BENEMÉRITA UNIVERSIDAD AUTÓNOMA DE PUEBLA

Facultad de Ciencias de la Computación

SEGURIDAD CON FIREWALLS EN SERVIDORES: UN ANÁLISIS COMPARATIVO CON HERRAMIENTAS OPEN SOURCE

Tesis para obtener el título de:

Licenciado en Ingeniería en Ciencias de la Computación

Presenta:

Alejandra Loaiza Ruiz

Director de Tesis:

M.C. Ana Claudia Zenteno Vázquez

Ciudad Universitaria, México, Puebla, octubre 2023.

DEDICATORIA /AGRADECIMIENTOS

Dedico el resultado de este trabajo a mi familia, principalmente a mis padres Gloria y José Agustín, quienes me han guiado y apoyado durante toda mi vida. Gracias por enseñarme a afrontar las dificultades de la vida sin perder nunca la cabeza ni morir en el intento, por enseñarme los valores que hacen grande a una persona y sobre todo por brindarme su inmenso amor como padres.

Me atrevo a decir que este inmenso logro también es suyo, pues soy el reflejo de lo que ustedes son, el gran equipo que somos para poder cumplir mis sueños, pues día a día han sacrificado muchas cosas para ustedes, para que yo pudiera cumplir uno de mis grandes sueños, siempre, todos y cada uno de mis logros, serán dedicados para ustedes, los amo.

También quiero dedicar este trabajo a mis cuatro hermanos Miguel Ángel, David, José Agustín y Cristina, quienes han sido un ejemplo a seguir, no solo profesionalmente sino personalmente, sus experiencias de vida me han enseñado a no perderme y quienes me enseñaron disfrutar mis tiempos de estudiante a lo máximo, por todos sus consejos y enseñanzas gracias.

De igual forma agradezco a mi gran amiga, quien se convirtió en familia, Diana, gracias inmensamente por compartir conmigo grandes momentos, por las risas, las grandes anécdotas, las fiestas, pero sobre todo por el inmenso apoyo durante la carrera pues no solo fue el de la preparación profesional, si no que las vivencias personales que me hicieron crecer, muchas gracias amiga, te quiero mucho.

También quiero agradecer a aquellas personas que estuvieron conmigo durante la elaboración de mi trabajo de tesis, principalmente a mi maestra, gran amiga y asesora de Tesis, Ana Claudia Zenteno Vázquez, que a pesar de la distancia fue una gran guía para poder realizar este trabajo, pero sobre todo porque contribuyo de una manera enorme para amar mi carrera, gracias por compartirme sus conocimientos y permitirme trabajar con Usted.

A todos y cada uno de los que han sido una parte integral de mi camino académico y personal y sobre todo a Dios por los caminos tan perfectos que construye para llegar hoy a donde he llegado.

MUCHAS GRACIAS

RESUMEN

Los actuales riesgos a los que nos enfrentamos como sociedad y que, de un momento a otro nos colocan en escenarios totalmente distintos nos obligan a adoptar nuevos hábitos. La emergencia sanitaria por COVID-19 obligó a toda la población a desistir de sus rutinas cotidianas, los ámbitos laboral y escolar se tuvieron que adaptar a una nueva forma de realizar sus respectivas funciones desde sus hogares y gracias a la tecnología esto fue posible. Teniendo un computador en casa y conexión a internet, la mayoría de las personas pudieron continuar con sus actividades. Sin embargo, el número personas conectadas creció exponencialmente, y cobró importancia el que cada usuario tuviera seguridad en la conexión y transacciones que realizaba. Actualmente, la seguridad con la que navegamos, principalmente el cómo protegemos a nuestros equipos y nuestra información, es de suma importancia para poder tener privacidad, sobre todo si nuestros equipos están siempre conectados a la red de redes (internet). La seguridad es un tema muy importante desde siempre, por supuesto el poder proteger nuestra información. En la actualidad hemos escuchado hablar mucho de ciberataques, infiltraciones a los equipos, intrusos que nos pueden robar datos confidenciales, hacer perder información valiosa o incluso impedirnos acceder a servicios en la red. Cada usuario en el mundo trabaja con un equipo que funciona con la ayuda de un Sistema Operativo, ya sea Windows, MacOS o GNU/Linux. En la actualidad ya hay más usuarios que prefieren usar GNU/Linux, pero surgen las preguntas sobre cómo están protegidos y si es necesario tomar medidas de seguridad usando Linux. La seguridad, en GNU/Linux, como ocurre con Windows o MacOS, no la da un solo sistema, ni aplicación, y tampoco la da un solo administrador o usuario, sino que es un

concepto multifactorial. Existen actualmente diferentes herramientas, entre ellas los *firewalls* que pueden brindar cierto tipo de seguridad a nuestros equipos. El propósito de este trabajo de tesis es brindar un análisis comparativo de la implementación de estas herramientas en beneficio de la protección de nuestro mayor activo: la información.

ÍNDICE

ÍNDICE DE TABLAS

Capítulo 1

1.1. Redes de computadoras

1.1.1. Definición

Hoy en día las redes de computadoras tienen diversas formas de operar en el entorno, en la actualidad han intervenido en la vida cotidiana de los seres humanos, pues sin darnos cuenta son una necesidad para poder llevar a cabo nuestras actividades diarias. Desde realizar las tareas y poder comunicarnos entre individuos, por medio de redes sociales como lo son WhatsApp, Facebook, Twitter, además de facilitar la vida son ahora un mecanismo importante para la comunicación. Además, las redes de computadoras nos permiten trabajar remotamente, pues no necesitamos estar presencialmente con nuestros compañeros de oficina para poder trabajar en conjunto, existen herramientas que permiten que el trabajo sea fluido, entre ellas se encuentran Google Drive, Dropbox, Zoom, por mencionar algunas. En general las redes de computadoras en la actualidad han contribuido de manera positiva a la sociedad y en el desarrollo de las actividades diarias.

Una red de computadoras, es una serie de nodos o puntos que están interconectados por un medio físico (cable) de comunicación. Una red de computadoras es el conjunto de ordenadores autónomos conectados por medio de señales las cuales autorizan la transmisión y recepción de datos, un equipo de cómputo no solo es una computadora, también lo son las tabletas electrónicas, teléfonos y sensores inteligentes. *(Fox Pamela., s.f.).*

Los principales elementos de una red desde la perspectiva del software, es que cuenta con un sistema operativo complejo el cual se compone de diferentes capas lógicas, de esta forma permite a varias personas trabajar con los mismos recursos, así mismo proporciona un control de acceso a la red en

cuanto a seguridad de conexión, seguridad de acceso a los recursos, coordinando al mismo tiempo dichos accesos simultáneos y a menudo administra colas en espera para dispositivos exclusivos.

Los ordenadores que están conectados a una red están divididos en dos categorías en función a las acciones que se lleven a cabo sobre esta. En la figura 1 se observa el modelo cliente – servidor con las funciones que cada uno realiza.

Cliente- Servidor

- Cliente: solicitante de servicios
- Servidor: otorga los servicios

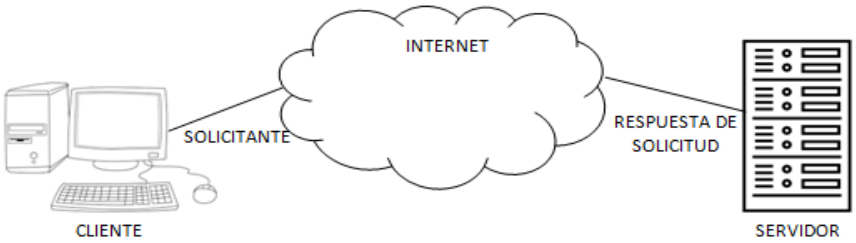


Fig. *1: Modelo Cliente servidor (Elaboración propia)*

APLICACIÓN DE NEGOCIOS

El uso tradicional que suelen darle las empresas es la compartición de recursos, pues las empresas suelen tener una cantidad considerable de computadoras, las cuales podrían tener por separado. Sin embargo, en algún momento conviene conectarlas entre sí, para poder extraer y correlacionar información acerca de la compañía. *(S. Tanenbaum, A., 2003)*

APLICACIÓN DOMÉSTICA

Para la aplicación doméstica de las redes de computadoras suelen usarse los mensajes instantáneos, por ejemplo: existen en la actualidad grupos de noticias mundiales, en donde se debaten diferentes temas inimaginables. En la figura 2 se observa el tipo de comunicación de persona a persona *(peer to peer) en* la cual no hay clientes ni servidores fijos.

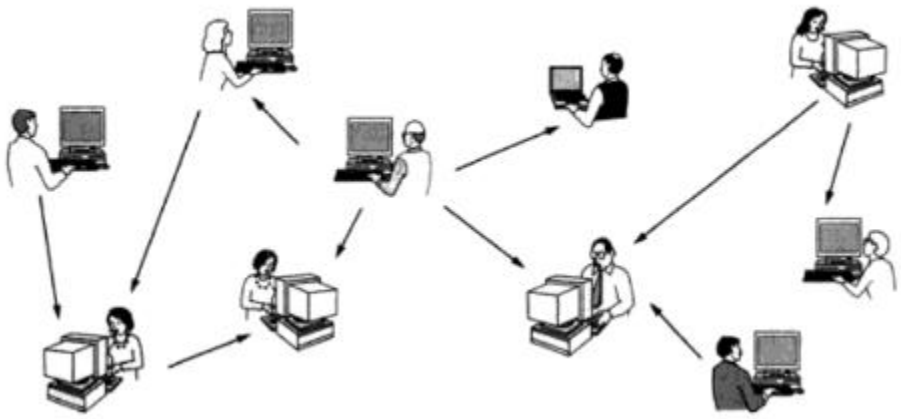


Fig. 2: SISTEMA PEER TO PEER, no hay clientes ni servidores fijos (S. Tanenbaum, Pearson Educación, 2003)

Los sistemas operativos de red son capaces de pedir y ofrecer servicios, sin embargo, dan prioridad a una u otra posibilidad. Por el contrario, un sistema operativo del servidor proporciona servicios más eficientes, capaz de soportar hardware avanzado y administrar capacidades como memoria y espacio en disco. En la figura 3 se muestra el uso compartido de archivos e impresoras para redes, programador de paquetes QoS (QualityofService), habilitar el protocolo de internet versión 4 (TCP/IPv4), controlador de protocolos LLDP (Link Layer Discovery Protocol) de Microsoft, habilitar el protocolo de internet versión 6 (TCP/IPv6).

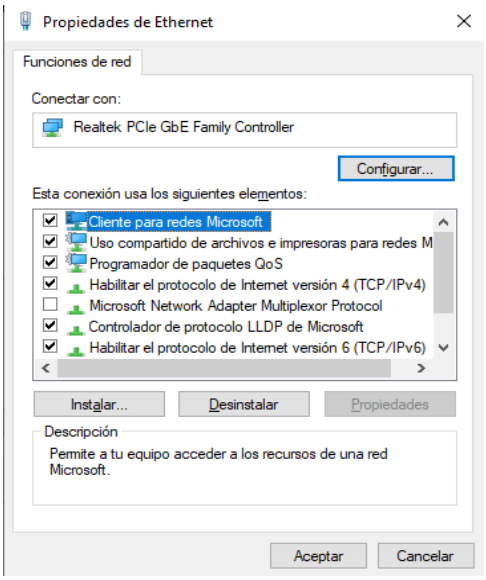


Fig. 3: PROPIEDADES DE RED EN UN CLIENTE WINDOWS 1 PRO (Captura de pantalla, Cliente para redes)

Dentro de las redes de computadoras existen varias formas de construir una red, desde la forma más sencilla hasta la más compleja, a esta se les denomina topología o forma lógica de una red la cual es la forma de tender el cable a estaciones de trabajo individuales por muros, techos y techos del edificio, para ello dada una situación es como se determina la topología adecuada. Gráficamente cada una de las topologías se muestra como en la figura. 4: *(Sanchez, Y.& Bolaños, C., 2021)*

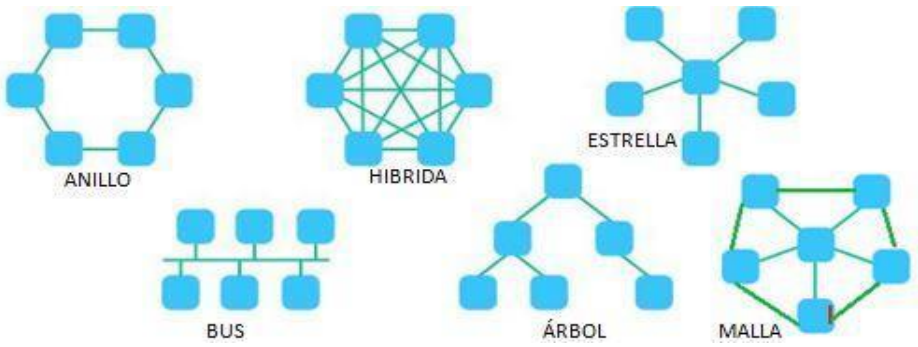


Fig. 4: TOPOLOGÍA DE REDES (Khan Academy, 2022)

- ANILLO: Red de ordenadores conectados entre sí, formando la estructura de anillo, va comprobando los datos de envió, en el caso de que no sea ella la receptora, va pasando la información hasta llegar a su destino, por lo que la información podría o no pasar por todos los nodos para llegar a su receptor.

- HÍBRIDA: Esta red se utiliza para necesidades concretas, pues en ella se combinan dos o más topologías.

- MALLA: En esta topología todos los nodos están conectados con los demás, es decir tienen conexiones en todas las direcciones y envían los mensajes por la mejor ruta.

- ESTRELLA: Para esta topología cada dispositivo de red tiene su propio canal, por lo que no genera colapso ni saturación alguna, pues si cae o se daña algún nodo, no cause problema en los demás.

- BUS: En esta topología los datos se transmiten por un solo canal al cual están conectados todos los dispositivos.

- ÁRBOL: Topología de modelo jerárquico, esta cuenta con un dispositivo central al que se conectan los nodos, compartiendo el mismo canal de comunicaciones, la información llega a todos los nodos, partiendo de una raíz.

  En la siguiente tabla se observa las distintas topologías que existen, en donde se mencionan sus ventajas y sus desventajas, de esta forma podemos tener un mejor rango de comparación para ver cual se apega a nuestras necesidades.

TOPOLOGÍA	VENTAJAS	DESVENTAJAS
ANILLO	La conexión provee una organización de igual a igual para todas las computadoras.	Tarda en la entrega de información al pasar por todos los nodos.
HÍBRIDA	Flexibilidad, capacidad de adaptarse y ampliarse con las condiciones óptimas posibles.	Se utiliza una cantidad de cableado significante.
ESTRELLA	No se generan colapsos ni saturación, cada dispositivo de red tiene su propio canal	Si es el conmutador el que falla, caería toda la red.
BUS	Fácil instalación, Si falla uno de los dispositivos los demás seguirán funcionando con normalidad.	Todos los dispositivos conectados a la red ven los mensajes de todos los demás, problemas de congestión, colisión y bloqueo.
ÁRBOL	Permite la fácil resolución de problemas y es mucho más rápida que las demás.	Si se cae el dispositivo central todo el segmento también cae
MALLA	todos tienen conexiones en todas las direcciones, cuenta son la posibilidad de enviar el mensaje por distintas rutas o caminos, inexistencia de interrupción en las comunicaciones,	En caso de falla buscan otra más lejana

Tabla 1 "Topologías", distintas topologías que existen.

Se usan diferentes tipos de términos para referirse a redes, esto de acuerdo a sus especificaciones como tamaño y características. Entre los tipos de redes que existen son: *(VNIVERSITAT DO VALENCIA, 2022).*

- LAN: Local Area Network. Son redes de área local y comúnmente son las más utilizadas para el intercambio de datos y recursos, se utilizan para conectar equipos en espacios pequeños, una de sus características es que permite que múltiples nodos se interconecten y su inconveniente es que los nodos que se pueden conectar a una LAN son limitados.

- WAN: Wide Area Ne twork. Las redes de área amplia es cuando varias redes LAN se conectan entre sí, dentro de las más comunes están las líneas telefónicas y satélites.

- MAN: Metropolitan Area Network. Esta red cuenta con mayor alcance pues al ser una Red de Área Metropolitana el principal medio conductor en la transferencia de información que se emplea es la fibra óptica, suelen ser estables y resistentes a interferencias radioeléctricas.

- WLAN: Wireless Local Network, esta es una Red de Área Local Inalámbrica, su intercambio de información se realiza por medio de ondas de radio, sin embargo, su gran inconveniente es la inseguridad, pues cualquier otra persona si cuenta con acceso a una terminal inalámbrica podría conectarse a un punto privado si este no cuenta con las medidas de seguridad necesarias.

- WMAN: Wireless Metropolitan Network, es la versión inalámbrica de la Red de Área Metropolitana, para ésta, el alcance es mucho mayor, está presente en comunicación como WiMAX.

- WWAN: Wireless Local Area Network. Esta red de inalámbrica de área amplia, cuenta con una cobertura geográfica bastante amplia, utiliza sistemas como Wifi y LMDS (Sistema de Distribución Local Multipunto.

- SAN: Storage Area Network. Es una red de área de almacenamiento, es bastante utilizada principalmente por empresas de mayor tamaño, puesto que permite conectar varias unidades de almacenamiento a redes de área local o LAN.

- PAN: Personal Area Network. Esta es una red de área personal la cual conecta los dispositivos cercanos al usuario en un entorno reducido.

1.1.2. Evolución

A lo largo de la historia las redes de computadora han tenido mucho que escribir, los avances en ella han sido significativos y sobre todo han tenido un impacto enorme para la comunicación mundial. En la tabla 2 se observa una breve descripción de la evolución de las redes de computadoras, (*School, T., 2022, 14 febrero)*.

AÑO	EVENTO
1957	Creación de la Advance Research Projects Agency (ARPA)
1965	ARPA patrocinó un programa para tratar de analizar las redes de comunicación, usando computadoras
1967	ARPA convocó una reunión en Ann Arbor (Michigan), en la cual se discuten por primera vez aspectos sobre la futura ARPANET
1968	ARPA hizo llamado a empresas y universidades, esto con el objetivo de construir la futura red, de la que la universidad de California ganó su propuesta.
1969	Construcción de la primera red de computadoras, a la cual se le denominó ARPANET, compuesta por cuatro nodos situados en la UCLA (Universidad de California de Santa Bárbara, L.A).
1970	ARPANET comenzó a trabajar con el protocolo Host-to-host
1971	Nació el programa e-mail, creado por Ray Tomlinson
1972	Se realizó el primer chat vía correo, es aquí donde se crea el famoso @ como la tecla de puntuación, para la separación del nombre de usuario y de la máquina.
1973	Se realizó la primera conexión internacional de la ARPANET en el colegio universitario de Londres. Para ese entonces contaba con 2000 usuarios y la mayor cantidad de tráfico la generaba el intercambio de correo electrónico.
1974	Se publicó el primer artículo del protocolo de control de transmisión (TCP)
1975	Se probaron los primeros enlaces vía satélite, cruzando el océano de Hawái a Inglaterra, primeras pruebas de TCP de la mano de Stanford, UCLA y UCL.
1980	Se creó redes particulares como la CSNET el cual proporciona servicios sin acceso a la ARPANET
1982	Se nombró a TCP e IP como el conjunto de protocolos
1985	Para la resolución de nombre de dominios asume la responsabilidad ISI
1989	Se desarrolló la World Wide Web (WWW) por Tim Berners-Lee
1990	Desaparece ARPANET
1993	Se crea el navegador MOSAIC
1997	Se publica el primer estándar WiFi 802.11
1998	Nace GOOGLE, navegador sencillo de usar
2001	Aparece la red 3G, la cual empieza a operar en Japón
2004	Nace Facebook, red social más importante hasta la actualidad

2005	Nace Youtube, red creada por Chad Hurley, Steve Chen y Jawn Karim en San Bruno, California.
2009	Se aprueba la recomendación de la IEEE 802.11n, evolución tecnológica de la serie de recomendaciones 802.11, de redes LAN inalámbricas.
2014	Se aprueba la IEEE 802.11ac, permite comunicación de datos inalámbricas hasta de 7 Gb/s.

Tabla 2. Evolución de las redes de computadora

1.2. Seguridad en redes

La seguridad de red es la actividad diseñada para la protección de acceso, uso e integridad de red y datos, a las cuales incluye tecnologías de hardware y software. Además de que están orientadas a diversas amenazas, evita el ingreso y propagación a través de la red, pues de esta forma se tiene una red eficaz que administra el acceso. *(Cisco,19 de marzo de 2020)*

La seguridad combina varias capas de defensa en el perímetro y red de esta forma solo los usuarios autorizados tienen acceso a los recursos de red.

La seguridad de red beneficia totalmente pues cambia nuestra manera de vivir, trabajar, aprender y entretenernos. Hoy las organizaciones exigen a clientes y empleados proteger su red, pues de esta forma se protege información que pudiera ser confidencial de los ataques.

Dentro de los sistemas de redes se utilizan definiciones sobre:

- VULNERABILIDAD: evento que desencadena incidentes en la organización de los sistemas, produciendo daños en sus activos.

- AMENAZAS: ocurrencia de materialización de una amenaza sobre un activo el cual es el recurso del sistema, para que la organización funcione correctamente.

- RIESGOS: Posibilidad que produzca un impacto determinado en un activo de la organización.

Existen diferentes tipos de implementaciones de seguridad para redes entre las cuales están:

1. FIREWALLS: Programa de software o dispositivo hardware que evita que aquellos usuarios que no están autorizados puedan acceder a la red, de esta forma se impide el tráfico sospechoso y solo que fluya el tráfico.

2. DETECCIÓN Y PREVENCIÓN DE INTRUSIONES: estos se pueden implementar detrás de un firewall de esta forma se refuerza la seguridad, el cual trabaja en paralelo con su predecesor, además de que se encuentra en medio de la dirección de origen y su destino.

3. CONTROL DE ACCESO A LA RED (NAC): Estando en la primera línea de defensa, exactamente realiza el control de acceso a la red, verifica estado de punto final, los dispositivos que cuentan con esta descripción son las computadoras portátiles, teléfonos inteligentes, simplemente para que se pueda asegurar una mayor seguridad y las actualizaciones correspondientes a los dispositivos.

4. SEGURIDAD EN LA NUBE: Protege los recursos en línea, datos confidenciales, pérdidas, robos o filtraciones. Es por ello que se requiere de una política de seguridad muy sólida, métodos de seguridad, arquitectura firewall.

5. REDES PRIVADAS VIRTUALES: Es un software que protege la identidad del usuario cifrando los datos y enmascarando la dirección IP y la ubicación, cuando se está usando una VPN, no se está entrando directamente a internet si no a un servidor seguro que posteriormente se conectará a internet en su nombre.

6. PREVENCIÓN DE PÉRDIDAS DE DATOS (DLP): Estrategias y herramientas implementadas para garantizar a los usuarios de puntos finales no compartan información maliciosamente o accidental la información que es confidencial que este fuera de una red corporativa, esta seguridad se emplea en tarjetas de crédito información financiera y de salud. Monitorean redes corporativas y en la nube utilizando cifrado.

7. PROTECCIÓN DE PUNTOS FINALES: Implica la protección de todos los puntos finales que se conectan a su red, aunque esto es complejo, el servicio de seguridad administrativa puede ayudar a mantener dispositivos, datos y red seguros.

8. GESTIÓN UNIFICADA DE AMENAZAS (UTM): Con estos dispositivos se pueden mejorar costos y capacidad de gestión de protección, pues se utilizan múltiples herramientas de seguridad como firewalls, VPN, IDS, filtrado de contenido web y software antispam.

9. PUERTA DE ENLACE WEB SEGURA: Evita que el tráfico de red no autorizada ingrese a la red interna, de esta forma protege a los usuarios que pudieran entrar a sitios maliciosos.

1.2.1. Seguridad con hardware

La seguridad con hardware son los dispositivos físicos usados para escanear sistemas o para controlar el tráfico de datos, como firewalls, cortafuegos o servidores proxy.

Protección del equipamiento tecnológico de amenazas externas o robo provocado por el mal uso erróneo del hardware. Este equipamiento controla el acceso de usuarios y personas externas al entorno, ya sea por medios basados en controles, basados en mecanismos de identificación y autenticación por contraseñas o dispositivos biométricos.

No solo controla acceso y protección, también la red para que no existan puntos en los que pueda existir la intromisión además de regular que el cableado sea el adecuado para que se garantice el funcionamiento de la red y su disponibilidad.

De acuerdo a las estadísticas: *(ARREAGA CARPIO, G. I. S. S. E. L. I. V. E. T. T. E., 2010)*

- un 10% de los ataques informáticos se consuma desde el exterior.
- un 40% perpetran personas relacionadas con el sistema y que tienen acceso a él.
- Un 50% son ocasionados por el personal como consecuencias de actos de venganza.

Esto solo representa en datos generales de la mayoría de las organizaciones. Al realizar esta protección tienen como finalidad proteger, asegurar la integridad y disponibilidad de los equipos, sistema y red.

El hardware forma parte de los elementos más caros por lo que cuidar de la seguridad es de suma importancia, pues en caso de alguna amenaza el sistema corre peligro de generar pérdidas irrecuperables.

Dentro de los riesgos principales a los que nos enfrentamos para la protección de hardware son:

- ACCESO FÍSICO:

Si se descuida el acceso físico, es muy fácil que alguien realice cualquier ataque, pues tendría acceso a todo el sistema. Es por ello que se dice que la mayoría de los ataques son triviales.

Para prevenir los ataques es importante limitar los equipos, tener mecanismos de autenticación para el ingreso, además de mecanismos biométricos como analizadores de retina, huellas dactilares o de voz, tarjetas inteligentes, videocámaras.

- DESASTRES NATURALES

Siempre es bueno tomar en cuenta los posibles escenarios a los que nos enfrentamos como los desastres naturales, pues de lo contrario puede presentarse algo muy grave, en muchas ocasiones son quienes dañan más a los dispositivos de hardware en especial si no se tienen una implementación de controles preventivos y correctivos que impidan que los desastres naturales afecten el hardware y por consecuente el sistema.

Para prevenir o limitar problemas derivados de accidentes en el uso cotidiano de los equipos, tenemos que cuidar los aspectos siguientes:

1. Humedad
2. Exponer los equipos al polvo.
3. Incendios y humedad

- ALTERACIONES DEL ENTORNO

Todo puede ser afectado y alterado por factores distintos a lo cual surgen variaciones y por ende da problemas en el funcionamiento del hardware.
Entre estas se encuentran:

1. Ruido eléctrico
2. Daños por falta adecuada
3. Alimentación eléctrica

Para poder prevenir estas afecciones es importante el uso de estabilizadores de tensión, aire acondicionado en el momento adecuado, dar mantenimiento y limpieza a los ventiladores y disipadores, revisar que no exista humedad o polvo que afecte a los dispositivos de instalar tomas de tierra o filtros reguladores.

1.2.2. Seguridad con software

La seguridad con software es aquella que se dedica a proteger los programas, aplicaciones y software instalado en el equipo de cómputo, además de orientarse a la resistencia proactiva de posibles ataques.

Dentro de ellos el más conocido el antivirus, los cuales detectan y eliminan virus informáticos, si se ocupa un buen antivirus este actualiza y detecta incluso un nuevo virus. El software de seguridad generalmente incluye compuestos de: *(Ittgweb., 29 de mayo de 2016)*

- Cortafuegos
- Programa antivirus
- Software para filtrar contenidos
- Control de sitios web
- Filtro anti spam
- Software contra publicidad no deseada.

1.3. Firewall

1.3.1. Definición

El firewall es un dispositivo ya sea de hardware o software de seguridad de la red que monitorea el tráfico de red entrante y saliente, el cual decide si bloquea o permite específico en función de un conjunto definido de reglas de seguridad. Los Firewall establecen una barrera entre redes internas protegidas y controladas. Un firewall es un sistema de seguridad para redes, en ellas se evalúan los movimientos de tráfico, que pasan a través de dicha red, se podría decir que un firewall es una barrera la cual indica que una conexión puede ser peligrosa. *(Richar93., 19 de abril de 2021)*

VENTAJAS

Blindar la seguridad de la información que se mueva a través de la red.

- Es una medida de defensa para el ingreso de hackers.
- Es una de las primordiales barreras defensivas contra el programa malintencionado (virus).

DESVENTAJAS

- En varias situaciones puede verse limitada la rapidez de la conexión.
- Nuevos virus son capaces de evitar a ciertos Firewall, primordialmente aquellos que se esconden dentro del programa de nuestros propios grupos.
- No sustituye al programa antivirus, por cierto, es imprescindible instalar un antivirus gratuito o de pago para defender mejor los equipamientos.

1.3.2. Tipos de firewall

Como lo venimos mencionando, los firewalls tienen la finalidad de brindar seguridad y privacidad a nuestros dispositivos digitales y redes de conexión.

Es por ello que existen diversos tipos de firewall *(Técnico. 2020, 19 agosto)*

- *Nivel de Aplicación de Pasarela*: Este tipo emplea y analiza aplicaciones específicas, es decir como aquellas que permiten que un dispositivo tenga el control sobre otro y también las que establecen conexión entre dos ordenadores para intercambiar información.
- *Circuito a nivel de pasarela*: Los métodos de este tipo son para permitir la conexión de un usuario a un circuito, una vez establecido el acceso, no hay ningún tipo de restricción.
- *Firewall de capa de red o de filtrado de paquetes*: Realiza análisis constates en todas las formas de identificación de los usuarios y dispositivos. Por lo que al final se registran direcciones IP de origen y destino.
- *Firewall de capa de aplicación*: El trabajo de este es ser un intermediario para filtrar los accesos según los criterios que se establecieron para su funcionamiento. Es considerado uno de los más seguros hasta ahora.
- *Firewall personal*: Este firewall controla el tráfico de manera eficiente, desde un dispositivo hasta otro, el cual permite o no acciones.
- *Traducción de direcciones de red (NAT*): Con este firewall es posible que podamos mantener oculta la IP real del ordenador para proteger la información, este sistema no es exactamente clasificado como de seguridad, pero al haber protección de información podemos considerar que ya hay un método de defensa.

- *Firewall de hardware*: Este firewall defiende redes y dispositivos, es un equipo simple pues solo cuenta con componente físico y lógico. El dispositivo se conecta a redes. Ordenadores o servidores para establecer la protección. Como por ejemplo los routers.
- *Firewall predeterminado*: En la mayoría de los equipos los sistemas operativos cuentas con una protección predeterminada, que protege principalmente el componente lógico, es por ello que se considera de un alto nivel de defensa. Los ejemplos más comunes son:

    1. Windows defender
    2. Firewall de Mac
    3. UFW

Capítulo 2

2.1 Zona DMZ

Es una red que permite la protección de una red de área local (LAN) interna del tráfico no confiable, en otras palabras, es una subred que se encuentra entre la internet pública y privada. Lo que hace es crear una capa adicional de protección para los datos confidenciales que se encuentran almacenados en redes internas, el cual utiliza firewalls para la filtración de tráfico.

(¿Qué es una DMZ y por qué la usaría? | Fortinet, s. f.)

Los servicios de una DMZ incluyen:

1. Servidores DNS
2. Servidores FTP
3. Servidores de correo
4. Servidores proxy
5. Servidores web

Como conclusión podemos decir que una DMZ (zona desmilitarizada) permite que una organización acceda a redes no confiables, en este caso internet, además de que al mismo tiempo garantiza que una red privada o red de área local estén seguras.

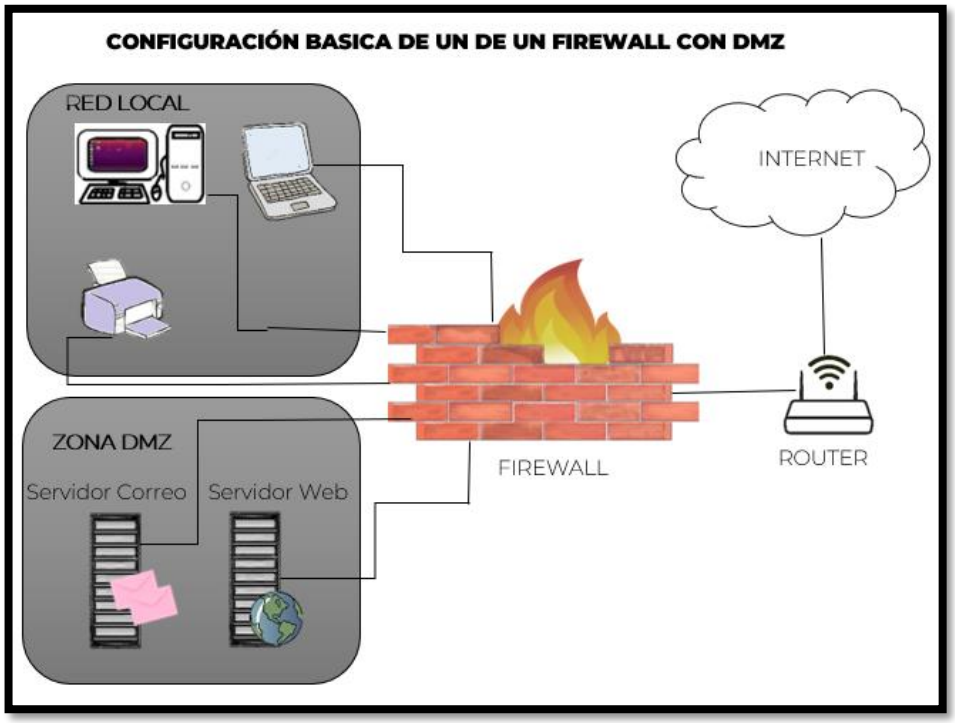


Figura 5: "Configuración básica de un firewall con DMZ".

2.2 Principales riesgos de seguridad en redes

A lo largo de la historia dentro de la seguridad en redes, se han presentado varios escenarios, en los que la falta de seguridad ha causado diversos problemas, por ejemplo:

1. El ataque DDoS (Denegación de Servicio Distribuido) detiene la calefacción en Finlandia en medio del invierno. *(Metropolitan., 2016, 7 noviembre)*

A finales de octubre en la Ciudad de Lappeenranta ubicada en el Este de Finlandia, un ataque de Denegación de Servicio Distribuido detuvo la distribución de calefacción en al menos dos propiedades, dicho ataque deshabilitó las computadoras que controlan la calefacción. La empresa encargada de la administración de distribución VALTIA, mencionó que se desactivaron temporalmente los sistemas que controlan la calefacción central y la circulación de agua caliente.

El sistema fue derribado por el ataque a la red, en un ataque DDoS la red está sobrecargada por el tráfico de múltiples ubicaciones con el objetivo de hacer que el sistema falle. El especialista en mantenimiento de edificios, Sami Orasaari, confirma que a menudo se descuida la seguridad de la automatización de edificios. Hay bastantes empresas que no quieren invertir en firewalls, en este caso, los dispositivos objetivo fueron atacados porque se descubrió que eran vulnerables y los atacantes han escaneado la red para encontrar más de ellos. En este caso la solución habría sido relativamente sencilla, bloqueando o reduciendo al máximo el tráfico procedente de la red mediante un Firewall.

2. Infiltraciones en cuentas de Instagram para promover el SPAM de citas para adultos. *(DigiCert., 2014, 12 marzo)*

En todo el año, DigiCert notó cómo se producían infiltraciones en cuentas de Instagram y se usaban para fomentar spam de citas para adultos. Este fenómeno coincidía con un informe anterior sobre infiltraciones en cuentas de Twitter para divulgar vínculos a sitios de citas para adultos, que presentaba ciertas similitudes con esta nueva campaña.

3. COVID-19 y Ciberseguridad. *(Nieto, A., 2020, 2 junio)*

Aun cuando las compañías contaran en el pasado con soluciones robustas de estabilidad en sus oficinas, la dinámica ha cambiado con el home office, donde los empleados permanecen en sus viviendas laborando o realizando uso de dispositivos particulares sin la misma defensa y volviéndose más vulnerables a cualquier ataque. La estabilidad está evolucionando ya que ahora las organizaciones deben buscar la manera de defender a los empleados que trabajan a partir de su hogar; en torno al 80% de la fuerza gremial migró a aquel esquema, según Eustolio Villalobos, country Manager para México, Centroamérica y el Caribe en SonicWall. “Habrá varios cambios

para alargar la estabilidad de la red de las organizaciones hacia la vivienda de los empleados, las empresas tienen que pensar en la estabilidad tipo cebolla; las resoluciones ya las poseemos y los canales se permanecen entrenando en lo cual necesita el usuario", describió.

4. El "inusualmente agresivo" ciberataque del que Microsoft acusa a China (y por qué no es simplemente una nueva crisis de ciberseguridad). *(BBC News Mundo., 9 de marzo de 2021)*

Desde el 2 de marzo, Microsoft informó que sus sistemas estaban siendo atacados. La filtración se aprovecha de una vulnerabilidad de Microsoft Exchange, o del robo de contraseñas, para hacerse pasar por alguien que tiene acceso autorizado al sistema. Si logra ingresar de esa manera, el atacante puede tomar control de la cuenta de correo de manera remota y robar datos. Microsoft ha señalado a un grupo conocido como Hafnium de ser los responsables del ataque con el respaldo del gobierno de China. China ha negado las acusaciones. Voceros de Microsoft han dicho que Hafnium "ataca principalmente entidades en EE.UU.", robando información de organizaciones como "investigadores de enfermedades infecciosas, firmas de abogados, instituciones educativas, contratistas de defensa, centros de pensamiento de políticas públicas y ONG".

5. La Generalitat sufre un ciberataque a sus comunicaciones y aplicaciones durante tres horas. *(PaÃ-s, E., 2021, 3 diciembre)*

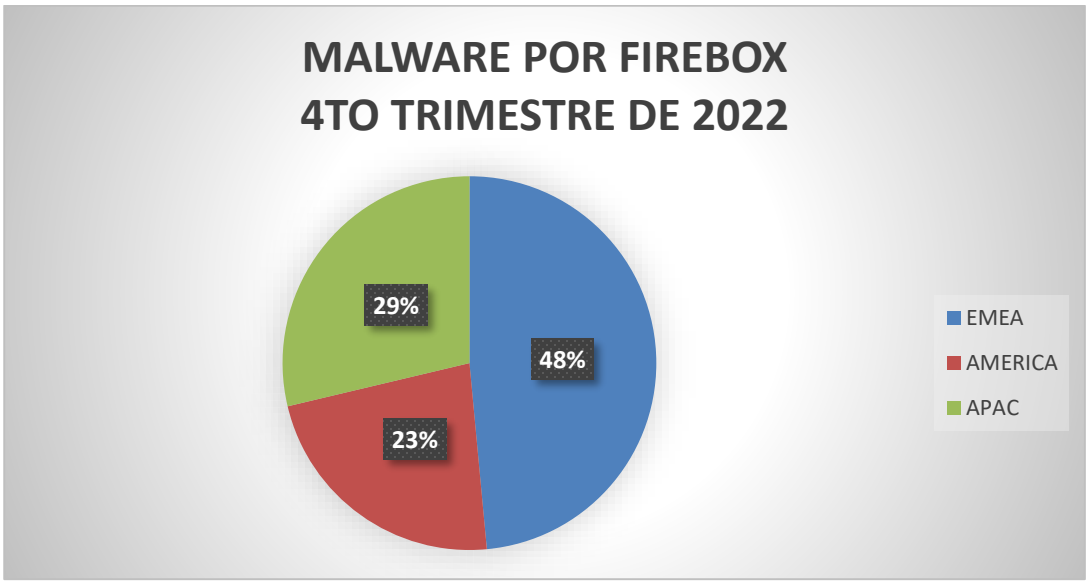
El Govern de la Generalitat ha sufrido la noche de este viernes un ciberataque que ha perjudicado a su nudo de comunicaciones y a unas 2.000 de sus aplicaciones. El vicepresidenteJordi Puigneró, que lidera el Departamento de Políticas Digitales, ha asegurado este sábado en una entrevista en Rac-1 que el Govern investiga los principios del ciberataque, que fue "el más potente en los últimos años en Cataluña con diferencia". La seguridad en los servidores es de suma importancia, nuestra información está expuesta al mundo entero si no nuestros equipos están desprotegidos, es por ello

que, los firewalls en servidores son de suma importancia, pues permiten navegar de forma segura en la red.

2.3 Estadísticas de intrusiones a redes sin firewall

Las intrusiones son la violación a las políticas de seguridad de un sistema, los intrusos suelen utilizar técnicas que alteran la arquitectura del sistema para así poder superar el proceso normal de autentificación. *(El nuevo informe de seguridad de WatchGuard Technologies revela una explosión del malware evasivo en el cuarto trimestre de 2019, 2020)*

De acuerdo a WatchGuard® Technologies líder global en seguridad e inteligencia en red, protección avanzada de *endpoints* (dispositivo informático remoto), autenticación multifactor (MFA) y Wi-Fi seguro, las intrusiones han aumentado de acuerdo al su último informe correspondiente al cuarto trimestre del año 2022, en el que habla de los ataques y amenazas de seguridad de red las cuales fueron analizadas por investigadores de WatchGuard Threat Lab . En dicho análisis encontraron una cifra récord de malware evasivo, esto aumenta en un 33 % lo que indica un nivel de amenazas “zero-day” más alto. Las amenazas a la red continuaron en ascendencia en América recibiendo la gran mayoría de ataques.



Graf. 1: Porcentaje de ataques en el cuarto trimestre del 2022. (WatchGuard Threat Lab, 5 de abril de 2022)

Se incrementan las tendencias observadas de trimestres anteriores pues dichas amenazas comúnmente pueden detenerse en el perímetro, es decir configurando los firewalls para descifrar y analizar el tráfico de datos entrantes, desafortunadamente este paso es uno de los que muchas organizaciones no implementan.

2.4 Análisis de principales intrusiones

Lo que intenta hacer una intrusión es acceder a determinada información para poder manipularla y de esta manera hacer que el sistema no funcione de forma correcta y segura, inclusive poder dejar al sistema inutilizable.

Dentro de las intrusiones más comunes principalmente están:

USUARIO FRAUDULENTO

Como su nombre lo indica se refiere a aquel usuario que accede de manera ilegal a los recursos.

Un ejemplo muy común es el famoso “phishing” (suplantación de identidad) el cual consiste en el envió de correos electrónicos los cuales son fraudulentos los cuales dirigen a los usuarios a páginas webs falsas, aparentando ser las reales. De esta forma solicitan información personal o bancarias.

Figura 6: Usuario Fraudulento “phishing”.

SUPLANTADOR

Es alguien que no tiene nada que ver con el acceso legítimo dentro de una organización, pero que ha obtenido la identidad de un usuario legítimo y ha obtenido acceso al nivel de causar daño.

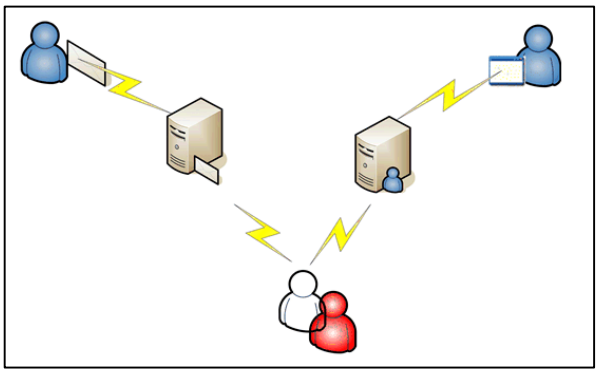


Figura 7: Suplantación mediante mensajería y correo electrónico. (BetaFred, 2018)

USUARIO CLANDESTINO

Una persona que puede realizar la gestión total del sistema de una organización.

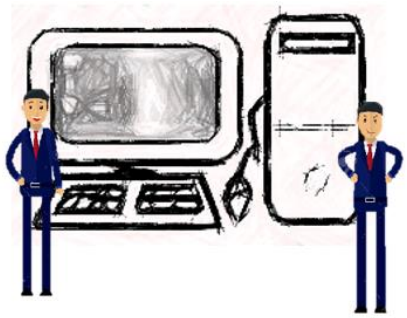


Figura 6: Suplantación "Usuario Clandestino".

2.5 Costo de firewalls de hardware y software y tabla comparativa

Bien podríamos pensar que proteger nuestros equipos podría salirnos costoso, pero existe una variedad para poder hacerlo de una manera más accesible, si bien las empresas deben invertir en su seguridad y el tema monetario no debería ser un problema, existen varias opciones también para ellas. En la tabla 4 podemos observar una comparativa de algunos firewalls y podemos percatarnos que los firewalls de software son gratuitos, por lo que para la protección personal de nuestros equipos es buena opción optar por ellos.

FIREWALL DE HARDWARE	COSTOS	FIREWALL DE SOFTWARE	COSTOS
Ubiquiti Unifi Security Gateway (USG) pro 4 port	$6,353.96	IPCop Firewall	GRATUITO
Firewall RED	$3,794.33	Vuurmuur	GRATUITO
Bitdefender Box 2	$1,014.81	pfSense	GRATUITO
Cortafuegos de seguridad de Internet inteligente (FIREWALL ZYXEL USGFLEX200BUN 4 PUERTOS)	$19,440.00	IPFire	GRATUITO

Tabla 3. Tabla comparativa (costos) de firewall de hardware y software.

Podemos concluir que el usar firewall en nuestros equipos, es de vital importancia, ya que hoy en día estamos mayormente expuestos a amenazas. El uso de redes sociales y demás aplicaciones modernas que se han introducido a la sociedad, vulnerando la información que manejamos en nuestros dispositivos electrónicos, con la herramienta del firewall podemos tener la tranquilidad de que estamos navegando en un entorno un poco más seguro.

Capítulo 3

3.1 Linux

3.1.1. Historia

Fundado en 1991 por Linus Torvalds, quien el objetivo principal era realizar un sistema operativo similar y compatible con UNIX. (*Aguilar, L. (2023, 7 junio)).*

Linux es un sistema operativo completamente libre, lo que lo hace gratuito, dicho sistema se puede usar libremente en cualquier equipo y de forma legal ya que no pertenece a ninguna compañía de ahí su forma libre, a diferencia de otros sistemas operativos grandes Linux es totalmente personalizable de dicha forma se puede satisfacer a cada usuario dependiendo a las necesidades, además de ser muy flexible ya que se puede utilizar en distintos dispositivos como servidores, supercomputadoras, teléfonos móviles y dispositivos IoT.

3.1.2. Características

Entre las características más importantes del Sistema Operativo Linux son:

- **Gratuito**: esta es una de las razones por las que muchos usuarios eligen Linux, ya que es un sistema operativo que se distribuye bajo licencias de código abierto, lo que lo hace aún más accesible.
- **Código Abierto**: la finalidad de que sea de código abierto es que más usuarios puedan ver y modificarlo para adaptarlo a las necesidades que se tengan.
- **Multitarea**: el ser multitarea significa que puede ejecutar varios programas al mismo tiempo, lo que hace que se empareje a otros sistemas como Windows y MacOs.

- **Multiusuario**: el que sea multiusuario quiere decir que muchos usuarios acceden a aplicaciones y recursos de una manera segura y simultánea, cada usuario podrá acceder solo a los archivos a los que tiene permitido, es decir, aunque varios usuarios puedan entrar a la vez la información jamás va a ser vulnerable ante los demás.
- **Personalizable**: es efectivamente esta una de las grandes ventajas que tiene Linux pues se puede usar al modo que en su momento queramos.

EJEMPLOS DE FIREWALL DE HARDWARE.

(Tpempresas.com, 14 de noviembre de 2019)

Los firewalls de hardware son dispositivos físicos que ayudan a la protección de un sistema. Algunos ejemplos son:

1. UBIQUITI UNIFI SECURITY GATEWAY (USG)

Firewall y enrutador de hardware avanzado que admite velocidades Gigabit Ethernet e inclusive más. El dispositivo está entre Internet y el enrutador WiFi local, enrutando todo el tráfico inclusive previo a que llegue al enrutador.

2. FIREWALL RED

La funcionalidad IPS está reducida a 100 Mbits. Consulte el archivo “hoja de especificaciones” en este listado, o la guía de compatibilidad en el lugar de construcción para enrutadores que funcionan con Firewall.

3. BITDEFENDER BOX 2

Se conecta a su enrutador (Wi-Fi sin malla / sin Google) y salvaguarda una porción sin límite de dispositivos conectados a Internet y Wi-Fi usando Total Security 2020 Unlimited, nuestra suite de estabilidad de red multiplataforma con cada una de las funcionalidades que asegura que todos sus dispositivos Windows, Mac, iOS, Android e IoT se encuentren salvaguardados.

4. CORTAFUEGOS DE SEGURIDAD DE INTERNET INTELIGENTE CUJO.

SEGURIDAD DE INTERNET 24/7. CUJO AI asegurar todos los dispositivos conectados a su enrutador WiFi. Los algoritmos de IA garantizan la protección contra el acceso remoto, el malware, el phishing y más. CUJO AI es el antivirus para todos los dispositivos inalámbricos en el hogar.

EJEMPLOS DE FIREWALL DE SOFTWARE

(Solvetic Sistemas., 13 de octubre de 2017)

Los firewalls de software básicamente son programas informativos que se instalan, existen varias opciones las cuales dependerán del equipo y el uso que se le dé al mismo. Algunos ejemplos de son:

1. IPTABLES

Herramienta de línea de comandos, esta herramienta es usada con frecuencia para configurar y administrar el conjunto de reglas de filtrado de paquetes, es una de las herramientas de firewall más usadas y tiene la capacidad de filtrar todos los paquetes en la pila de red dentro del mismo kernel. Dentro de sus características principales están:

- Enumera el contenido del conjunto de reglas del filtro de paquetes.

- Inspecciona sólo los encabezados de los paquetes lo cual hace el proceso mucho más ágil.
- Permite agregar, quitar o modificar reglas según las necesidades en los conjuntos de reglas de filtro de paquetes.
- Soporta copia de seguridad y restauración con archivos.

2. IPCOP FIREWALL

Figura 7: logo oficial (IPCop, 2022).

Esta herramienta de firewall de linux está dirigida a usuarios del hogar SOHO (Small office, Home Office), (pequeñas oficinas), la interfaz web es muy fácil de usar, esta puede configurar un equipo como una VPN para proporcionar un entorno seguro en internet. Las características de esta herramienta son:

- Interfaz Web codificada por color la cual nos permite monitorear los gráficos de rendimiento para CPU, memoria y disco, así como el rendimiento de la red
- Visualiza y rota automáticamente registros
- Soporte de múltiples idiomas
- Proporciona una actualización estable y fácilmente implementable segura y agrega parches actuales a nivel de seguridad

El sitio oficial para poder usar este firewall es: *(IPCop - Home, 2016).*

3. SHOREWALL

Figura 8: logo oficial (Shorewall, 2022).

Esta es una herramienta de configuración de gateway o firewall, esta herramienta es de alto nivel y nos permite configurar filtros de red, pues nos permite definir requisitos de firewall en un conjunto de archivos de configuración definidos mediante entradas. Este no usa el modo de compatibilidad ipchains de Netfilter y puede aprovechar las capacidades de seguimiento de estado de conexión de Netfilter. Dentro de sus principales características están:

- Usa las instalaciones de seguimiento de conexión de Netfilter para filtrado de paquetes con estado
- Soporta una amplia gama de aplicaciones de routers, firewall y gateway
- Administración de cortafuegos centralizada
- Interfaz GUI con el panel de control de Webmin
- Soporte múltiple de ISP
- Soporta Masquerading y reenvío de puertos
- Soporta VPN

El sitio oficial para poder usar este firewall es: *(Shorewall, s. f).*

4. UFW – UNCOMPLICATED FIREWALL

Figura 9: logo oficial (UFW , 2022).

En la actualidad está posicionado como uno de los firewall más dinámicos, simples y útiles de usar. UFW es un programa desarrollado para administrar un firewall de netfilter, su interfaz es de línea de comandos, además de proporcionar un marco simple para administrar netfilter. Sus principales características son:

- Compatible con IPV6
- Opciones de registro extendido con conexión y desconexión
- Supervisión del estado del firewall xz
- Marco Extensible
- Puede ser integrado con aplicaciones
- Permite añadir, eliminar o modificar reglas de acuerdo a las necesidades.

5. Vuurmuur

Vuurmuur *Firewall*

Figura 10: logo oficial (Vuurmuur, 2022).

Administrador de firewall construido sobre iptables, su configuración completa mente es a través de una GUI de Ncurses, la cual permite la administración remota segura a través de SSH o en la consola, soporta conformación de tráfico, además de que cuentan con potentes funciones de monitoreo las cuales permiten al administrador ver los registros, conexiones y uso de ancho de banda en tiempo real. Sus características son:

- No requiere de amplios conocimientos de iptables
- Posee sintaxis de reglas legibles por humanos
- Soporta IPv6 (experimental)
- Incluye modelado del tráfico
- Ncurses GUI, no se requiere X
- El proceso de portforwarding se hace muy simple
- Fácil de configurar con NAT
- Incluye política predeterminada segura
- Totalmente manejable a través de ssh y desde la consola (incluyendo desde Windows usando PuTTY)
- Scriptable para la integración con otras herramientas
- Incluye características anti-spoofing
- Visualización en tiempo real

- Visualización de la conexión en tiempo real
- Cuenta con registro de auditoría: todos los cambios se registran
- Registro de nuevas conexiones y malos paquetes
- Contabilidad del volumen de tráfico en tiempo real

El sitio oficial para poder usar este firewall es: *(Vuurmuur Firewall, s. f.).*

6. pfSense

Figura 11: logo oficial (pfSense, 2022).

Distribución de software de firewall, router de red de código abierto la cual está basada en el sistema operativo FreeBSD, este es usado para reglas de firewall, además de que puede incluir varios paquetes de software libre para poder tener funcionalidades adicionales. Sus características son:

- Altamente configurable y actualizado desde su interfaz basada en Web
- Se puede desplegar como firewall perimetral, enrutador, servidor DHCP y DNS
- Se puede configurar como punto de acceso inalámbrico y punto final VPN
- Ofrece Trafficshaping e información en tiempo real sobre el servidor
- Balanceo de carga entrante y saliente.

El sitio oficial para poder usar este firewall es: *(P.F.S.E.N.S.E. 2022)*

7. IPFire

Figura 12: logo oficial (IPFire, 2022).

Ha sido diseñado con diversos parámetros de modularidad y alto nivel de flexibilidad. lo que permite fácilmente implementar muchas variaciones tales como un firewall, un servidor proxy o una gateway VPN, Su diseño modular asegura totalmente que el funcionamiento sea exactamente según la configuración. Sus desarrolladores se centraron más en que esta herramienta sea de alta seguridad y por tal motivo la desarrollaron como un cortafuego, sus características están basadas en diversos segmentos que son:

- Verde: Indica un área "segura". Es donde se alojan todos los clientes regulares. Se compone generalmente de una red local cableada.

- Rojo: Indica "peligro" en la conexión a Internet. No se permite que nada de Red pase a través del firewall a menos que como administradores lo configuremos específicamente.

- Azul: Representa la parte "inalámbrica" de la red local (su color fue elegido porque es el color del cielo). Debido a que la red inalámbrica tiene el potencial de uso por parte de los usuarios, se identifica de manera única y las reglas específicas gobiernan a los clientes en ella. Los clientes de este segmento de red deben estar autorizados explícitamente antes de que puedan acceder a la red.

- Naranja: Se conoce como la "zona desmilitarizada" (DMZ). Todos los servidores que están públicamente accesibles están separados del resto de la red aquí para limitar las brechas de seguridad.

El sitio oficial para poder usar este firewall es*: (IPFire.org - IPFireDevelopmentTeam, s. f.)*

8. SmoothWall&SmoothWall Express

Figura 13: logo oficial (smoothwall, 2022).

Cortafuego de código abierto con interfaz web altamente configurable, la interfaz es conocida como WAM (Web Access Manager), el diseño hace más fácil el uso de su configuración, se configura a través de una GUI basada en WDB (Works DataBase), por lo que no requiere un conocimiento en Linux para poder usarla. Las características de SmoothWall&SmoothWall Express son:

- Soporta LAN, DMZ y redes inalámbricas, además de External
- Filtrado de contenido en tiempo real
- Filtrado HTTPS
- Proxies de soporte
- Visualización de registros y monitor de actividad de firewall
- Gestión de estadísticas de tráfico por IP, interfaz y consulta
- Facilidad de copia de seguridad y restauración.

El sitio oficial para poder usar este firewall es: *(Smoothwall-Home, s. f.)*

9. ConfigServer Security Firewall (CSF)

Figura 14: logo oficial (ConfigServer, 2022).

Basada en concepto de firewall de inspección de paquetes stateful y soporta casi todos los entornos de virtualización. Los sistemas en los que pueden ser instalados son:

- RedHat Enterprise v5 a v7
- CentOS v5 a v7
- CloudLinux v5 a v7
- Fedora v20 a v26
- OpenSUSE v10, v11, v12
- Debian v3.1 - v9
- Ubuntu v6 a v15
- Slackware v12 y dentro de sus características están las siguientes:
    - Script de cortafuegos SPI iptables directo
    - Cuenta con un proceso Daemon que comprueba los errores de autenticación de inicio de sesión para: Courier imap, Dovecot, uw-imap, Kerio, openSSH, cPanel, WHM,

Webmail (sólo servidores cPanel), Pure-ftpd, vsftpd, Proftpd, Páginas web protegidas por contraseña (htpasswd), fallos de mod_security (v1 y v2) y Exim SMTP AUTH.

- Concordancia de expresiones regulares
- Seguimiento de inicio de sesión POP3 / IMAP para reforzar los inicios de sesión por hora
- Notificación de inicio de sesión SSH
- Notificación de inicio de sesión SU
- Bloqueo excesivo de la conexión
- Integración de interfaz de usuario para cPanel, DirectAdmin y Webmin
- Fácil actualización entre versiones desde cPanel / WHM, DirectAdmin o Webmin
- Actualización sencilla entre versiones de shell
- Preconfigurado para trabajar en un servidor cPanel con todos los puertos estándar de cPanel abiertos
- Preconfigurado para trabajar en un servidor DirectAdmin con todos los puertos DirectAdmin estándar abiertos
- Autoconfigura el puerto SSH si no es estándar en la instalación
- Bloquea el tráfico en las direcciones IP del servidor no utilizadas: ayuda a reducir el riesgo para el servidor

- Alerta cuando los scripts de usuario final envían emails excesivos por hora con el fin de identificar scripts de spam
- Informes de procesos sospechosos: reportes de vulnerabilidades potenciales que se ejecutan en el servidor
- Reporte excesivo de procesos de usuario
- Bloquear el tráfico en una variedad de listas de bloques incluyendo DShield Block List y Spamhaus DROP List
- Protección de paquetes BOGON
- Configuraciones preconfiguradas para seguridad de firewall bajo, medio o alto (sólo servidores cPanel)
- IDS (IntrusionDetectionSystem) donde la última línea de detección le avisa de los cambios en los binarios del sistema y de la aplicación
- SYN Protección contra inundaciones, y muchas más.

El sitio oficial para poder usar este firewall es: *(ConfigServerServices., s. f.)*

3.2 Máquinas Virtuales

Una máquina virtual no es más que solo un sistema el cual carga a otro dentro de este, para poder simular una maquina PC, la cual nos ayuda a que no tengamos que realizar particiones a nuestro disco de la maquina real para poder introducir algún otro sistema operativo.

Existe un diferente número de herramientas para máquinas virtuales sin embargo las mejores máquinas virtuales que podemos encontrar son:

- Virtual Box

Es muy sencilla de utilizar además de que es una herramienta gratuita y se puede elegir entre una gran mayoría de opciones, la configuración es sencilla.

Una de las pocas desventajas que se podría consideras es que solo permite asignar un máximo de 128MB o 256MB de memoria gráfica.

- VMWARE

Al ejecutar las virtualizaciones en las máquinas virtuales, permite restaurar la maquina al haber recibido un fallo o ataque.

Tiene eficiencia de energía, creación de entorno de pruebas. Y finalmente esta herramienta es de pago.

- PARALLELS DESKTOP 14.

Para usar este programa debemos pagar, sin embargo, te ofrece una prueba gratuita, por lo que es una gran desventaja.

- GNOME BOXES.

Esta herramienta es específica para Linux, es decir está especializada en crear máquinas virtuales en entorno Linux.

- BOOT CAMP.

Esta es una herramienta exclusiva en Mac para poder virtualizar Windows en ella.

Todas ellas tienen el mismo fin el cual es crear un sistema operativo dentro de otro sistema operativo, sin embargo, al realizar un análisis y sin mucho adentramiento en las diferentes herramientas para virtualización, se optó por utilizar la más común y fácil de adquirir además de sus grandes ventajas de sencillez, la cual es VIRTUAL BOX

3.3 Comparativa de Firewalls para Linux

Para el Sistema Operativo Linux existe una cantidad considerable de firewall, en la tabla 5 se muestran algunos ejemplos:

NOMBRE DE FIREWALL	VENTAJA	DESVENTAJA
IPTABLES	• Se encuentra integrado con el sistema operativo	• Se debe ir probando de una por una en a consola hasta que funcione.
SHOREWALL	• Gran variedad de documentación. • Implementación rápida y sencilla.	• No contiene modo gráfico. • Debido a la gran documentación es muy difícil encontrar aspectos puntuales.

pfSense	• Interfaz web atractiva • Software libre • Implementación del protocolo. • Establece prioridades según el tipo de tráfico en la red.	• Gran parte de sus funciones no están documentadas por lo que hay que entrar a foros para poder tener un avance completo.
IPCOP	• Interfaz web atractiva • Fácil de configurar • Requerimientos mínimos • Software libre.	• Gran parte de sus funciones no están documentadas por lo que hay que entrar a foros para poder tener un avance completo.

Tabla 4. Comparación de algunos firewalls (ventajas y desventajas)

Aquí podemos ver que, con los ejemplos elegidos al azar, después de una comparación sencilla pero puntual, por sus mayores ventajas y menos desventajas se eligieron utilizar los firewalls de software para Linux PFSENSE e IPCOP.

Capítulo 4

4.1 Definición de firewalls a instalar

Después de un análisis sobre que firewalls poder usar, se eligieron dos que son:

4.1.1 pfSense

Está orientado a firewall (cortafuegos) basado en FreeBSD, el cual es muy popular a nivel profesional y doméstico, consume muy pocos recursos y tiene una interfaz gráfica completa e intuitiva. Es un software de libre por lo que tiene actualizaciones frecuentes de seguridad.

El rendimiento de este software es alto a comparación de otros pues inclusive ya ha sido catalogado como uno de los servicios de firewall más seguros y de mayor velocidad. Además de que es un software que tiene la función de reporte y monitoreo en tiempo real, lo que hace tener una buena ventaja a la hora de tener el control sobre el acceso a nuestra red privada.

Su principal característica es proporcionar seguridad a cualquier entorno doméstico y empresarial, el objetivo de este sistema es de usarse como firewall, pero también puede usarse como router principal ya que dispone de muchísimas opciones de configuración avanzadas.

4.1.2 IpCop

En principio, IpCop es un software que se enfoca en implementar funciones de Firewall, lo que nos permite asegurar nuestra red de una manera completamente transparente y con costos de implementación muy bajos porque los requisitos son mínimos y además es un software gratuito que elimina los costos de licencia.

IpCop está capado y solo tiene instaladas las herramientas justas para su función como firewall de esta manera limita el daño que pudiera hacer el intruso al sistema.

4.2 Descripción de los firewalls

pfSense

- Conexión red a red
- Conexión Host a Red
- Configuración Asistida
- Configuración de OpenVPN
- Visualización de estados (clientes)

IPCop

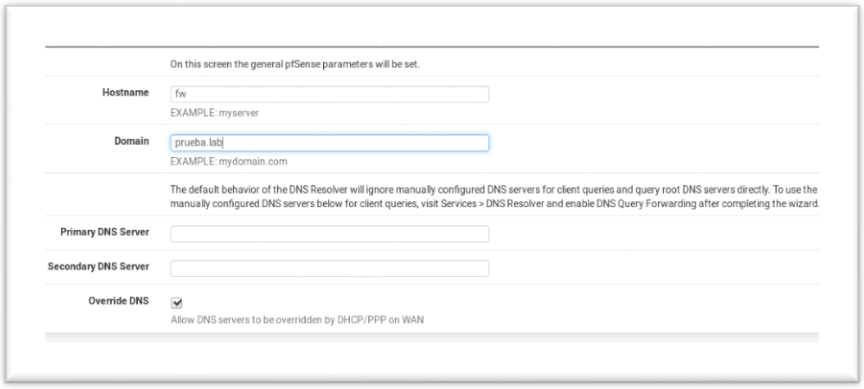
- Conexión Host a Red
- Exportación solo de certificados
- Visualización de estado de conexión y estadísticas

4.3 Configuración e instalación

Para la instalación de los firewalls es importante seguir ciertos pasos para que su funcionamiento sea el correcto y de esta forma tener la seguridad de que realizara correctamente su trabajo.

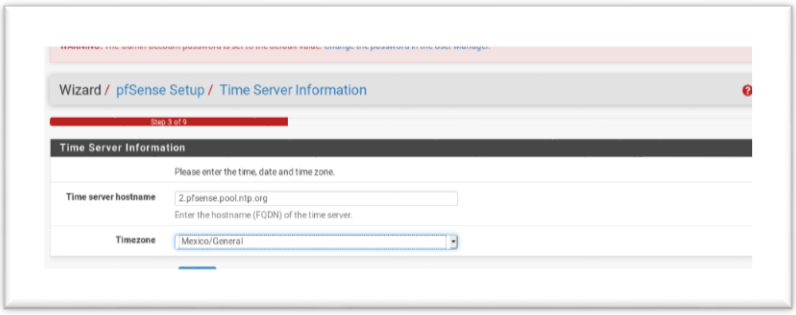
4.3.1. Configuración e instalación de pfSense

Vamos a cambiar el hostname por “fw” y en dominio ponemos “prueba.lab”, como se está utilizando DHCP, utilizamos la opción llamada “override DNS (sobre escritura del DNS)”



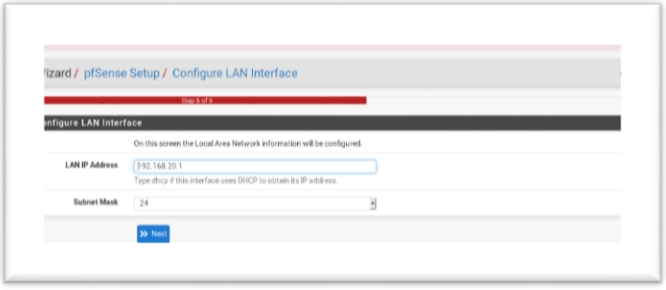
Captura de pantalla 1. Instalación y configuración de Pfsense

Seleccionamos el tiempo de zona:



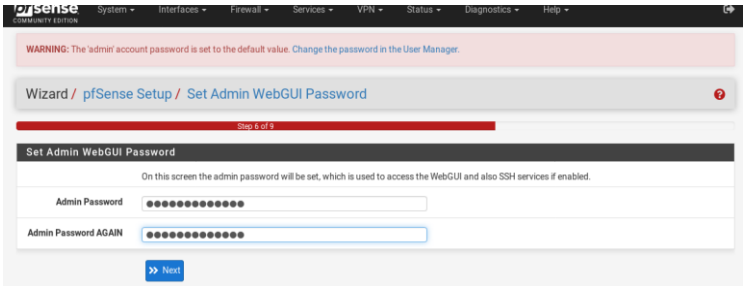
Captura de pantalla 2. Instalación y configuración de Pfsense

Verificamos que configuración de la red LAN esta bien 192.168.20.1 / 24



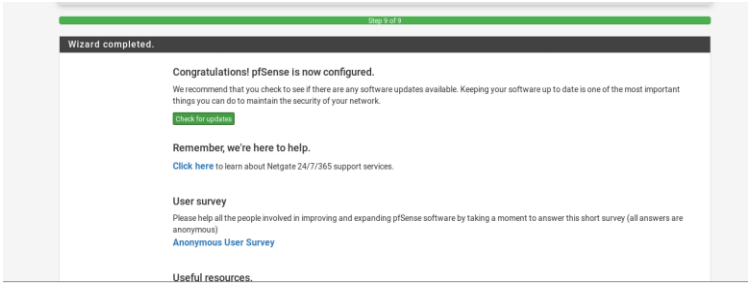
Captura de pantalla 3. Instalación y configuración de Pfsense

Ponemos una contraseña más robusta para el admin.



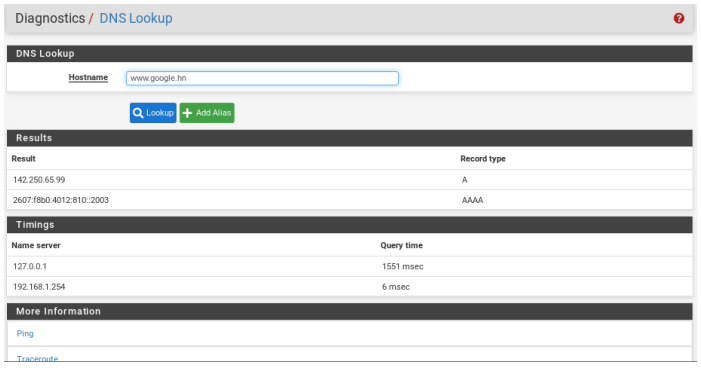
Captura de pantalla 4. Instalación y configuración de Pfsense

Se recargan todas las configuraciones y finalizamos



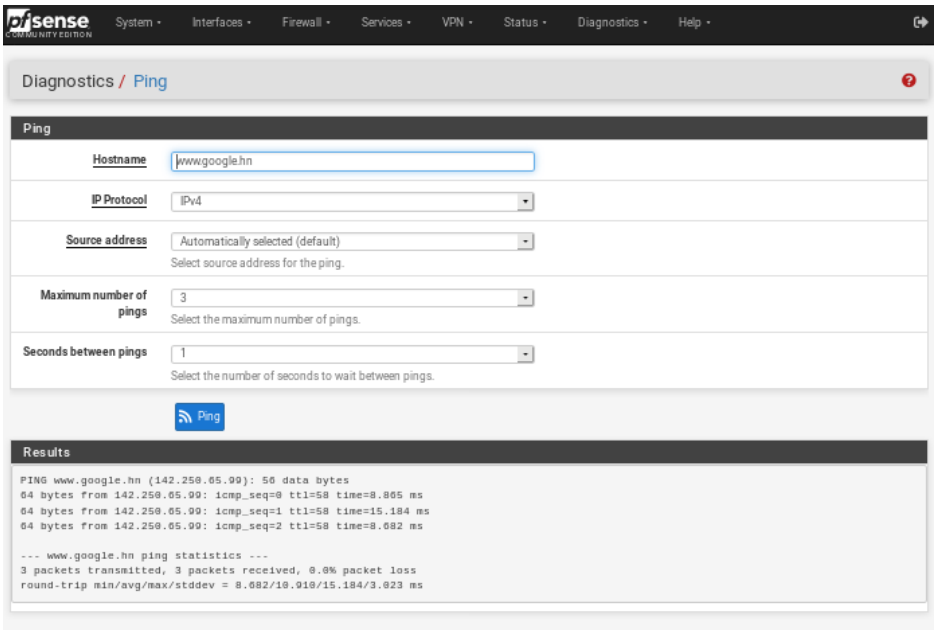
Captura de pantalla 5. Instalación y configuración de Pfsense

Comenzamos con una búsqueda DNS y verificamos que nos resuelva, lo que se muestra en la captura de pantalla siguiente son las direcciones IP de los servidores DNS del proveedor. Y también se muestra el local host 127.0.0.1.



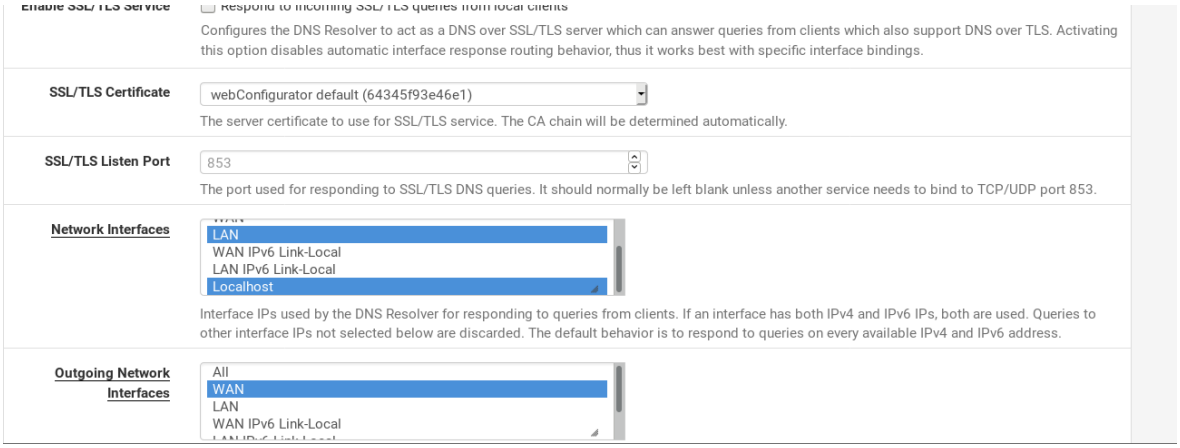
Captura de pantalla 6. Instalación y configuración de Pfsense

Verificamos que se pueda hacer ping hacia afuera y esperamos a que nos responda de manera factible, de esta manera sabemos que el servidor tiene conectividad con el internet. Para realizar una configuración básica lo que debemos verificar es que el ordenador (cliente) tenga conexión a internet y que se pueda navegar.



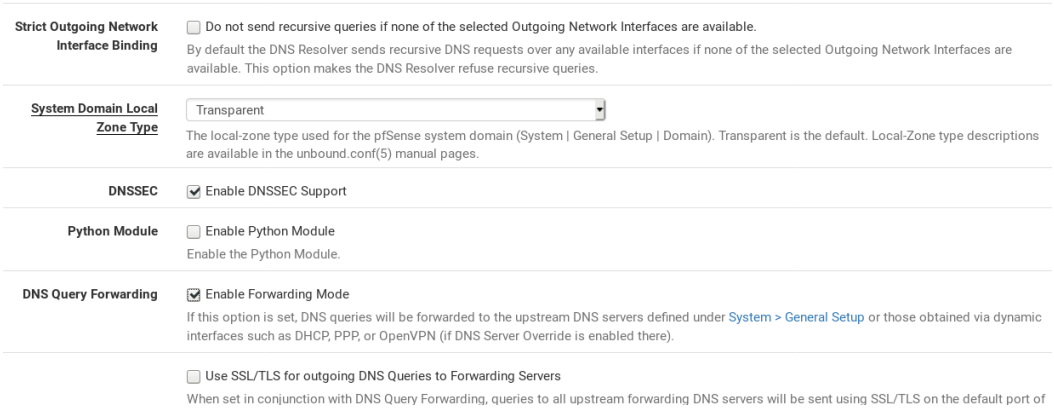
Captura de pantalla 7. Instalación y configuración de Pfsense

Modificaremos el DNS, en la parte de Network Interface seleccionaremos LAN (Red de Área Local) y Localhost, en la interface de salida seleccionamos WAN (Red de Área Amplia).

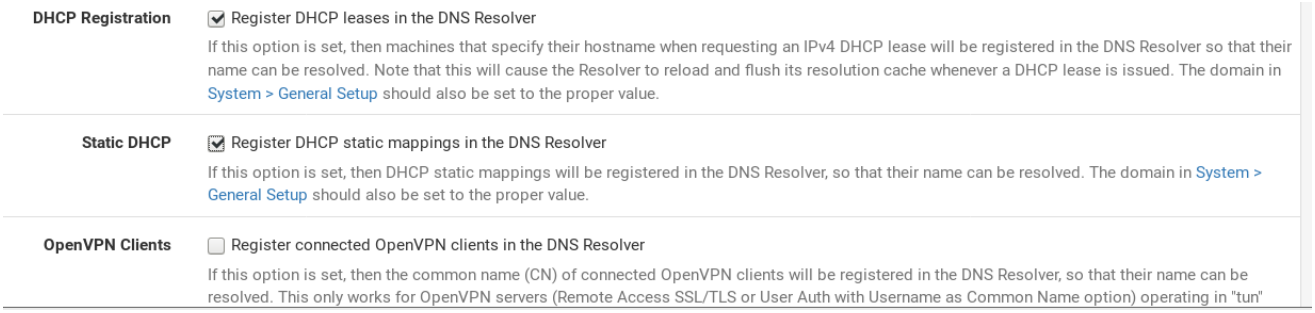


Captura de pantalla 8. Instalación y configuración de Pfsense

También seleccionamos la petición de redireccionamiento DNS (DNS Query Forwarding) y seleccionamos las opciones para los registros del DHCP tanto dinámico como estático.

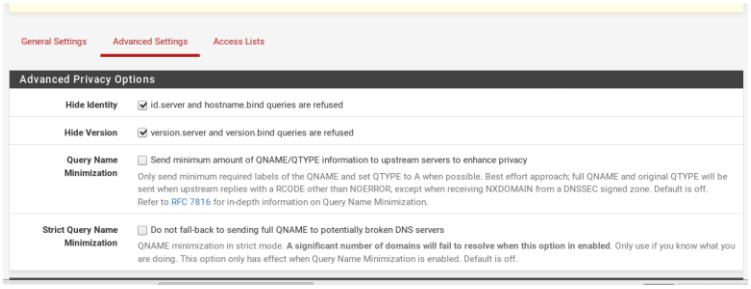


Captura de pantalla 9. Instalación y configuración de Pfsense

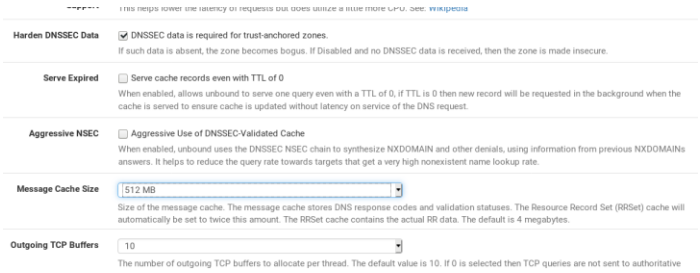


Captura de pantalla 10. Instalación y configuración de Pfsense

Nos vamos a las configuraciones avanzadas y en la parte del cache para el DNS seleccionamos 500 MB

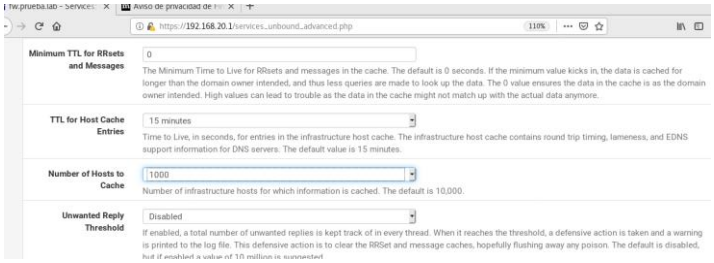


Captura de pantalla 11. Instalación y configuración de Pfsense



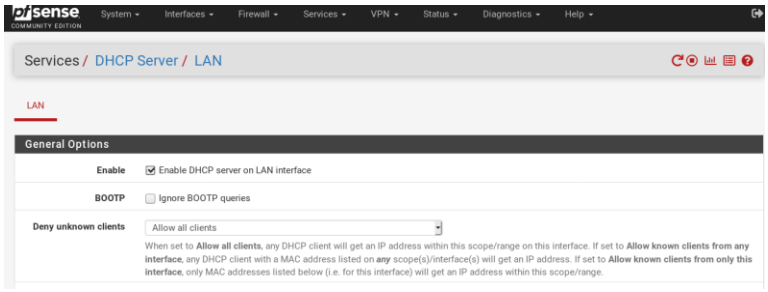
Captura de pantalla 12. Instalación y configuración de Pfsense

En el número de ordenador para Cache seleccionamos 1000 y procedemos a salvar la configuración



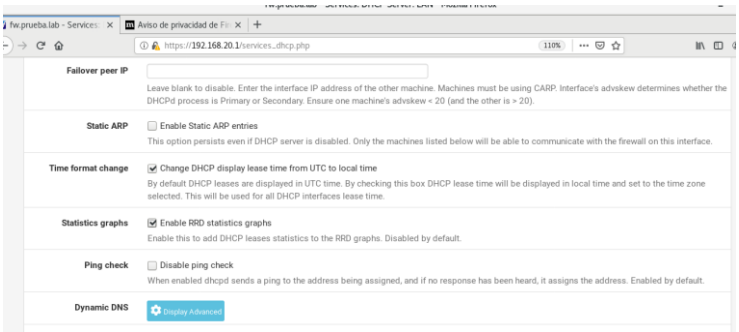
Captura de pantalla 13. Instalación y configuración de Pfsense

Nos vamos al Servidor DHCP se observa el rango que se configuró después de la instalación



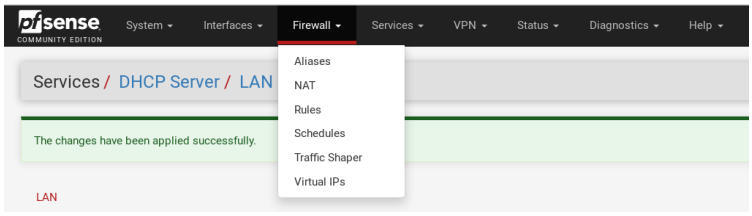
Captura de pantalla 14. Instalación y configuración de Pfsense

Se habilitan las opciones para cambiar el formato del tiempo y para que muestre la grafica de estadísticas y salvamos.



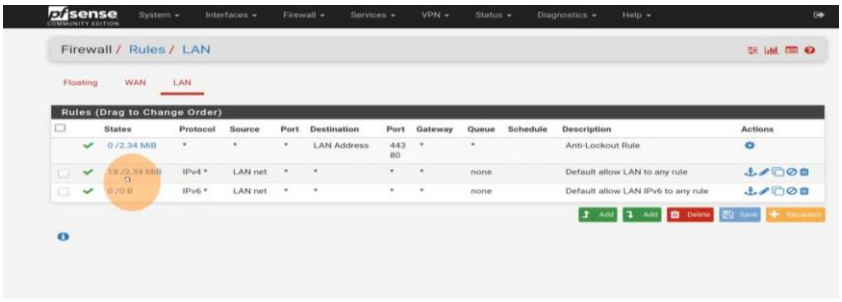
Captura de pantalla 15. Instalación y configuración de Pfsense

Nos vamos a las reglas del corta fuego, en donde podemos observar las pestañas floating, WAN y LAN.

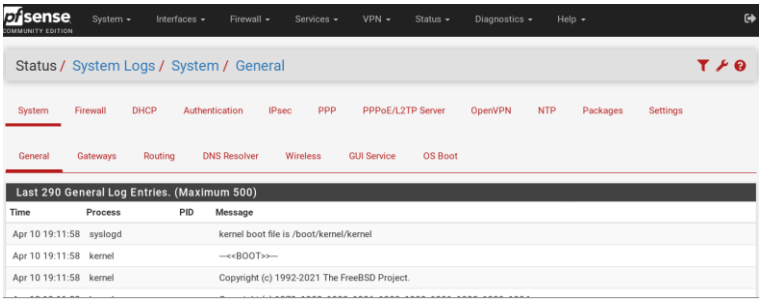


Captura de pantalla 16. Instalación y configuración de Pfsense

Nos vamos a la pestaña LAN en donde podemos observar tres reglas, la primera es una regla anti local, la cual no es necesaria al menos que necesitemos utilizarla para hacer ajustes en el servidor, la penúltima regla que aparece es para filtrar los paquetes de datos mediante el protocolo IPV4, se muestra el estado y finalmente la última regla que se observa es IPV6 la cual no se está utilizando así que se procede a eliminarla.

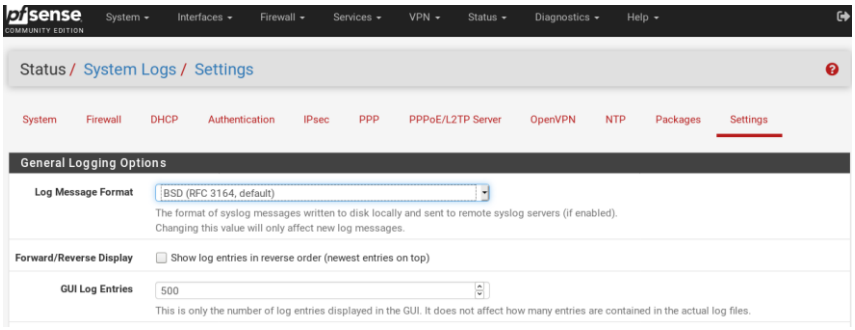


Captura de pantalla 17. Instalación y configuración de Pfsense



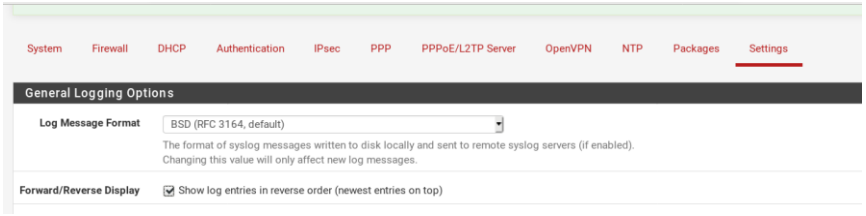
Captura de pantalla 18. Instalación y configuración de Pfsense

Posteriormente nos vamos a realizar una limpieza de los registros



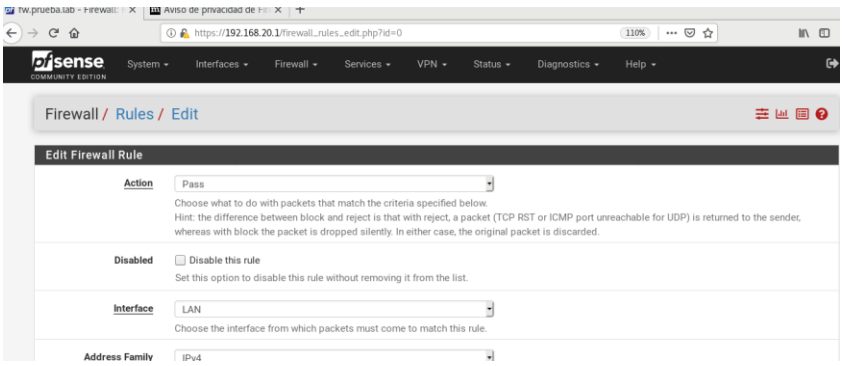
Captura de pantalla 19. Instalación y configuración de Pfsense

Seleccionamos la casilla para que nos muestre los registros de forma reversa (registros nuevos arriba, registros viejos abajo), salvamos las modificaciones.



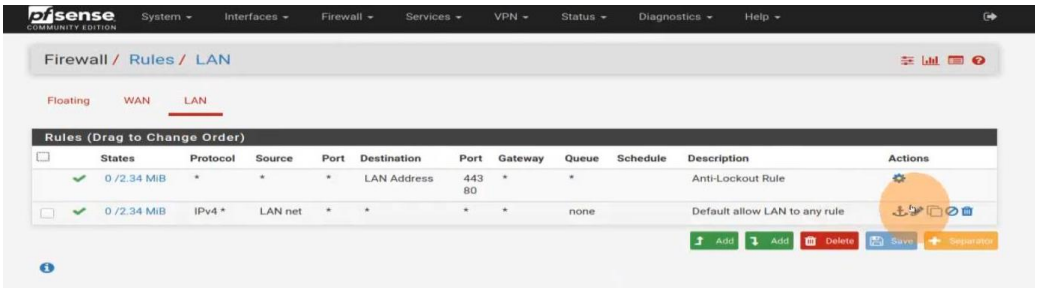
Captura de pantalla 20. Instalación y configuración de Pfsense

Volvemos a las reglas del cortafuego



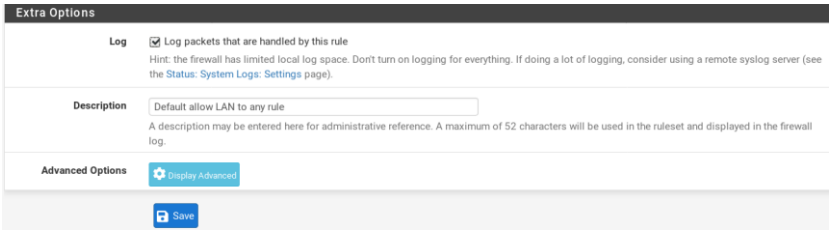
Captura de pantalla 21. Instalación y configuración de Pfsense

Y modificaremos la regla



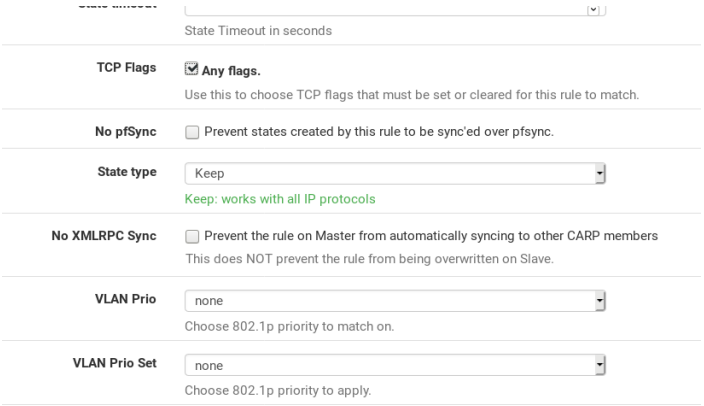
Captura de pantalla 22. Instalación y configuración de Pfsense

Habilitamos la casilla “Log” para que nos muestre todos los registros de los paquetes.



Captura de pantalla 23. Instalación y configuración de Pfsense

Habilitamos la opción de “TCP Flags” para utilizar todas las opciones Flags TCP y finalmente salvamos.

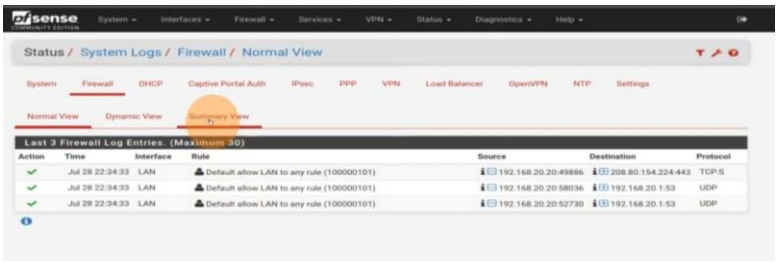


Captura de pantalla 24. Instalación y configuración de Pfsense

Finalmente verificamos que podamos navegar y posteriormente revisamos los registros del cortafuego.

Captura de pantalla 25. Instalación y configuración de Pfsense

Aquí se muestran los registros



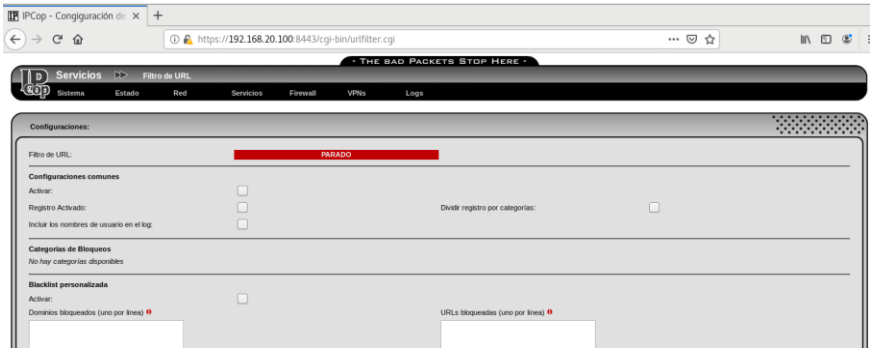
Captura de pantalla 26. Instalación y configuración de Pfsense

4.3.2. Configuración e instalación de IpCop

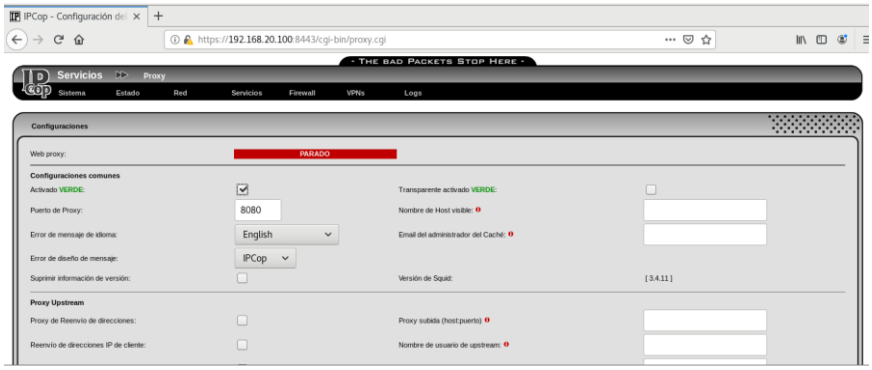
Ingresamos la dirección IP y se muestra la vista principal de nuestro firewall y observamos los servicios que nos ofrece nuestro firewall.

Captura de pantalla 27. Instalación y configuración de IpCop

Tenemos que habilitar el PROXY, el cual tenemos que habilitar en verde, puerto proxy 8080



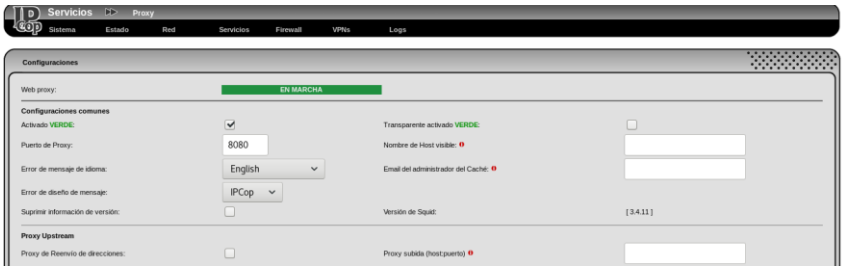
Captura de pantalla 28. Instalación y configuración de IpCop



Captura de pantalla 29. Instalación y configuración de IpCop

Nos muestra los puertos estándar permitidos y la red permitida que en este caso es la de nuestro firewall cliente, se guarda y se reinicia el proxy para guardar los cambios

Captura de pantalla 30. Instalación y configuración de IpCop



Captura de pantalla 31. Instalación y configuración de IpCop

Finalmente observamos que tenemos activado el administrador de red (VERDE) para permitir la navegación a internet en la Red de Área Local.

Captura de pantalla 32. Instalación y configuración de IpCop

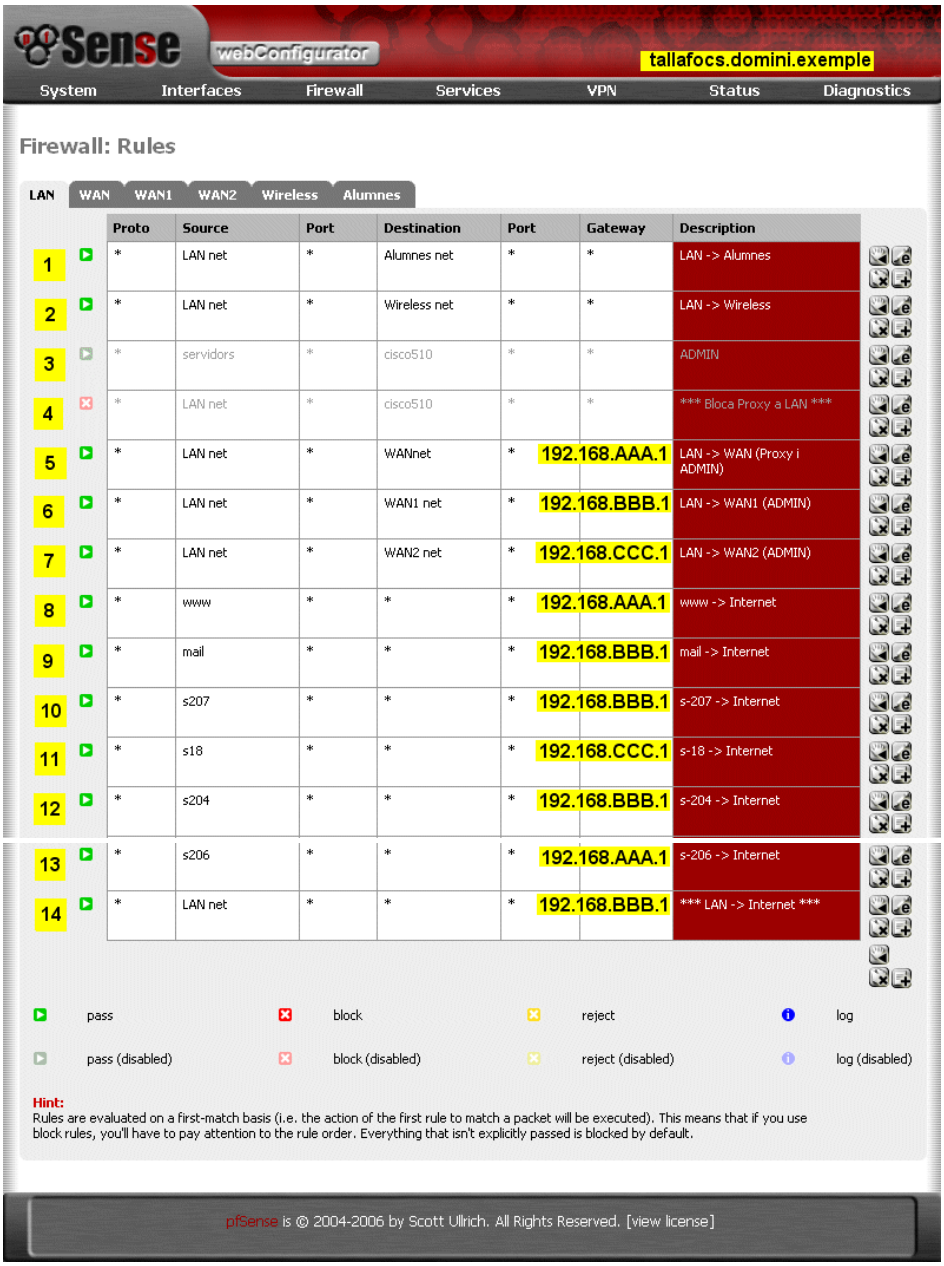
4.4 Definición de reglas de firewall

Los firewalls tienen reglas importantes para su buen desempeño y es importante establecerlas para tener una buena protección en nuestro equipo.

4.4.1 Reglas de pfSense

1. Permite cualquier acceso desde la red LAN a la red Alumnes.
2. Permite cualquier acceso desde la red LAN a la red Wireless.
3. Se permite cualquier acceso desde los servidores al servidor proxy, situado en la red WAN.
4. Se bloquea para el resto de ordenadores de la red LAN el acceso al servidor proxy (situado en la red WAN). De esta forma se fuerza la navegación directa, sin proxy (gracias a proxy.pac).
5. Cualquier ordenador de la red LAN puede ir a la red WAN, siendo la puerta de enlace la IP privada del router ADSL (Línea digital de banda ancha con gran capacidad para la transmisión de datos a través de la red de telefonía básica.) (192.168.AAA.1). En la práctica esto permite llegar al router ADSL (por ejemplo, para hacerle ping).
6. Lo mismo que el paso número 5, pero para WAN1. Permite administrar el router ADSL.
7. Lo mismo que el punto número 5 y 6, pero para WAN2. Permite administrar el router ADSL.
8. Se accede a www de la red LAN empleando el router.
9. Se accede a mail de la red LAN empleando el router.
10. s207 de la red LAN accede a Internet empleando el router.
11. s18 de la red LAN accede a Internet empleando el router.
12. s204 de la red LAN accede a Internet empleando el router.
13. s206 de la red LAN accede a Internet empleando el router.

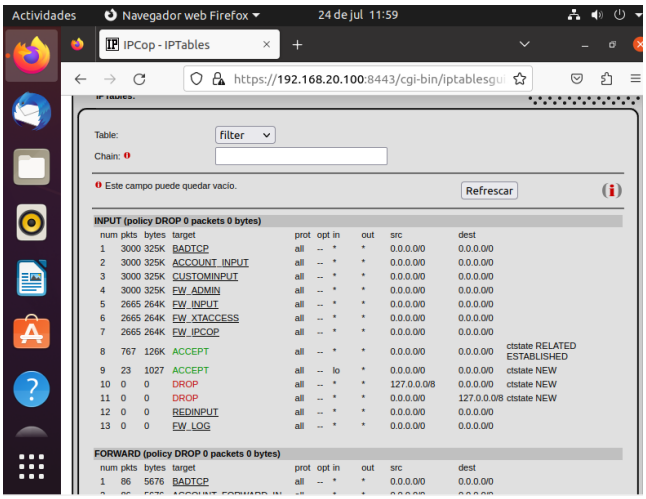
14. El resto de tráfico de la red LAN saldrá hacia Internet empleando el router.



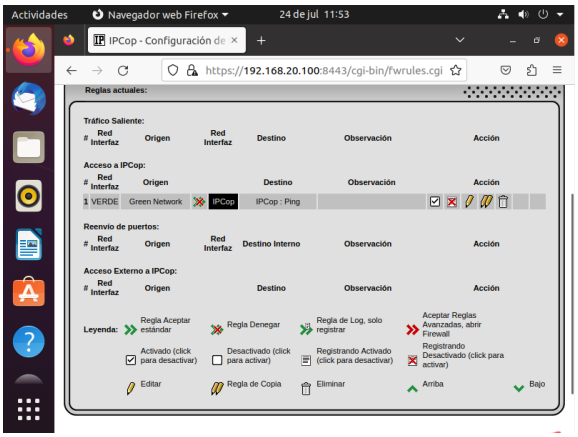
Captura de pantalla 33. Reglas de PfSense

4.1.2 Reglas de IpCop

Lo primero que haremos antes de empezar a definir nuevas reglas en nuestro firewall es comprobar que reglas se han definido en la instalación. En este caso podemos concluir que las reglas para IpCop las iremos agregando conforme las acciones que mas nos convengan o vallamos necesitando, es decir que con las reglas que se tienen por la instalación el firewall, cumple el funcionamiento correcto.



Captura de pantalla 34. Reglas de IpCop generadas desde instalación.



Captura de pantalla 35. Reglas de IpCop agregadas, ejemplo: denegación de ping a la red interna a IPCop.

Capítulo 5

5.1 Esquema de laboratorio de pruebas

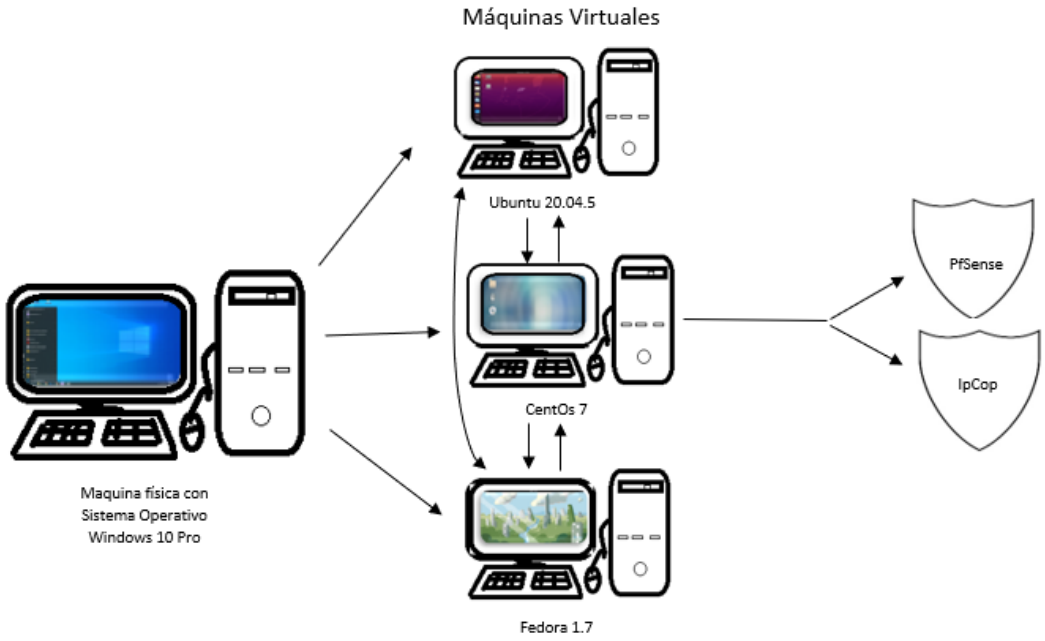


Figura 15. Esquema de laboratorio de pruebas.

5.2 Pruebas

Comentaremos las pruebas elaboradas a nuestros firewalls si tienen el funcionamiento optimo y cómo podemos realizar la conclusión al haber usado estos cortafuegos, además de la importancia verdadera de tener uno para poder proteger nuestros equipos.

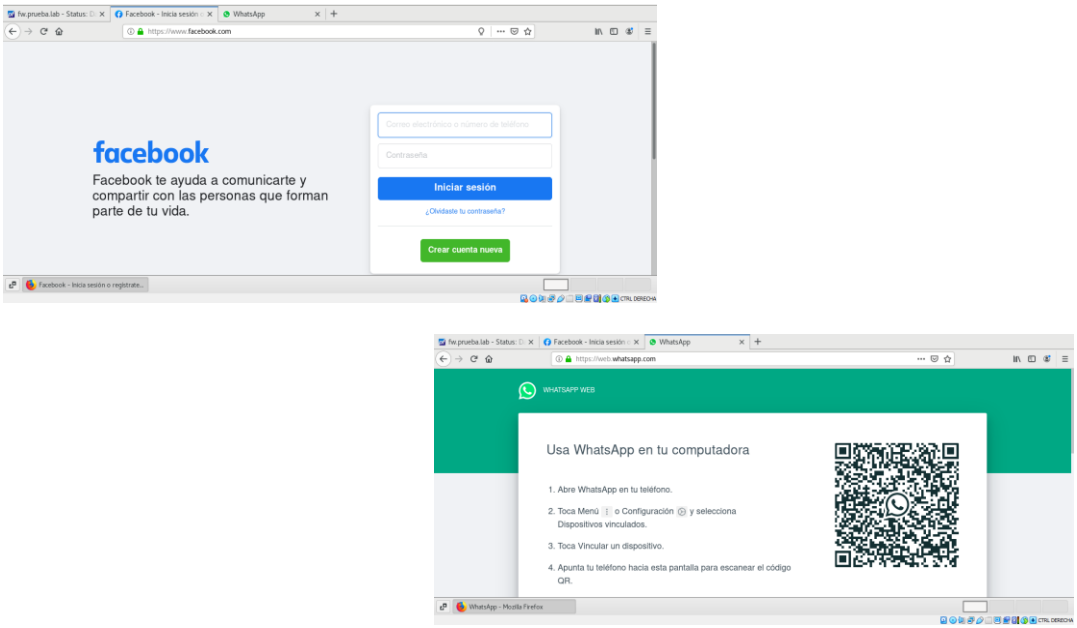
Para esta prueba realizamos el bloqueo de páginas de internet (Facebook y WhatsApp) por medio de ambos cortafuegos (firewall), realizamos la configuración en cada uno para ver su efectividad en protección.

5.3 Resultados

5.3.1 Bloqueo de páginas web con PfSense (Facebook y WhatsApp).

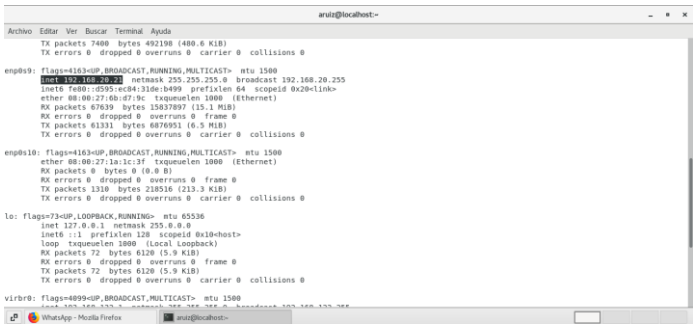
En primer lugar, se tiene la prueba de Pfsense, en la cual ocurrió la configuración siguiente:

1. Como primera instancia vamos a verificar que en nuestro navegador podamos acceder a la página de Facebook y WhatsApp.



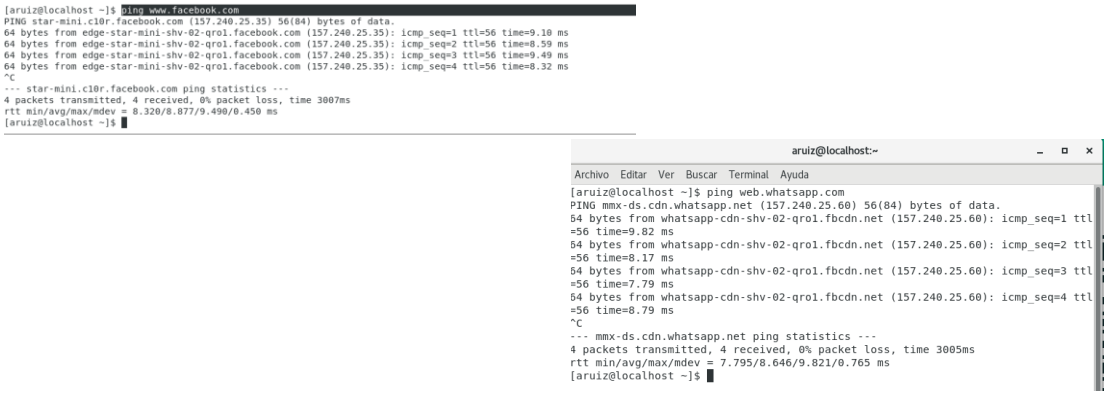
Captura de pantalla 36. Capturas de pantalla de los accesos a la paginas de Facebook y Whatsapp.

2. Una vez que se verificó el acceso procedemos a ingresar a la interface web grafica de firewall. Y verificamos mediante una terminal la dirección IP que está manejando con el comando ifconfig, en este caso la 192.168.20.21.



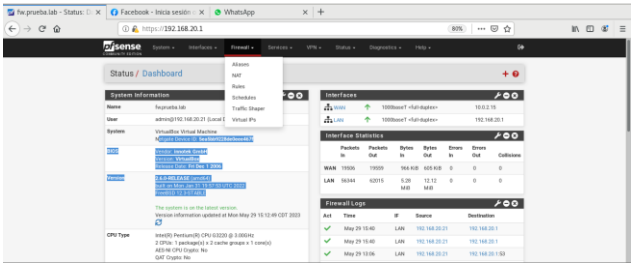
Captura de pantalla 37. Capturas de pantalla de los accesos a la paginas de Facebook y Whatsapp.

3. Ahora es importante verificar que hay comunicación con las páginas web, por lo que realizaremos “ping” hacia ellas y tomamos nota de las IP de cada una de las páginas en este caso vemos que Facebook tiene una ip de 157.240.25.35 y whatsapp de 157.240.25.60, pues las ocuparemos al momento de configurar en psfsense.



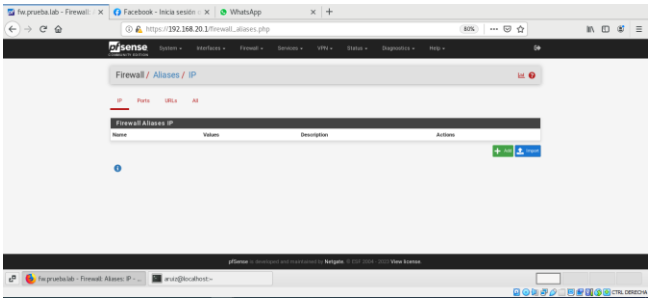
Captura de pantalla 38.. Capturas de pantalla de los accesos a la paginas de Facebook y Whatsapp.

4. Ahora procedemos a realizar la configuración correspondiente, en la interfaz podemos observar el menú y nos dirigimos a donde dice “firewall” y seleccionamos “aliases”



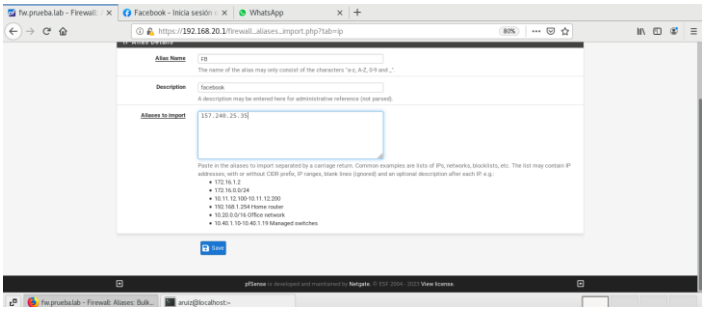
Captura de pantalla 39.. Capturas de pantalla de los accesos a la paginas de Facebook y Whatsapp.

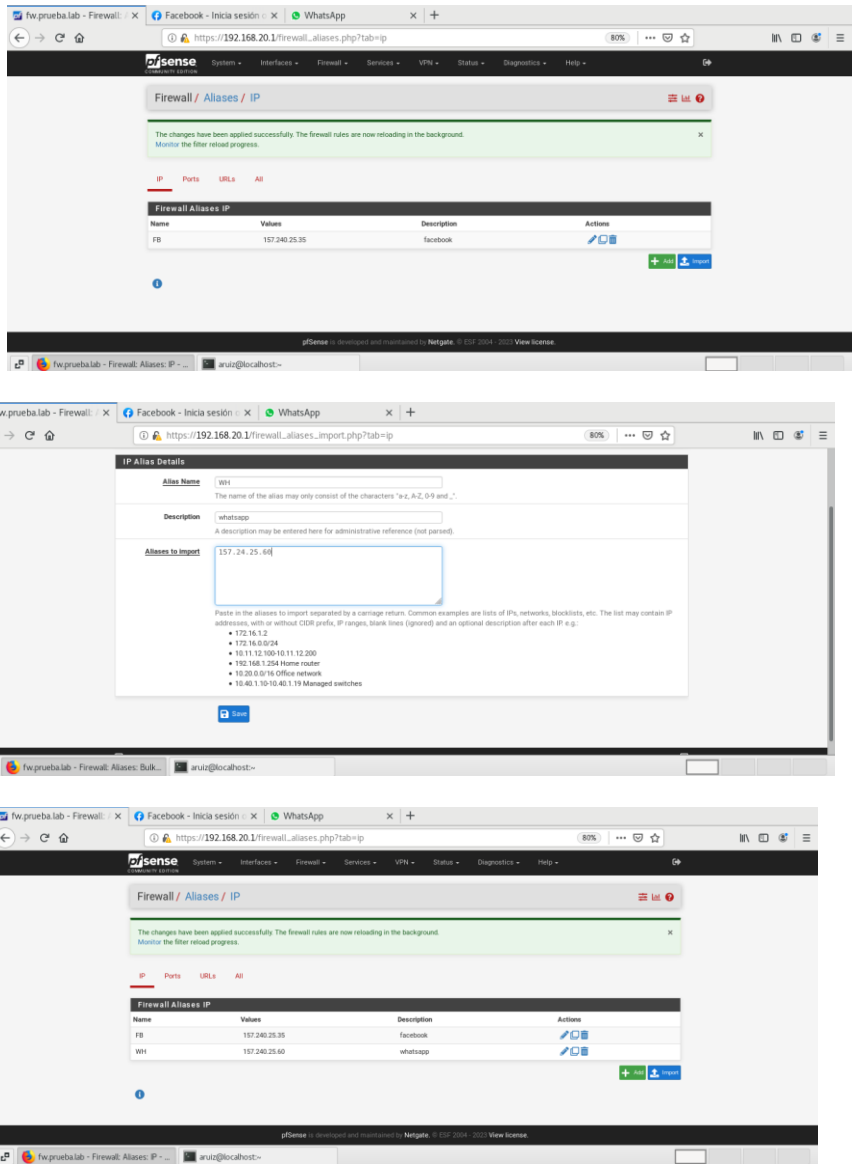
5. Posteriormente le damos en “Add”, aquí ingresaremos los datos para realizar el bloqueo para facebbook y whatsapp.



Captura de pantalla 40. Capturas de pantalla de los accesos a la paginas de Facebook y Whatsapp.

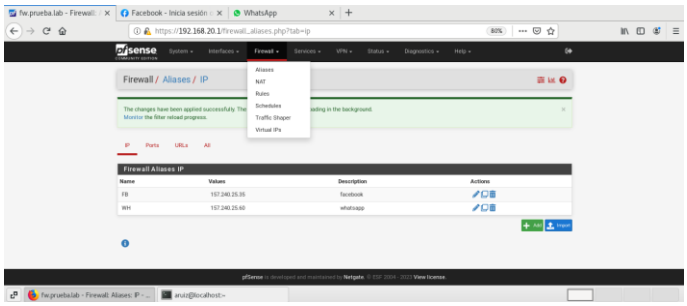
6. Llenamos los datos, se pondrá el nombre alias, la descripción y la IP que tiene asignada, se realizará para ambos casos.

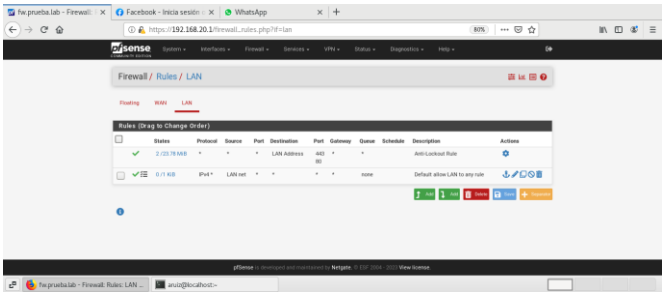




Captura de pantalla 41. Capturas de pantalla de los accesos a la páginas de Facebook y Whatsapp.

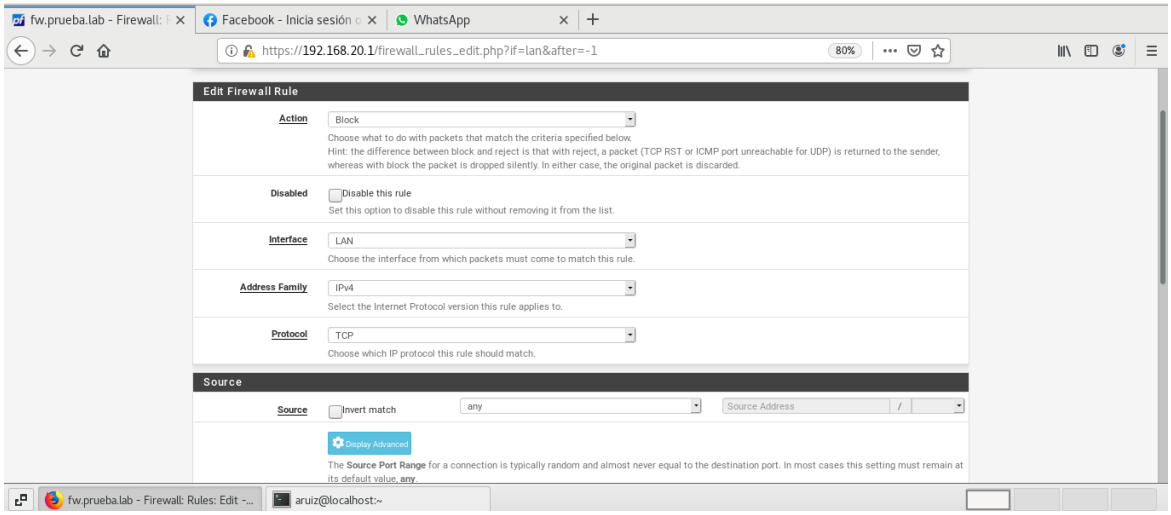
7. Nos dirigimos al menú y en “firewall” seleccionamos “Rules” y seleccionamos “Add”, pero el que tiene la flecha apuntando hacia arriba.

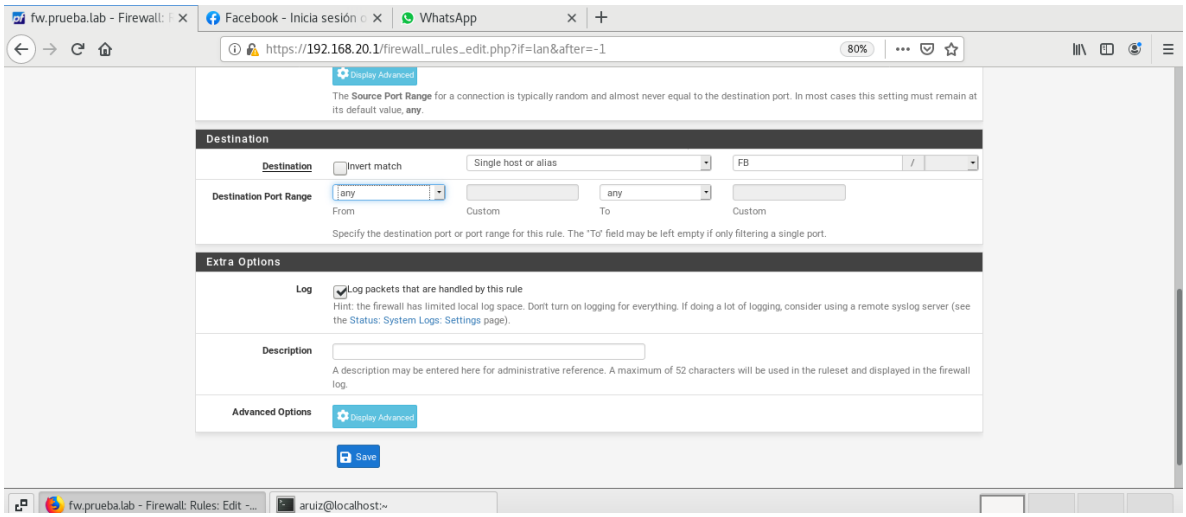




Captura de pantalla 42. Capturas de pantalla de los accesos a la paginas de Facebook y Whatsapp.

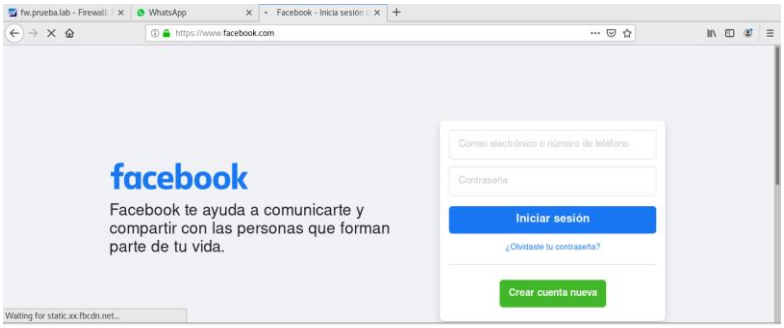
8. En esta parte seleccionaremos la opción “Block”, la interface “LAN”, la dirección familiar IPV4, el protocolo TCP, en el destino “Single host ar alias” y “FB” que fue el nombre alias que asignamos en el paso anterior número 6, en el puerto de rango de destino seleccionamos “any” y en opciones extras seleccionamos “Log” y salvamos.

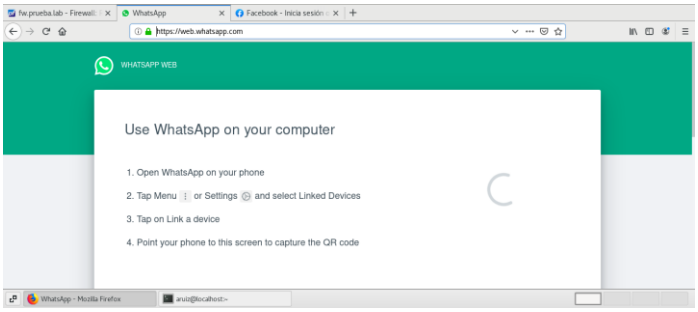




Captura de pantalla 43. Capturas de pantalla de los accesos a la paginas de Facebook y WhatsApp.

9. Finalmente procedemos a verificar que se haya realizado el bloqueo con éxito, miramos en la *captura de pantalla 44* que realizamos una recarga a la página y después de un tiempo de espera nos arrojó que la conexión había agotado. Mientras que la página de WhatsApp web cargó sin embargo nunca cargo el código QR, por lo que con ello probamos que efectivamente se realizó el bloqueo con éxito.



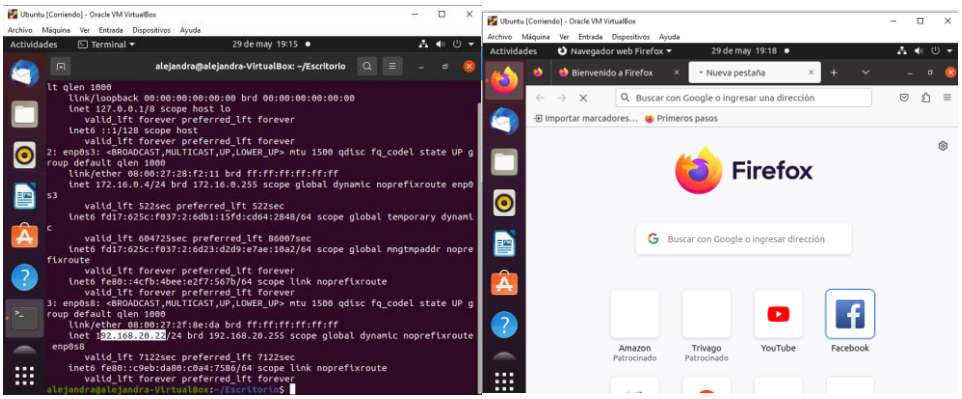


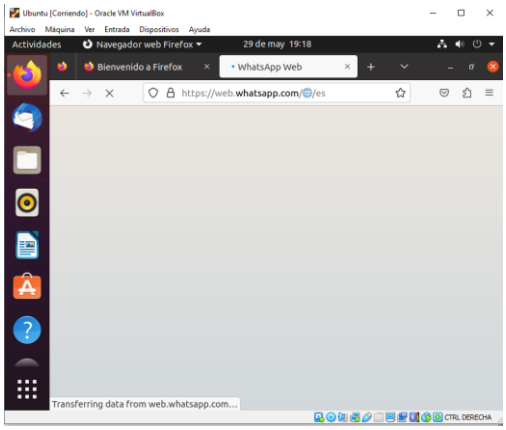
Captura de pantalla 44. Capturas de pantalla de los accesos a la paginas de Facebook y WhatsApp.

Como extra realizamos la prueba en otra máquina virtual *Ubuntu*, pues tuvo que realizarse en bloqueo de las páginas ya que las máquinas virtuales se encuentran conectadas entre sí.

De igual forma verificamos que este conectada en el rango de IP, miramos en la *captura de pantalla 44*, que efectivamente se encuentra así pues tiene la IP 192.168.20.22.

Miramos que tanto Facebook como WhatsApp no cargaron sus respectivas páginas, pues quedaron solamente cargando.

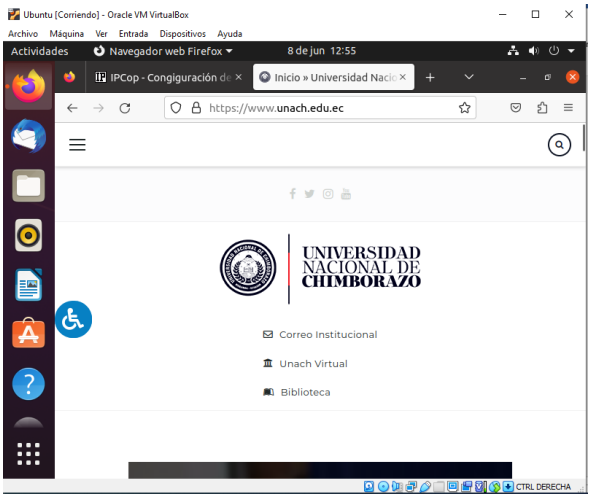




Captura de pantalla 45. Capturas de pantalla de los accesos a la paginas de Facebook y WhatsApp.

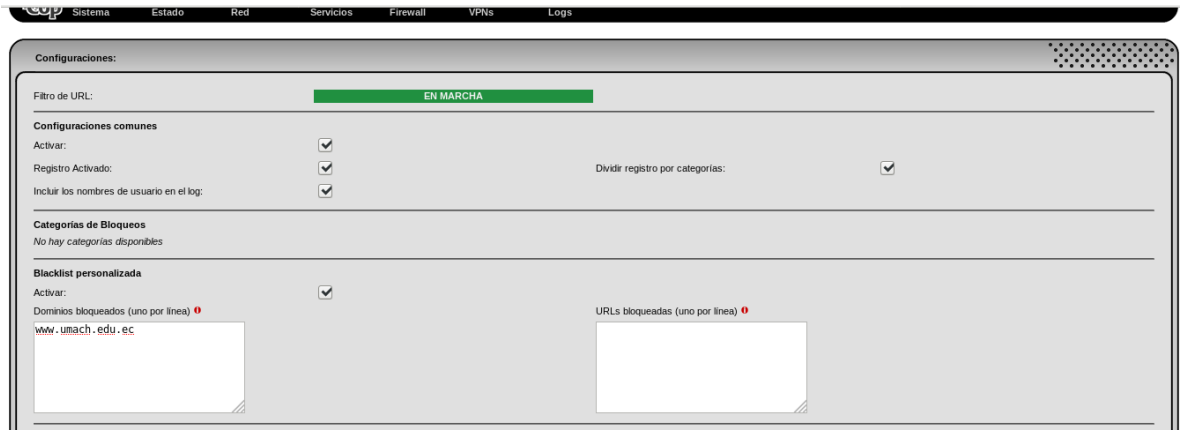
5.3.2 Bloqueo de páginas web con IpCop (UNACH página universitaria).

1. Como primer paso verificamos que efectivamente podamos ingresar a la página.

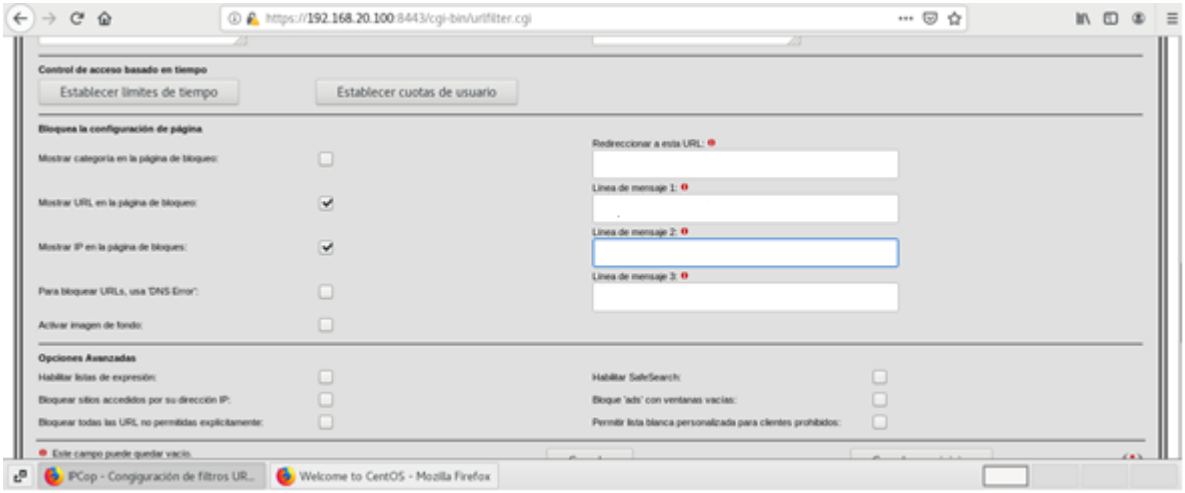


Captura de pantalla 46. Capturas de pantalla de los accesos a la paginas de Facebook y WhatsApp.

2. Posteriormente entramos a la configuración de IpCop, en donde nos iremos a “servicios” y posteriormente en “Filtro de URL”, inicialmente se muestra apagado, por lo que procederemos a ponerlo en marcha, seleccionamos las casillas que se muestran a continuación en la *captura de pantalla 47* y en la parte de blacklist personalizadas activamos casilla e ingresamos el dominio a bloquear. Continuamos con la selección de casillas como se muestra en la *captura de pantalla 48*

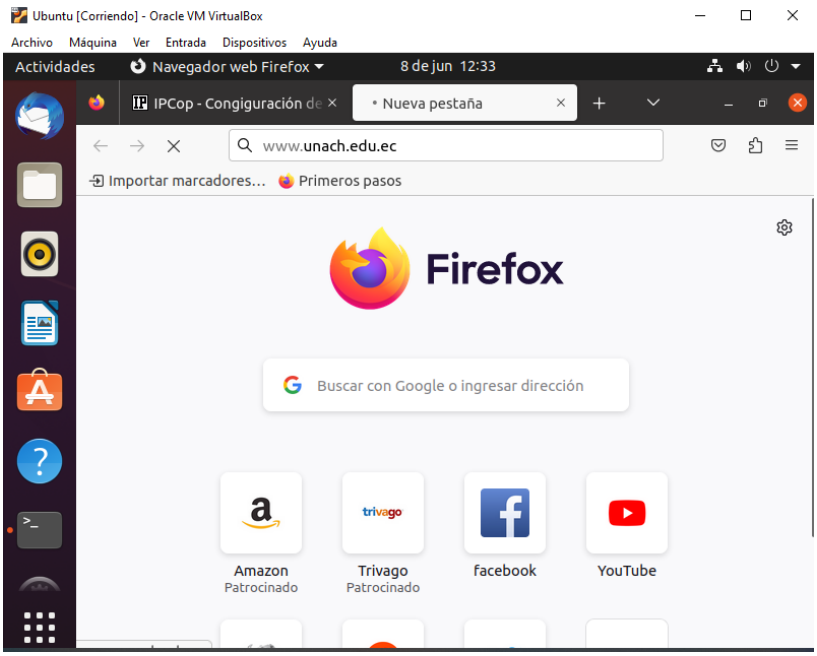


captura de pantalla 47. Capturas de pantalla de los accesos a la página UNACH.



captura de pantalla 48. Capturas de pantalla de los accesos a la paginas de Facebook.

3. Finalmente comprobamos que la página ya no cargo, en algunas ocasiones muestra el letrero de bloqueo, sin embargo, en este caso solo no respondió la página y se agotó el tiempo de espera.



captura de pantalla 49. Capturas de pantalla de los accesos a la paginas de Facebook.

5.4 Conclusiones

Vivimos en constantes cambios en nuestro entorno social, el cual va de la mano con nuestro entorno profesional, por ende, somos cada día más personas que manejamos un dispositivo electrónico, que obviamente está conectado a la red de internet, por ello es importante tener una seguridad eficaz para nuestros dispositivos, para no tenerlos vulnerables, es por ello que la finalidad de este trabajo fue comprobar que existen muchos tipos de protecciones para nuestros dispositivos.

Gracias a la variedad de firewall existente y que además nos permiten usarlos de forma gratuita muchas más personas podemos tener la capacidad de proteger nuestros equipos en la navegación diaria.

Debemos implementar mecanismos de seguridad es esencial en la protección de las redes y la información que contienen. Entre estos mecanismos, la consideración de una red de firewall cobra un valor importante para asegurar el perímetro de las redes.

Crear conciencia de la importancia de incluir seguridad con firewalls es fundamental en la era digital. Los firewalls actúan como guardianes de nuestra información en línea, protegiendo nuestros datos, sistemas y redes de amenazas cibernéticas. Sin esta conciencia, dejamos nuestras puertas digitales abiertas a posibles ataques y violaciones de seguridad.

Es prioritario valorar el tipo de firewall a adquirir, ya que muchos de ellos cuentan con soporte, mantenimiento y actualizaciones críticas para mantener la eficacia de su protección. Elegir el firewall adecuado no solo implica considerar sus capacidades técnicas, como el filtrado de paquetes, la inspección profunda de paquetes, la seguridad de aplicaciones y otras características técnicas, sino también evaluar la calidad del soporte y el mantenimiento que lo acompañan.

5.5 Trabajo Futuro

El trabajo futuro con los firewalls continuará evolucionando a medida que las amenazas cibernéticas se vuelvan más sofisticadas y las redes sean más complejas. Algunas de las tendencias que se pueden anticipar en el trabajo futuro con firewalls incluyen:

- Firewalls de Próxima Generación (NGFW): Los NGFW seguirán siendo una parte integral de la estrategia de seguridad, ya que incorporan características más avanzadas, como inspección profunda de paquetes, análisis de comportamiento y visibilidad de aplicaciones.
- Automatización de Seguridad: La automatización desempeñará un papel cada vez más importante en la configuración, administración y respuesta a amenazas en los firewalls. Esto permitirá una detección y respuesta más rápidas a ataques.

- Integración de Seguridad en la Nube: Con la creciente adopción de la nube, los firewalls se integrarán con soluciones de seguridad en la nube para proteger entornos híbridos y multi nube.
- Seguridad en el Internet de las Cosas (IoT): Con la proliferación de dispositivos IoT, se requerirán firewalls que puedan proteger estas redes y gestionar la gran cantidad de dispositivos conectados.
- Análisis de Amenazas Avanzadas: Los firewalls incorporarán capacidades avanzadas de análisis de amenazas para detectar ataques más complejos y amenazas internas.
- Seguridad de Aplicaciones Web: La protección contra ataques a aplicaciones web será esencial, y los firewalls desempeñarán un papel fundamental en la seguridad de las aplicaciones.
- Cumplimiento y Auditoría: Los firewalls seguirán siendo una parte crucial para cumplir con regulaciones de seguridad y realizar auditorías de cumplimiento.
- Habilidades en Seguridad de Red: Los profesionales de seguridad deberán desarrollar y mantener habilidades en la administración de firewalls, así como en la comprensión de amenazas y técnicas de mitigación.

Referencias

GOOGLE ACADÉMICO

1. Fox Pamela.(s.f.). *Redes de Computadoras*.

2. Sanchez, Y.& Bolaños, C. (2021). *DISEÑO Y SIMULACIÓN DE UNA RED DE COMUNICACIONES DE CONEXIÓN PUNTO A MULTIPUNTO DE TOPOLOGIA ANILLO PARA CONECTAR A TRES SEDES DE LA INSTITUCION EDUCATIVA DEPARTAMENTAL SAGRADO CORAZON DE JESUS DE PIVIJAY – MAGDALENA.* [Archivo PDF]

3. VNIVERSITAT DO VALENCIA (2022). *LAN, WAN, MAN y otras redes*

4. School, T. (2022, 14 febrero). *Historia y evolución de las redes informáticas*. Tokio School. Recuperado 28 de junio de 2022, de,

5. Cisco. (19 de marzo de 2020). *¿Qué es la seguridad de red?*

6. Ittgweb. (29 de mayo de 2016). *4.1 Seguridad de Software*.

7. Richar93. (19 de abril de 2021). *¿Qué es un Firewall? Características, ventajas y desventajas de usarlo.*

8. Tpempresas.com (14 de noviembre de 2019).*Los 10 mejores firewalls de hardware para redes domésticas y de pequeñas empresas 2022*

9. Solvetic Sistemas. (13 de octubre de 2017). *Mejores firewall para sistemas Linux 2018.*

10. Metropolitan. (2016, 7 noviembre). Ataque DDoS detiene la calefacción en Finlandia. Recuperado 10 de octubre de 2021.

11. DigiCert. (2014, 12 marzo). Infiltraciones en cuentas de Instagram para promover el spam de citas para adultos. Recuperado 11 de octubre de 2021,

12. Nieto, A. (2020, 2 junio). Seguridad en la red, prioridad para las empresas, una gran oportunidad para el canal. Recuperado 11 de octubre de 2021.

13. BBC News Mundo. (9 de marzo de 2021). *El "inusualmente agresivo" ciberataque del que Microsoft acusa a China (y por qué no es simplemente una nueva crisis de ciberseguridad).*

14. PaÃ-s, E. (2021, 3 diciembre). La Generalitat sufre un ciberataque a sus comunicaciones y aplicaciones durante tres horas. El PaÃ-s

15. El nuevo informe de WatchGuard Threat Lab muestra que los ataques de red están en su punto más alto en los últimos tres años. (2022, 5 abril). WatchGuard Technologies.

16. Técnico. (2020, 19 agosto). *8+ tipos de firewall - Actualidad tecnologica*. Actualidad Tecnologica.

17. Aguilar, L. (2023, 7 junio). Qué es Linux: el sistema operativo de código abierto. *ADSLZone*.

18. El nuevo informe de seguridad de WatchGuard Technologies revela una explosión del malware evasivo en el cuarto trimestre de 2019. (2020, 25 marzo). WatchGuard Technologies.

19. ¿Qué es una DMZ y por qué la usaría? | Fortinet. (s. f.). Fortinet.

LIBROS

1. (libro digital) S. Tanenbaum, A. (2003). *Redes De Computadoras* (4.ª ed., Vol. 912). Pearson Educación.

PUBLICACIONES

1. ARREAGA CARPIO, G. I. S. S. E. L. I. V. E. T. T. E. (2010). ANÁLISIS Y DISEÑO DE LA SEGURIDAD DE HARDWARE DEL DEPARTAMENTO TÉCNICO INFORMÁTICO DE LA CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES Y NETWORKING (Vol. 3339). UNIVERSIDAD DE GUAYAQUIL.

SITIOS OFICIALES

2. P.F.S.E.N.S.E. (2022). *pfSense® - World's Most Trusted Open Source Firewall*. Pfsense. Recuperado 12 de agosto de 2022.

3. *IPCop - Home*. (2016). IPCop. Recuperado 29 de agosto de 2022.

4. *Download*. (2022). CentOS. Recuperado 1 de septiembre de 2022.

5. *Shoreline Firewall (Shorewall)*. (s. f.).

6. *Vuurmuur Firewall*. (s. f.).

7. IPFire.org - IPFire Development Team. (s. f.). *www.ipfire.org - Welcome to IPFire*.

8. *Smoothwall-Home*. (s. f.).

9. *ConfigServer Security and Firewall (csf) – ConfigServer Services*. (s. f.).

Anexos

Manual de instalación de firewall pfSense

A continuación, se muestra por medio de ilustraciones el paso a paso de la instalación y configuración de pfsense.

1.- Descargar del sitio oficial de pfsense.

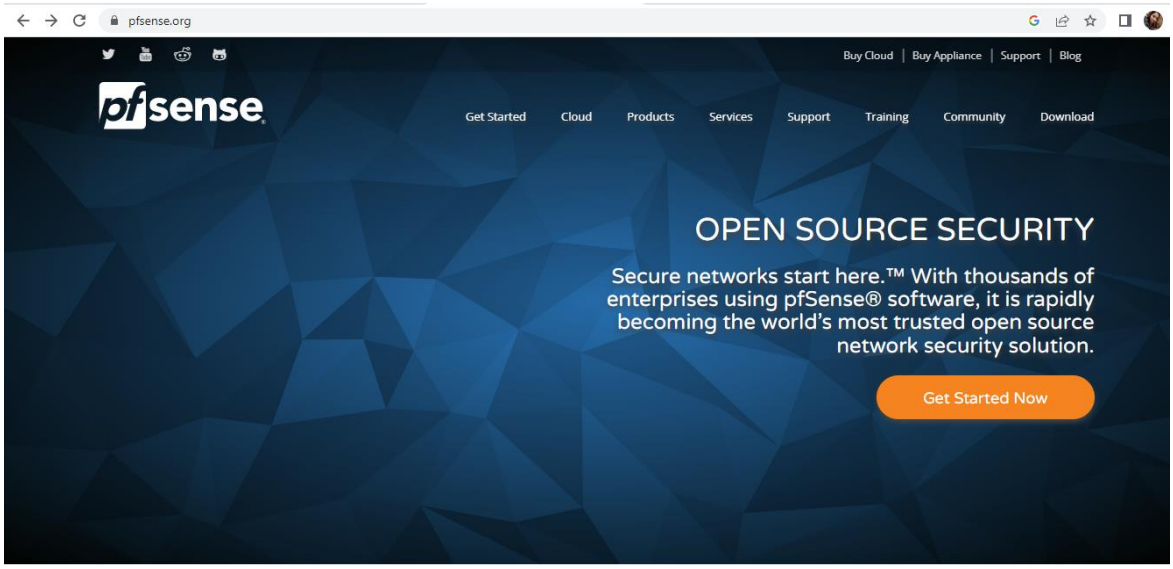


Ilustración 10

2.- Descargar la versión más reciente de pfsense

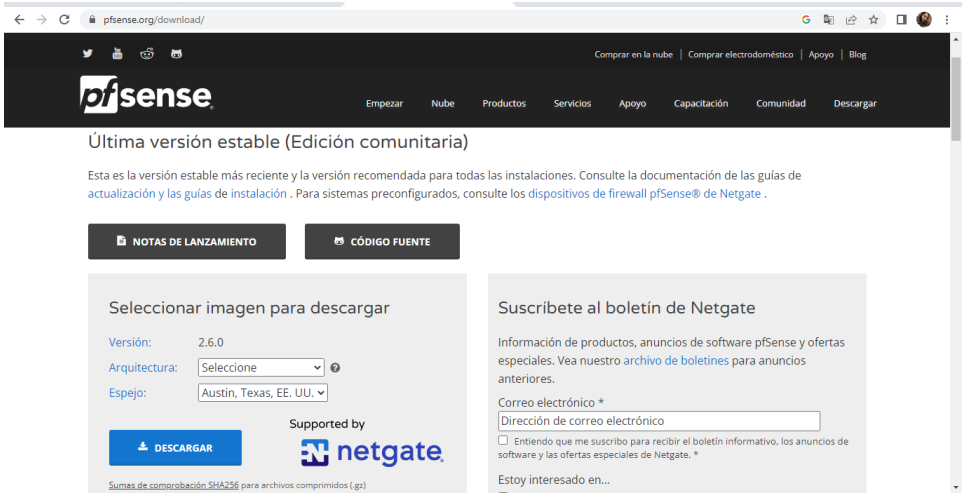


Ilustración 11

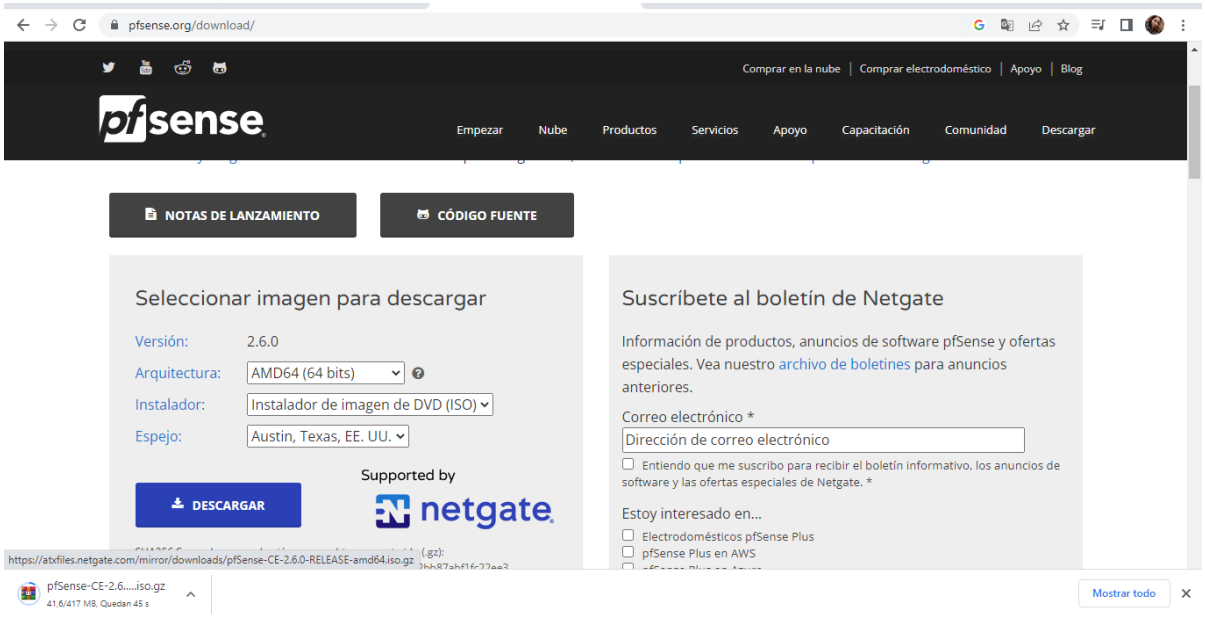


Ilustración 12

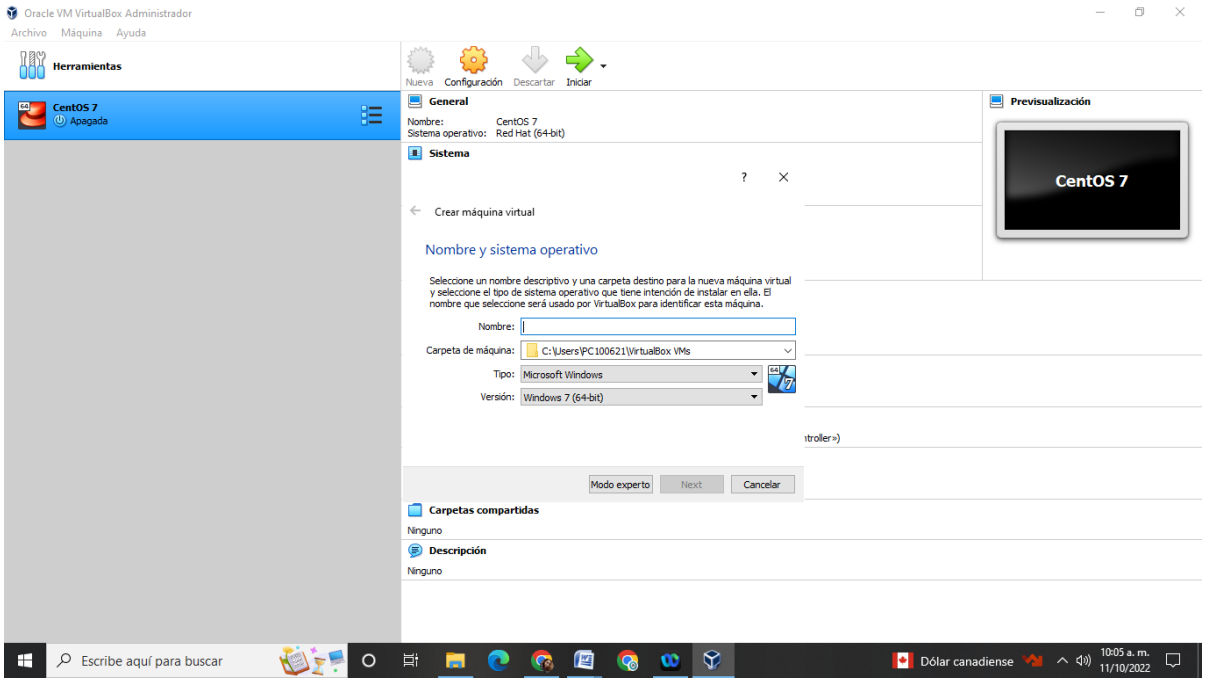


Ilustración 13

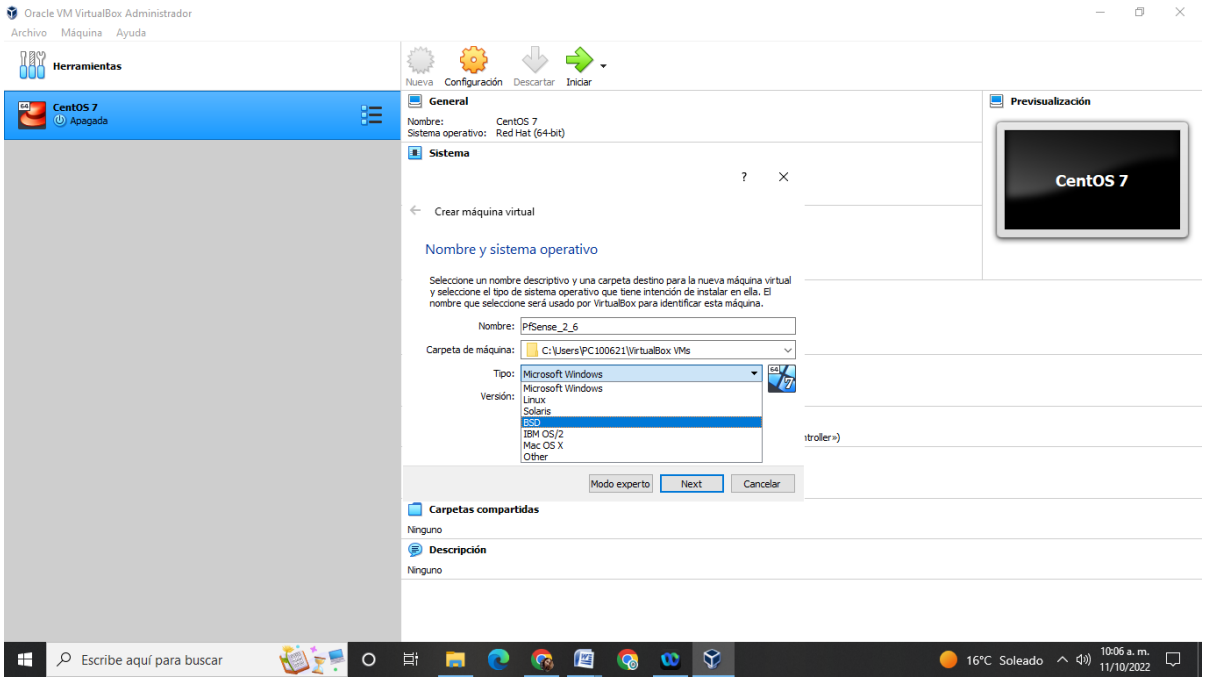


Ilustración 14

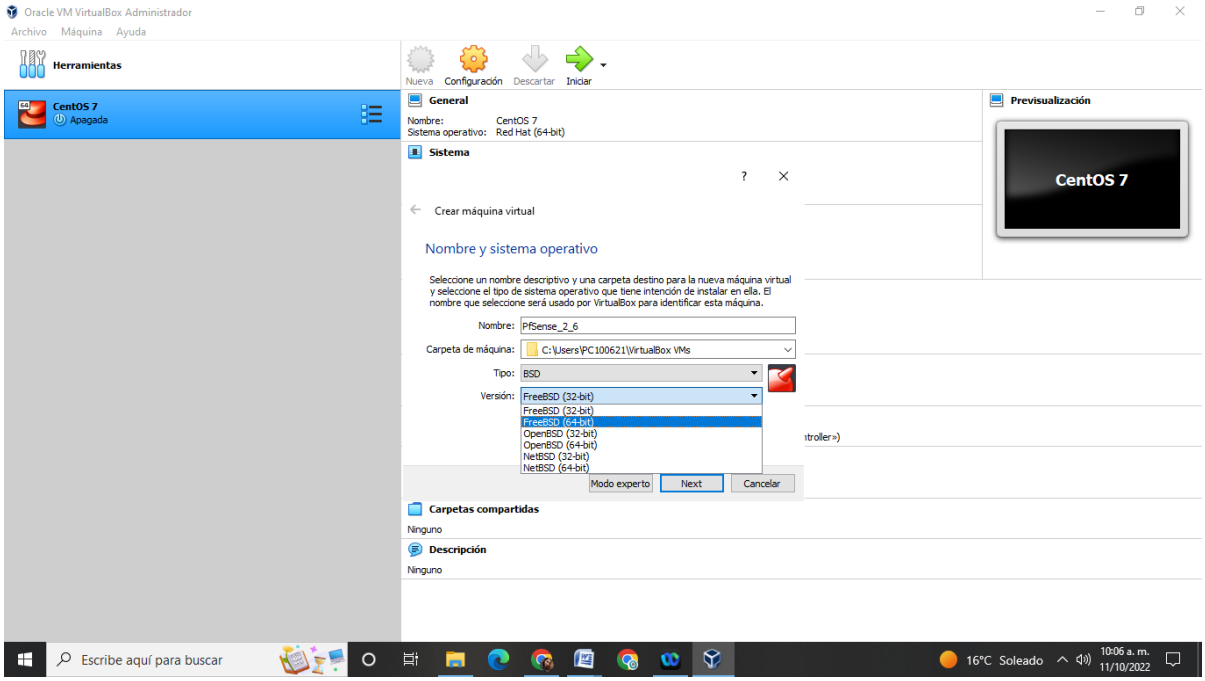


Ilustración 15

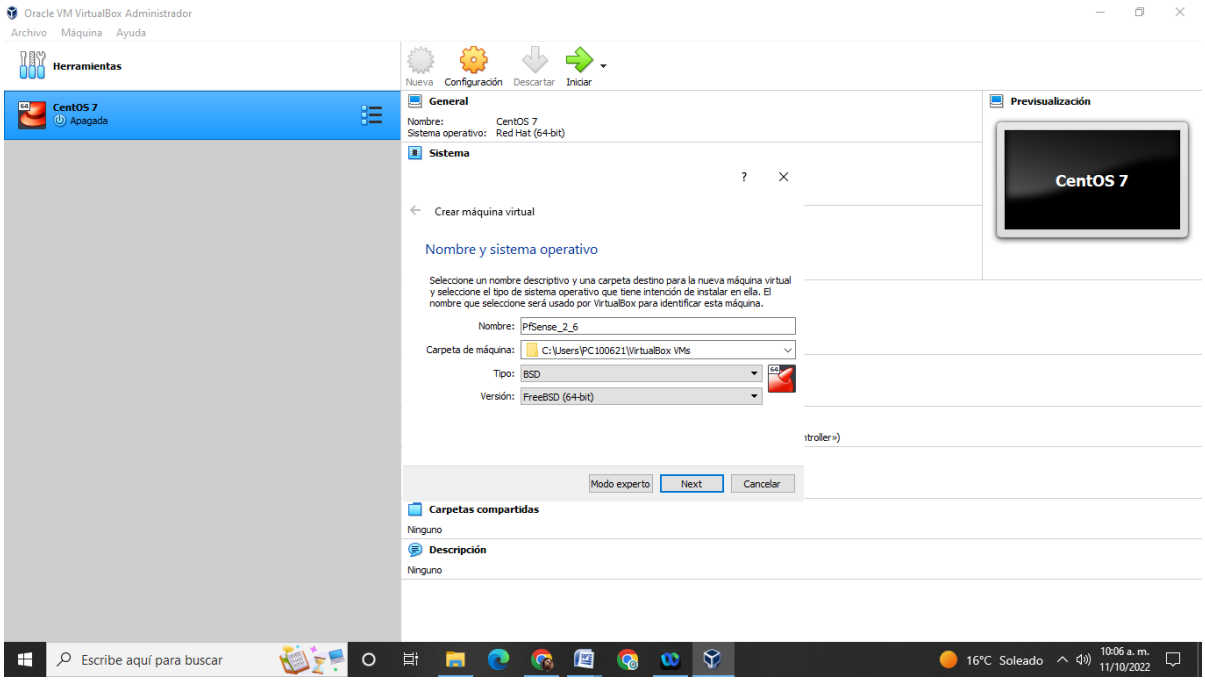


Ilustración 16

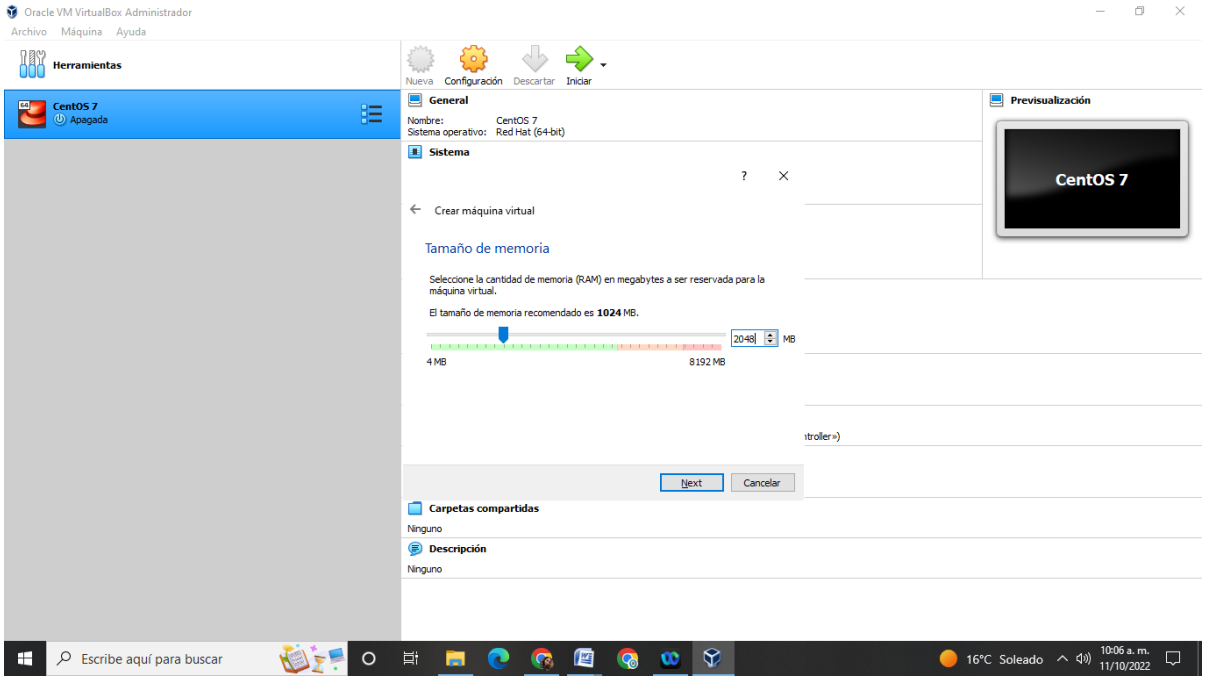


Ilustración 17

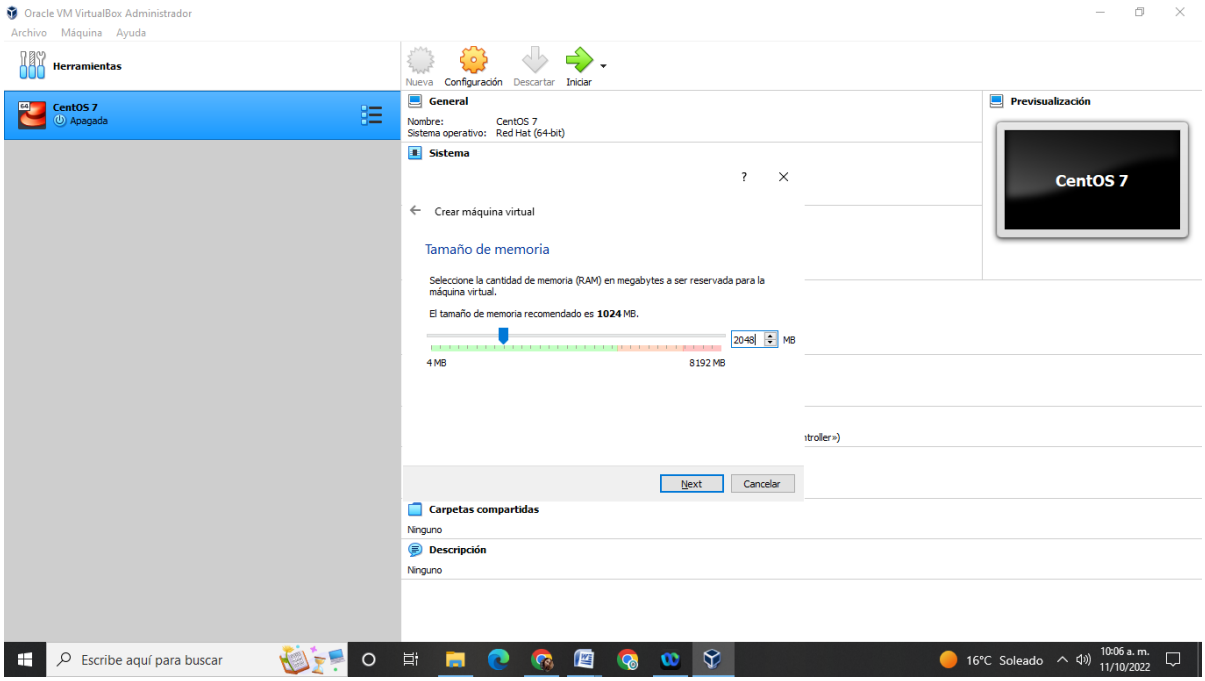


Ilustración 18

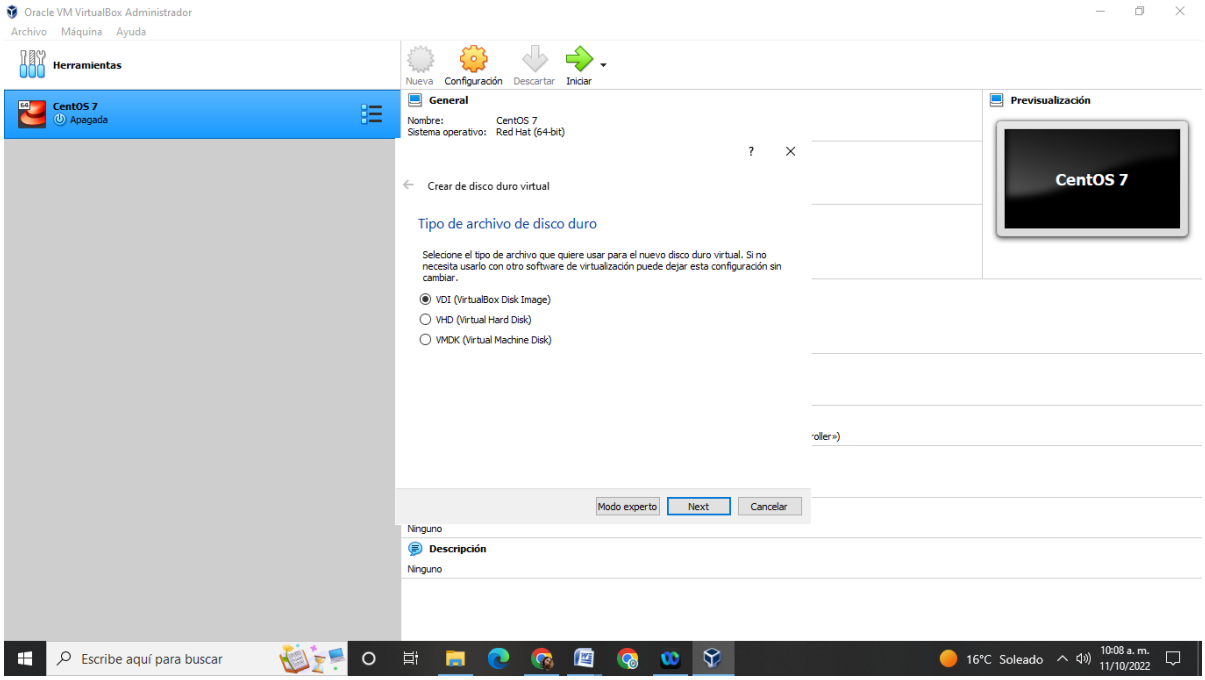


Ilustración 19

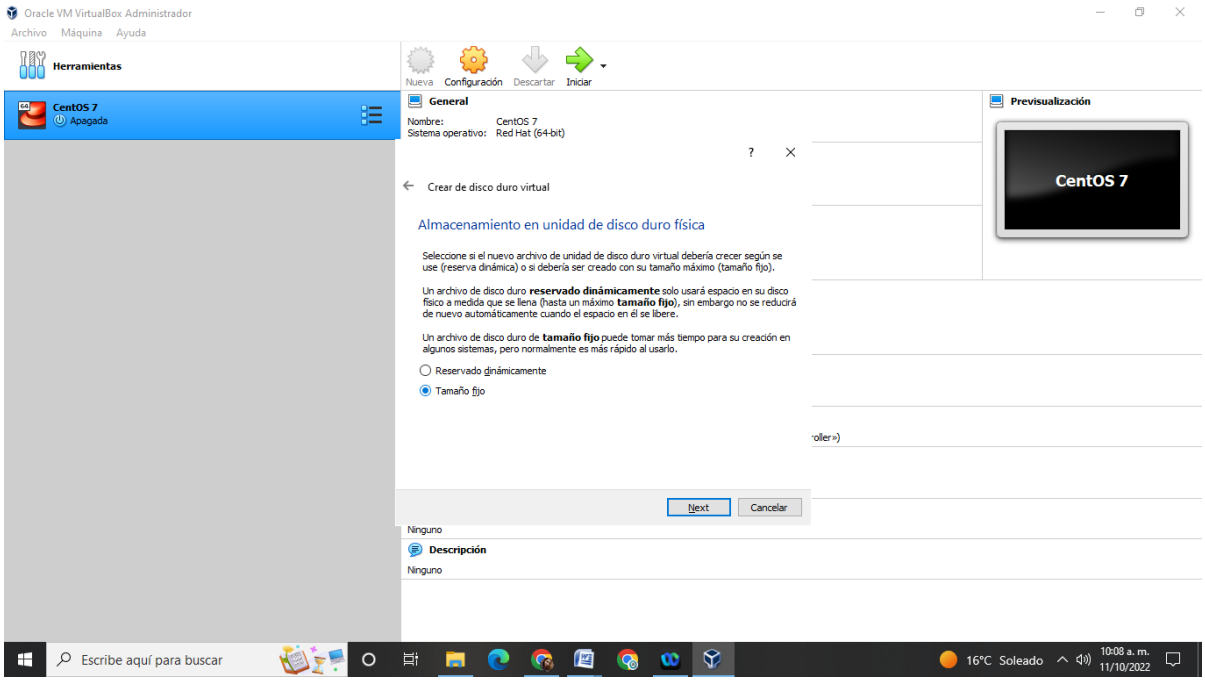


Ilustración 20

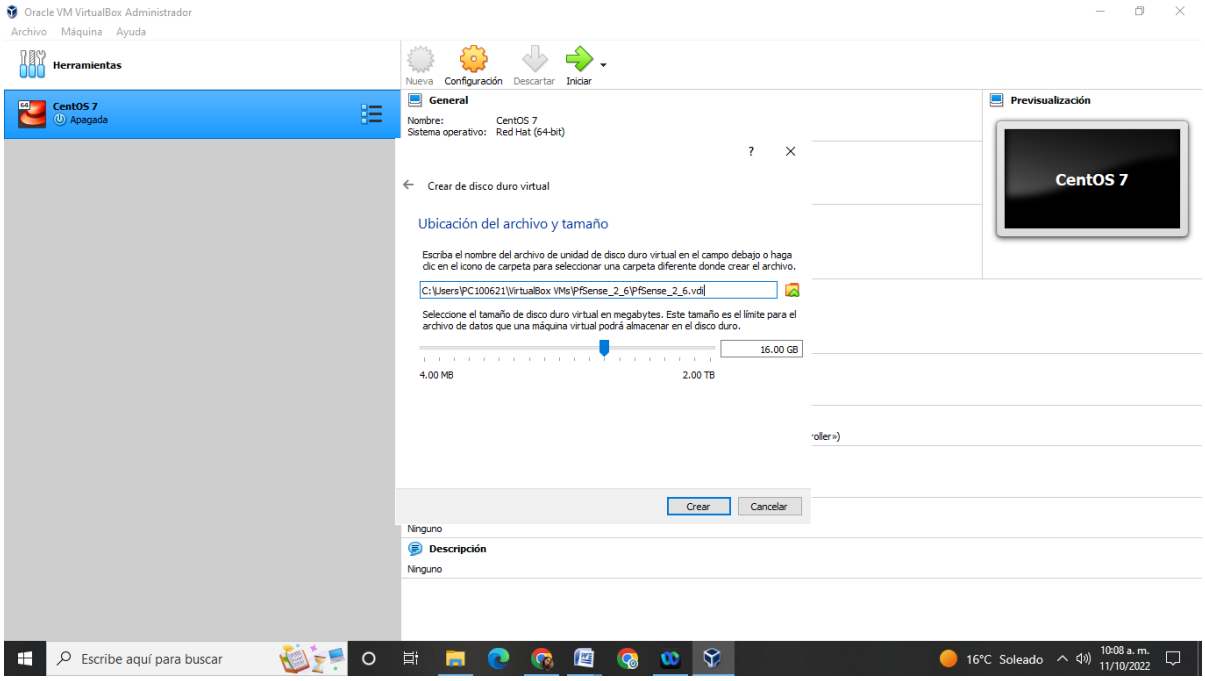


Ilustración 21

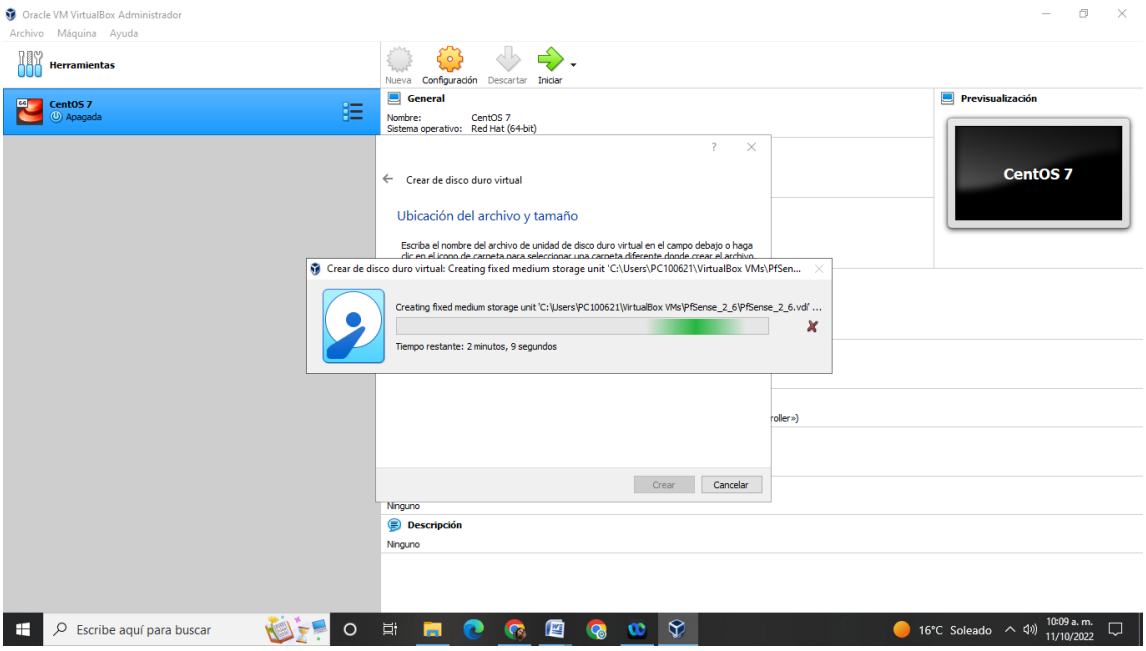


Ilustración 22

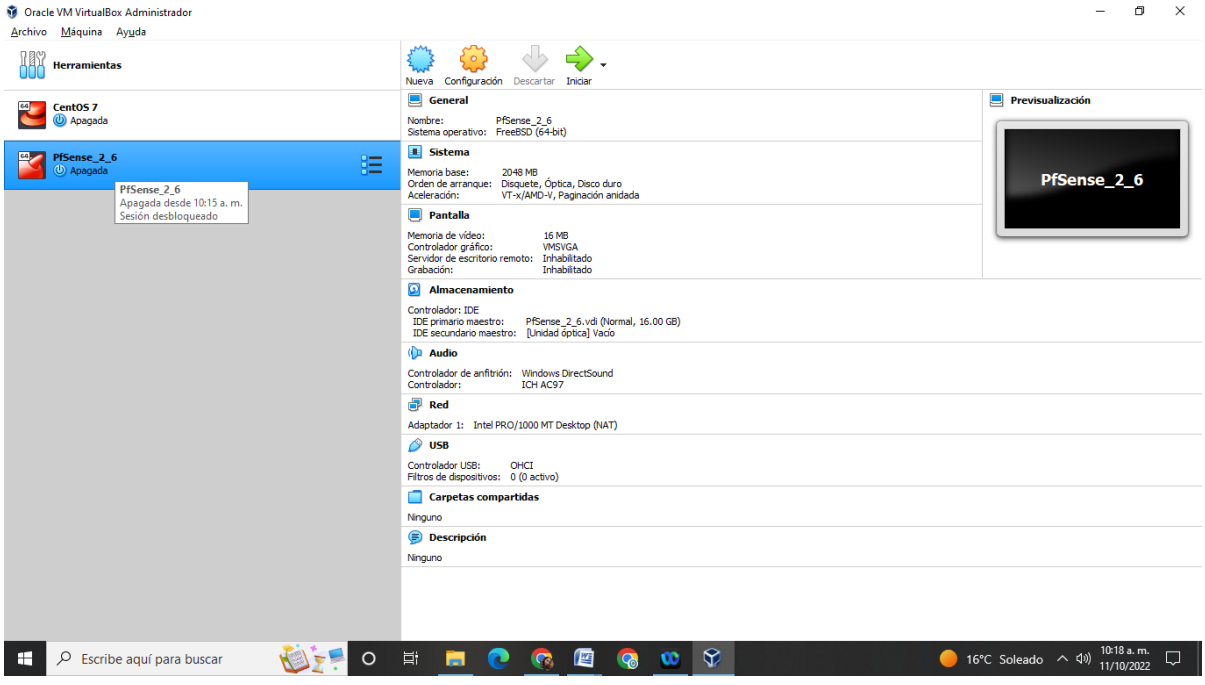


Ilustración 23

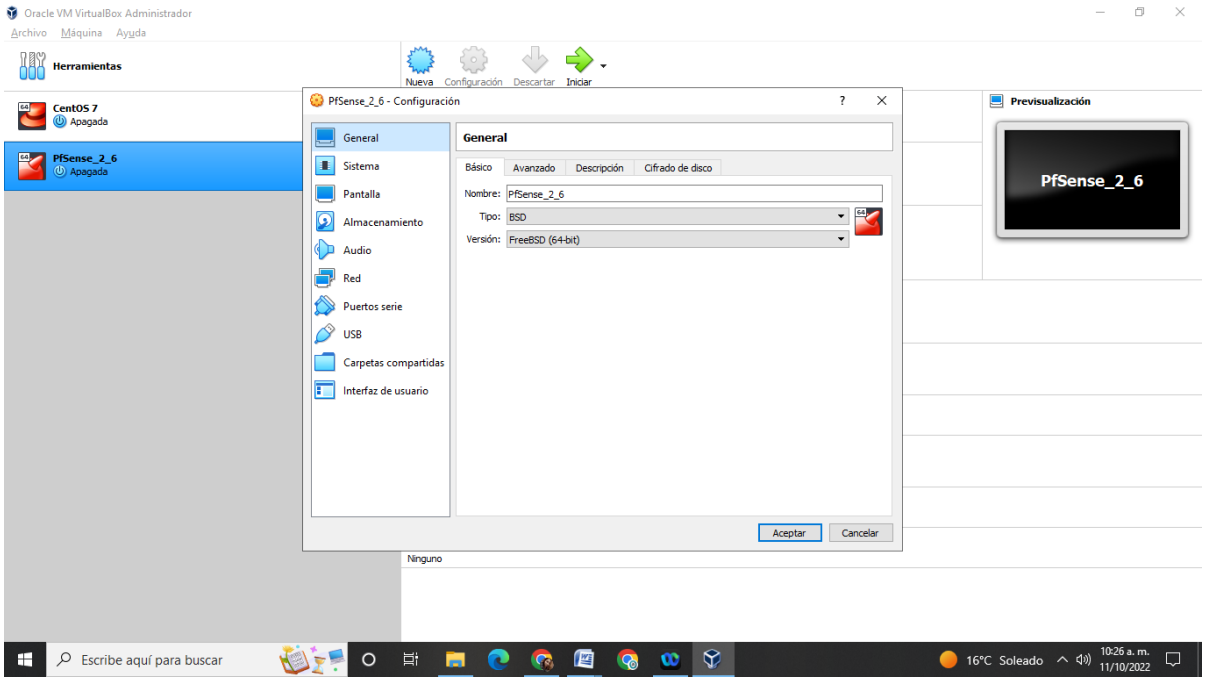


Ilustración 24

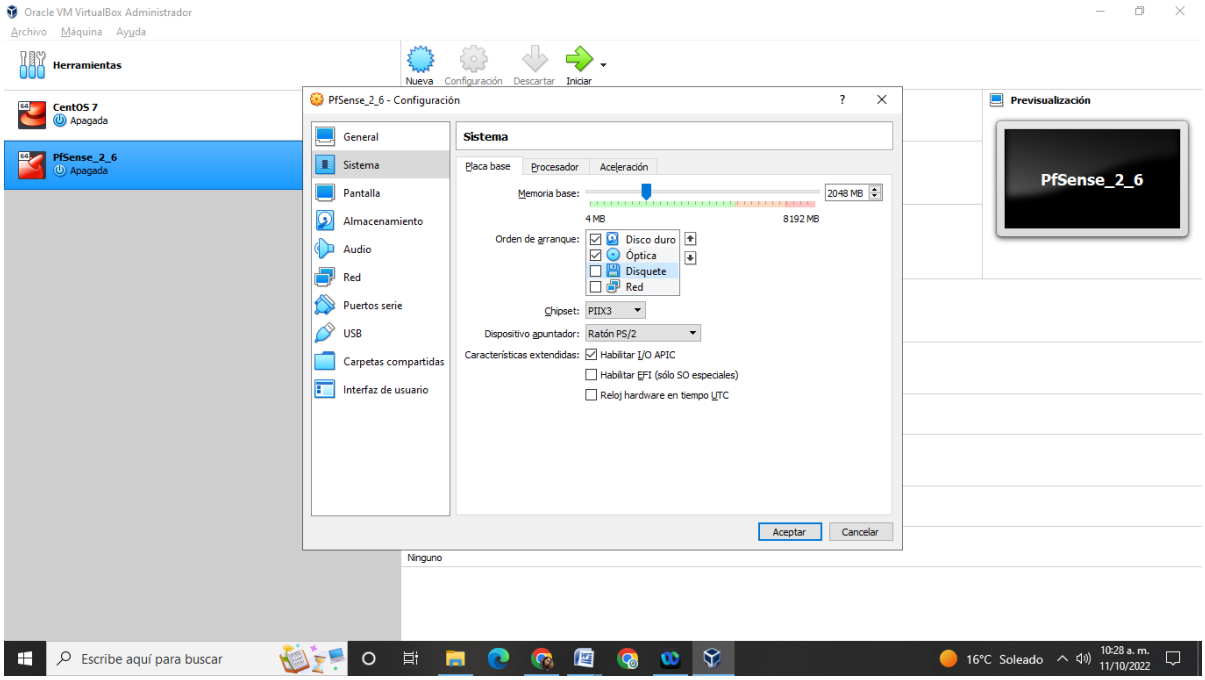


Ilustración 25

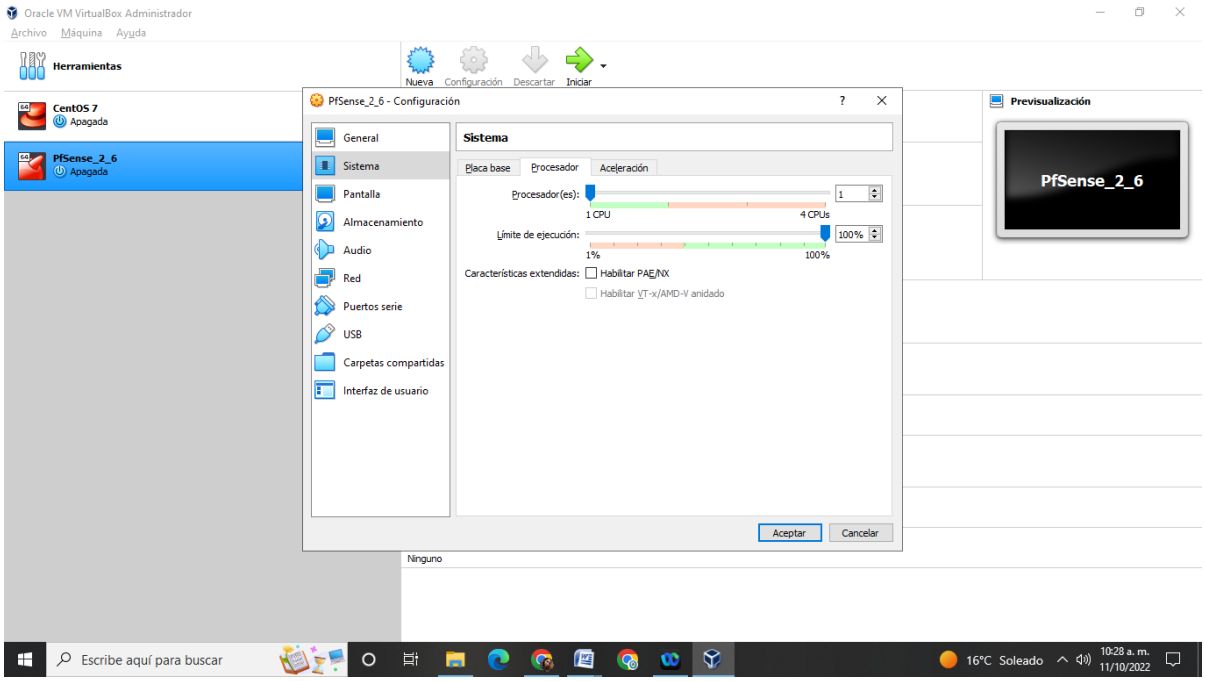


Ilustración 26

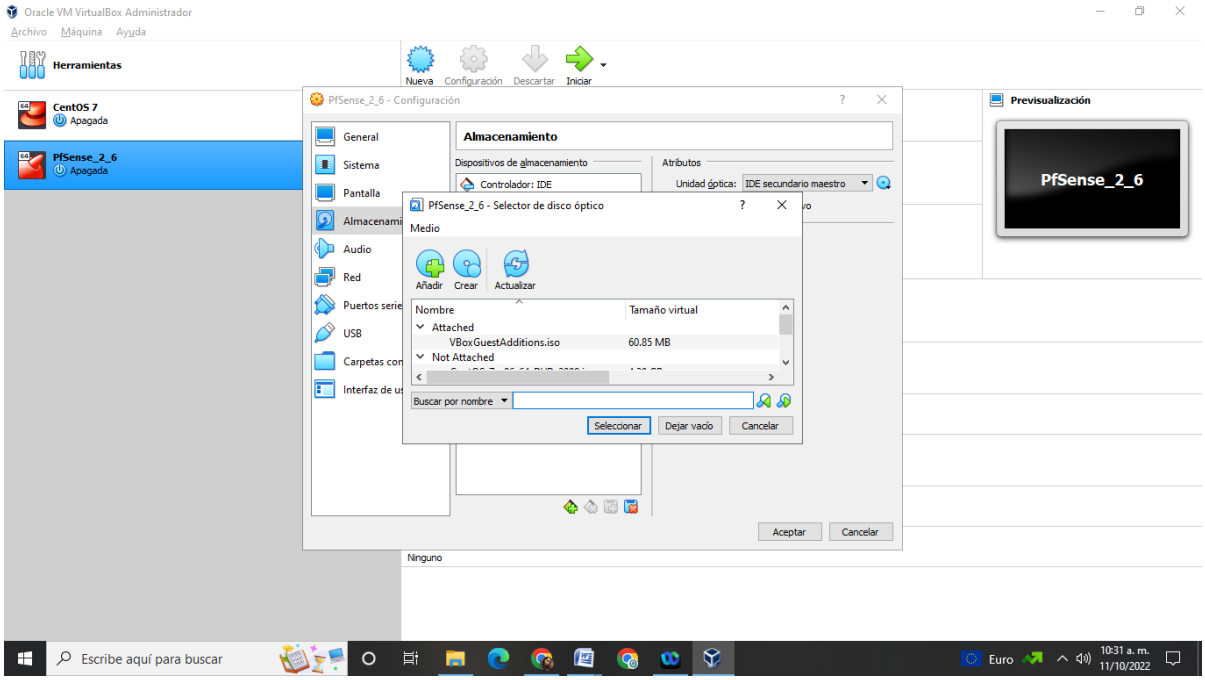


Ilustración 27

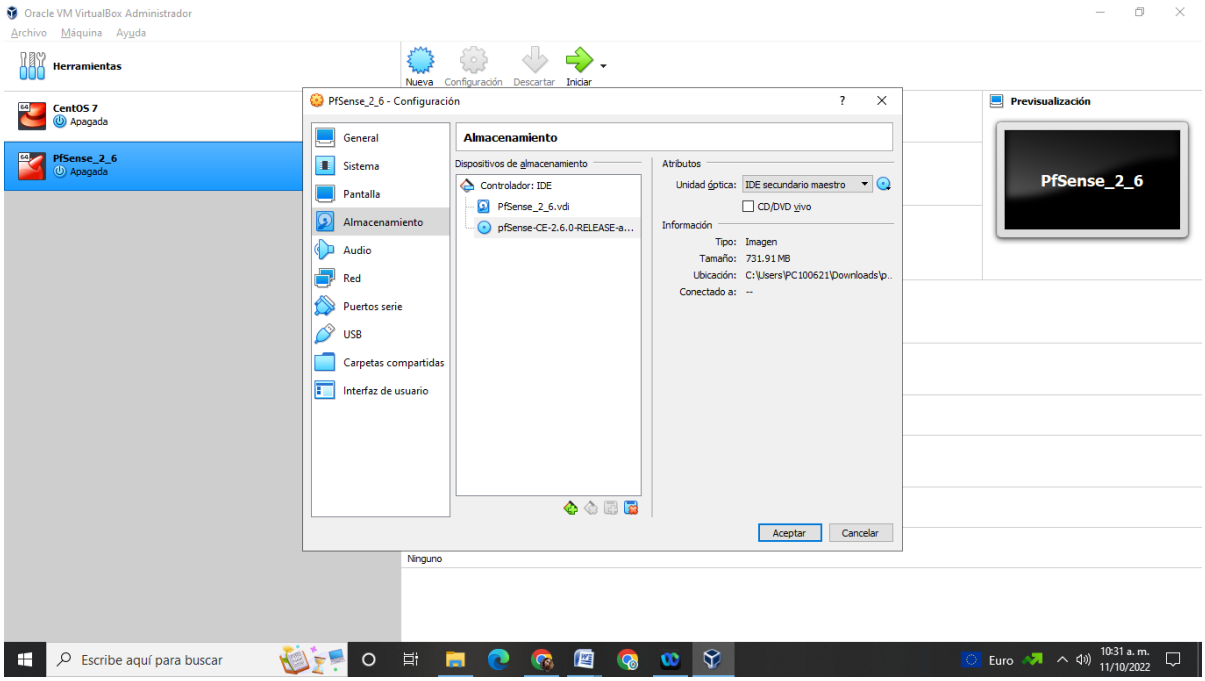


Ilustración 29

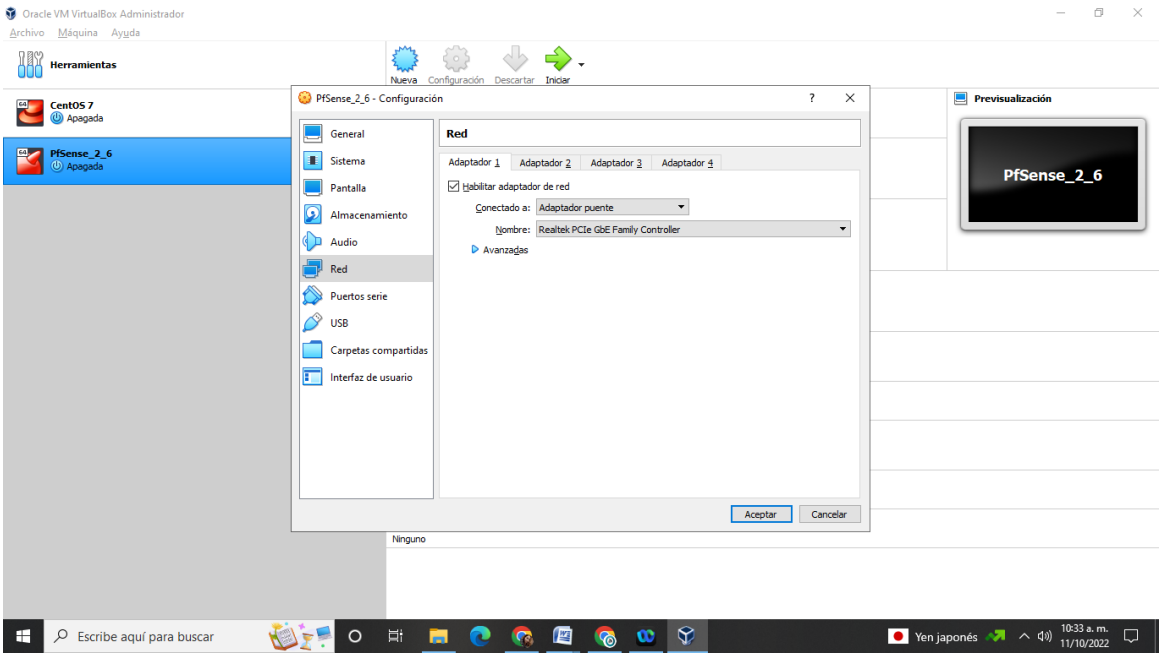


Ilustración 30

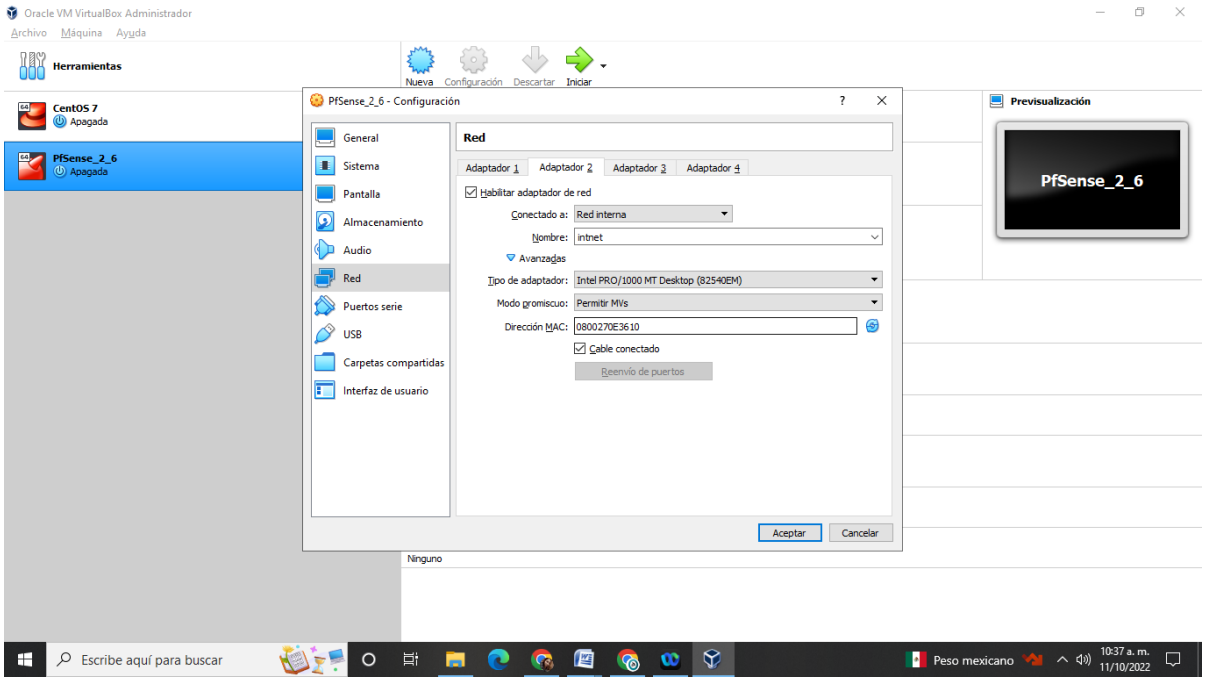


Ilustración 31

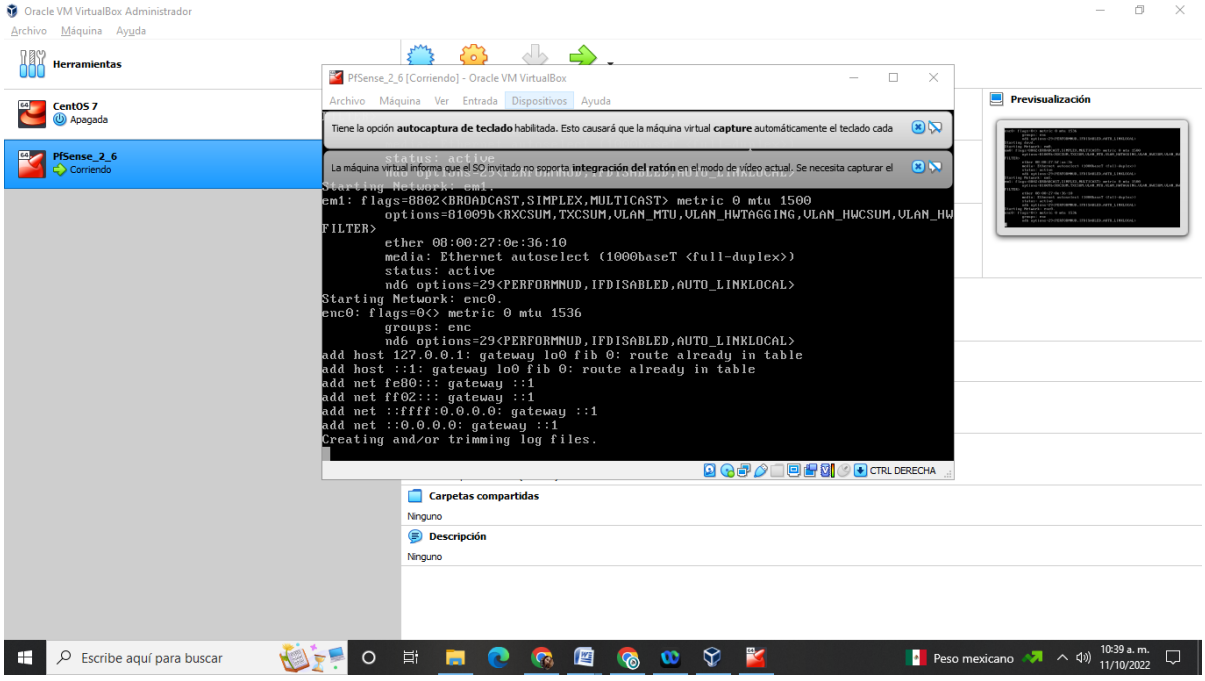


Ilustración 32

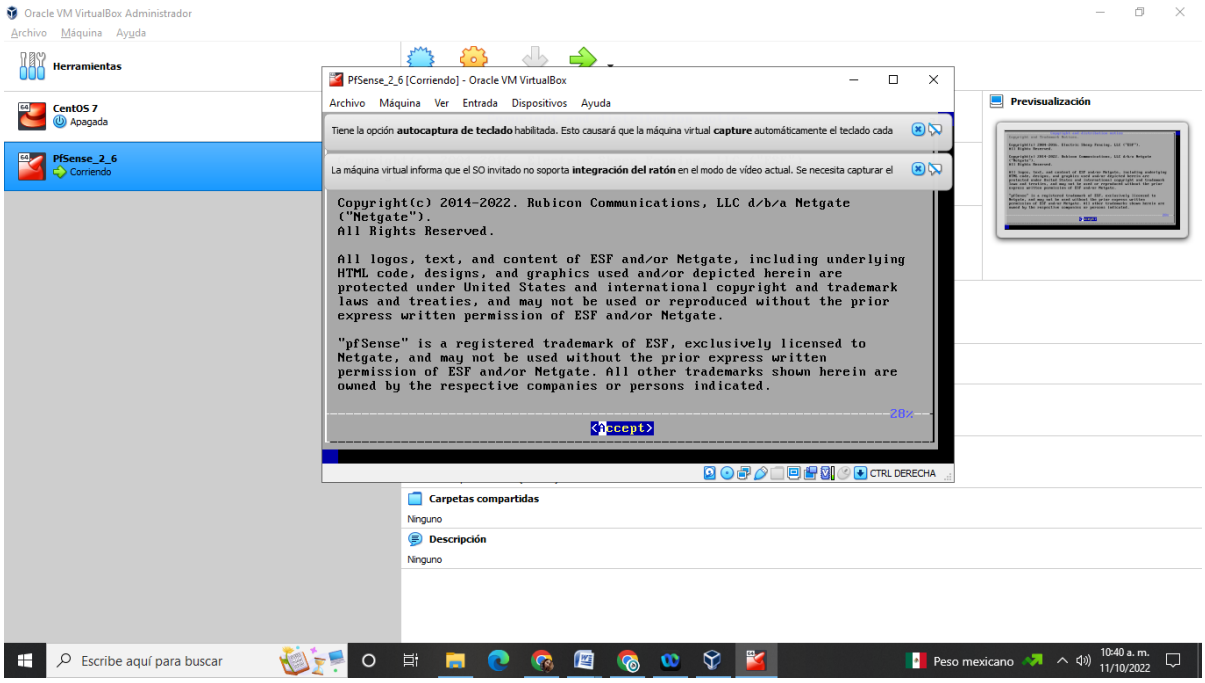


Ilustración 33

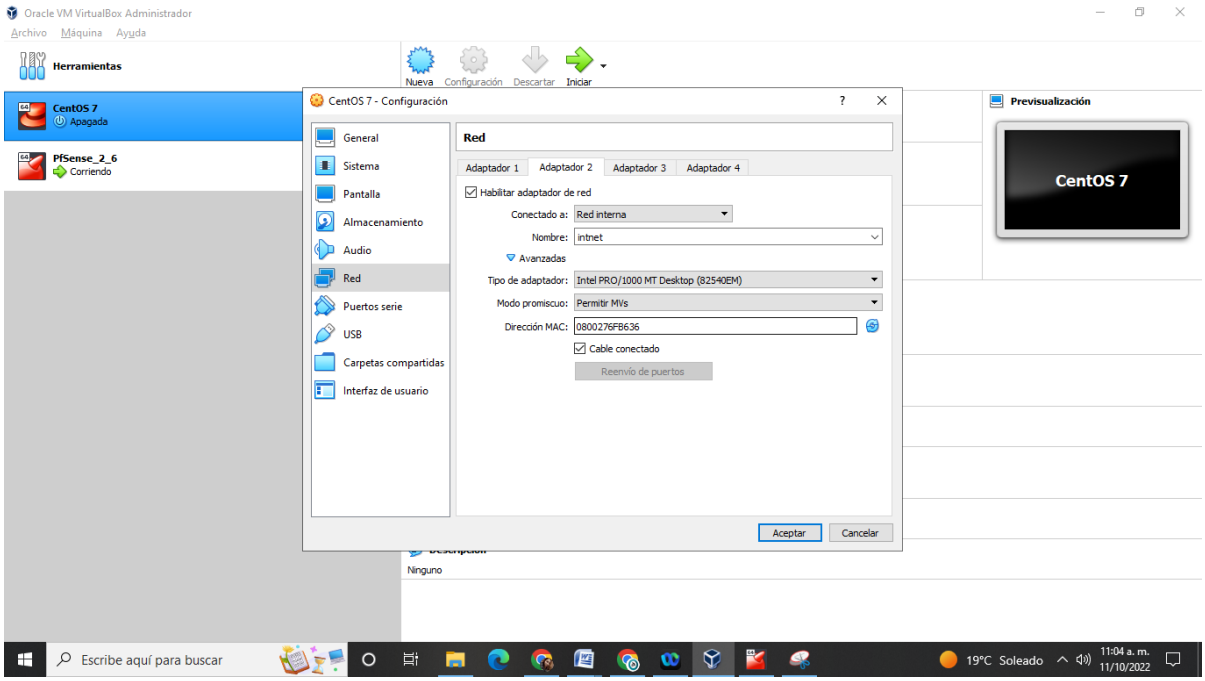


Ilustración 34

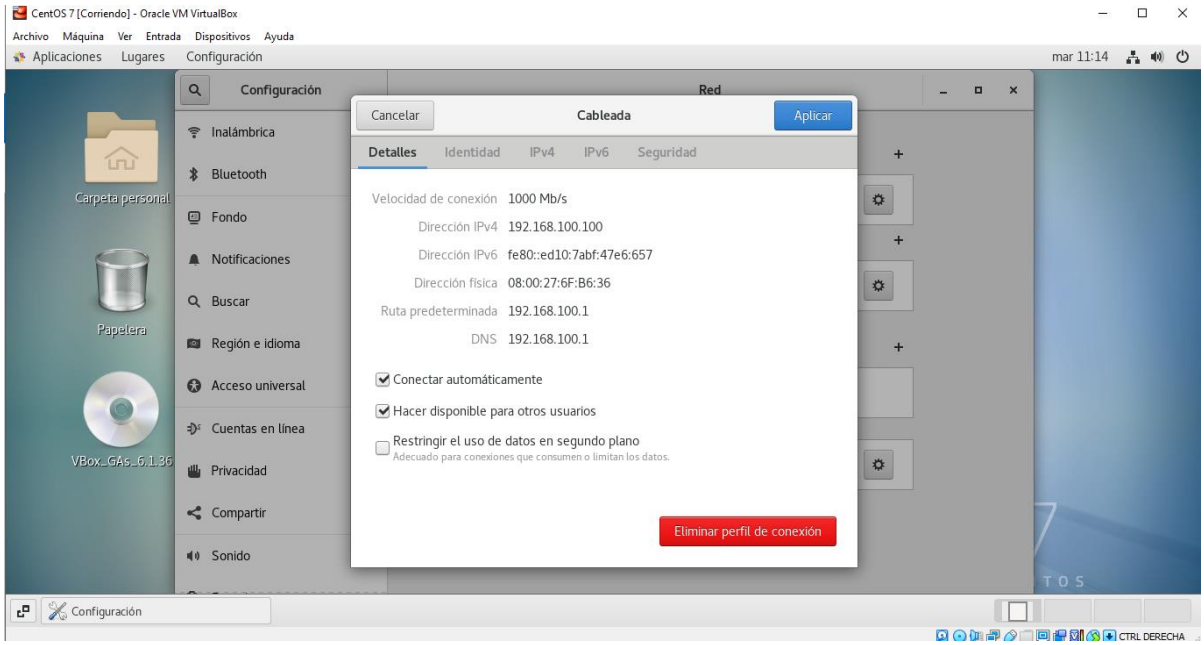


Ilustración 35

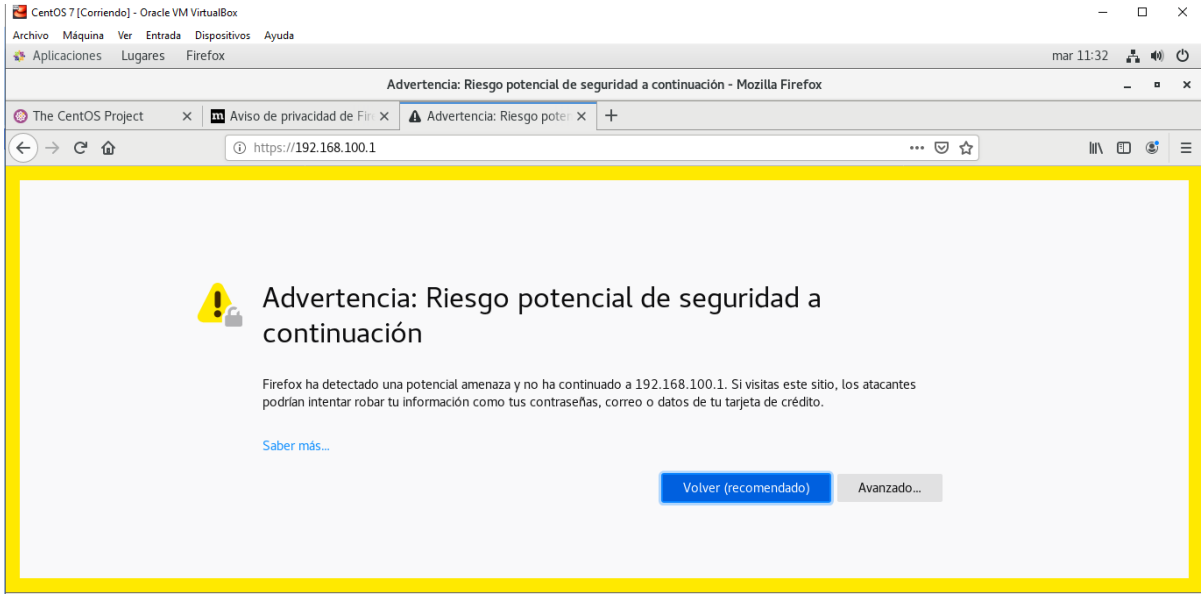


Ilustración 36

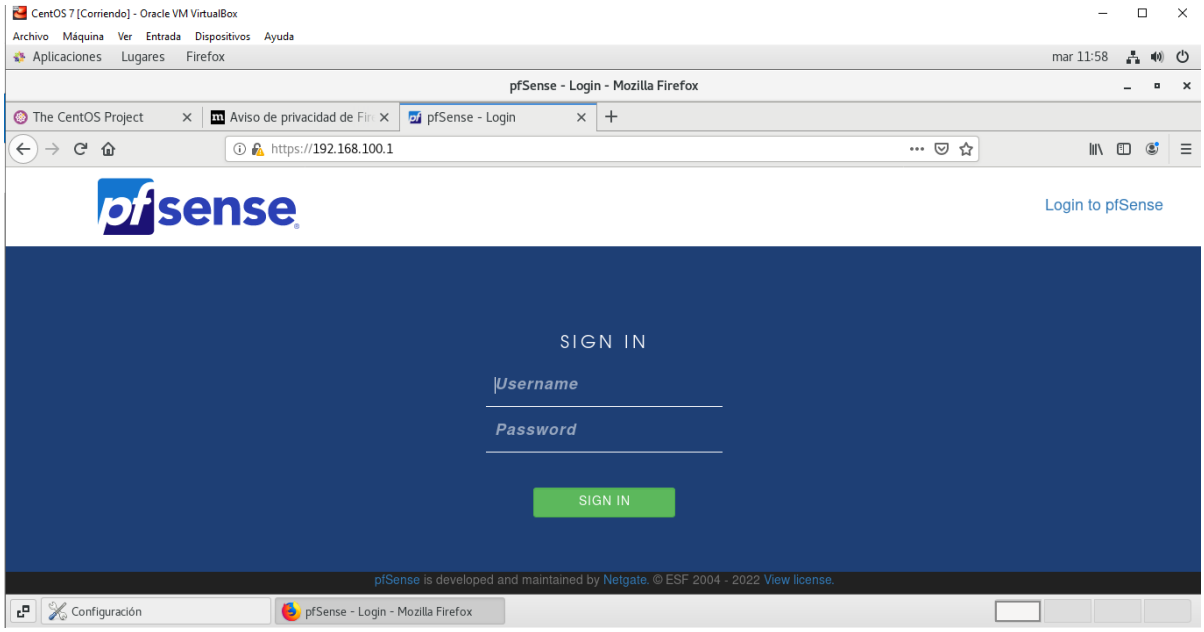


Ilustración 37

Manual de instalación de firewall IPCop

A continuación, se muestra por medio de ilustraciones el paso a paso de la instalación y configuración de IpCop.

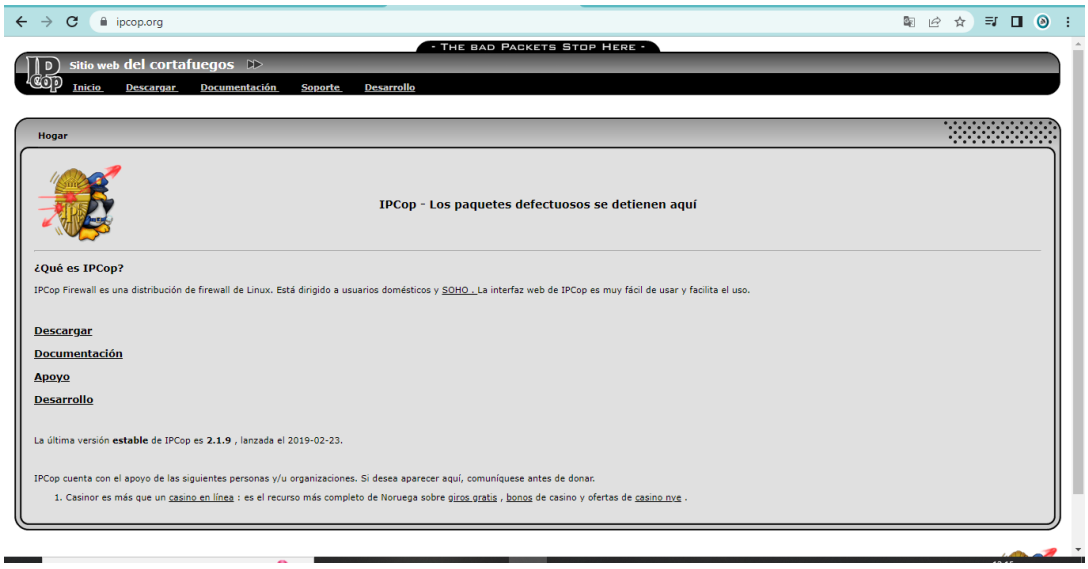


Ilustración 38

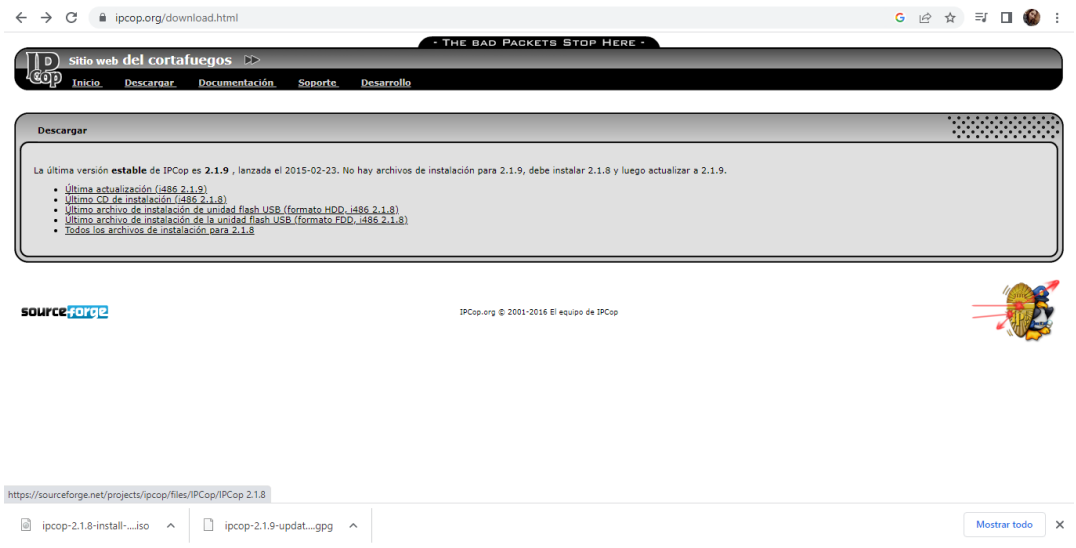


Ilustración 39

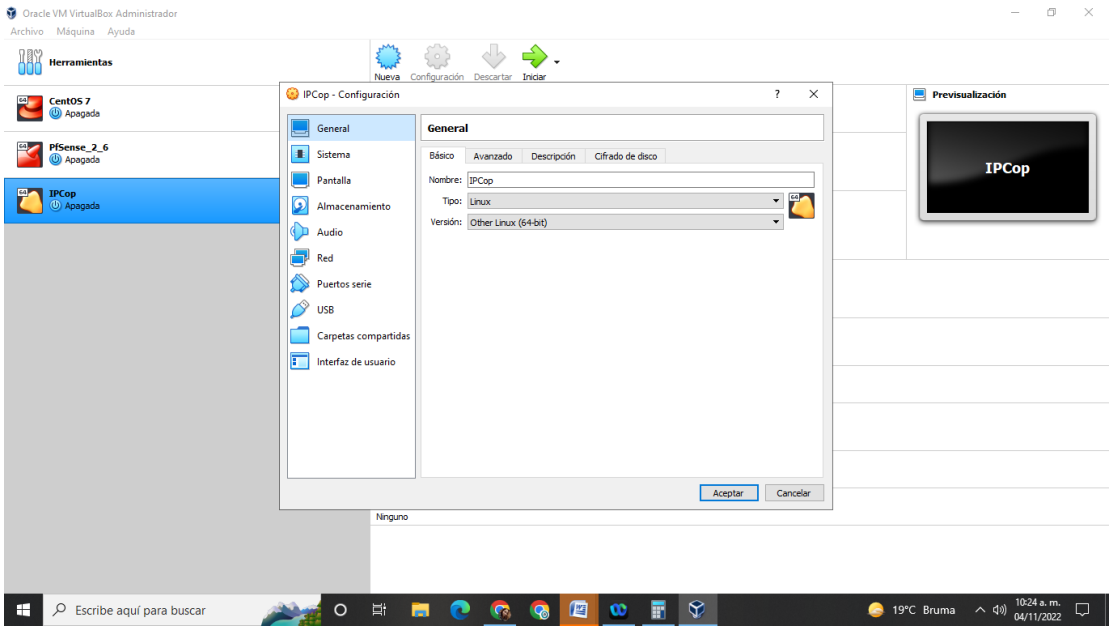


Ilustración 40

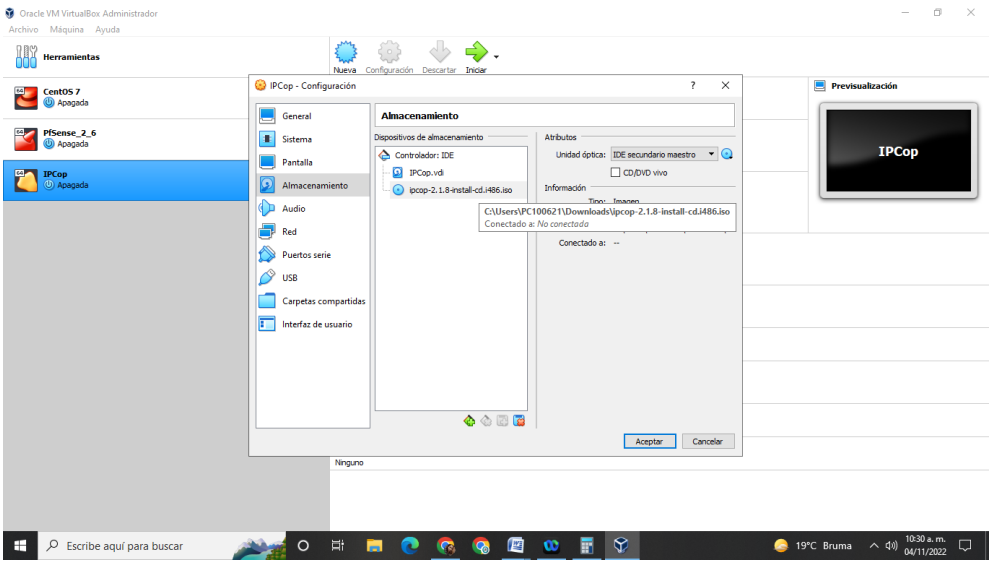


Ilustración 41

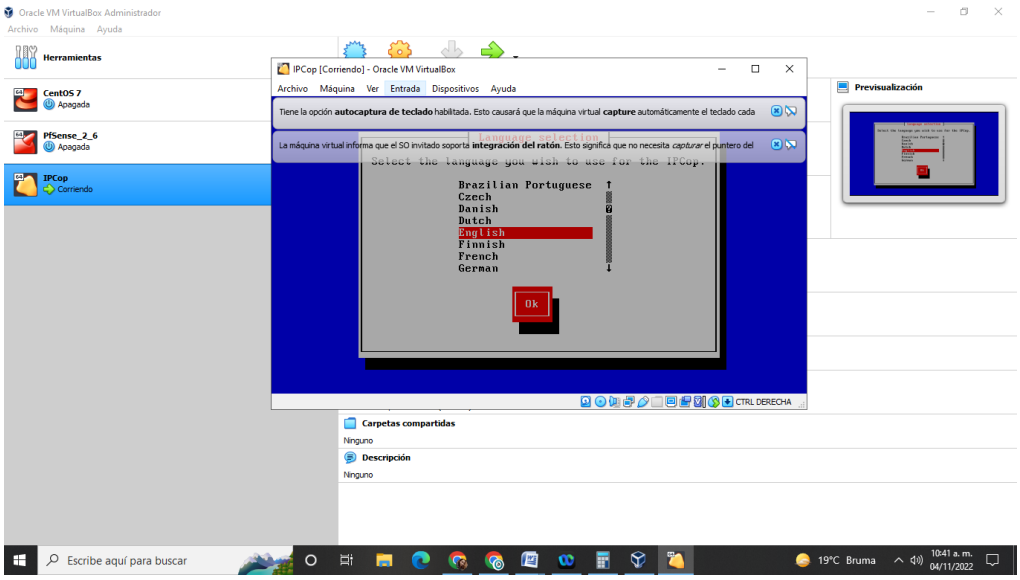


Ilustración 42

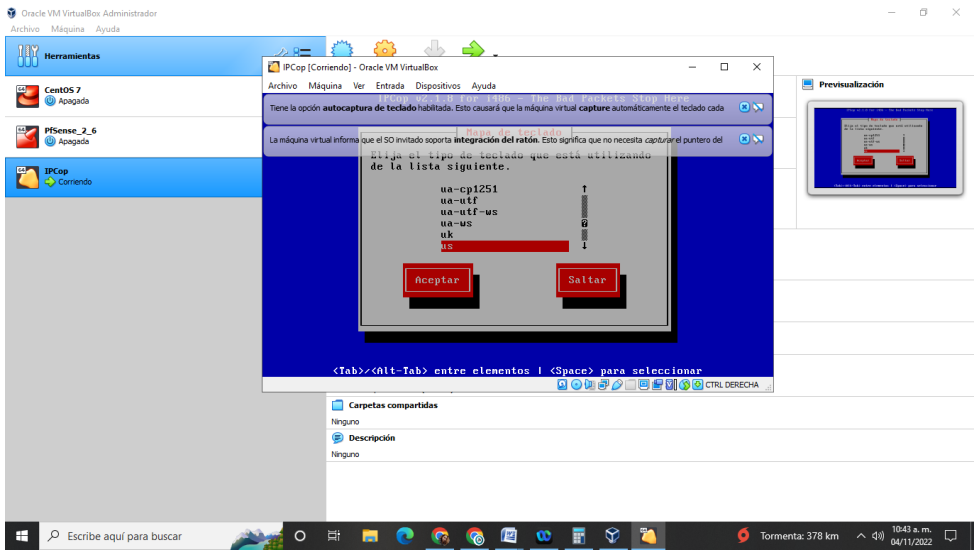


Ilustración 43

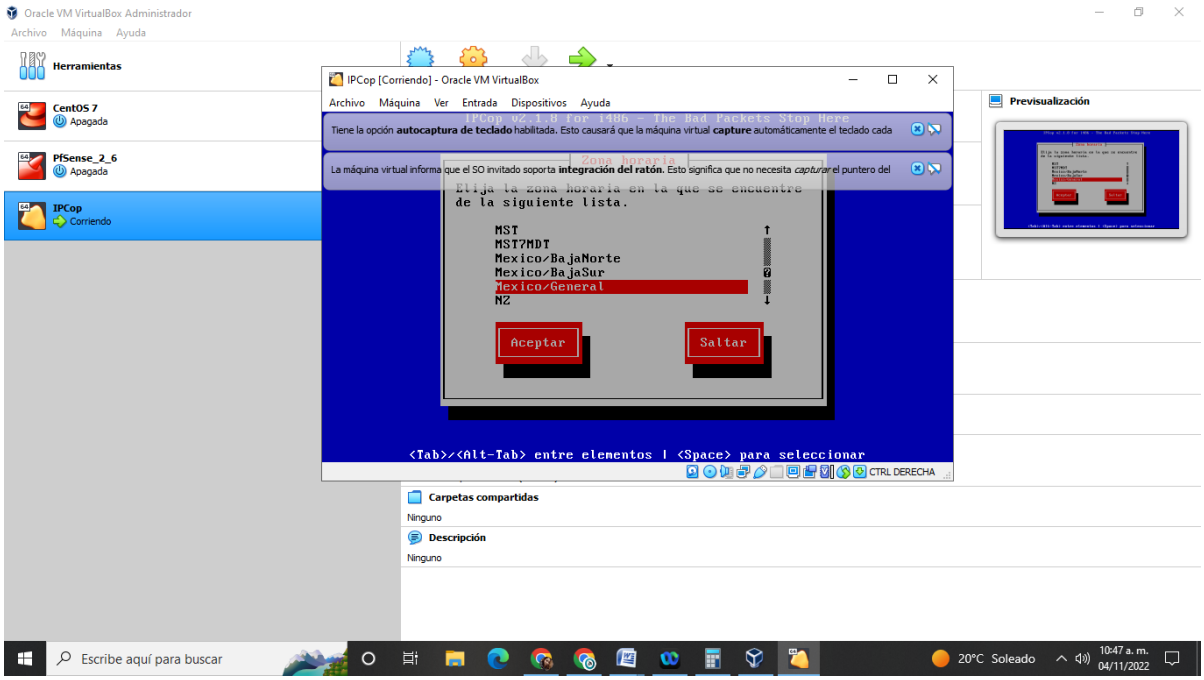


Ilustración 44

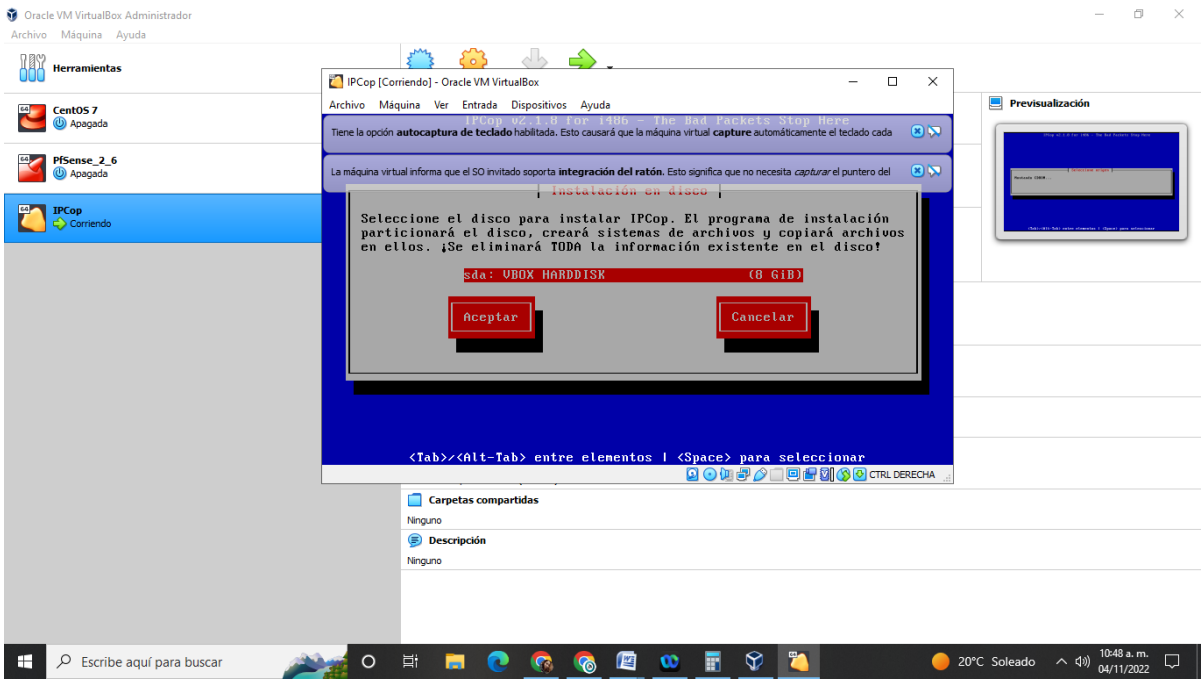


Ilustración 45

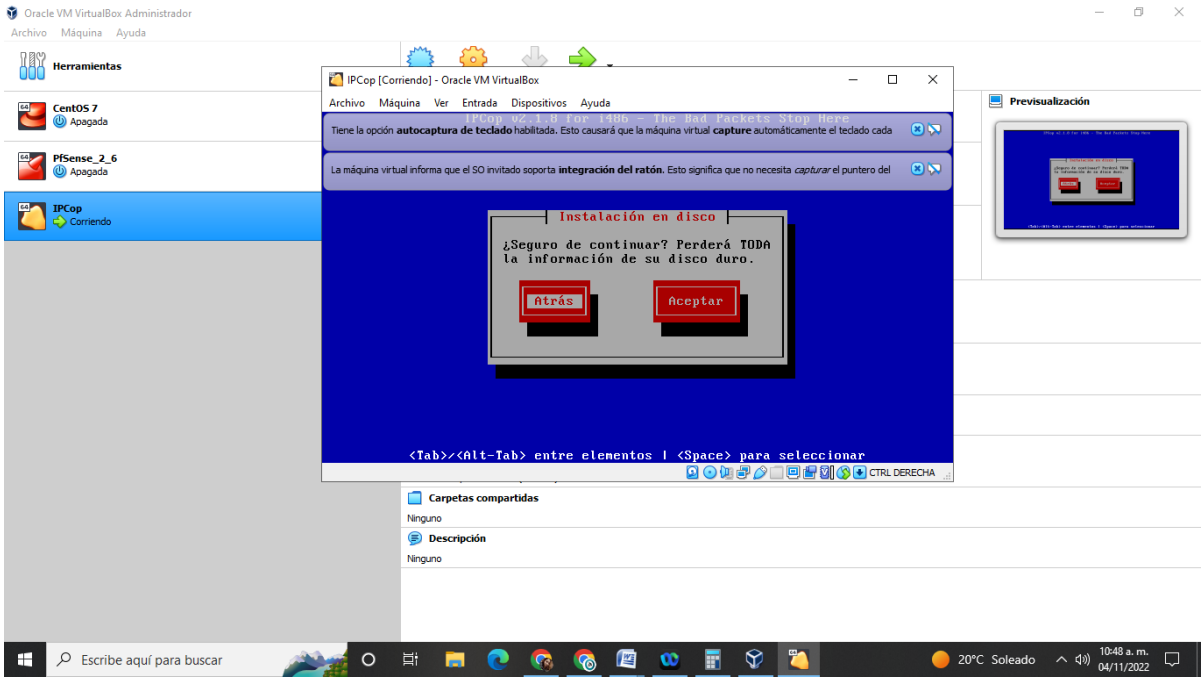


Ilustración 46

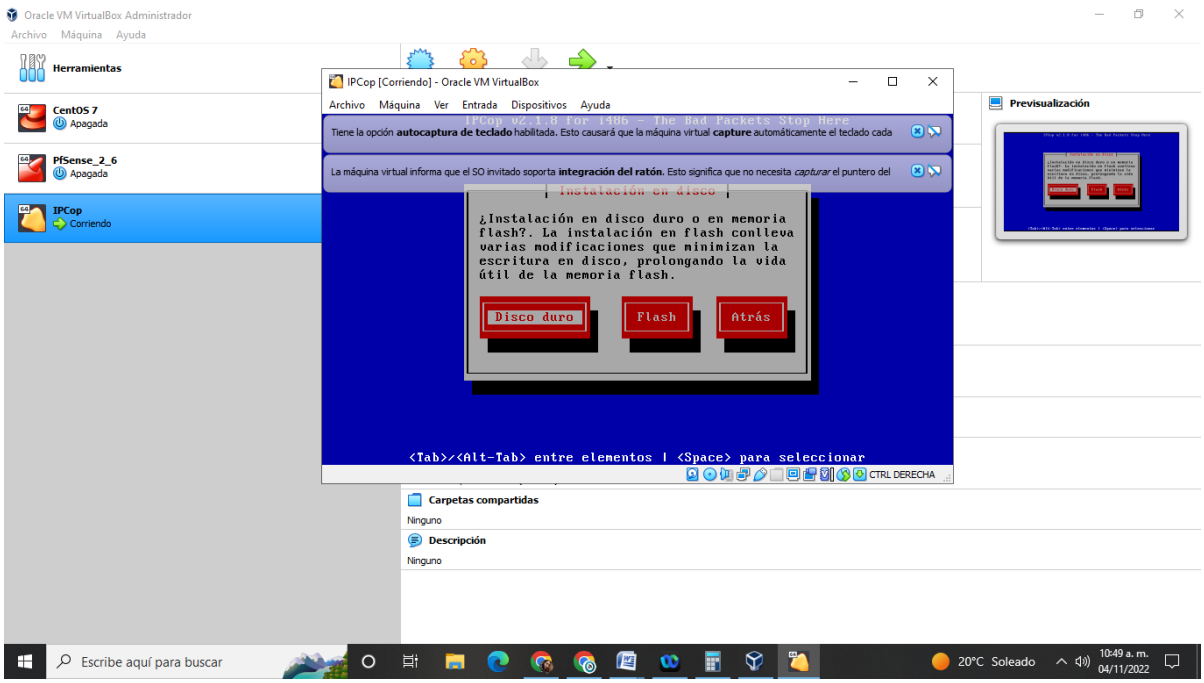


Ilustración 47

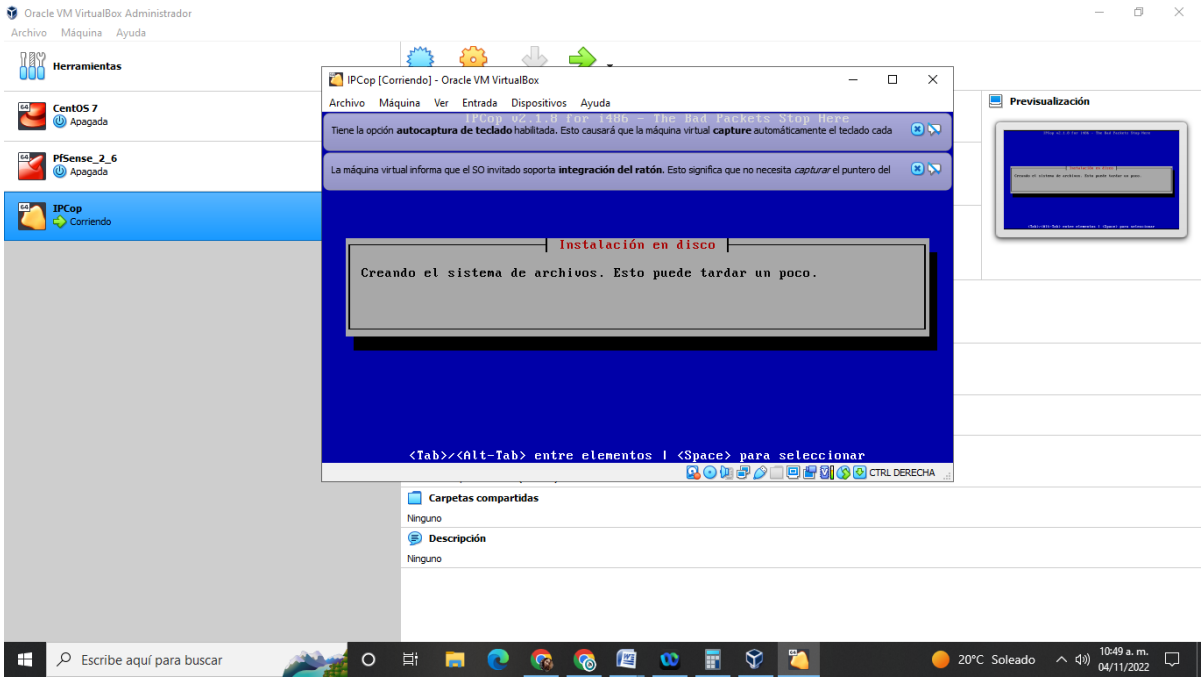


Ilustración 48

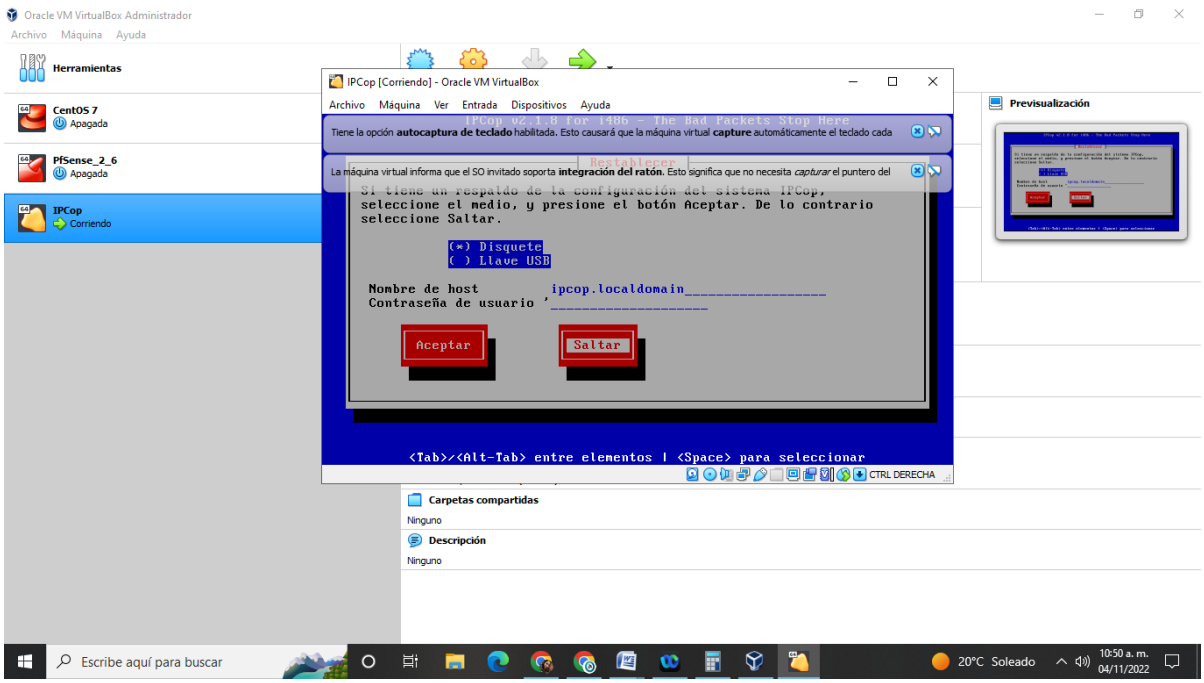


Ilustración 49

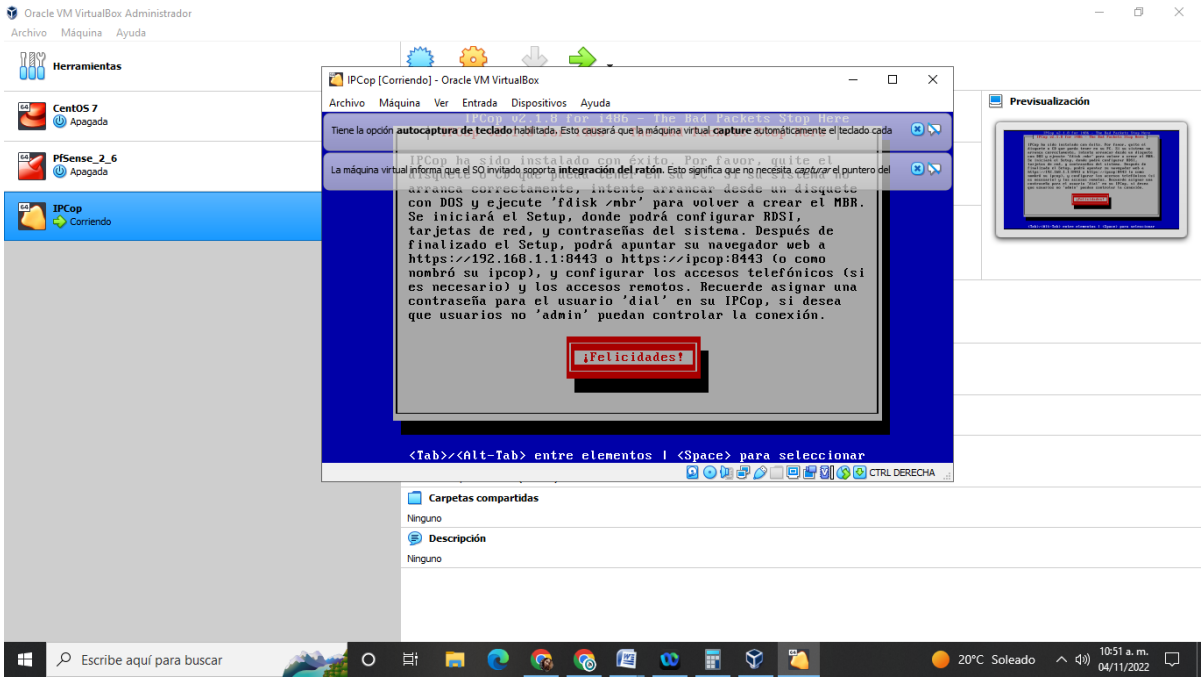


Ilustración 50

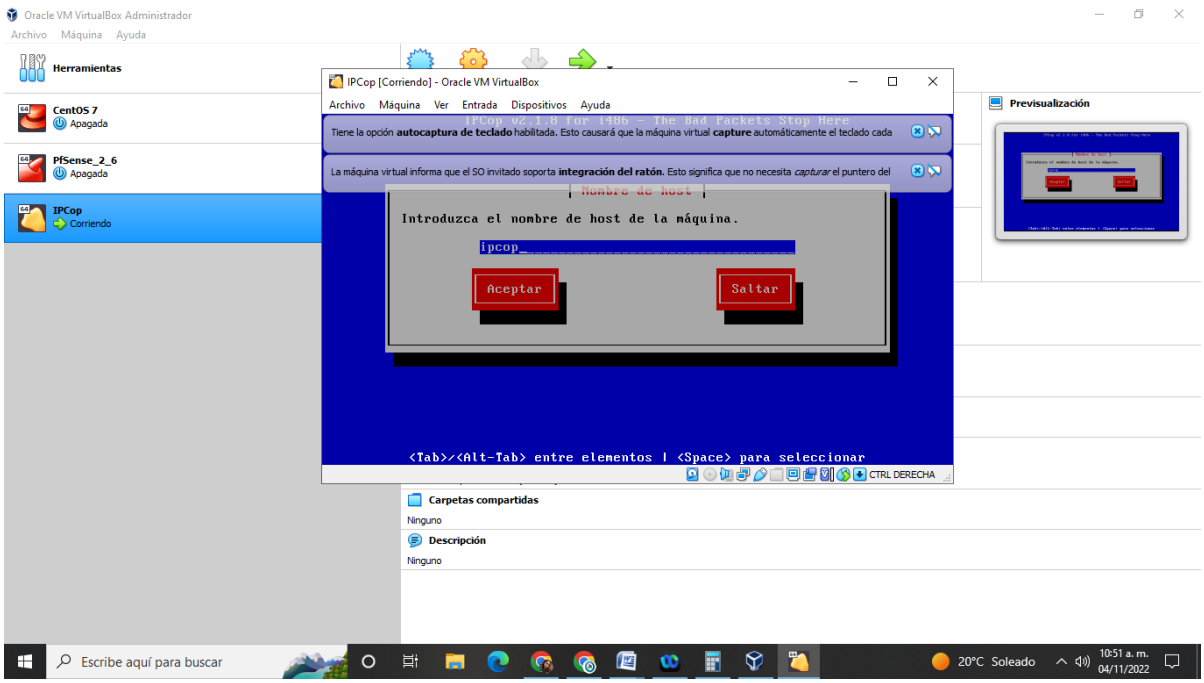


Ilustración 51

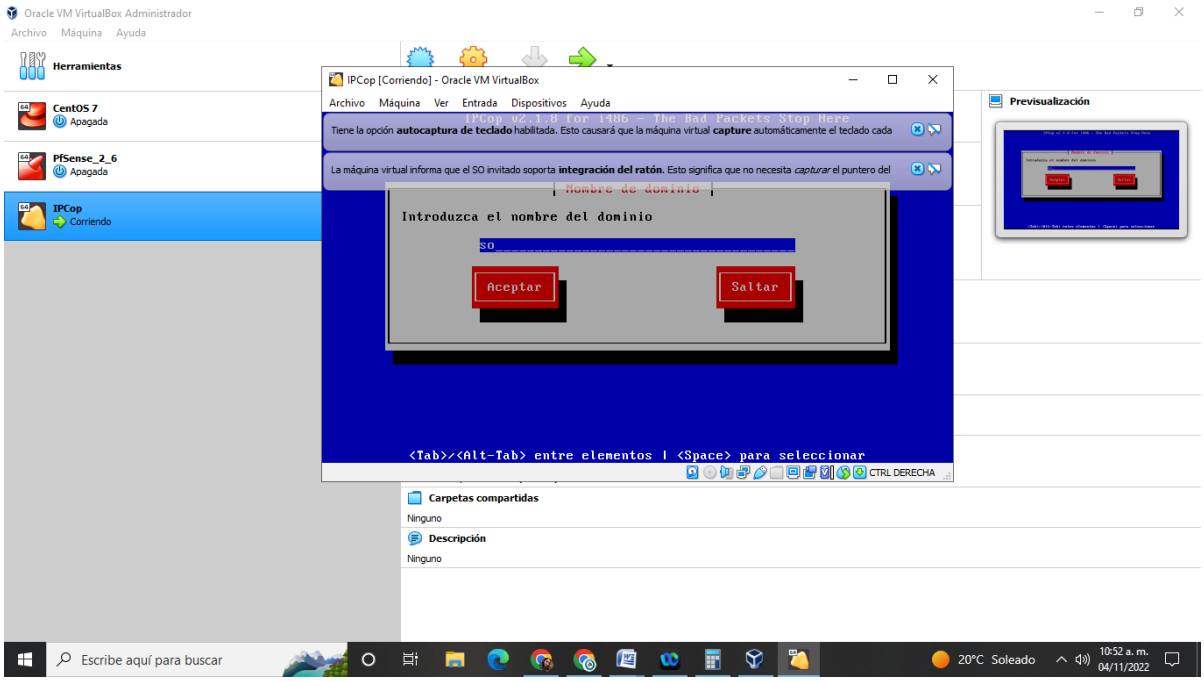


Ilustración 52

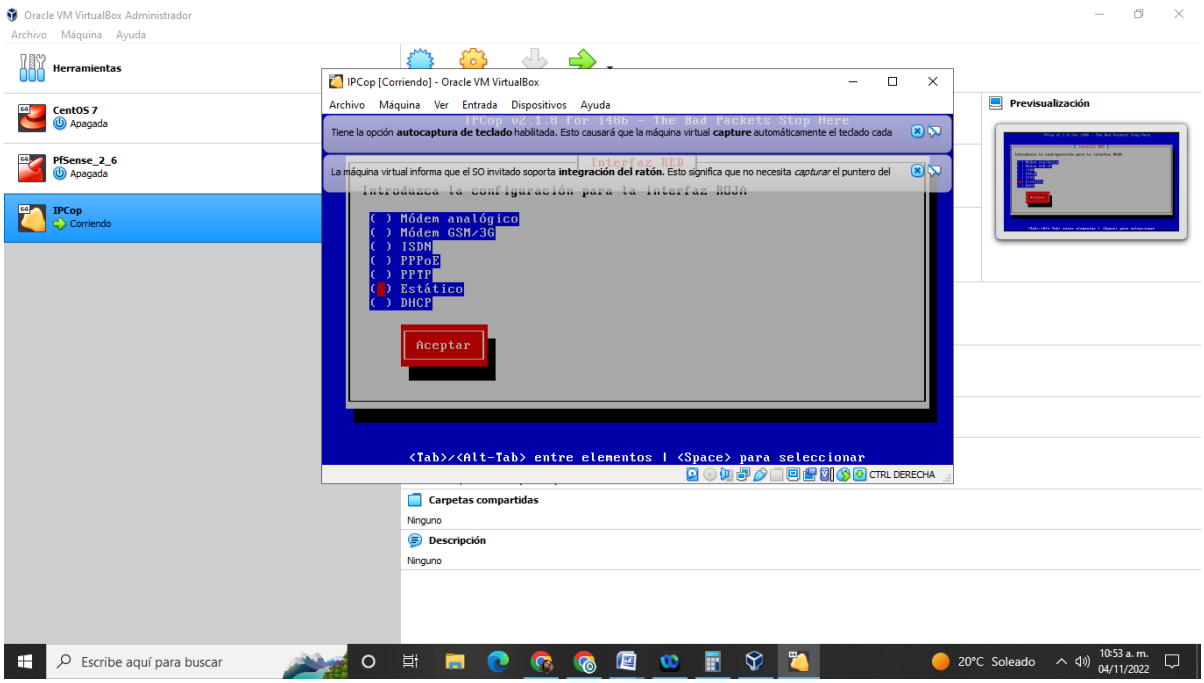


Ilustración 53

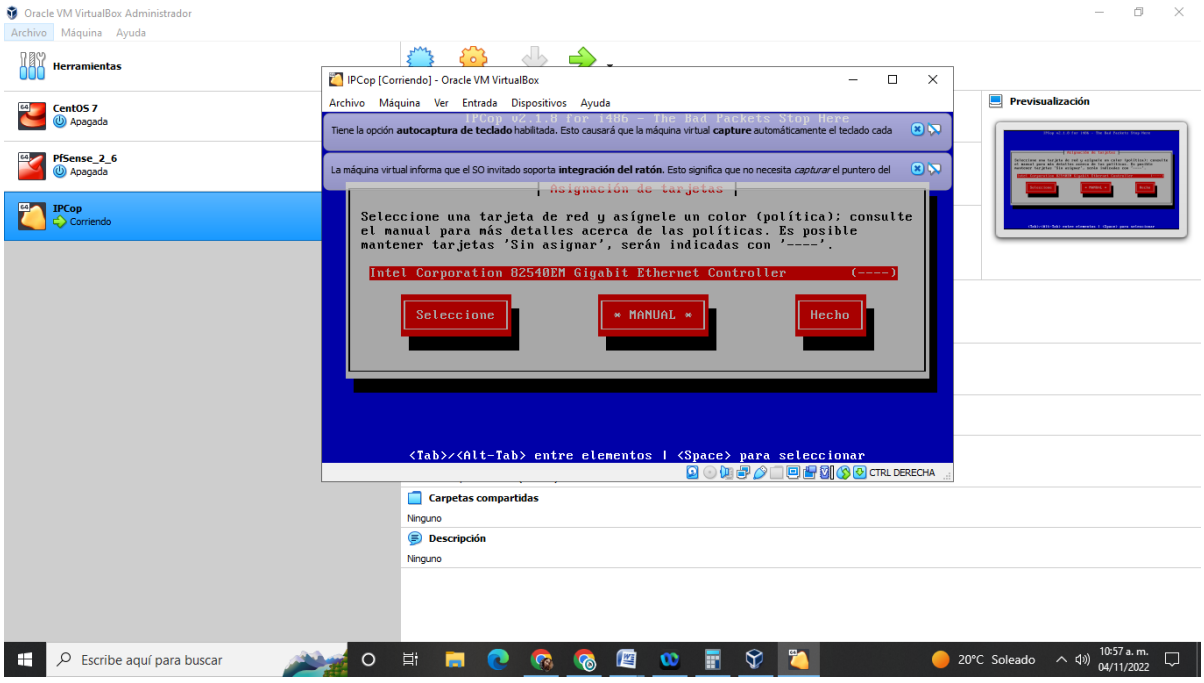


Ilustración 54

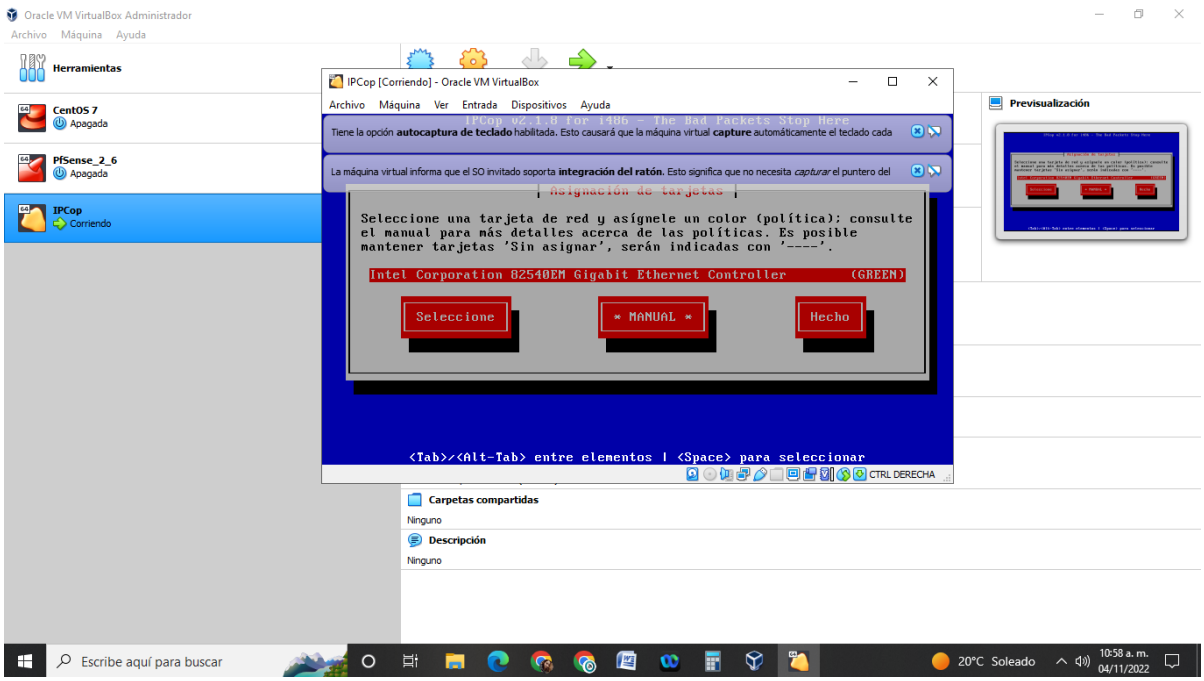


Ilustración 55

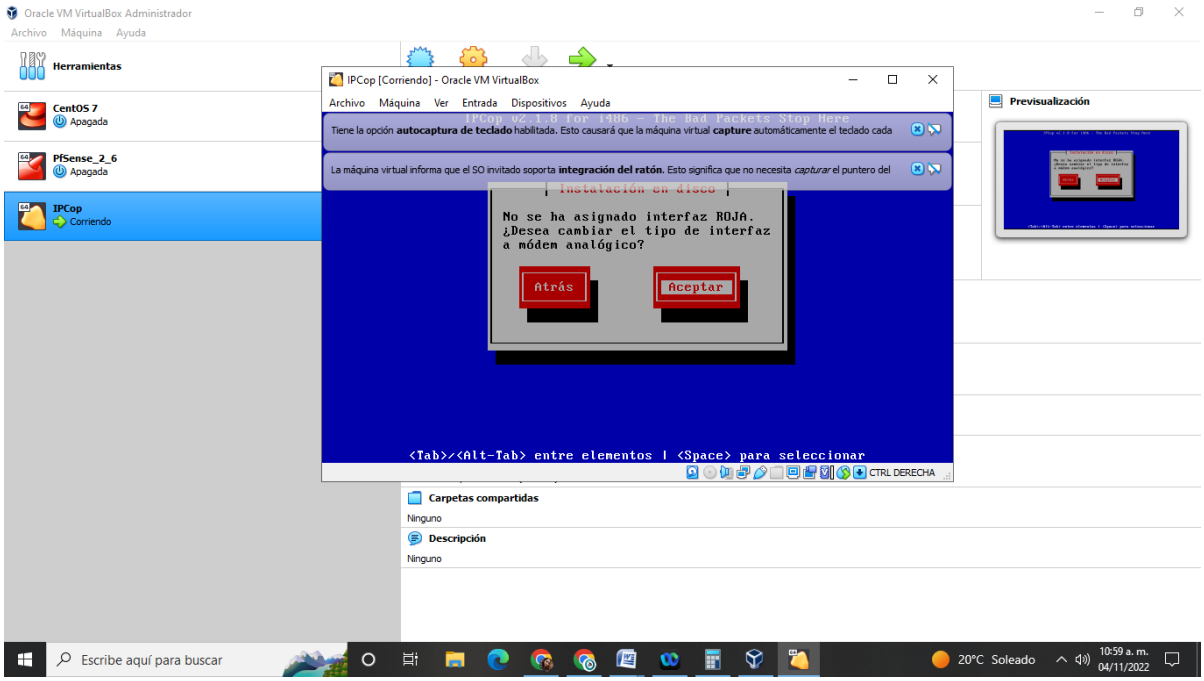


Ilustración 56

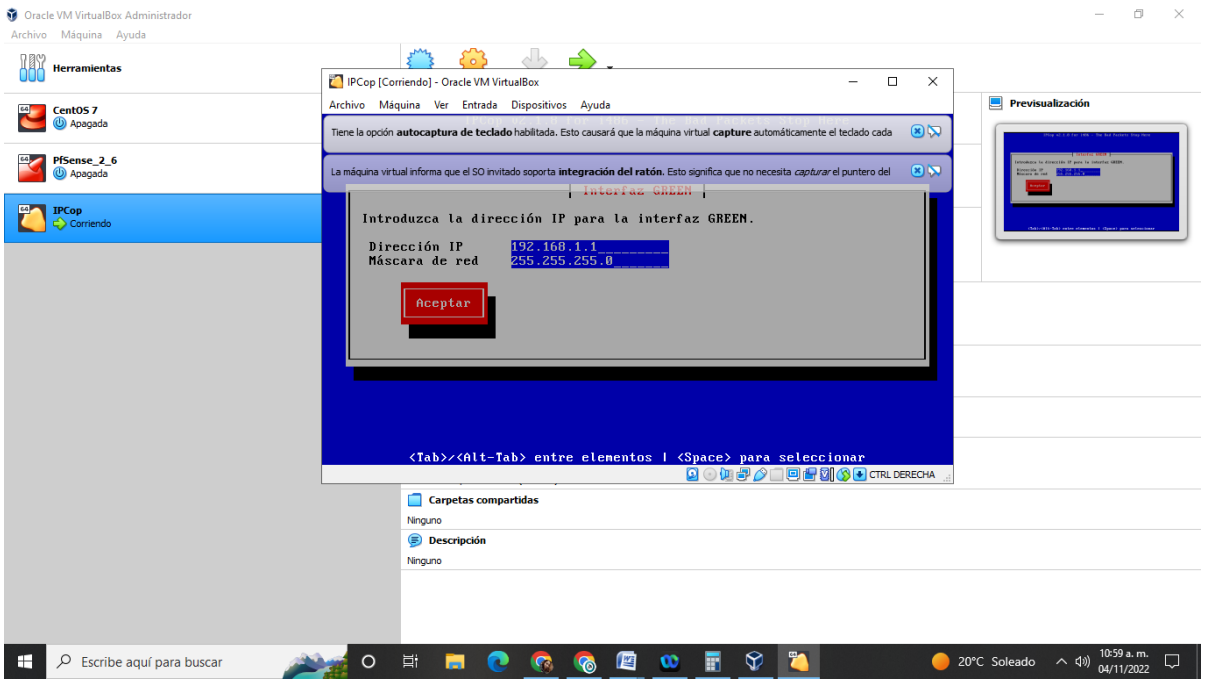


Ilustración 57

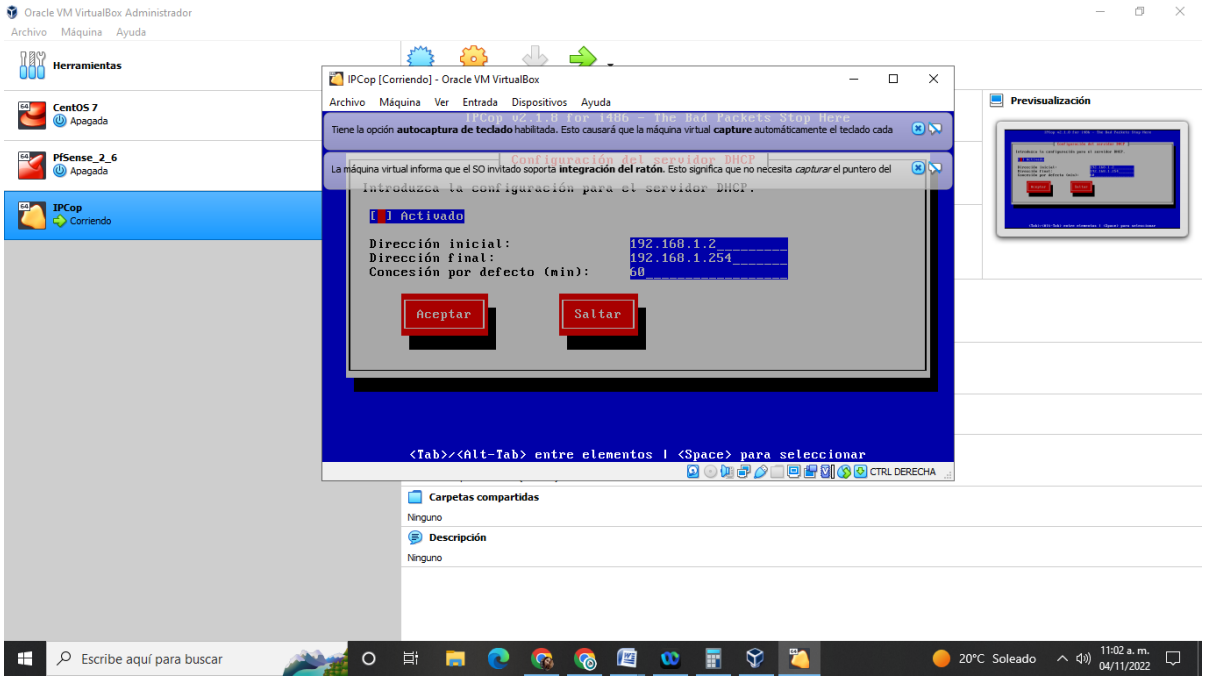


Ilustración 58

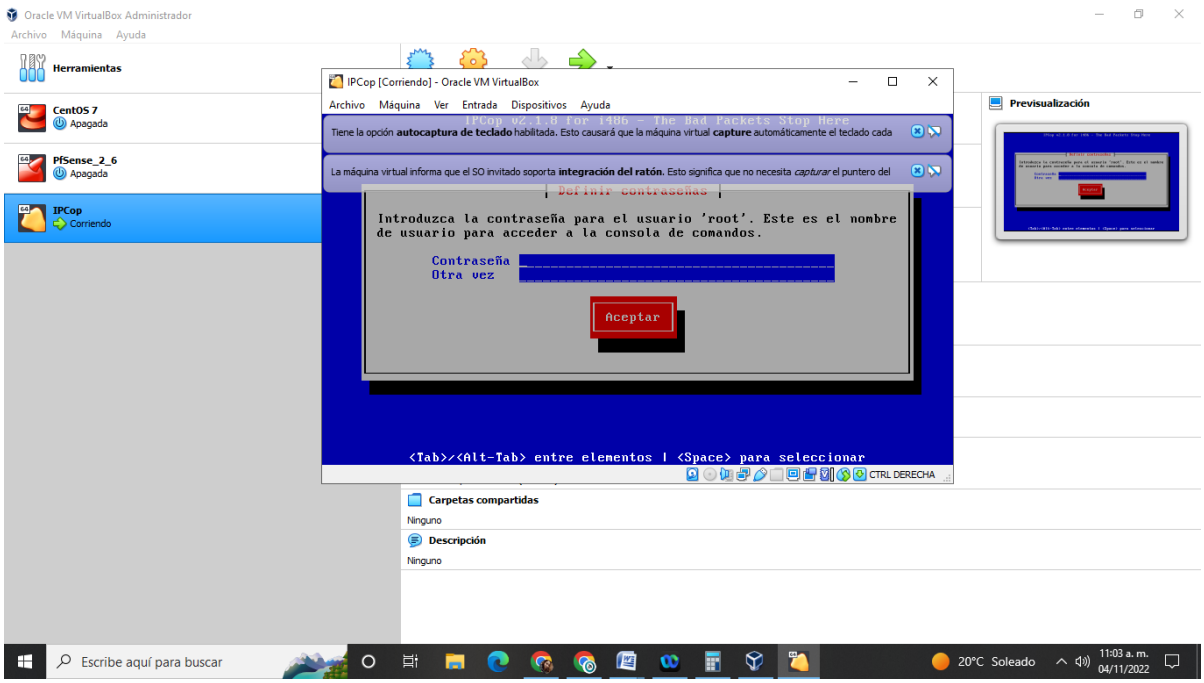


Ilustración 59

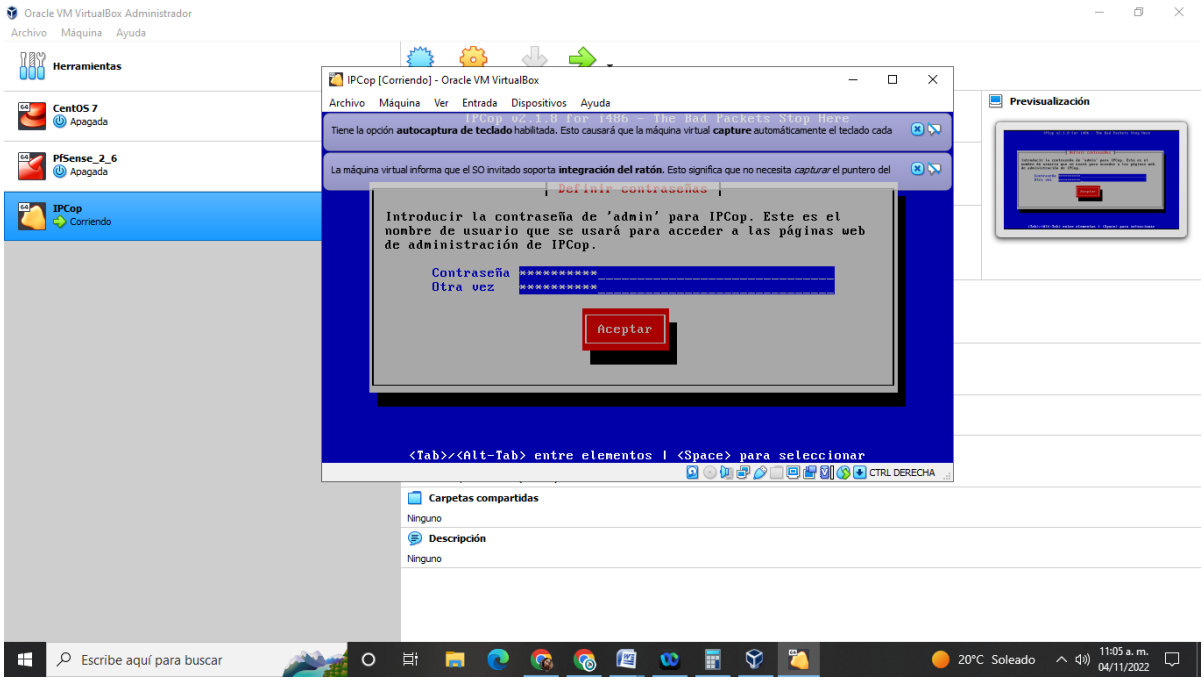


Ilustración 50

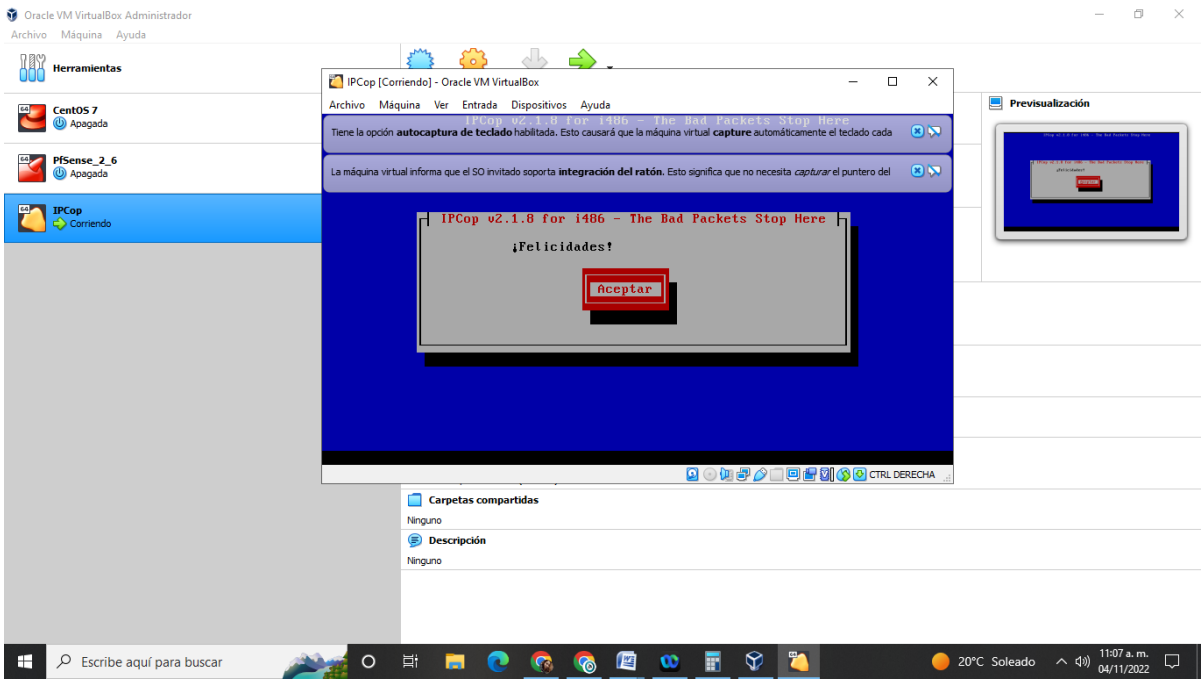


Ilustración 51

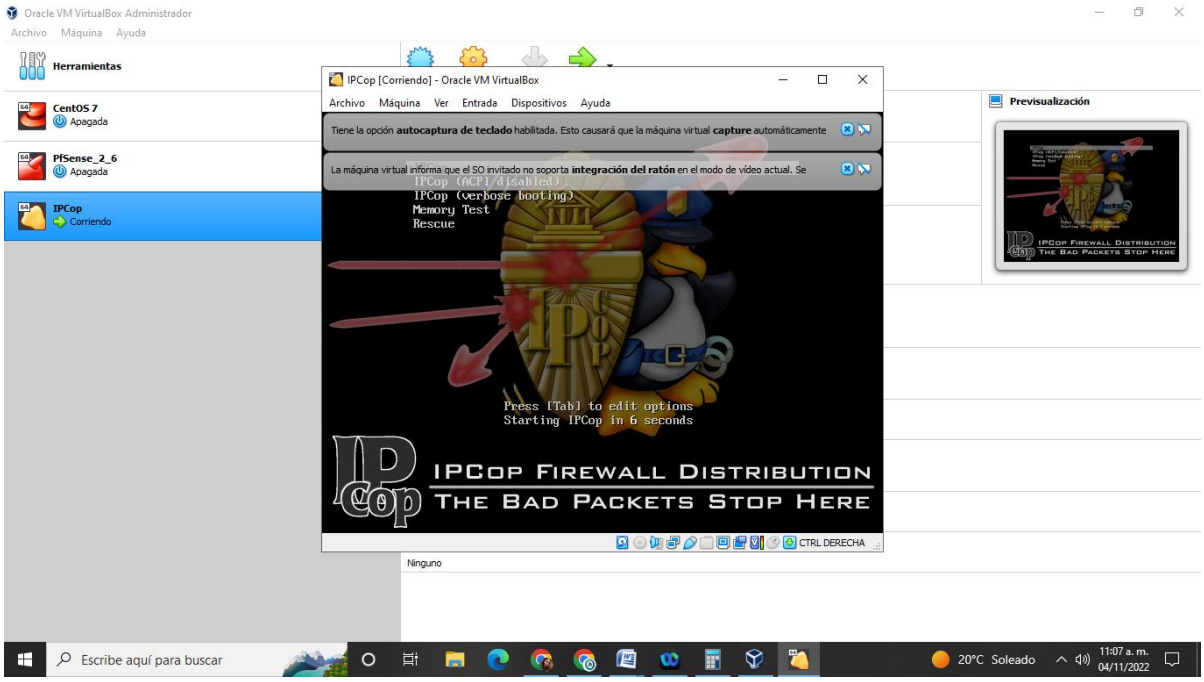


Ilustración 52

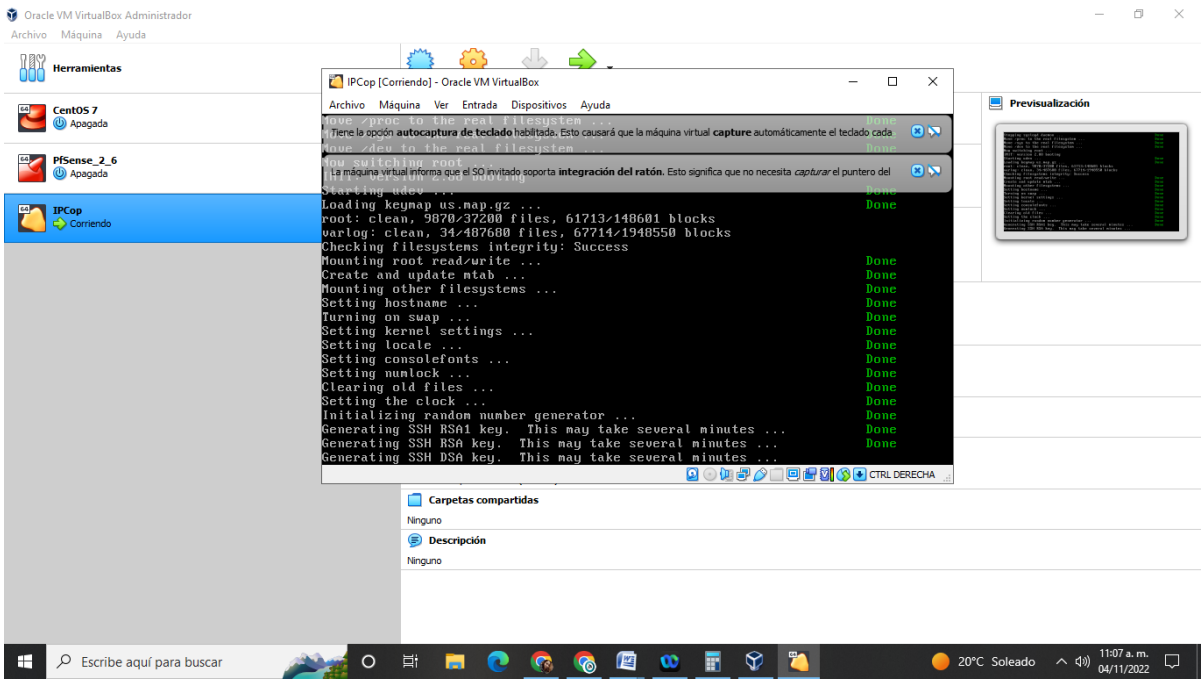


Ilustración 53

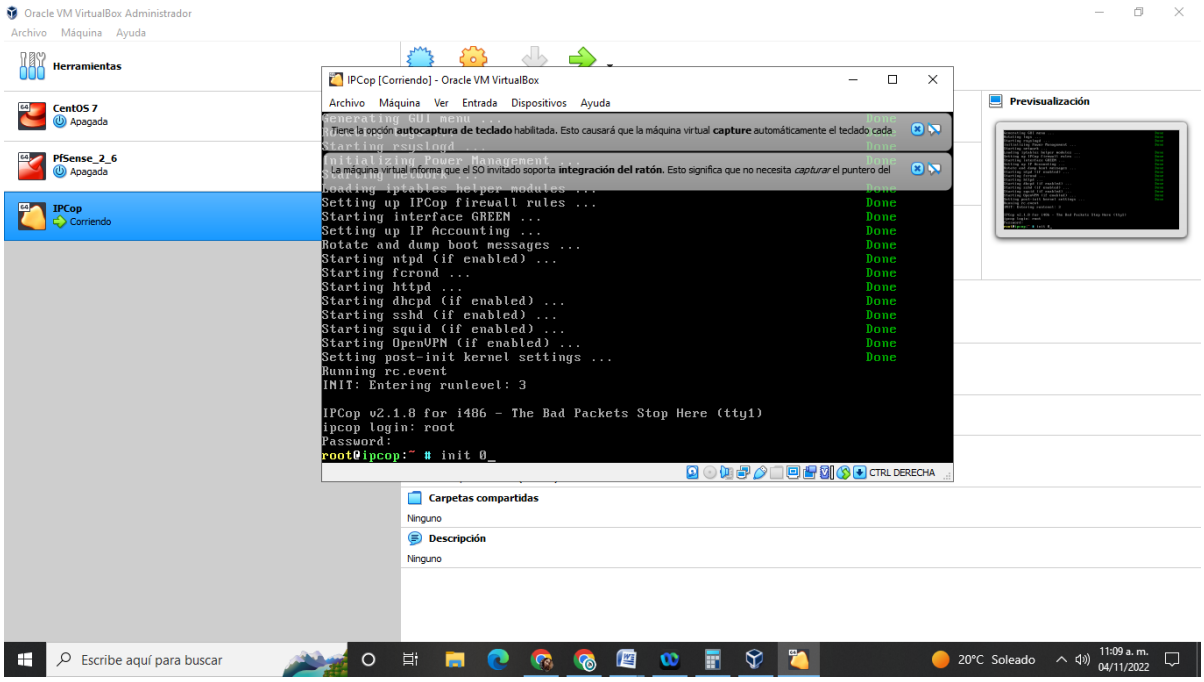


Ilustración 54

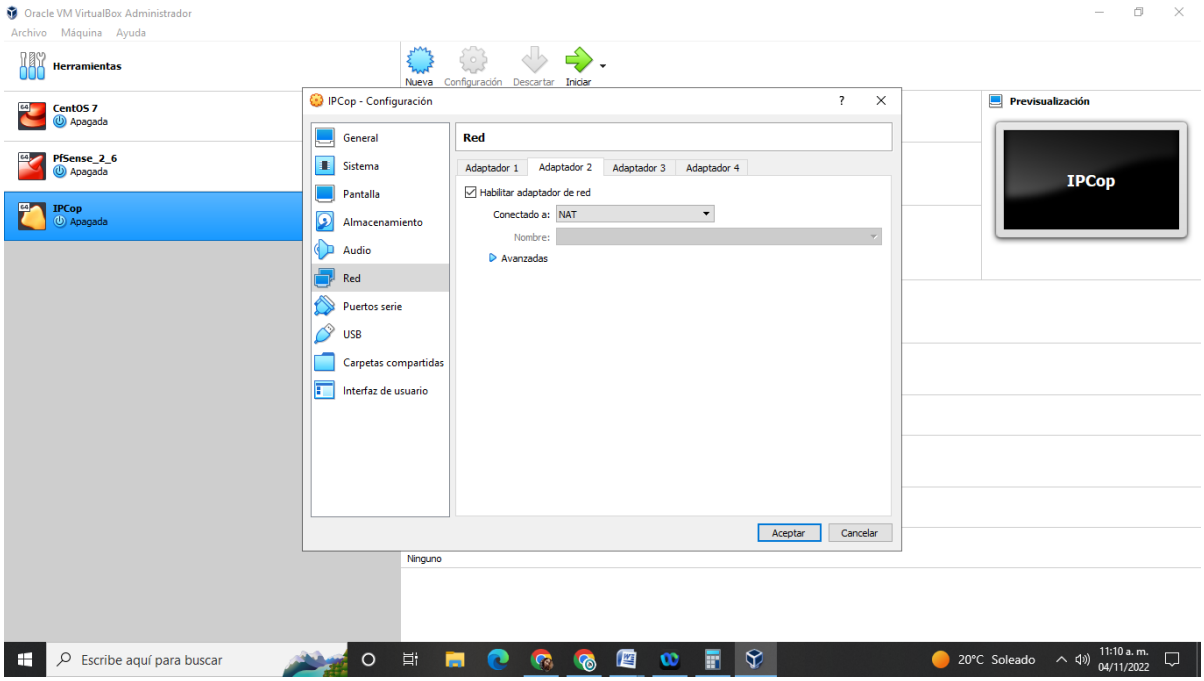


Ilustración 55

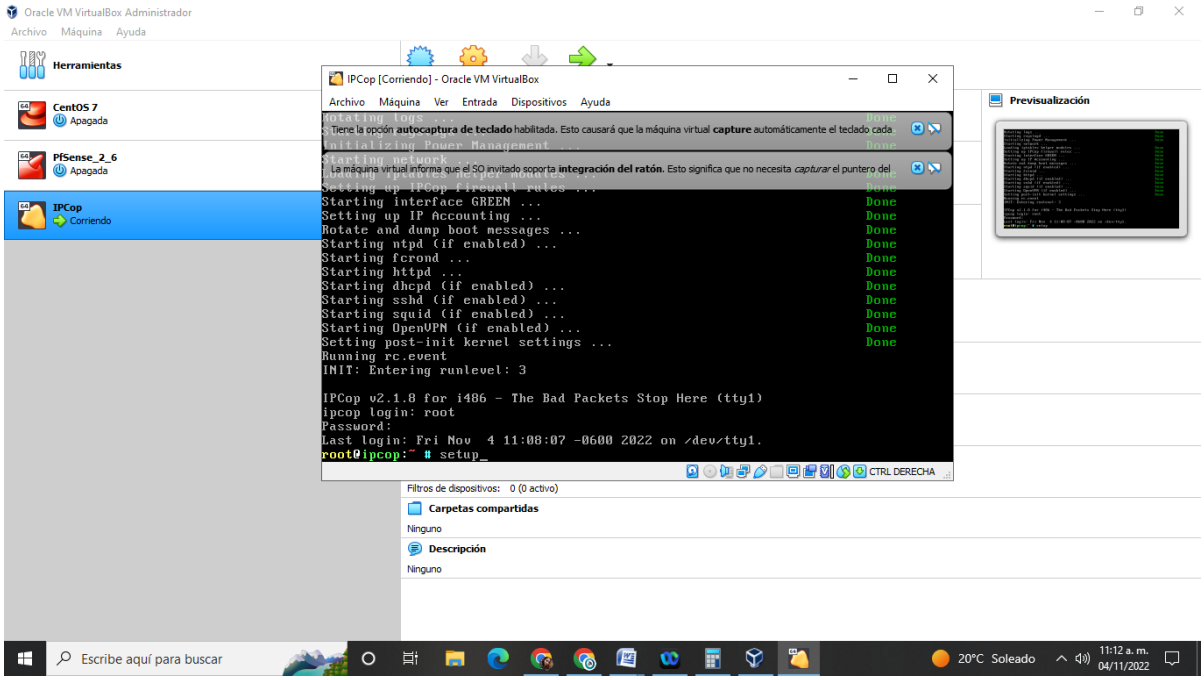


Ilustración 56

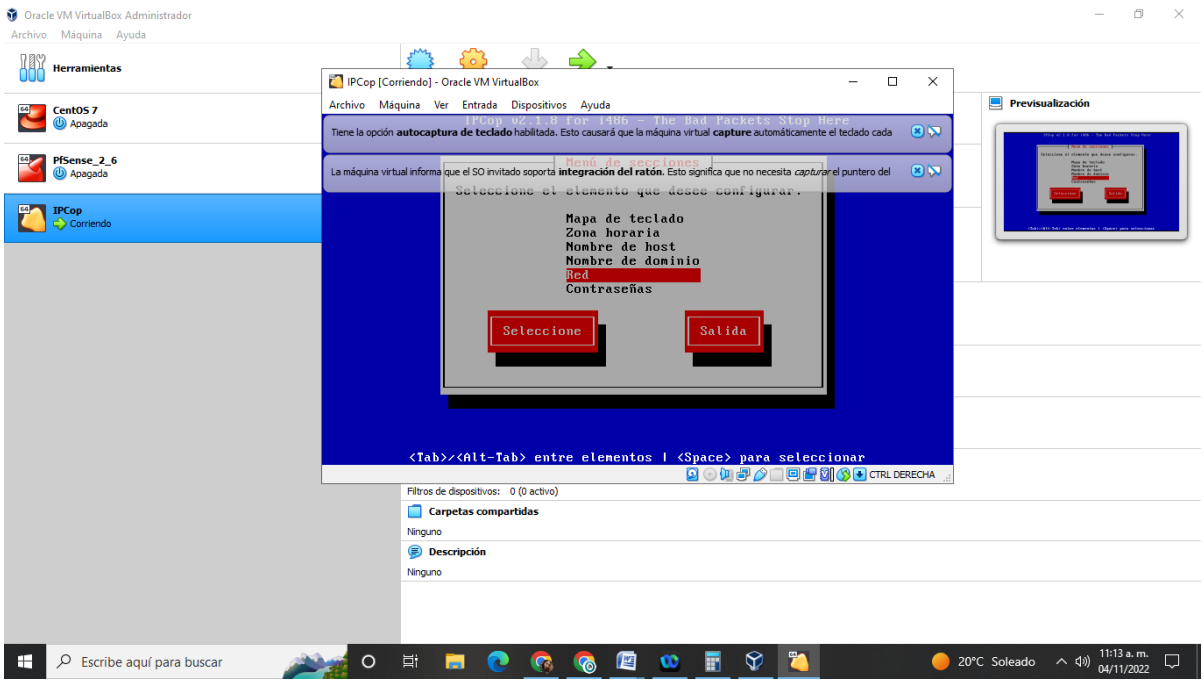


Ilustración 57

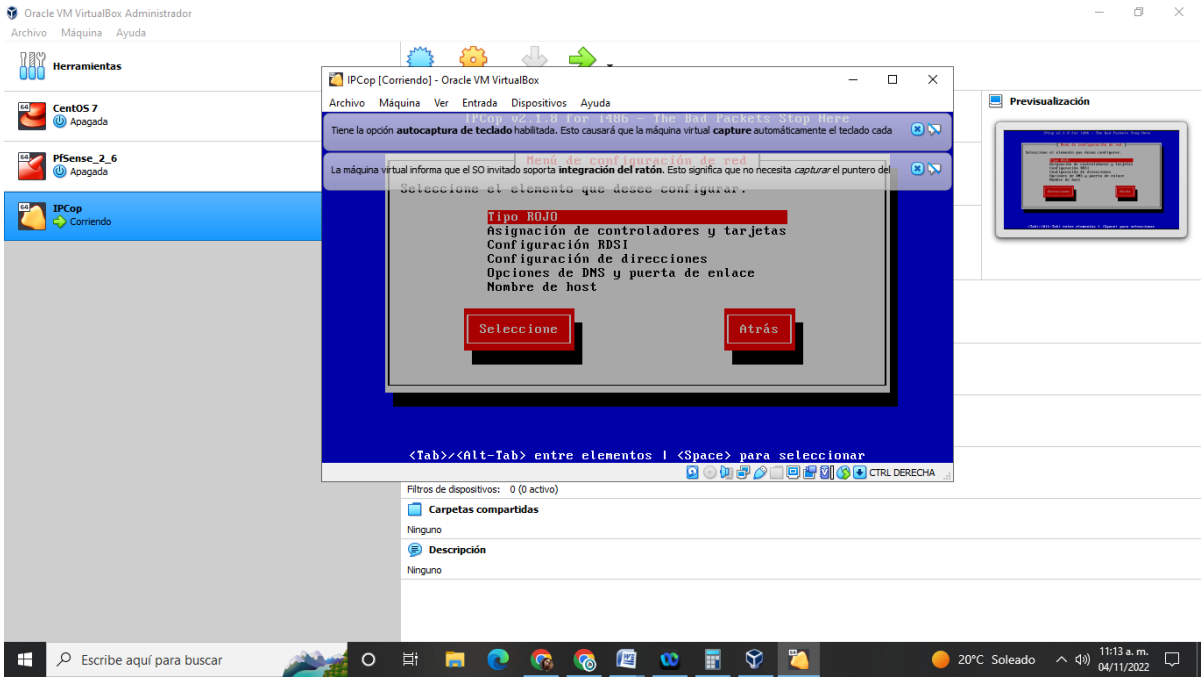


Ilustración 58

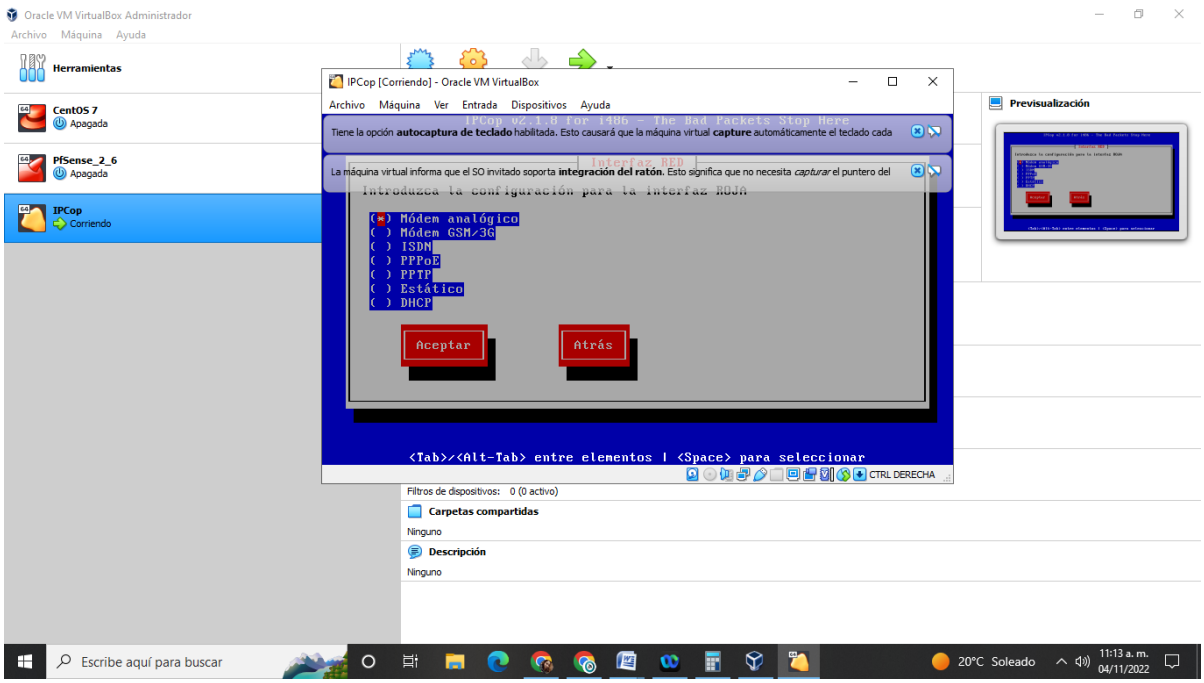


Ilustración 59

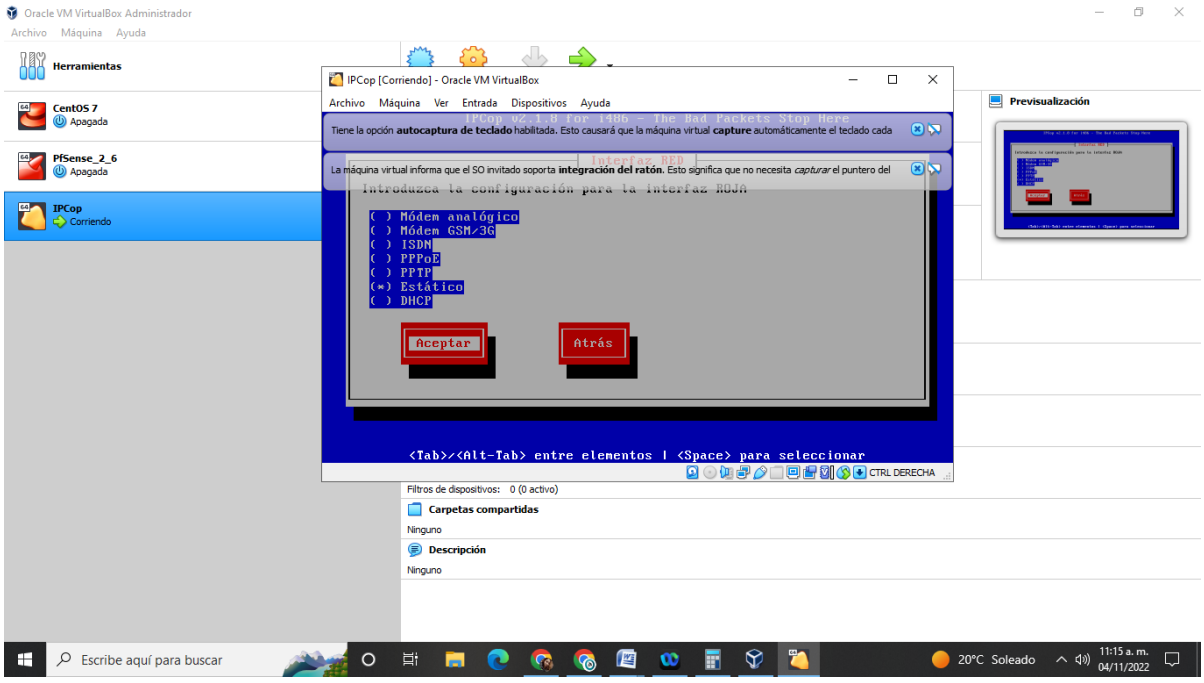


Ilustración 60

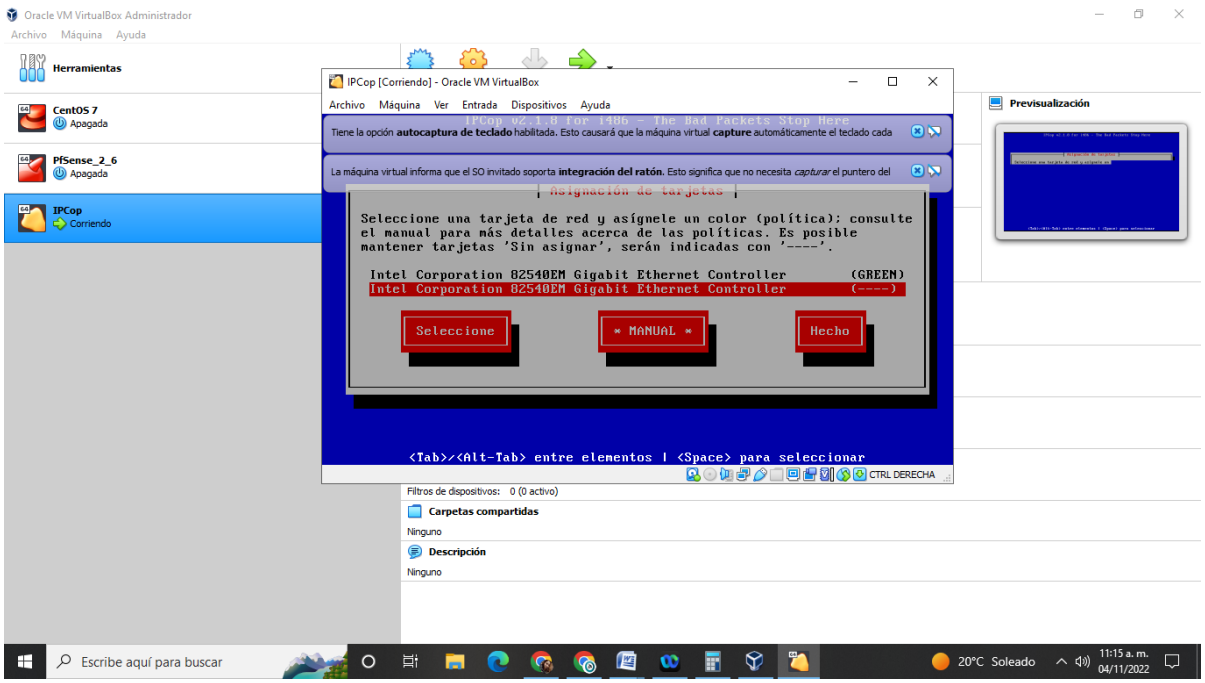


Ilustración 61

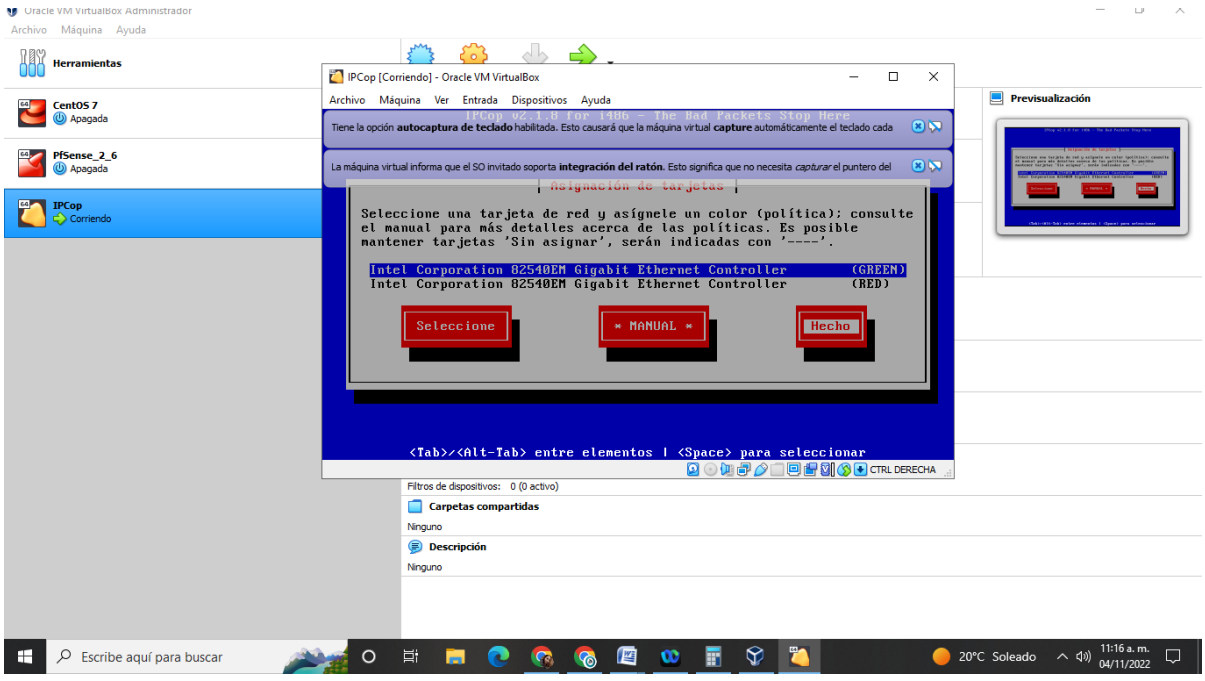


Ilustración 62

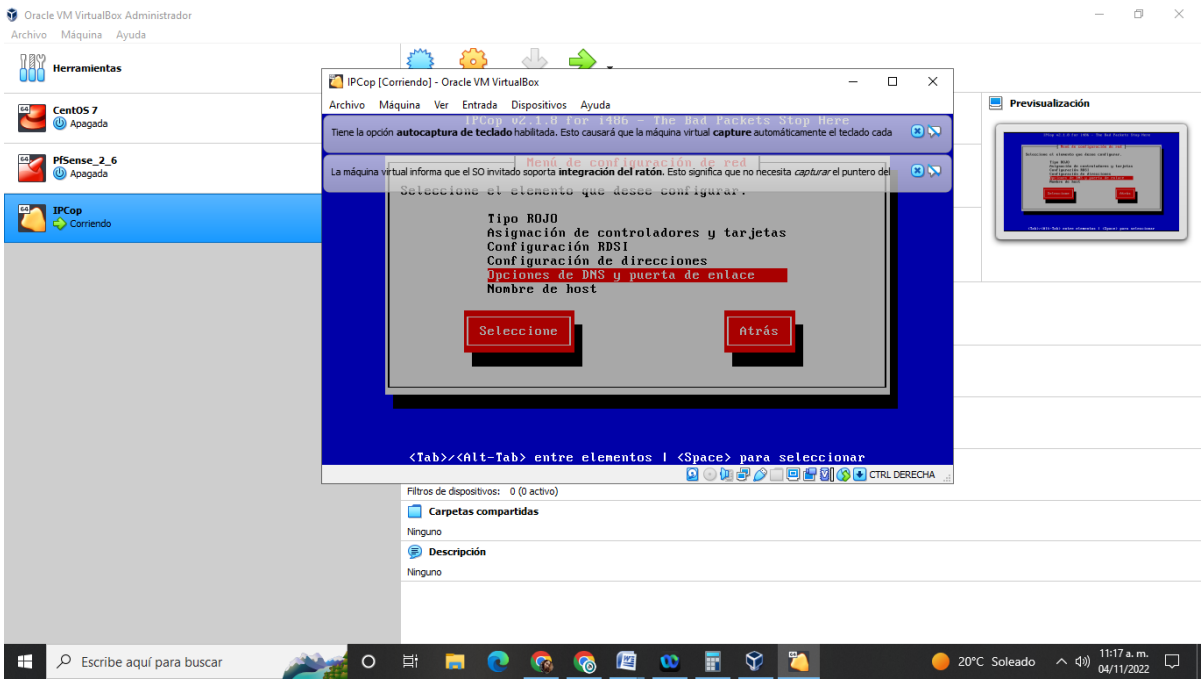


Ilustración 63

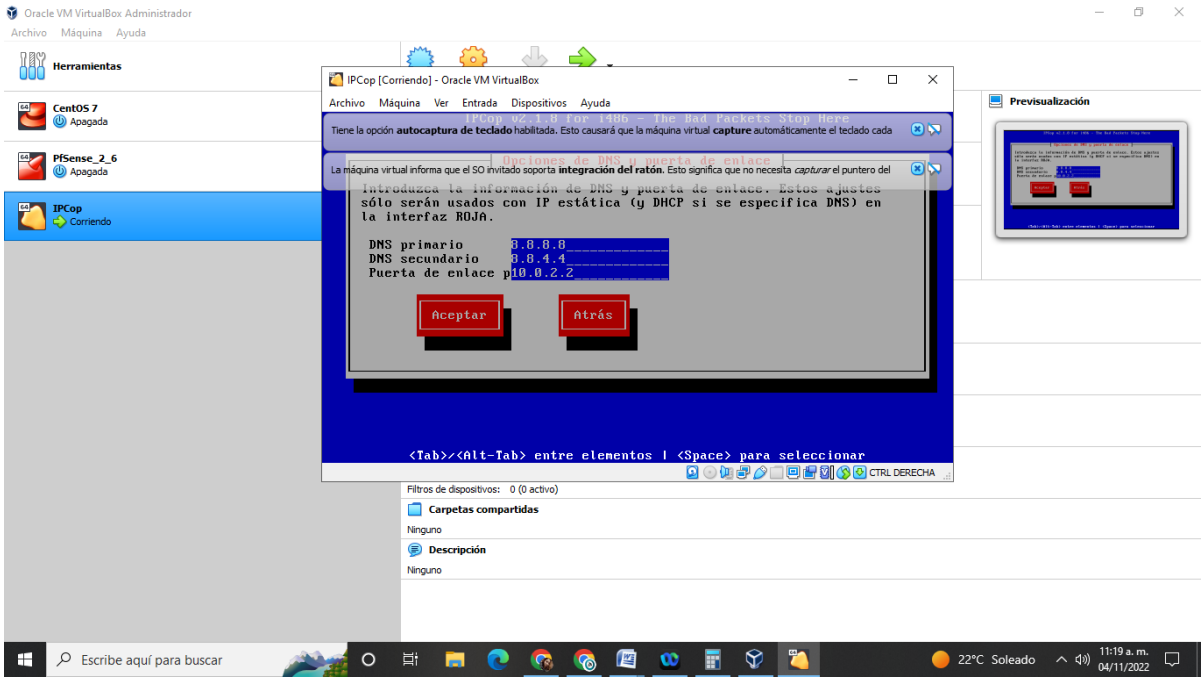


Ilustración 64

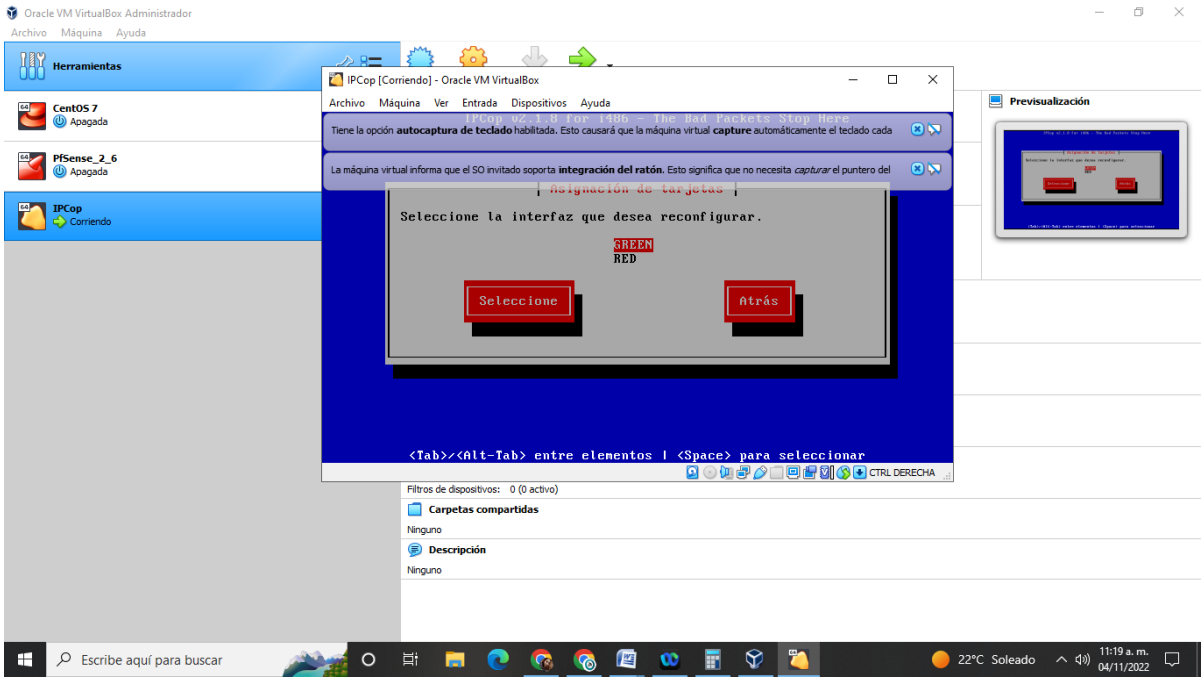


Ilustración 65

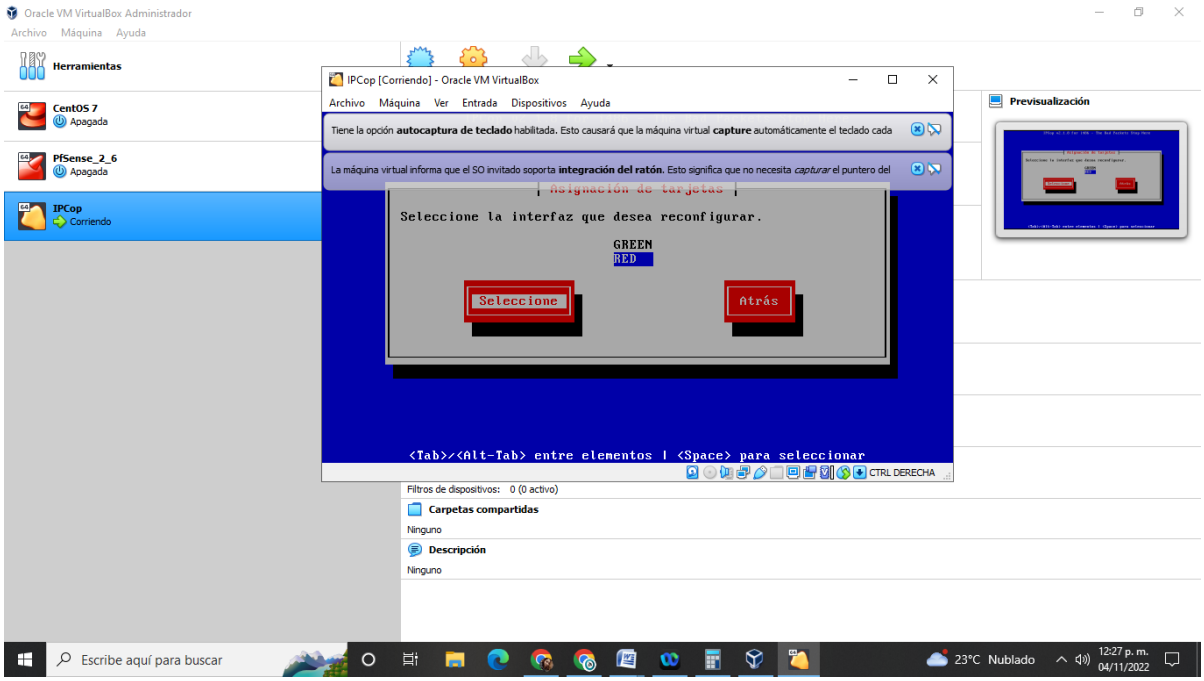


Ilustración 66

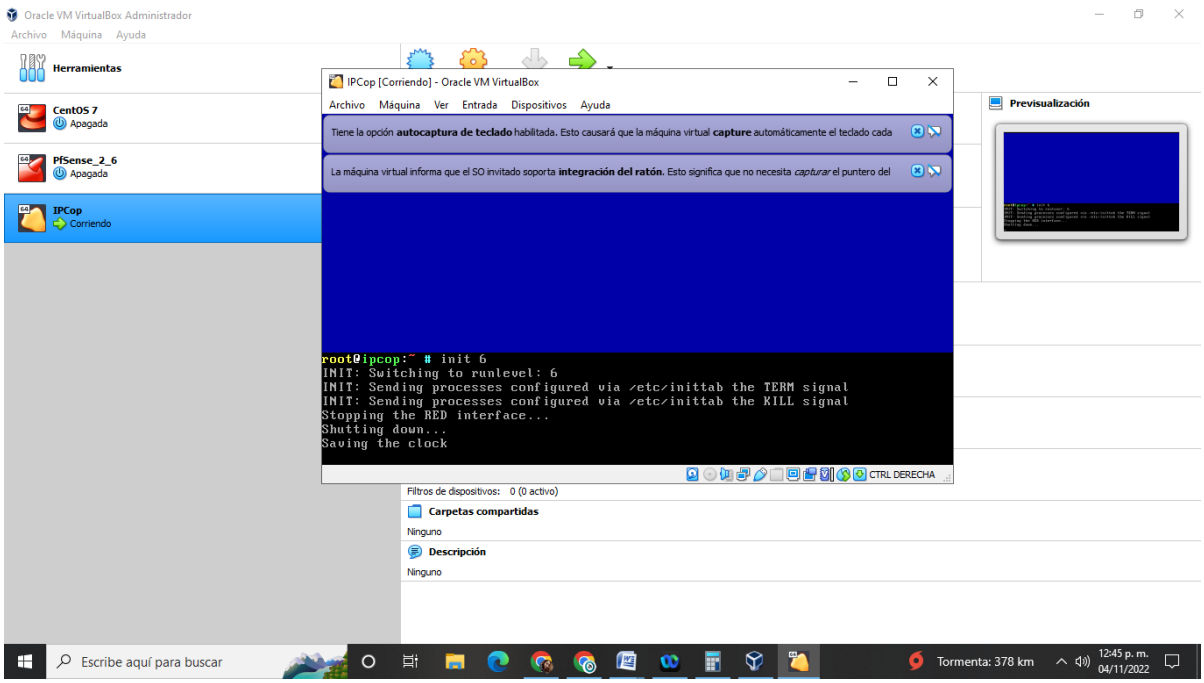


Ilustración 67

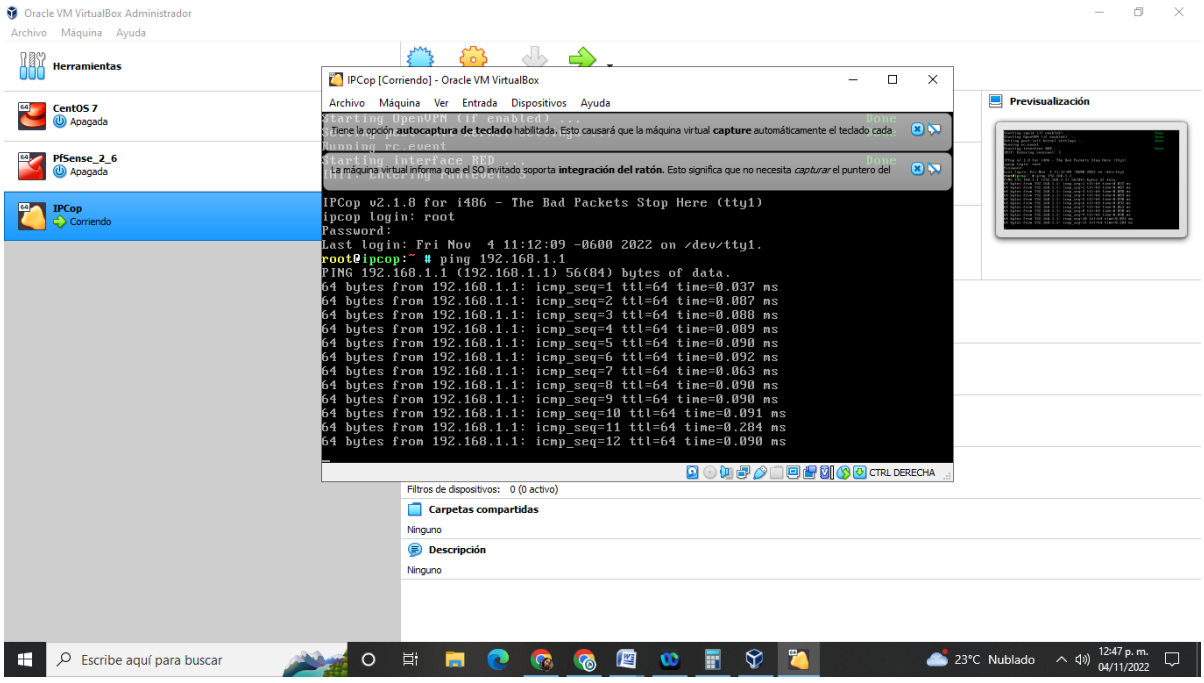


Ilustración 68

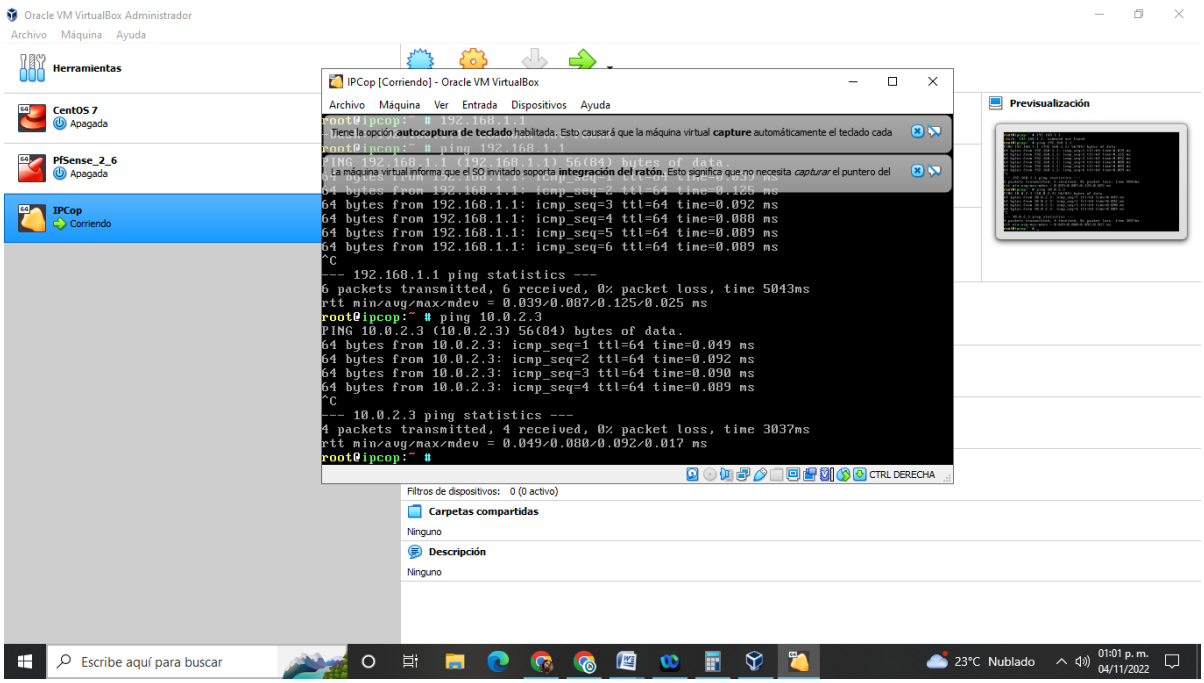


Ilustración 69

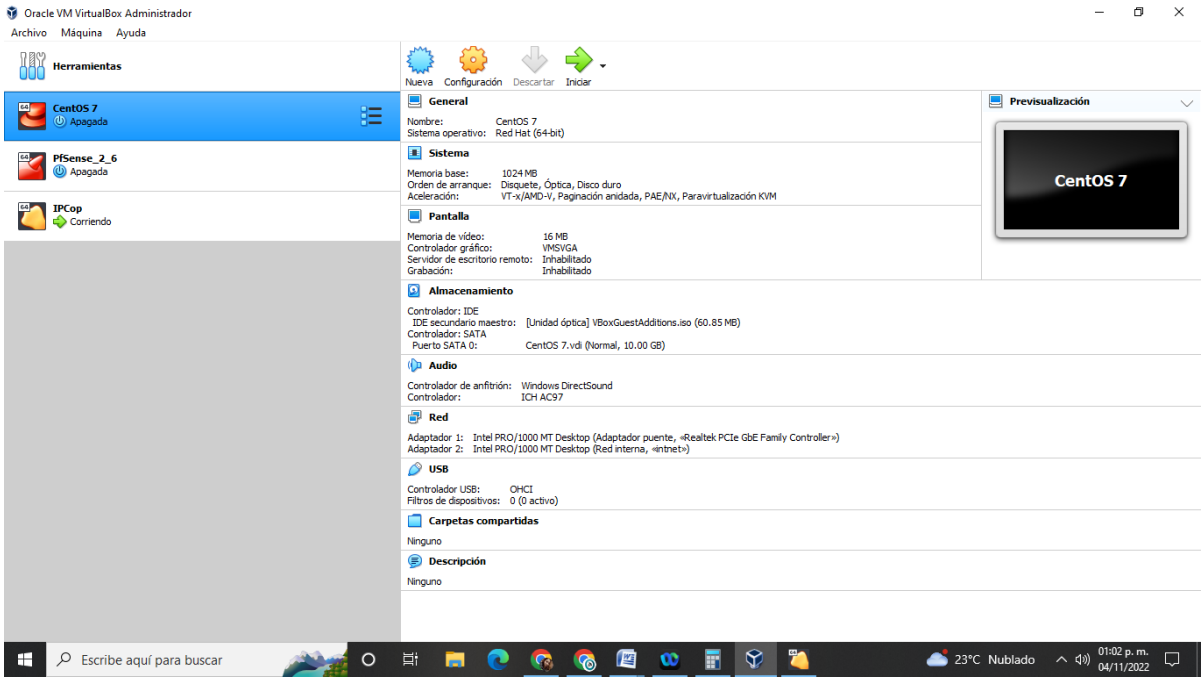


Ilustración 70

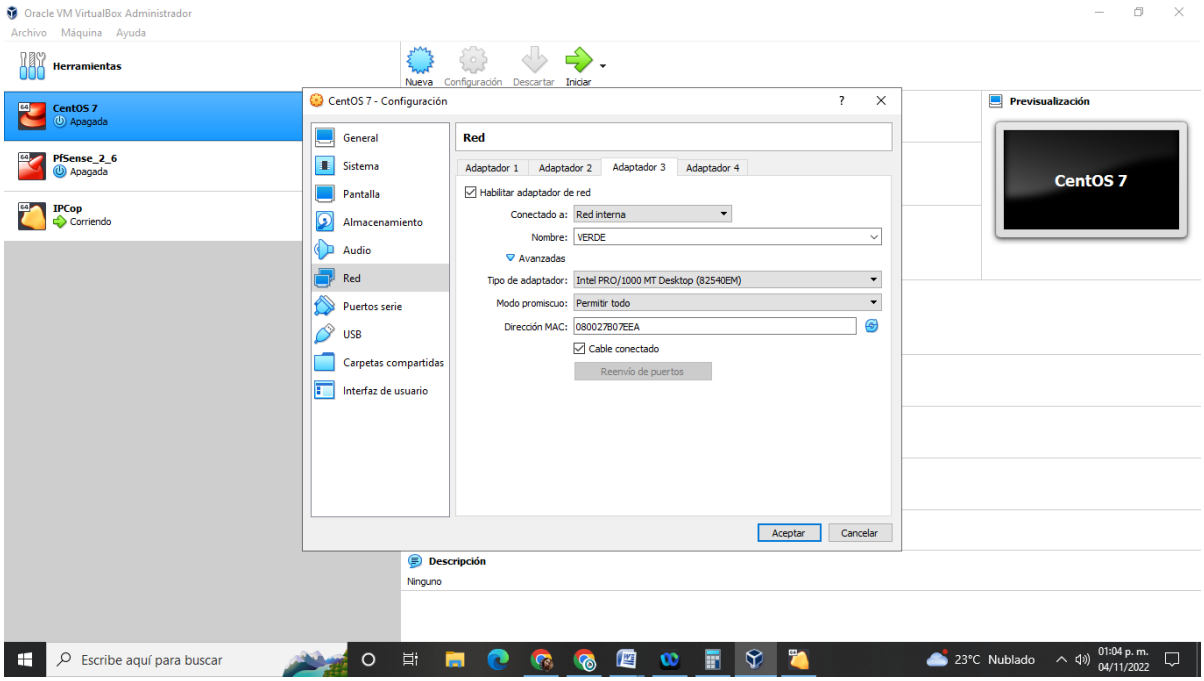


Ilustración 71

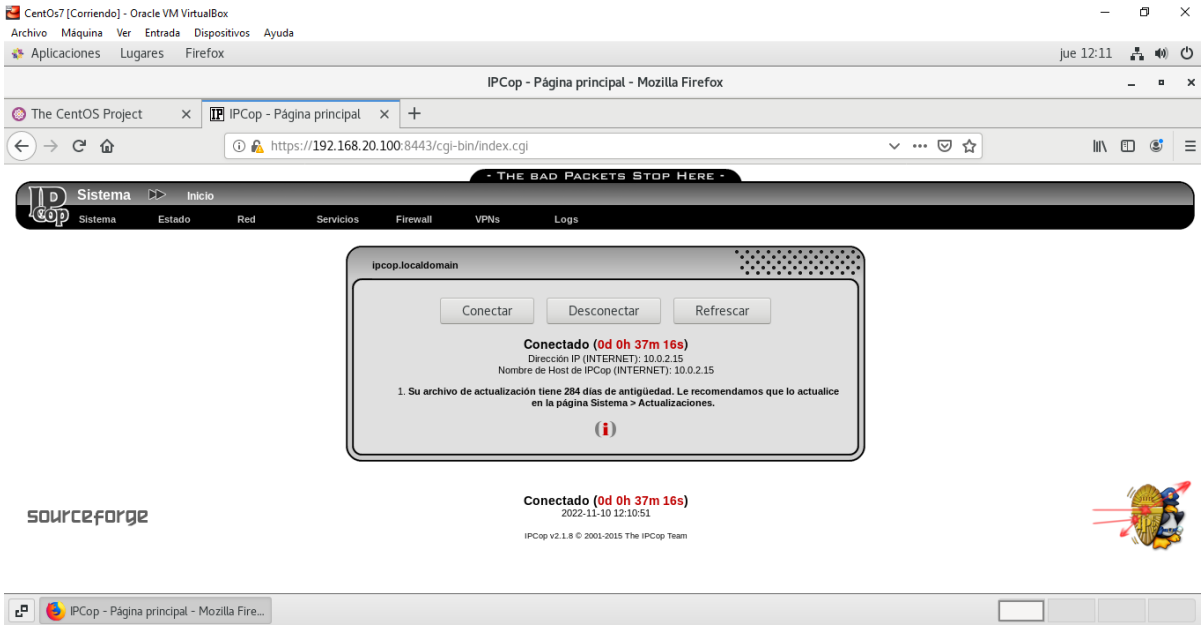


Ilustración 72

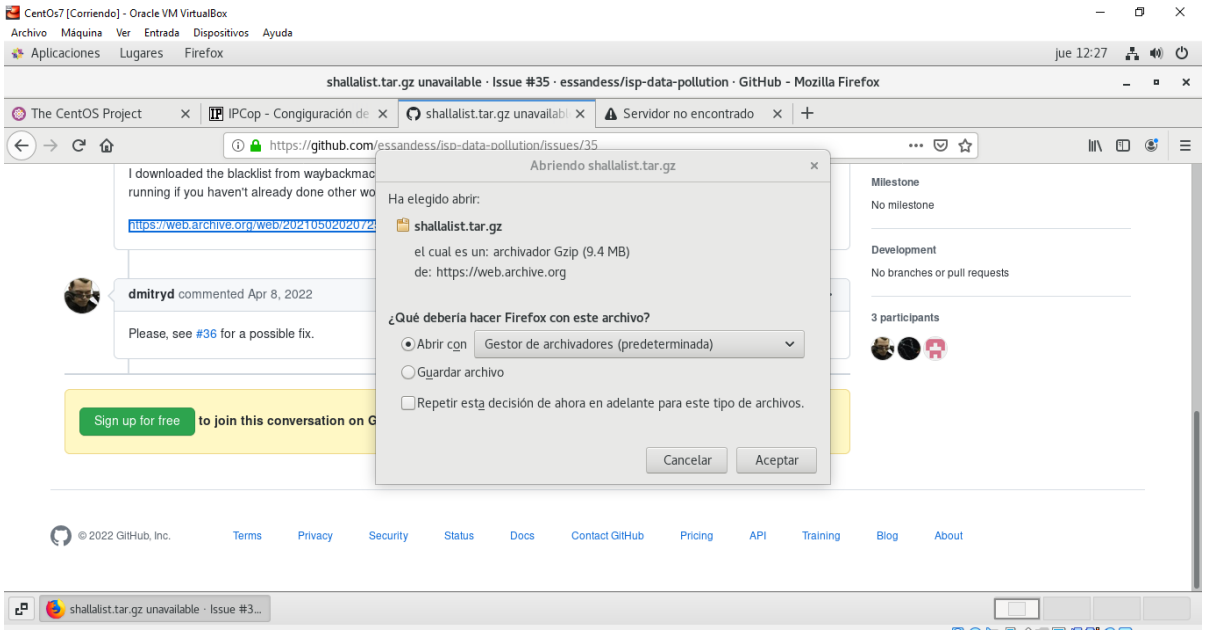


Ilustración 73

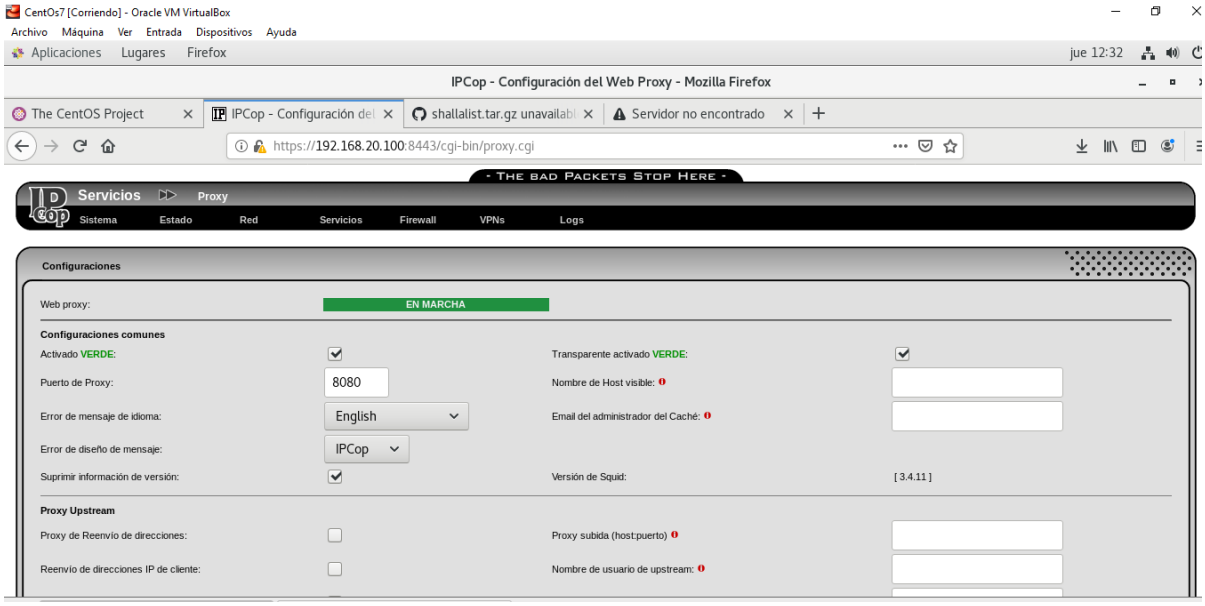


Ilustración 74

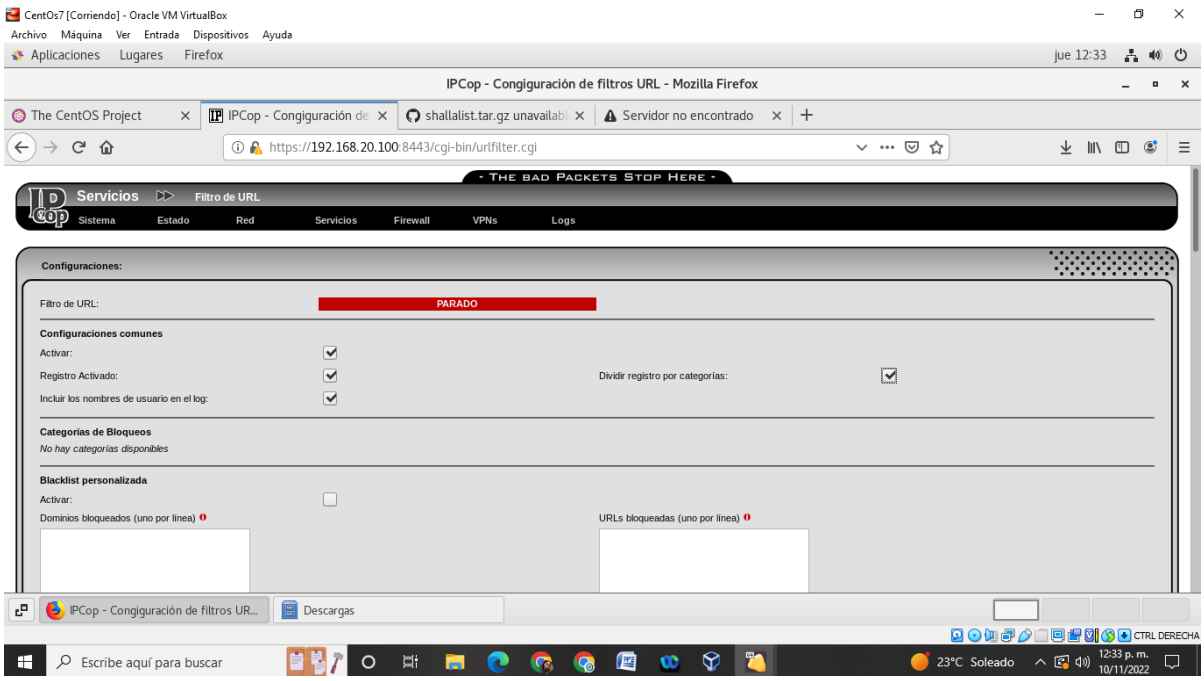


Ilustración 75

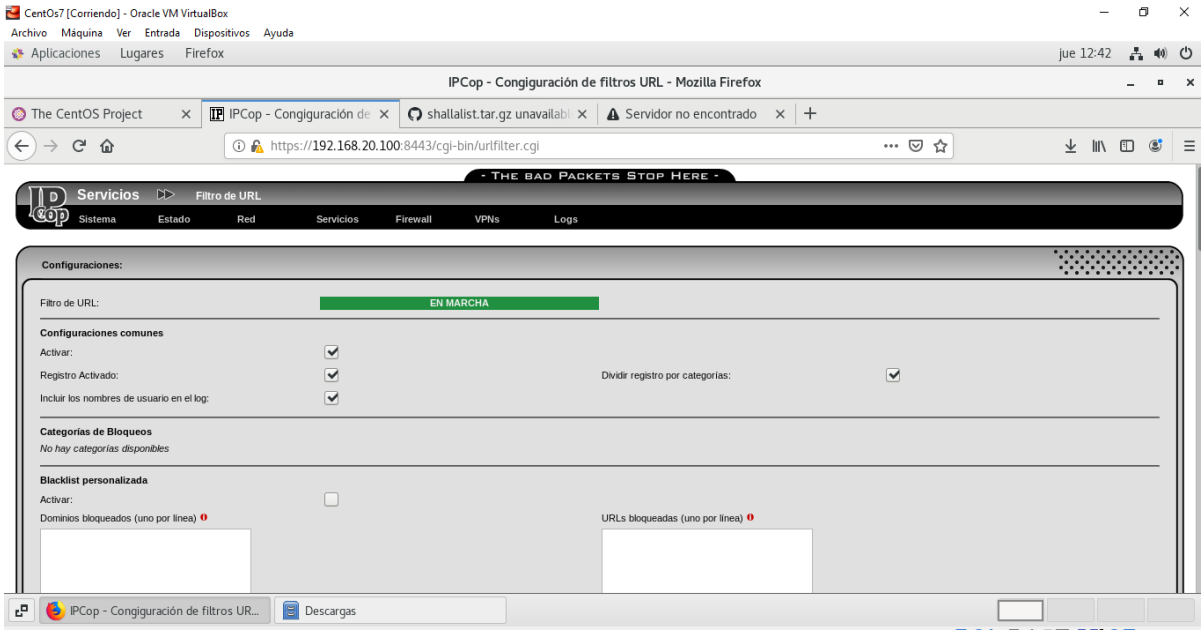


Ilustración 76

Ilustración 777

SEGURIDAD CON FIREWALLS EN SERVIDORES: UN ANÁLISIS COMPARATIVO CON HERRAMIENTAS OPEN SOURCE