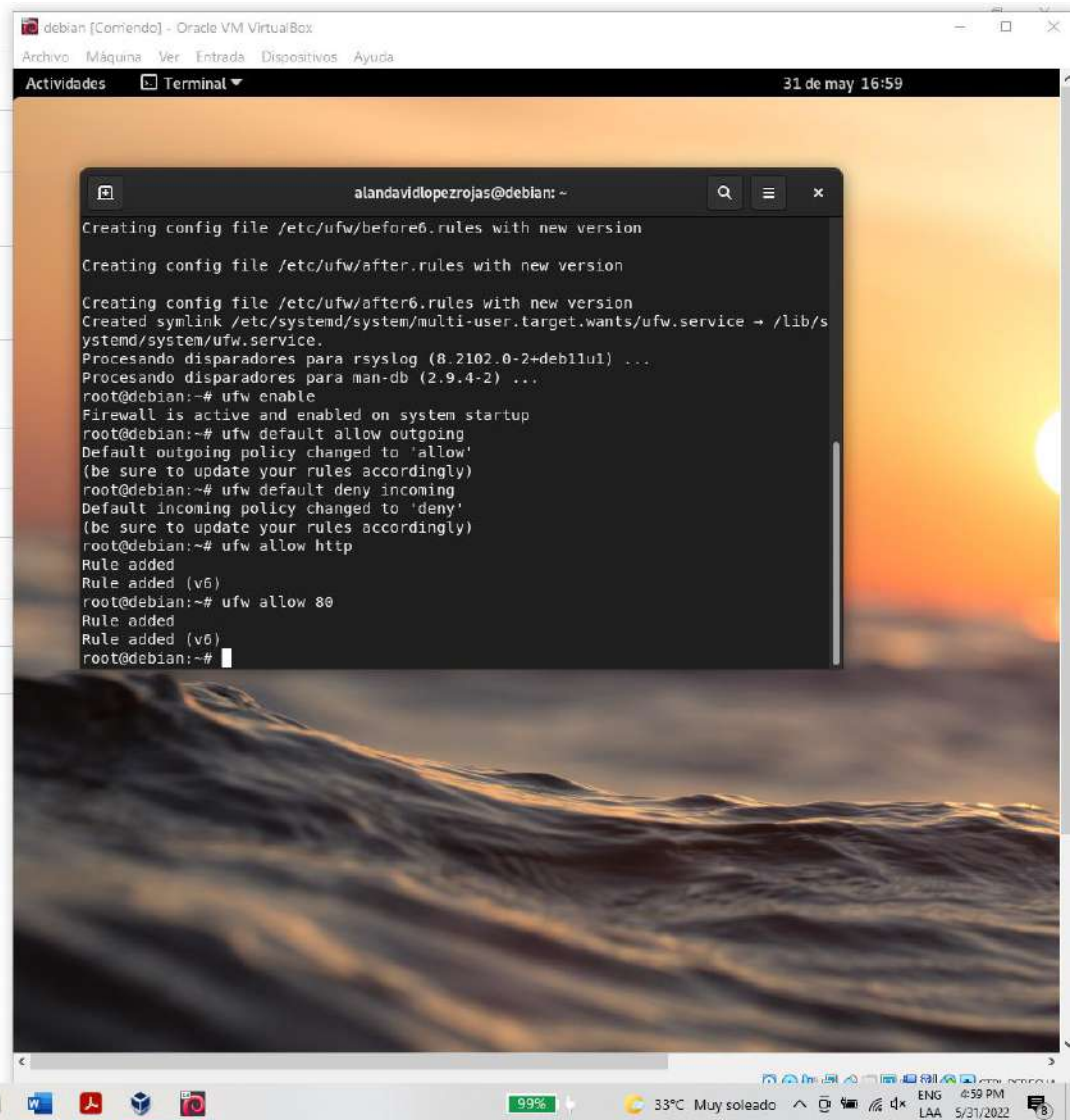
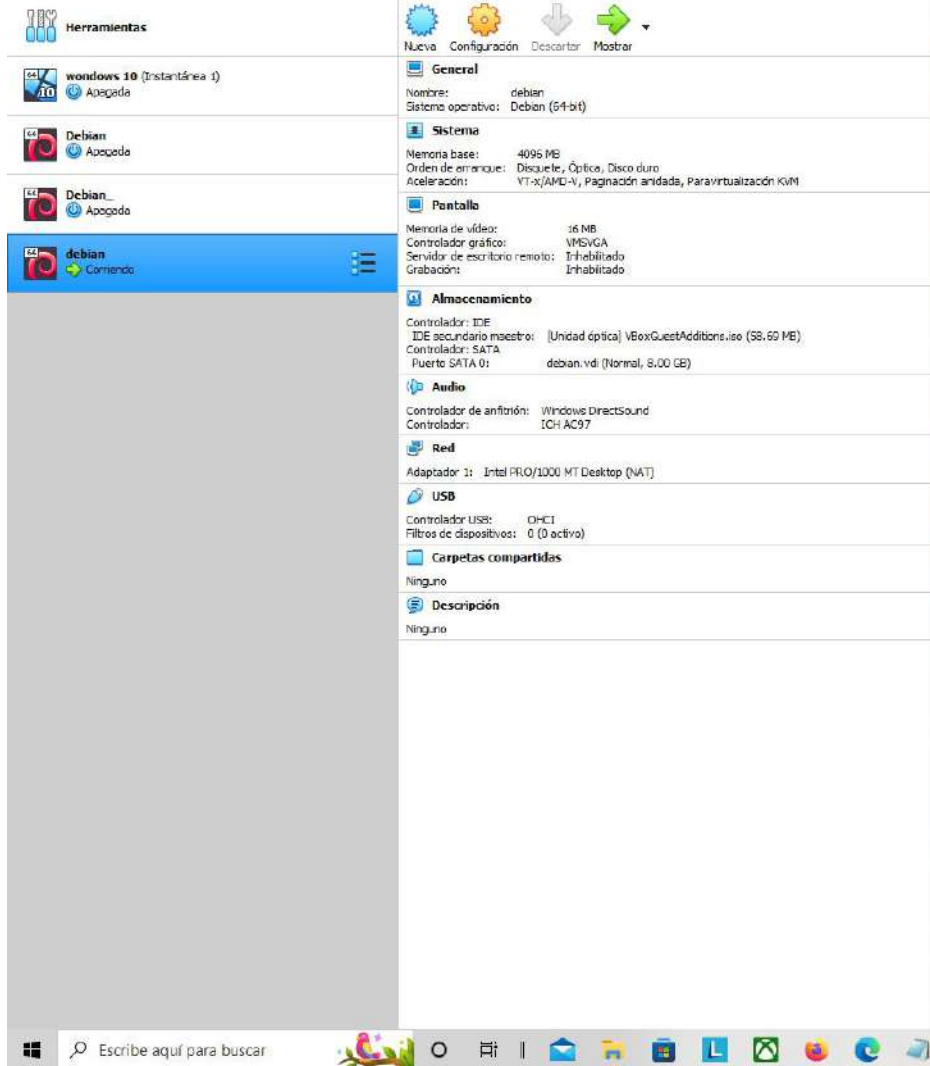
33°C Muy soleado

ENG 4:58 PM
LAA 5/31/2022

Para la siguiente configuración permitiremos abrir el puerto necesario para que funcione el motor web, en este caso el 80, con los comandos # ufw allow http que es el mismo comando que # ufw allow 80, uno es por medio de HTTP y el otro especificando el puerto, en este paso es muy importante especificar que puertos bloqueamos y cuales dejamos abiertos.

Oracle VM VirtualBox Administrador

Archivo Máquina Ayuda



Una vez aplicado las reglas, se puede ver su estado con el siguiente comando: `# ufw status verbose`.

The image shows the Oracle VM VirtualBox Administrator interface on the left and a terminal window on the right. The terminal window is titled 'debian [Comiendo] - Oracle VM VirtualBox' and shows the execution of UFW commands to configure firewall rules.

VirtualBox VM Settings for 'debian':

- General:** Nombre: debian, Sistema operativo: Debian (64-bit)
- Sistema:** Memoria base: 4096 MB, Orden de arranque: Discuete, Óptica, Disco duro, VT-x/AMD-V, Páginación anidada, Paravirtualización KVM
- Pantalla:** Memoria de vídeo: 36 MB, Controlador gráfico: VMSVGA, Servidor de escritorio remoto: Inhabilitado, Grabación: Inhabilitado
- Almacenamiento:** Controlador: IDE, IDE secundario maestro: (Unidad óptica) VBoxGuestAdditions.iso (58.60 MB), Controlador: SATA, Puerto SATA 0: debian.vdi (Normal, 8.00 GB)
- Audio:** Controlador de interfaz: Windows DirectSound, Controlador: ICH AC97
- Red:** Adaptador 1: Intel PRO/1000 MT Desktop (NAT)
- USB:** Controlador USB: OHCI, Filtros de dispositivos: 0 (0 activo)
- Carpetas compartidas:** Ninguna
- Descripción:** Ninguna

Terminal Output:

```
alandavidlopezrojas@debian: ~  
(be sure to update your rules accordingly)  
root@debian:~# ufw default deny incoming  
Default incoming policy changed to 'deny'  
(be sure to update your rules accordingly)  
root@debian:~# ufw allow http  
Rule added  
Rule added (v6)  
root@debian:~# ufw allow 80  
Rule added  
Rule added (v6)  
root@debian:~# ufw status verbose  
Status: active  
Logging: on (low)  
Default: deny (incoming), allow (outgoing), disabled (routed)  
New profiles: skip  
  
To Action From  
-- -- --  
80/tcp ALLOW IN Anywhere  
80 ALLOW IN Anywhere  
80/tcp (v6) ALLOW IN Anywhere (v6)  
80 (v6) ALLOW IN Anywhere (v6)  
root@debian:~#
```

Por último, para borrar una regla ya establecida, hay que ejecutar un delete a UFW. Para bloquear en vez de permitir, se usó el comando deny: # ufw delete allow http y # ufw deny http

The image shows the Oracle VM VirtualBox Administrator interface on the left and a terminal window on the right. The VirtualBox window displays the configuration for a VM named 'debian'. The configuration includes sections for General, Sistema, Pantalla, Almacenamiento, Audio, Red, and USB. The terminal window shows the execution of UFW commands to allow port 80, check status, delete the allow rule, and deny port 80.

VirtualBox Configuration:

- General:** Nombre: debian, Sistema operativo: Debian (64-bit)
- Sistema:** Memoria base: 4096 MB, Orden de arranque: Disco duro, VT-x/AMD-V: Paginación anidada, Paravirtualización KVM
- Pantalla:** Memoria de vídeo: 16 MB, Controlador gráfico: VMSVGA, Servidor de escritorio remoto: Inhabilitado, Grabación: Inhabilitado
- Almacenamiento:** Controlador: IDE, IDE secundario maestro: (Unidad óptica) VBoxGuestAdditions.iso (58.59 MB), Controlador: SATA, Puerto SATA 0: debian.vdi (Normal, 8.00 GB)
- Audio:** Controlador de sonido: Windows DirectSound, Controlador:ICH AC97
- Red:** Adaptador 1: Intel PRO/1000 MT Desktop (NAT)
- USB:** Controlador USB: OHCI, Filtros de dispositivos: 0 (0 activo)
- Carpetas compartidas:** Ninguna
- Descripción:** Ninguna

Terminal Output:

```
alandaavidlopezrojas@debian: ~  
Rule added (v6)  
root@debian:~# ufw allow 80  
Rule added  
Rule added (v6)  
root@debian:~# ufw status verbose  
Status: active  
Logging: on (low)  
Default: deny (incoming), allow (outgoing), disabled (routed)  
New profiles: skip  
  
To Action From  
--  
80/tcp ALLOW IN Anywhere  
80 ALLOW IN Anywhere  
80/tcp (v6) ALLOW IN Anywhere (v6)  
80 (v6) ALLOW IN Anywhere (v6)  
  
root@debian:~# ufw delete allow http  
Rule deleted  
Rule deleted (v6)  
root@debian:~# ufw deny http  
Rule added  
Rule added (v6)  
root@debian:~#
```


Conclusión

El firewall supervisa todo el tráfico de red y tiene permisos para identificar y bloquear el tráfico no deseado. El hecho de que hoy en día la mayoría de equipos estén conectados a internet facilita a los atacantes un sinnúmero de víctimas potenciales. Los atacantes sondean otros equipos conectados para determinar si son vulnerables a varias clases de ataques, el firewall puede evitar la propagación de códigos maliciosos a través de la red, accesos no autorizados o posibles intrusiones de terceros a la red privada o corporativa.

Básicamente podríamos decir que su utilidad es la de proteger nuestro equipo de posibles intrusos que puedan conectarse y robarnos datos personales, información, etc. Es por ello que su función es la de preservar nuestra seguridad y privacidad, proteger nuestra red y mantener a salvo la información guardada en el equipo.

A lo largo de este trabajo he aprendido que, si no disponemos de un firewall, aunque tengamos un antivirus bien configurado y de calidad, dejaríamos siempre una puerta abierta a posibles amenazas. Es por ello que es un buen complemento a nuestros programas de seguridad para evitar que un pirata informático o una persona no autorizada puedan conectarse de forma remota a nuestro ordenador y tomar el control del equipo.

Las amenazas se propagan de computadora a computadora sin que el usuario se entere. Si uno de esos equipos tiene una configuración de seguridad baja o vulnerabilidades sin parches, pueden infiltrarse en el sistema sin que el usuario se dé cuenta. Un buen número de gusanos y troyanos, también denominados “bots” se propagan de esta forma, usan internet para buscar equipos que infectar. El usuario nunca advertirá que su sistema está en peligro porque la amenaza se infiltra en su equipo sigilosamente por eso el firewall es el modo de proteger nuestra información en cualquier equipo.

Existen diferencias a la hora de instalar y configurar el firewall en diferentes sistemas operativos como en este caso en Windows y en Debian Linux, pero su función es la misma, proteger de intrusiones no deseadas en nuestros equipos.

Bibliografía

Manual de Firewalls. Marcus Goncalves. Editorial McGraw-Hill.

Jesús Ángel Pérez-Roca Fernández, José Antonio Pereira Suárez; FIREWALLS.
<http://sabia.tic.udc.es/docencia/ssi/old/2006-2007/docs/trabajos/06%20-%20Firewalls%20%5Bupdated%5D.pdf>