

UNIVERSIDAD AUTONOMA TOMAS FRIAS
CARRERA DE INGENIERIA DE SISTEMAS



SEGURIDAD DE SISTEMAS

SEGUNDO PARCIAL

INSTALACION Y CONFIGURACION DE PFSENSE
(PRIMERA PARTE)

ESTUDIANTES: Univ. Casandra Angelica Calderón Davalos

Univ. Erick Sergio Ferreira Camacho

DOCENTE: Ing. J. Alexander Duran

AUXILIAR: Univ. Rory Adriel Sanchez Flores

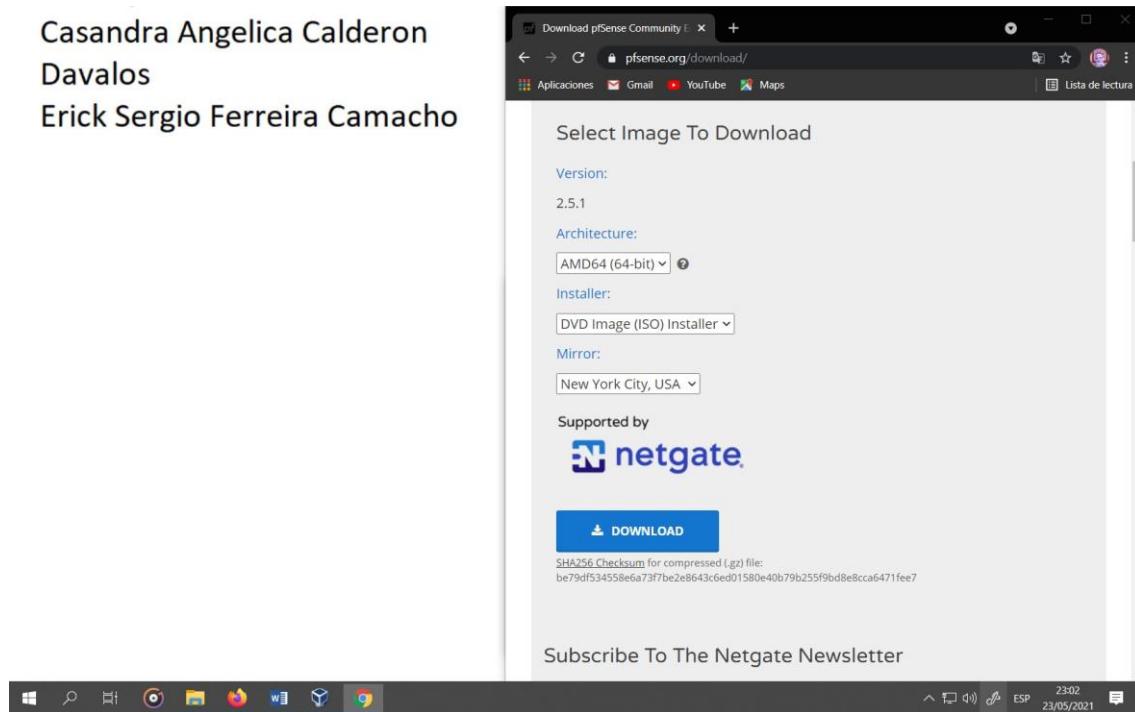
POTOSI - BOLIVIA

31 de Mayo del 2021

1. Realice la instalación y configuración de algunas de las versiones siguientes del firewall.

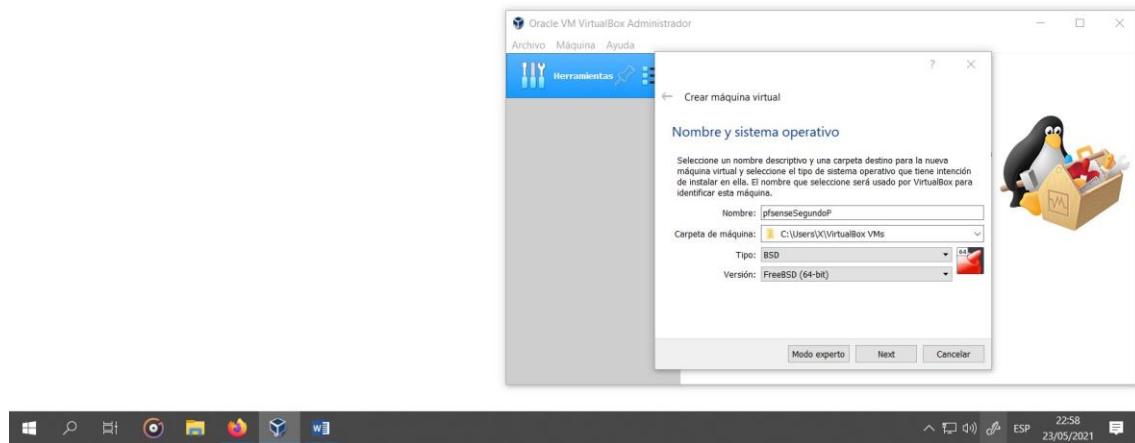
Iniciamos con la descarga de Pfsense con arquitectura de AMD 64 (64 bit) como un instalador ISO y mirror de New York City

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



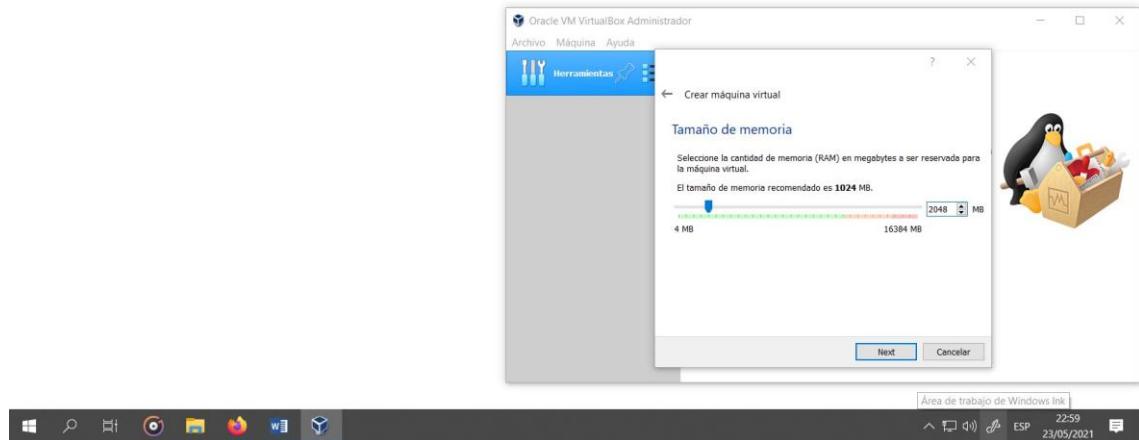
Seguimos con la instalación de pfsense de tipo BSD y versión FreeBSD (64-bit)

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



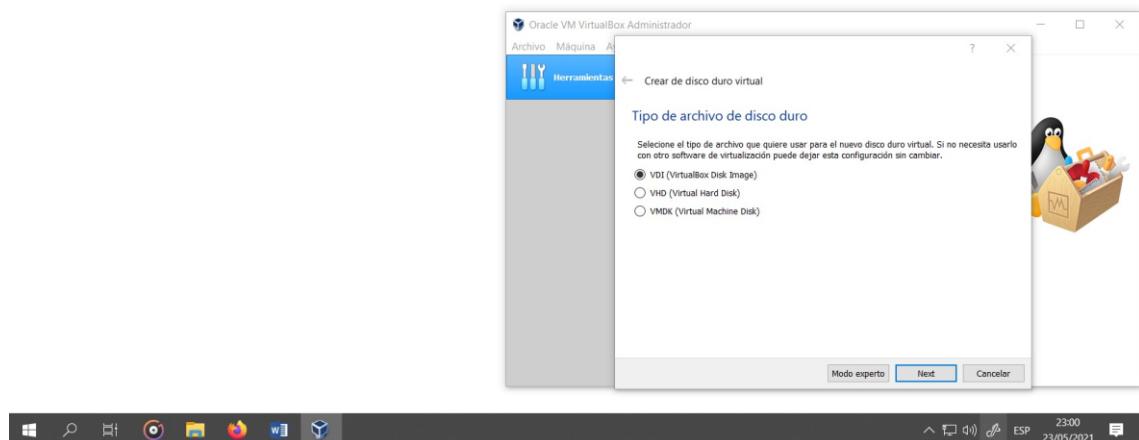
Le damos una ram de 2048 mb

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



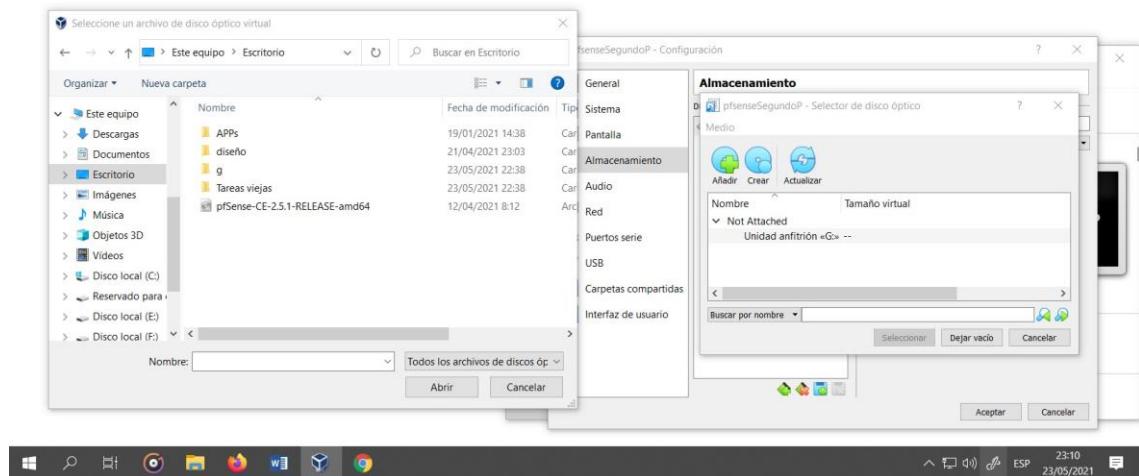
Creamos un disco virtual

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



Ingresamos a configuración > almacenamiento y seleccionamos un disco óptico elegimos la ISO descargada anteriormente.

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



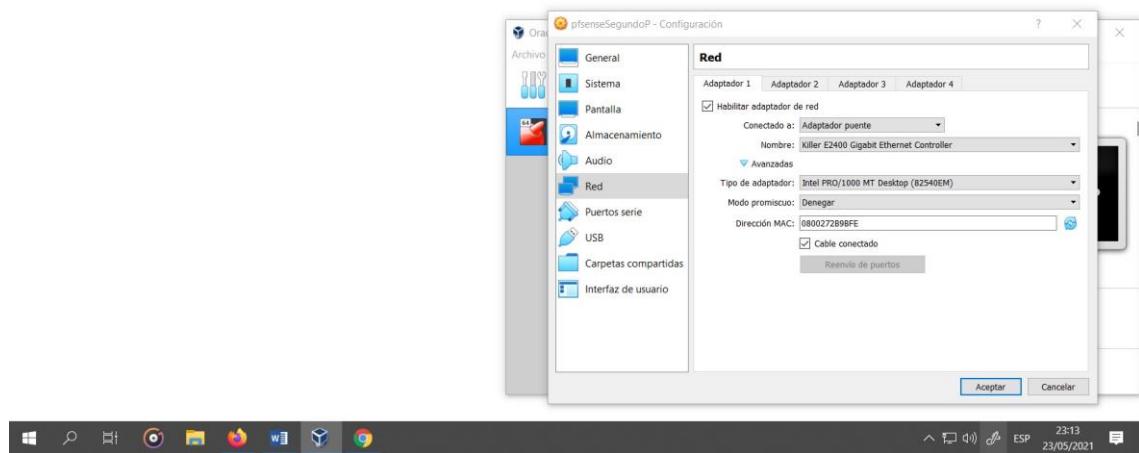
Realizar algunas restricciones a los usuarios:

Separar las Redes LAN, WAN además de una DMZ

Ahora nos dirigimos a Red ya habilitaremos 3 interfaces de red

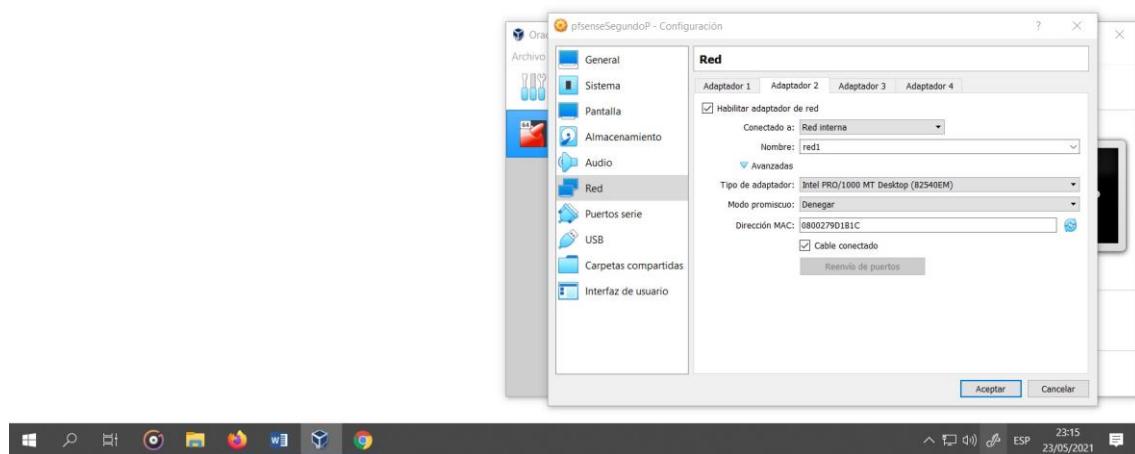
El adaptador 1 como adaptador puente ya que esa será como la WAN

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



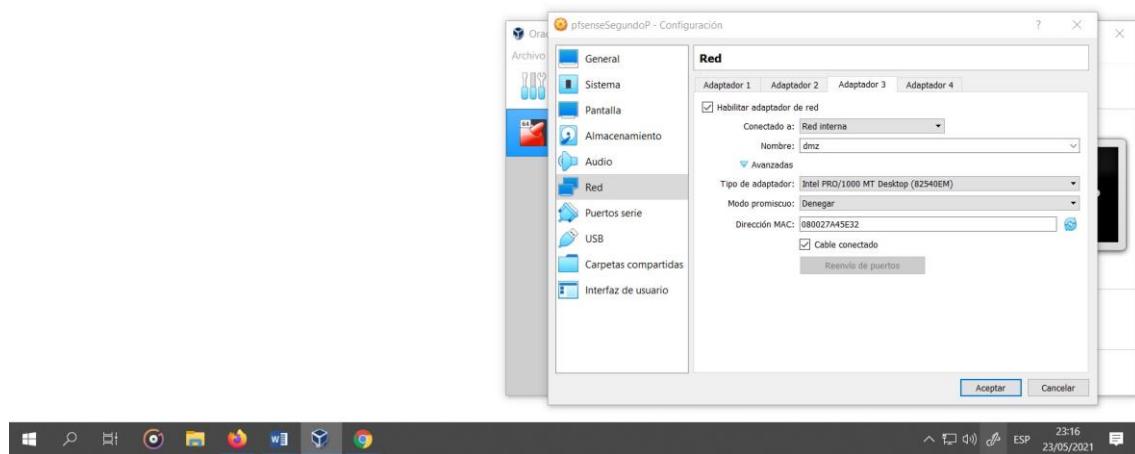
El adaptador 2 lo ponemos como una Red interna que actuara como nuestra LAN

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



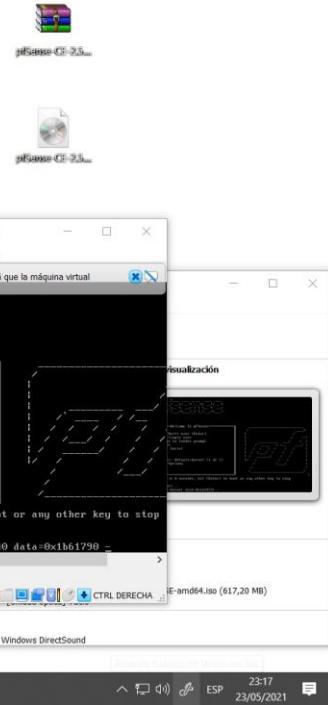
El adaptador 3 como Red interna con nombre “dmz”

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



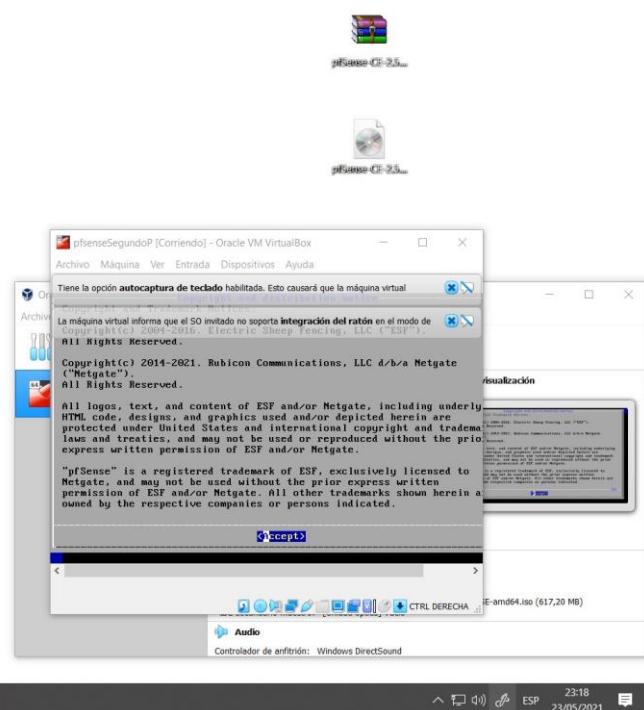
Pulsamos en aceptar para que se guarden todos los cambios y procedemos a iniciar

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



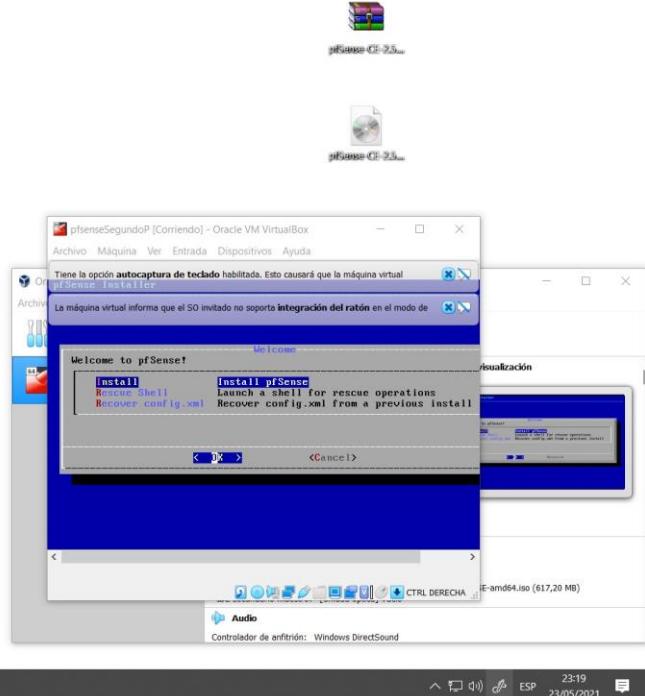
Automáticamente se iniciará, para su instalación pulsamos en “accept”

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



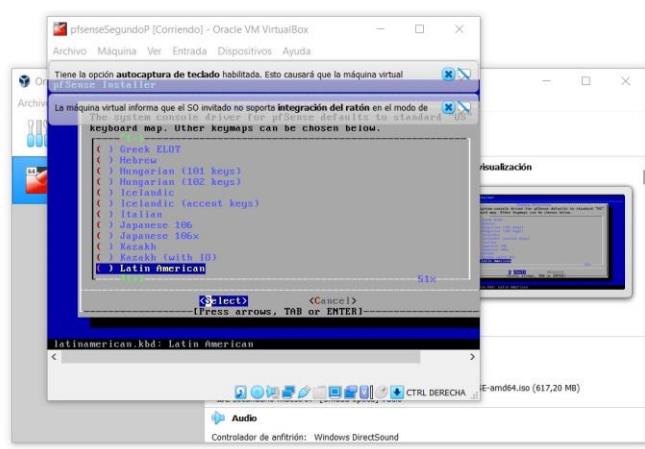
Elegimos la opción install pfSense

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



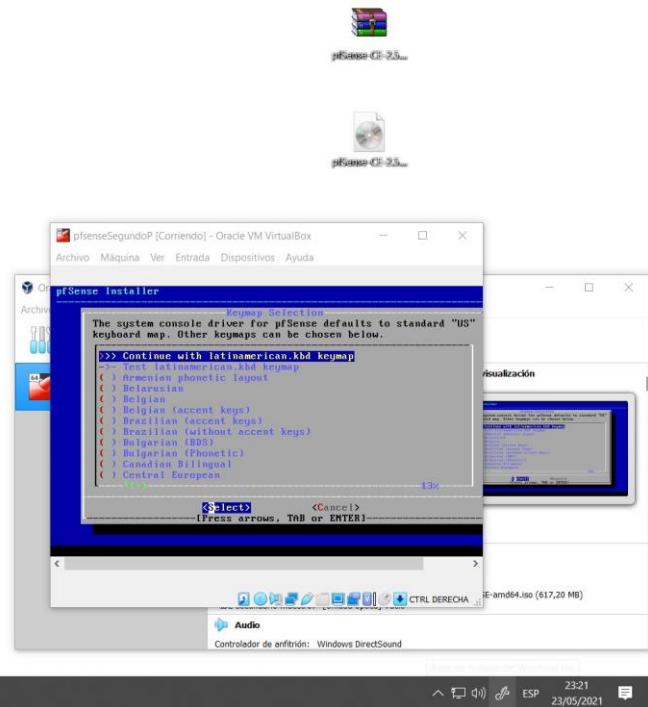
Seleccionamos idioma Latino Americano

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



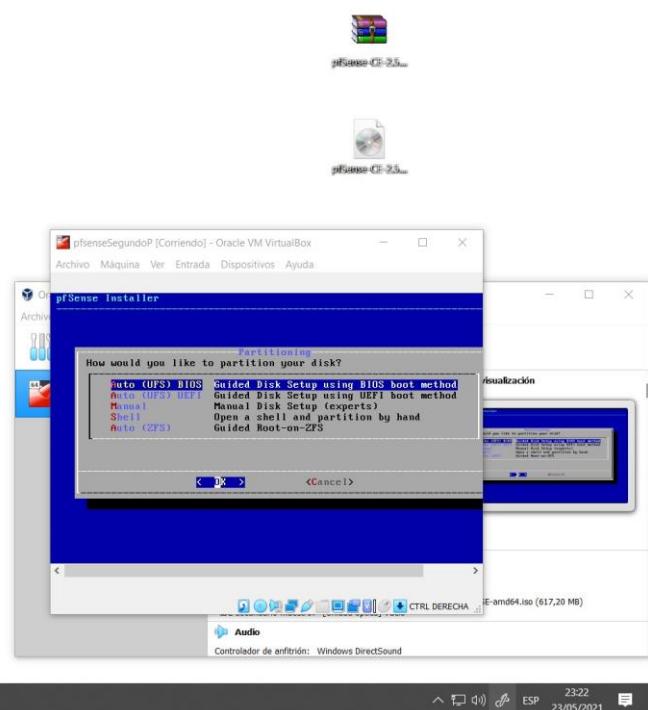
Y continuamos con la instalación.

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



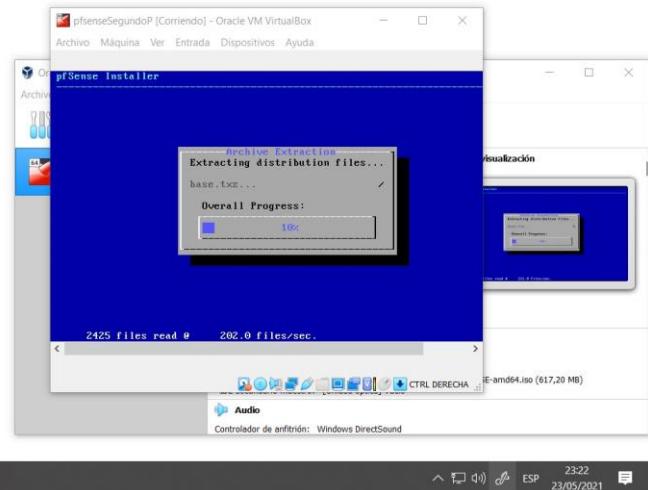
Seguimos como Auto (UFS) BIOS

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



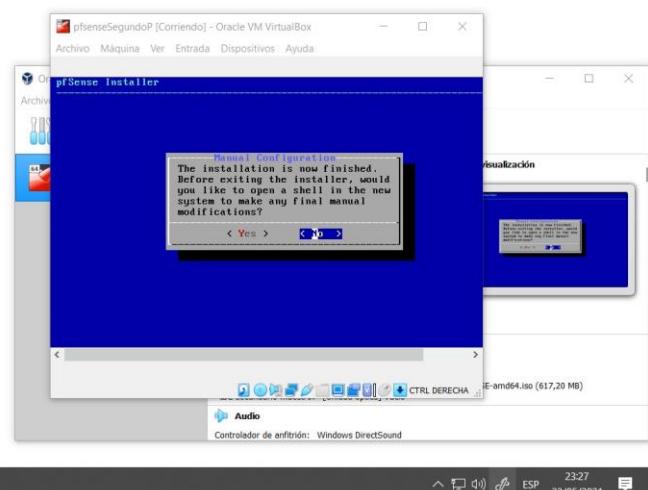
Esperamos a que se complete la instalación

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



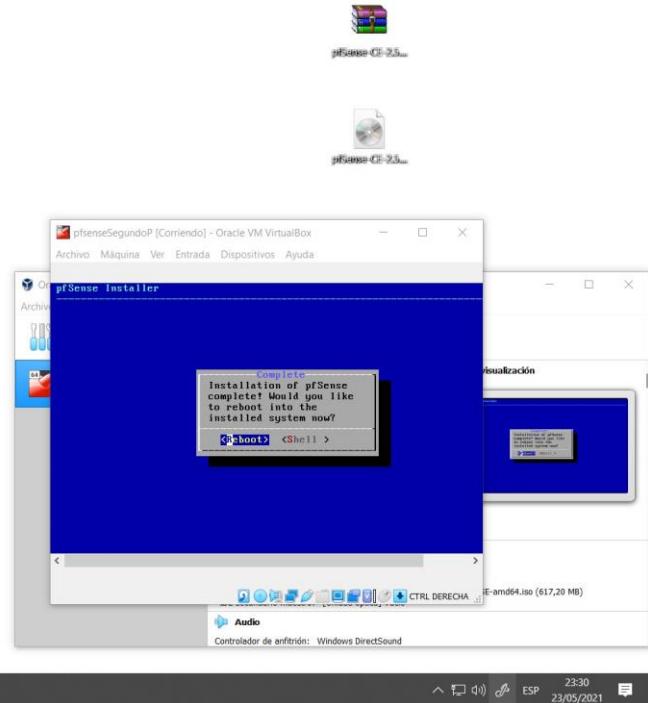
Nos saldrá una pantalla por si queremos modificar algo más le damos a No

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho

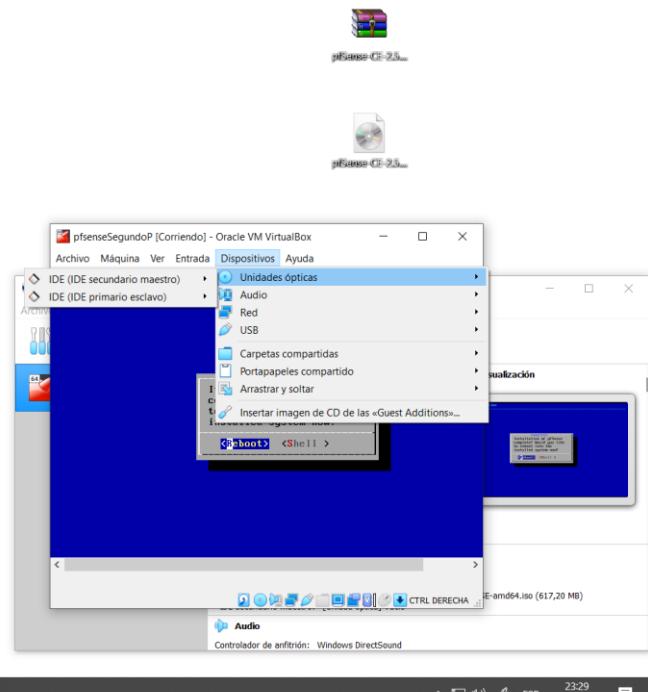


En la siguiente pantalla le daremos a la opción “Reboot” y seguidamente sacamos nuestra unidad óptica

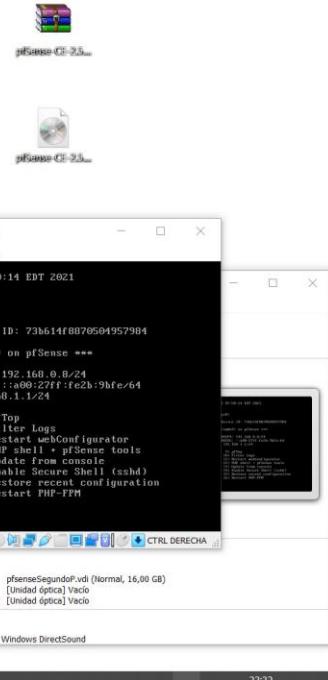
Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho

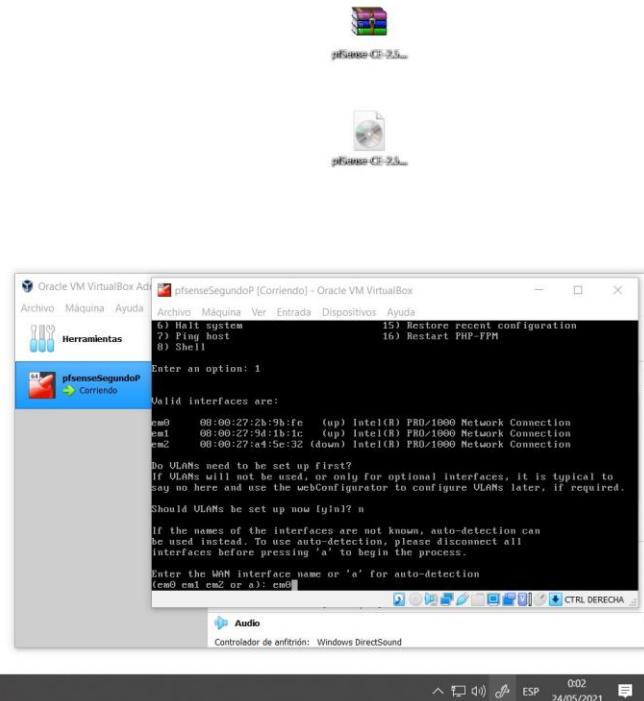


Cassandra Angelica Calderon
 Davalos
 Erick Sergio Ferreira Camacho



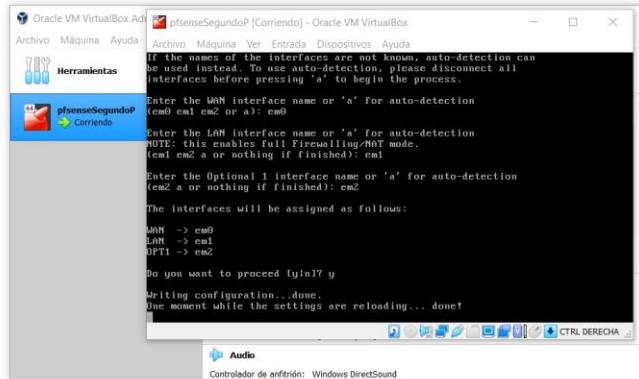
Elegimos la opción 1 nos saldrá una opción de VLANs a la cual pondremos una n de No introduciremos un nombre de la WAN como em0

Cassandra Angelica Calderon
 Davalos
 Erick Sergio Ferreira Camacho



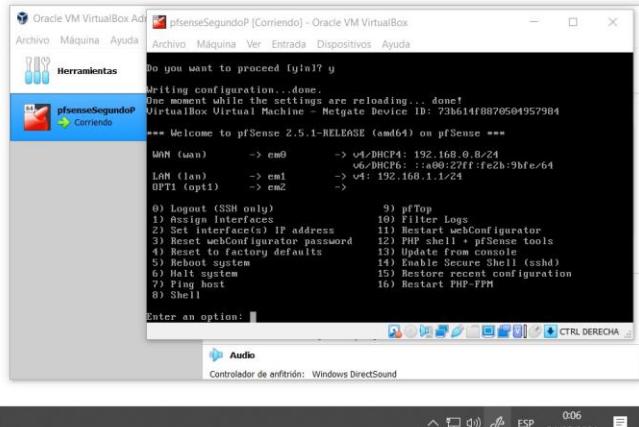
Seguidamente del nombre de la interfaz LAN em1 y la red opcional como em2 nos saldrá una pregunta de proceder a la cual damos y de Si y esperamos a que se apliquen los cambios

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



Una vez completado los cambios ya nos saldrán las 3 interfaces

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho

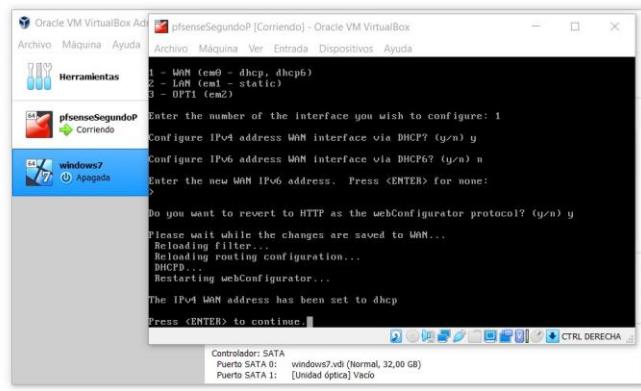


Servidor DHCP para asignar IPs dinámicas a los clientes de la LAN

Utilizara las siguientes direcciones LAN IP.172.16.X.Y/24. Donde X es el NUMERO DE SU GRUPO. Para la DMZ 10.20.X.Y/24. Donde X es el número de su grupo.

Para configurar las IP da las interfaces elegimos la opción 2 y elegiremos primero a la WAN que es la opción 1 y nos preguntara si queremos configurarlo vía DHCP de nuestro router a la cual responderemos y

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho

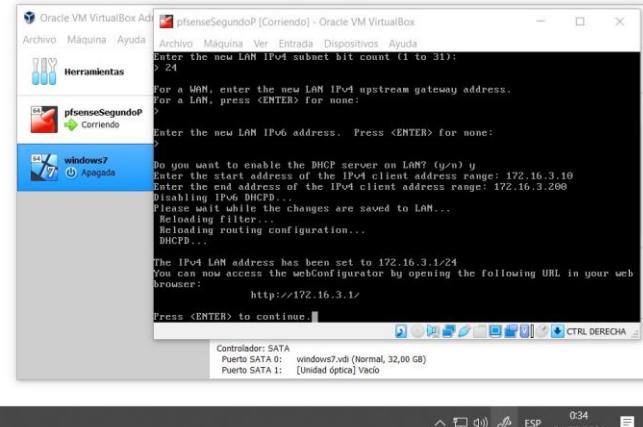


Volvemos a elegir la opción 2 para configurar la IP de LAN esta será la opción 2 acá nos pedirá ingresar la IP que en nuestro caso será la 172.16.3.1 seguidamente escogemos la máscara que queremos usar en nuestro caso la 24 presionaremos ENTER hasta que nos salga la pregunta de si queremos que habilitar el servidor DHCP para esta LAN a la cual responderemos "y" y seguidamente daremos los rangos con los que vamos a empezar el servidor seguidamente nos pedirá que demos el rango final y esperamos a que se nos configure

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho

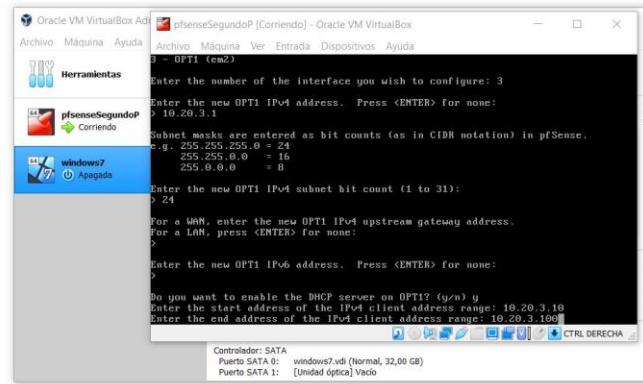


Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho

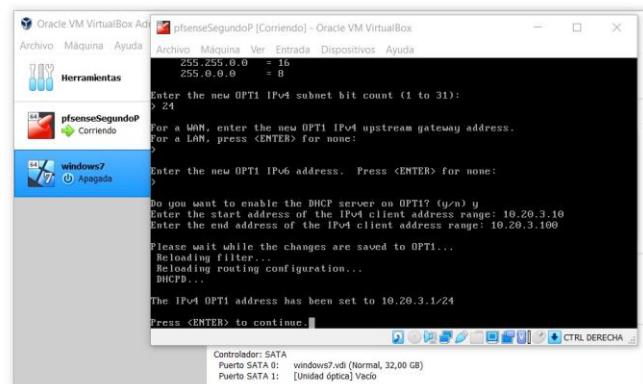


Ahora configuraremos la interfaz número 3 que llegaría a ser el dmz a la cual le daremos una IP de 10.20.3.1 con una máscara de 24 donde aceptaremos activar el servidor DHCP en dmz y le daremos un rango inicial de 10.20.3.10 y un rango final de 10.20.3.100 y esperamos a que termine de configurarse.

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



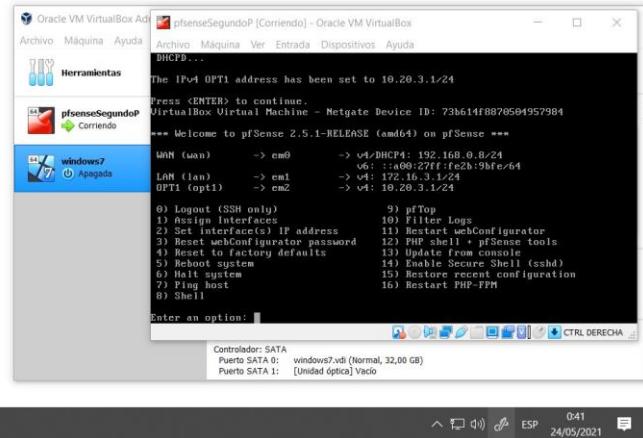
Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



040 ESP 24/05/2021

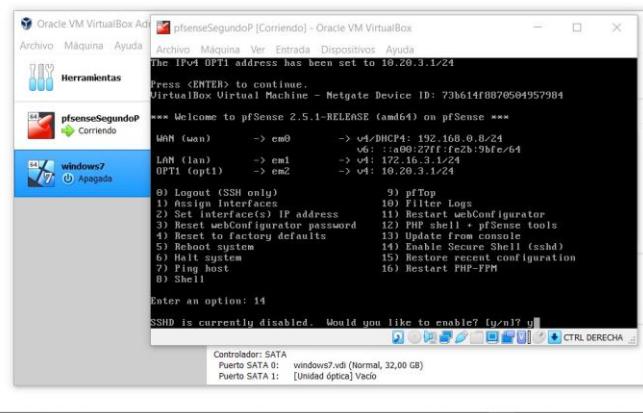
Se puede ver que nuestras 3 interfaces están configuradas tienen una IP y su mascara

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



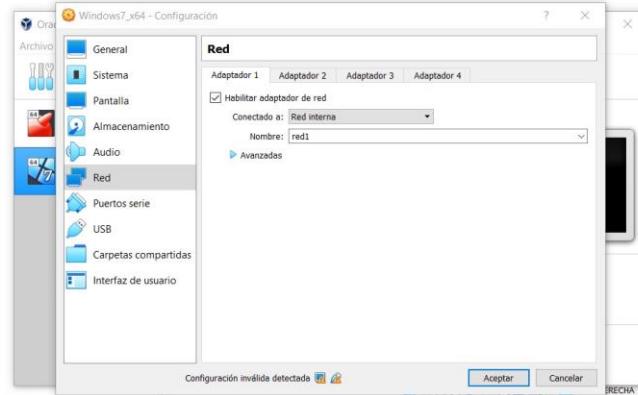
Seguidamente podemos habilitar el servicio SSH con la opción 14 donde nos pedirá una confirmación a la cual daremos y

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



Ahora podremos importar nuestra maquina Windows7 para poder acceder a nuestro servidor una vez configuremos en red que esté conectado a Red interna con nombre red1

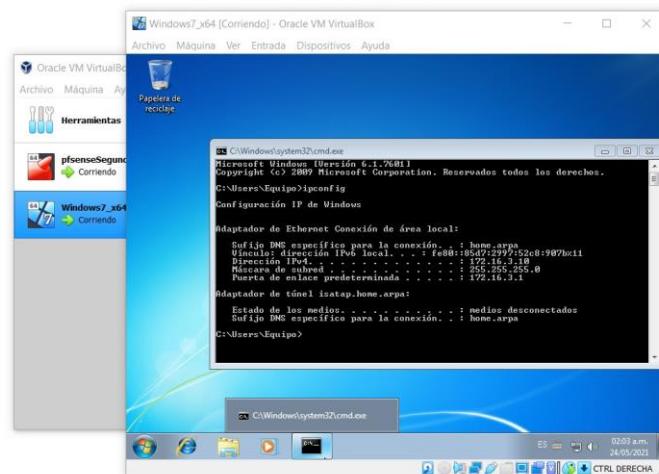
Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



Red LAN debe tener al menos 1 PC

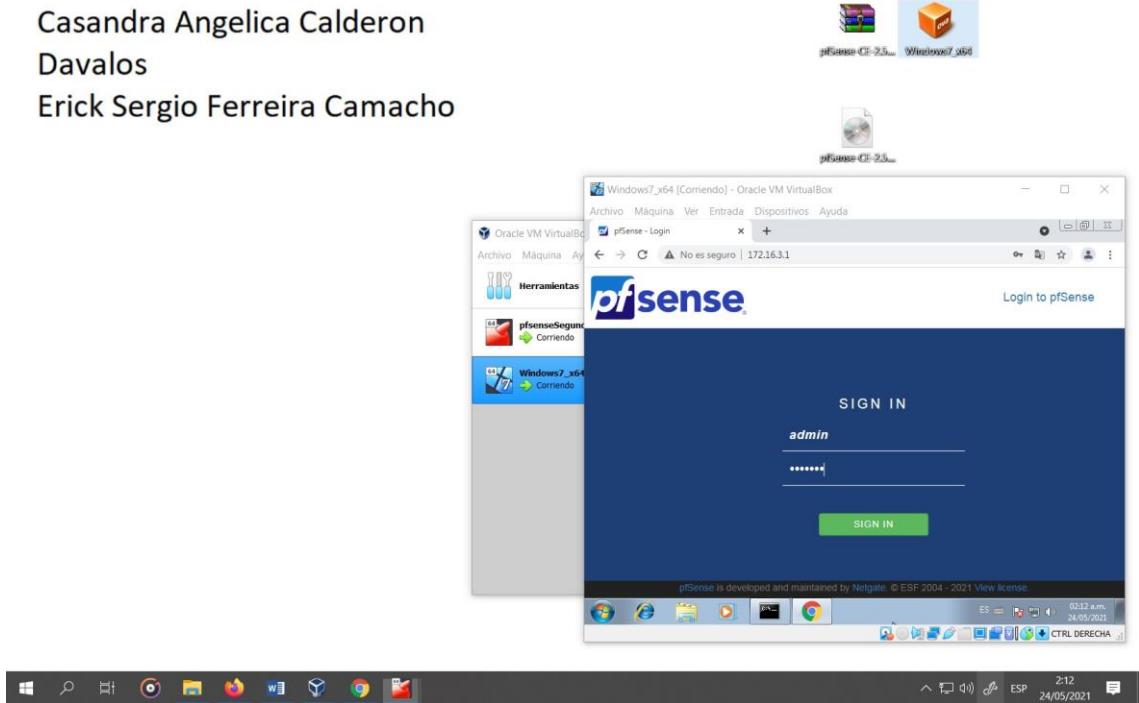
En la máquina virtual de Windows 7 podemos ver la IP que nos dio mediante cmd para observar que si está en el rango que habíamos dado

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho

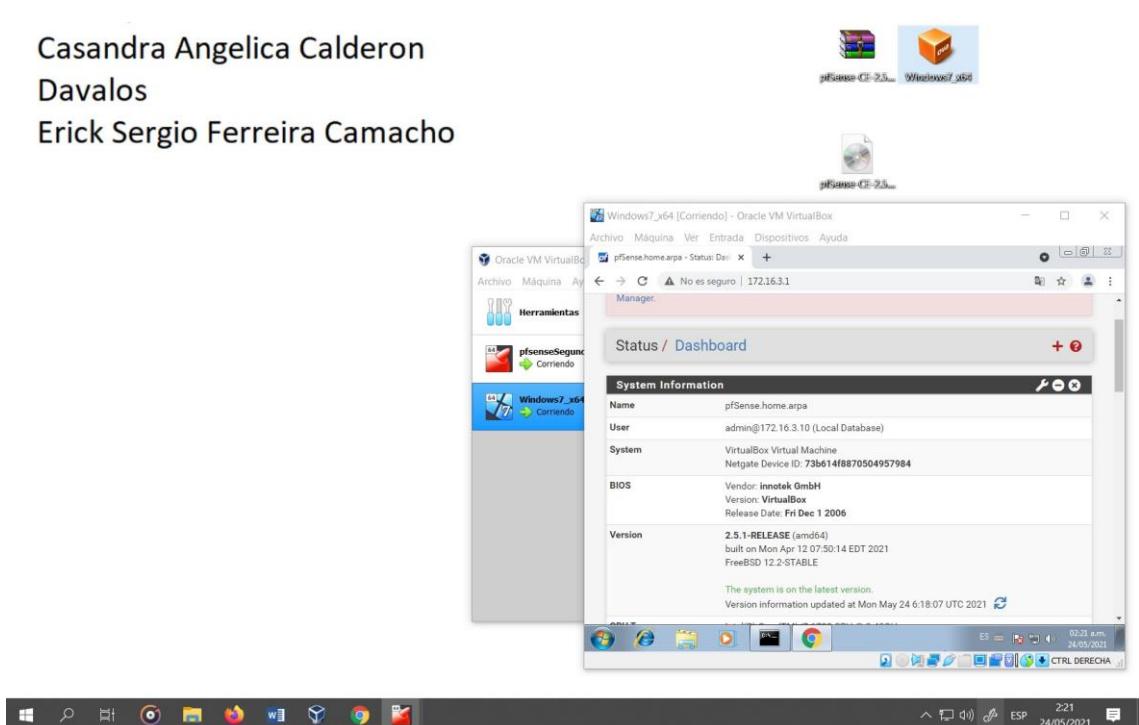


Abrimos un navegador y pones nuestra IP de la interface que llega a ser 172.16.3.1 y acá nos pedirá un usuario y una contraseña que por defecto llega a ser usuario admin contraseña pfSense

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



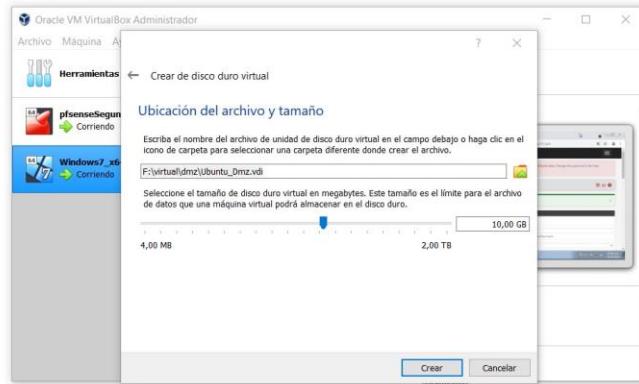
Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



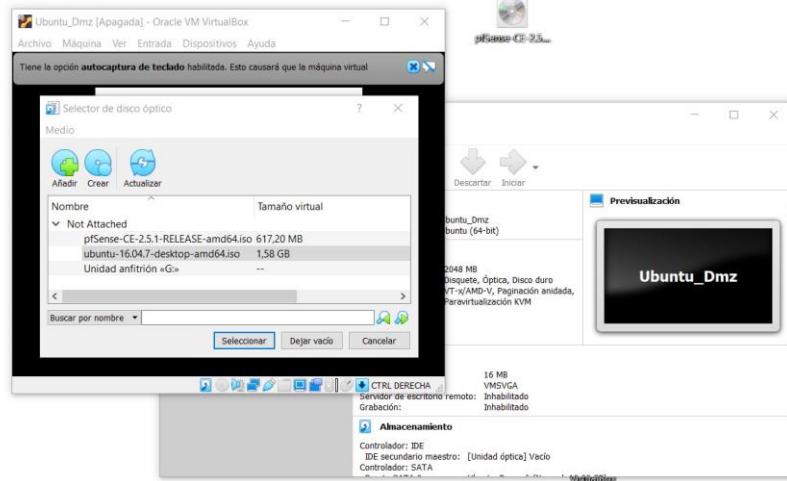
DMZ un servidor web (puede usar cualquiera)

Realizaremos la configuración del dmz se instalará un nuevo sistema operativo Ubuntu 16.04

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho

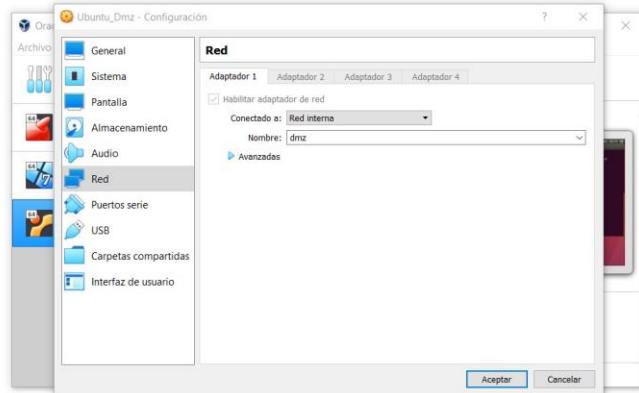


Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



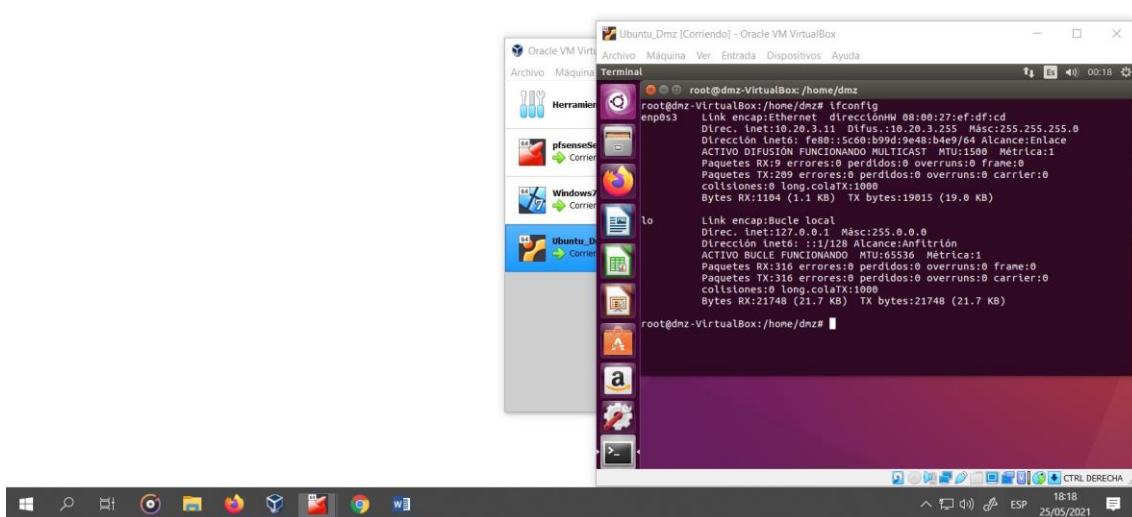
Para que el sistema operativo se conecte a la red DMZ ingresamos a la configuración en red, elegimos la opción de red interna, y de nombre le ponemos DMZ

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



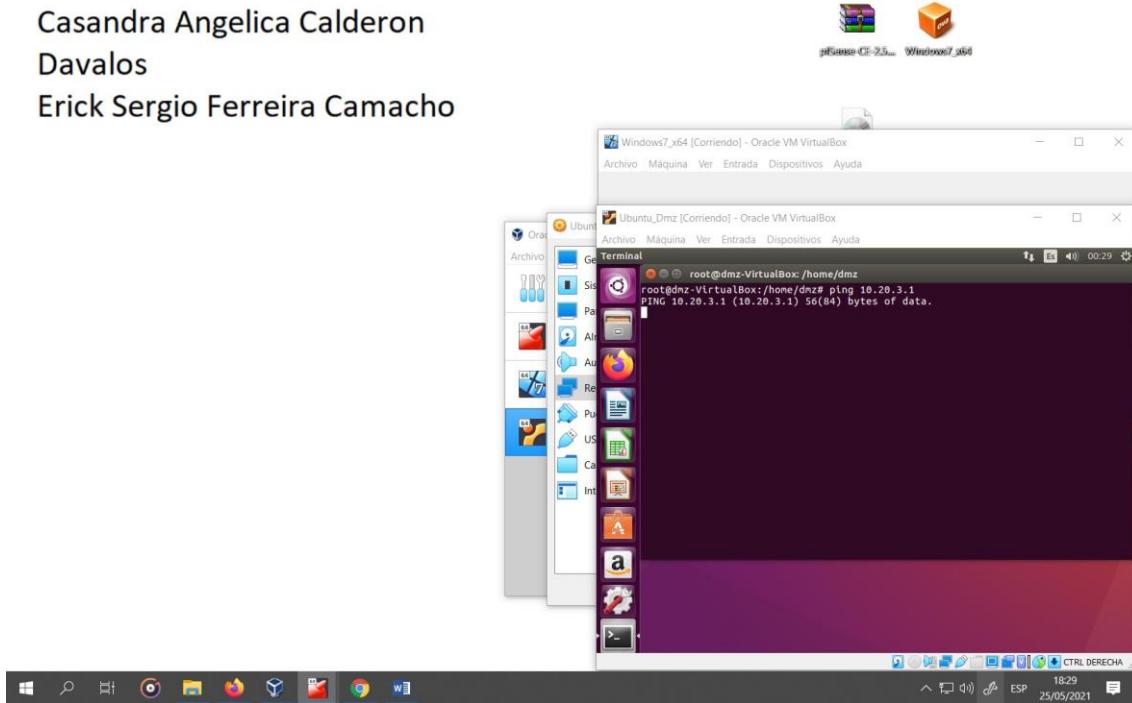
Para poder verificar ingresar al cmd y ponemos el comando ifconfig

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



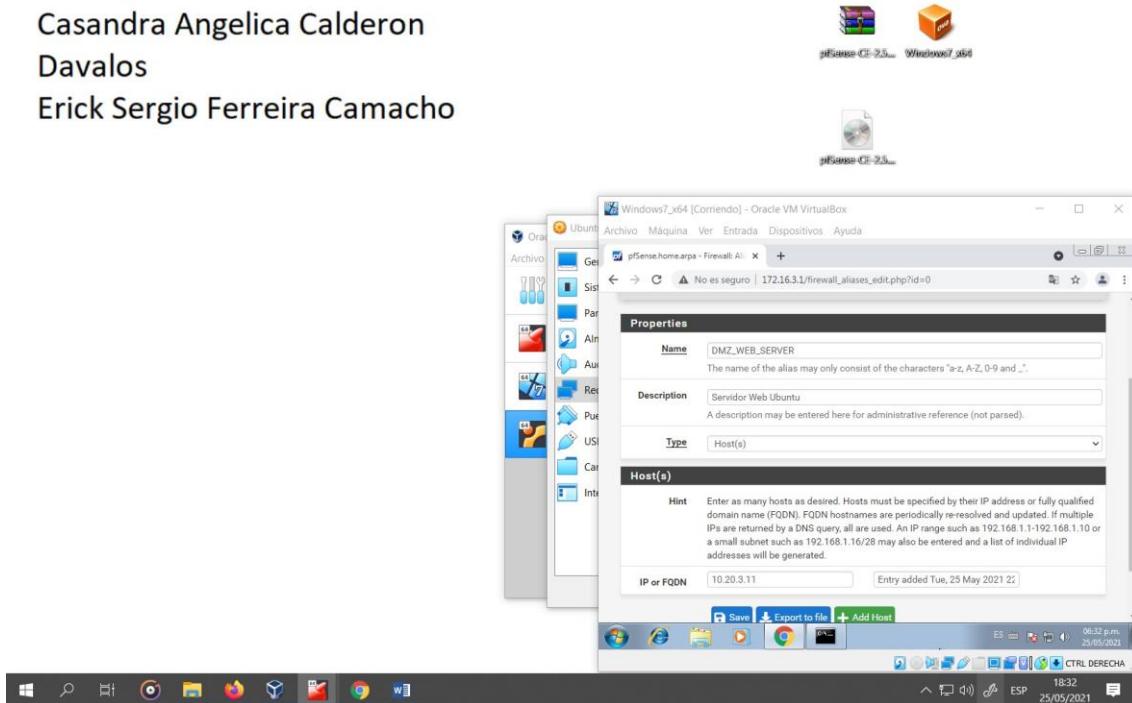
Configurando servicio dmz

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



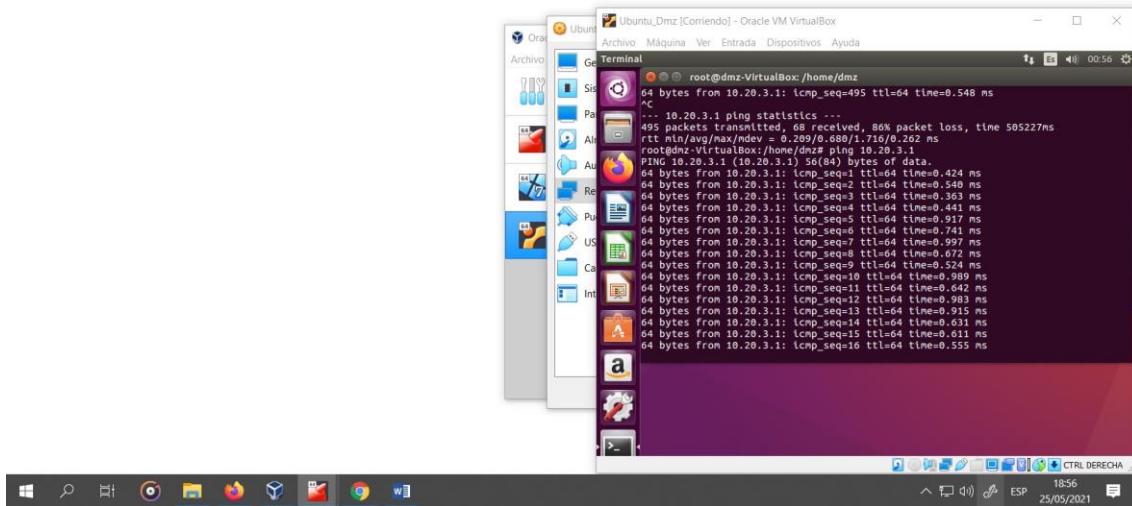
Ingresamos a la opción aliases para la creación del servidor dmz

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



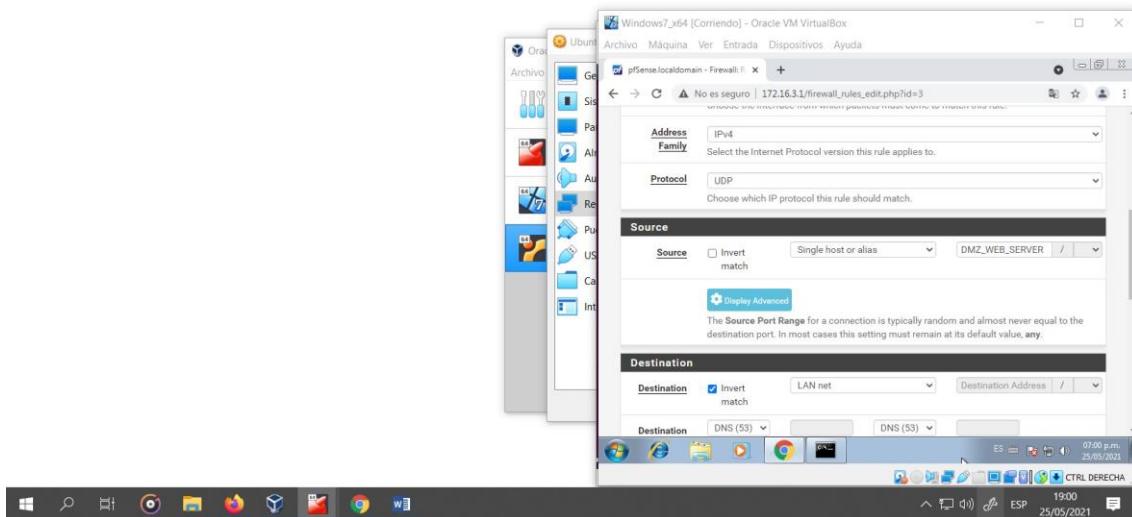
Agregamos una regla desde pfsense en rules con un protocolo ICMP que permitirá el ping

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



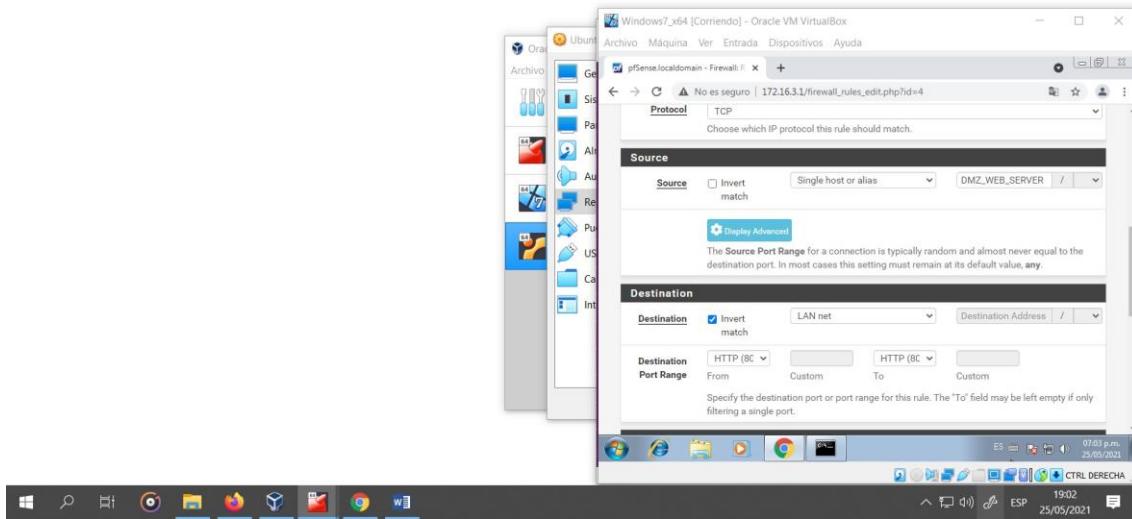
Agregamos una regla rule desde pfSense para permitir el DNS mediante protocolo UDP

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



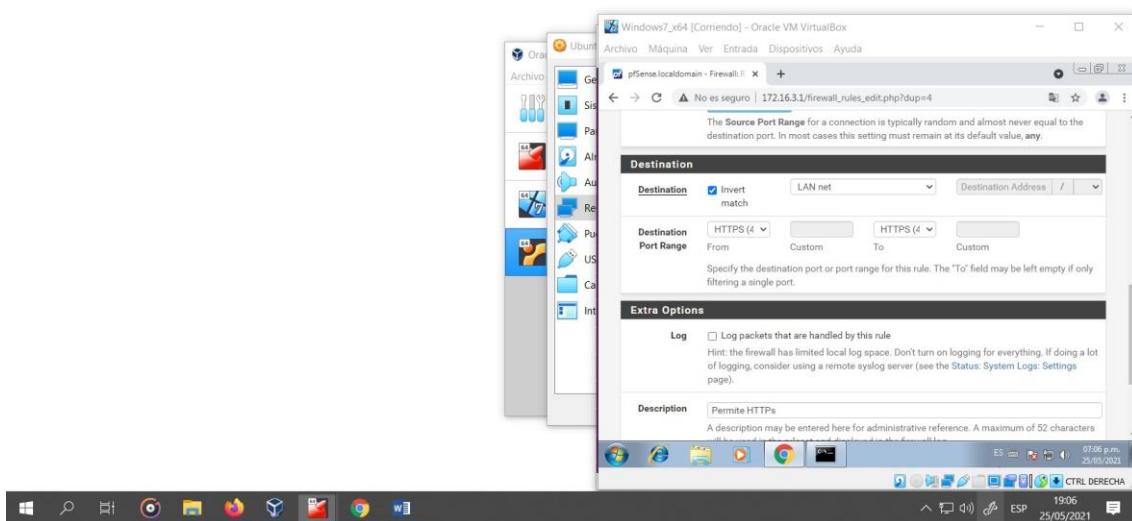
Agregamos una regla desde rule en pfSense para permitir el HTTP mediante el protocolo TCP

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



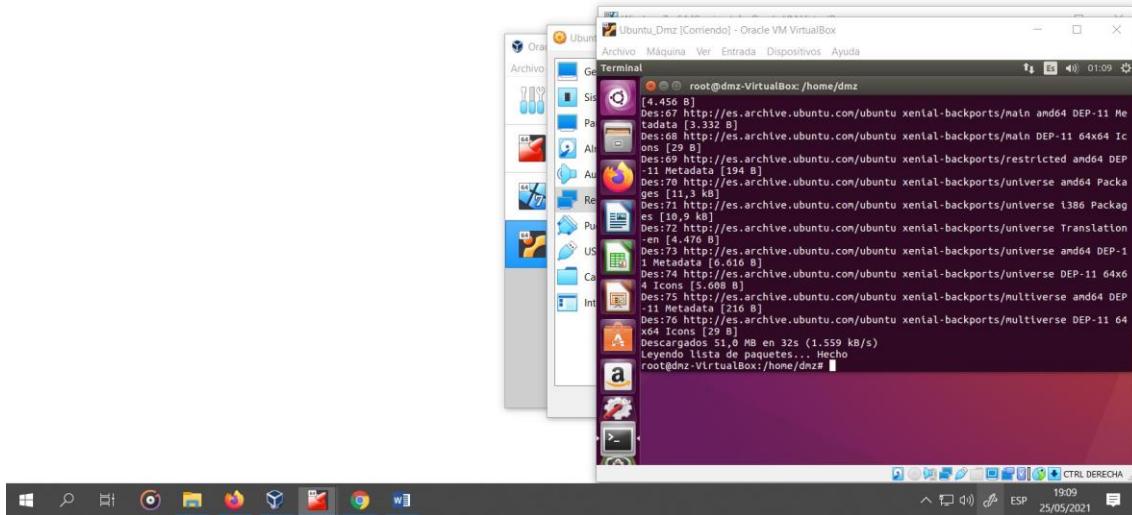
Agregamos una regla desde rule para permitir el HTTPS

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



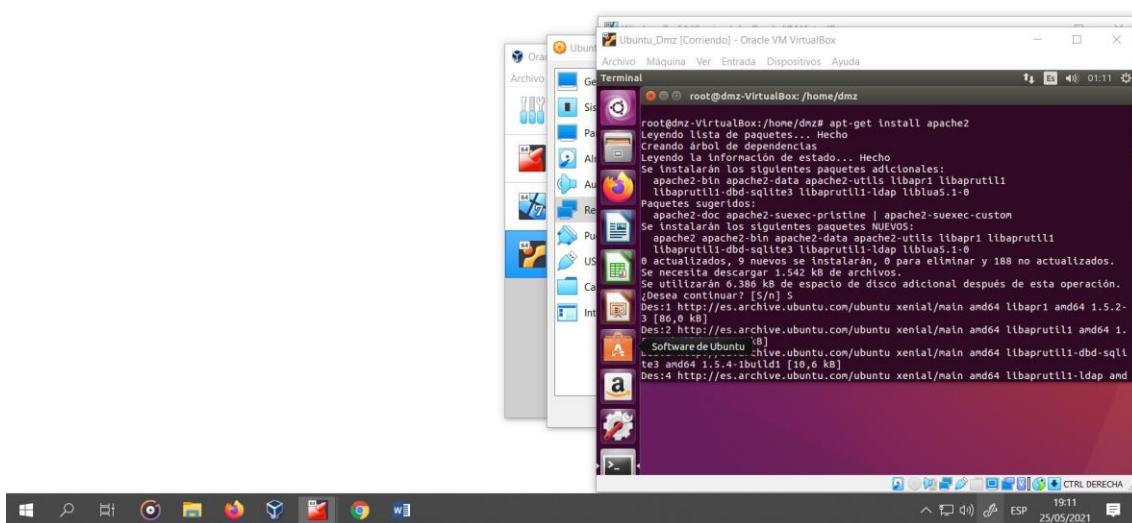
Con los protocolos agregados hacemos un apt-get update

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



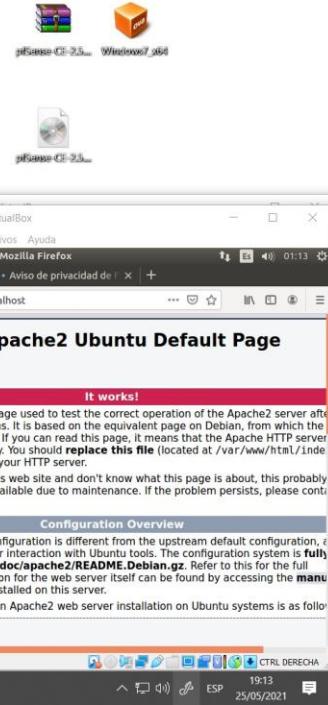
Procedemos a la instalación de apache mediante el comando apt-get install apache2

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



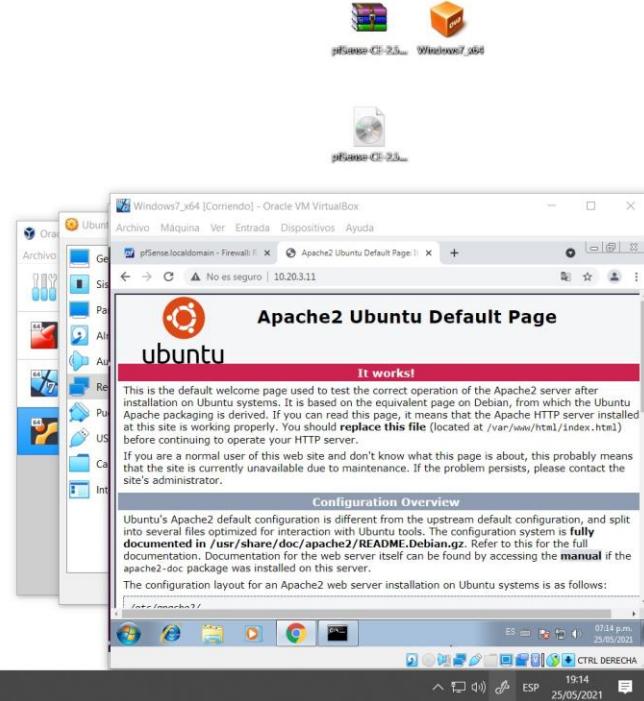
Entramos a apache2 desde Ubuntu mediante localhost/

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



Se puede ingresar al servidor web Ubuntu desde nuestro sistema Windows mediante la IP de la máquina de Ubuntu 10.20.3.11

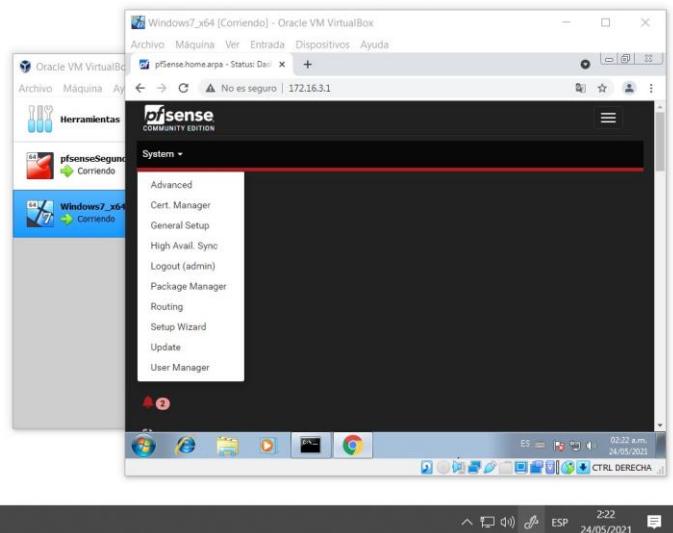
Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



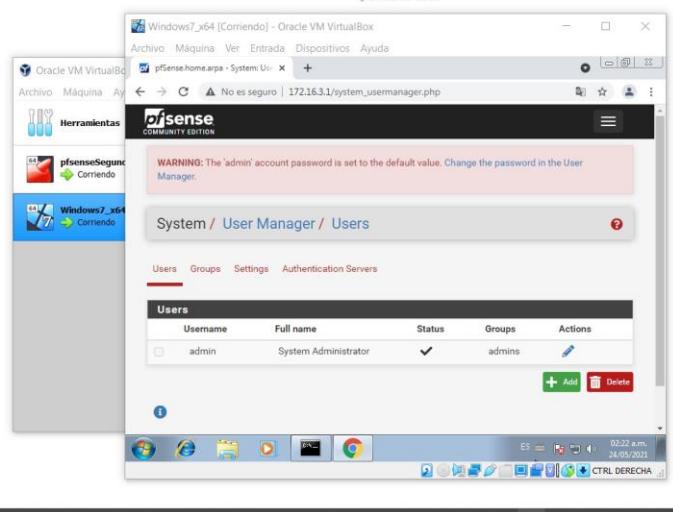
Crear usuarios (Use los nombres de integrantes de su grupo) para que el firewall les solicite autentificarse antes de acceder al Internet (Portal cautivo).

Para la creación de usuarios nos dirigimos a la parte superior izquierda elegimos el submenú System y en ella la opción User Manager

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho

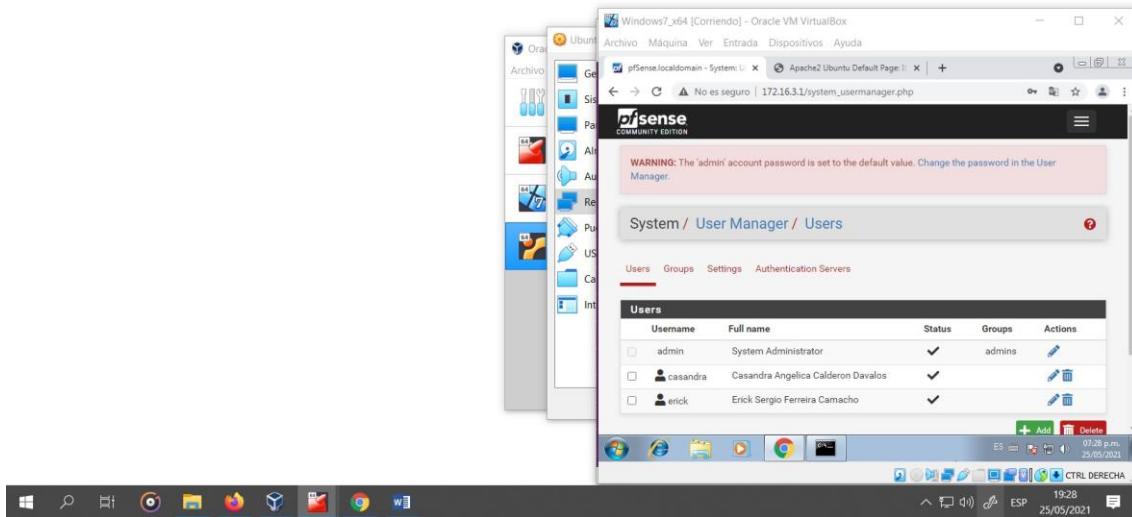


Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



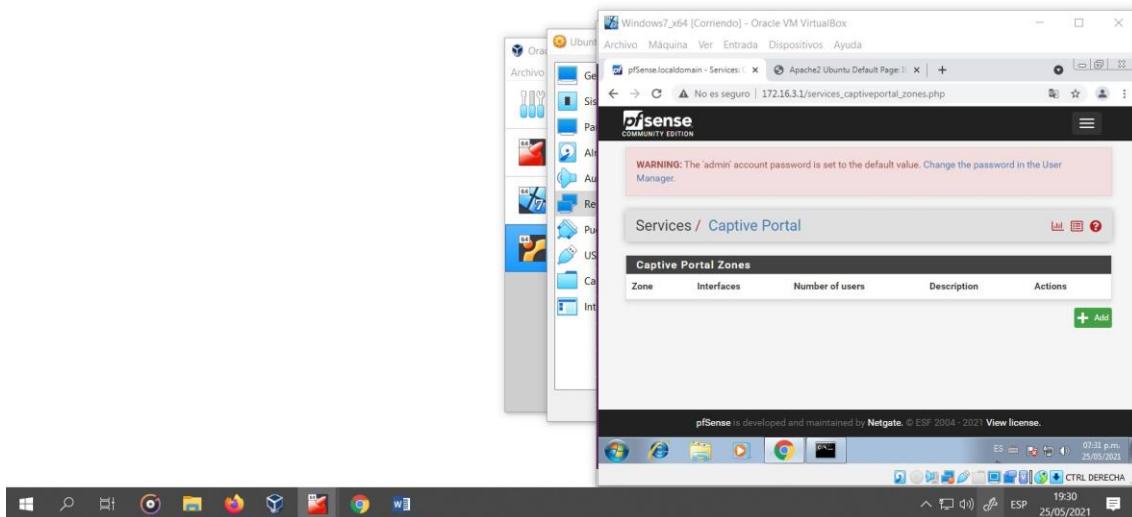
Presionamos en +Add donde le daremos un Username contraseña e ingresamos nuestros nombres completos

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



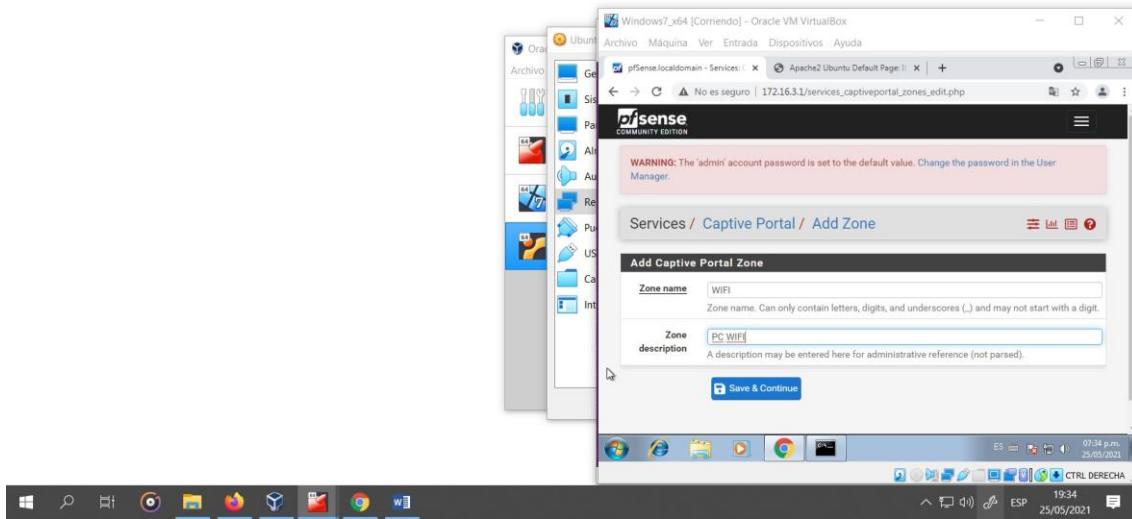
Para crear el portal cautivo ingresamos al menú Services y elegimos la opción Captive Portal

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho

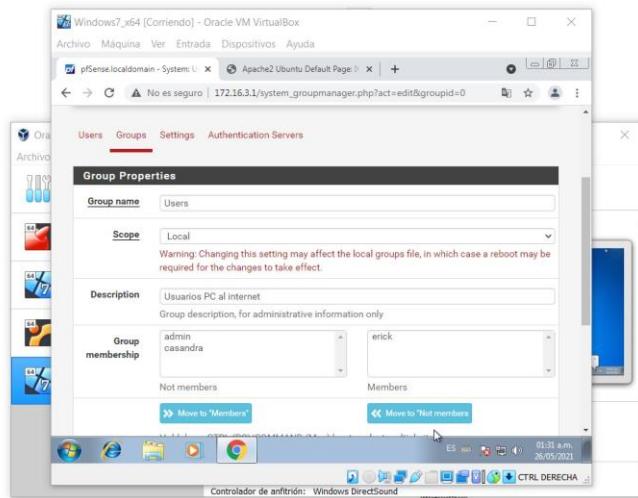


Donde nos pedirá el nombre de una zona y la descripción

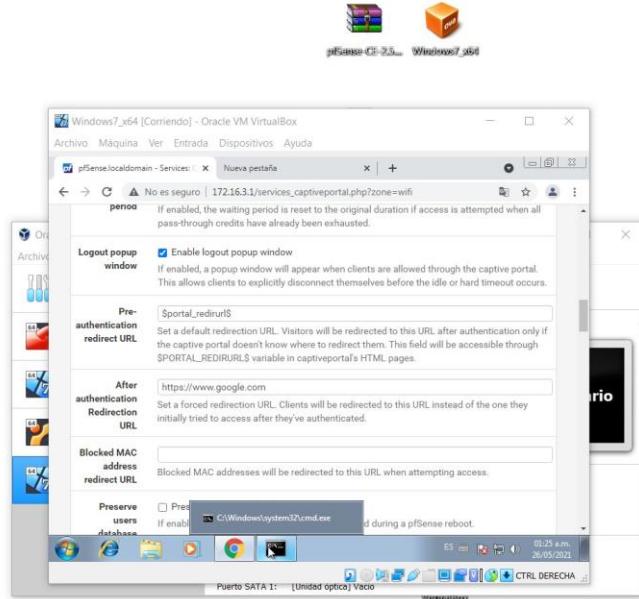
Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



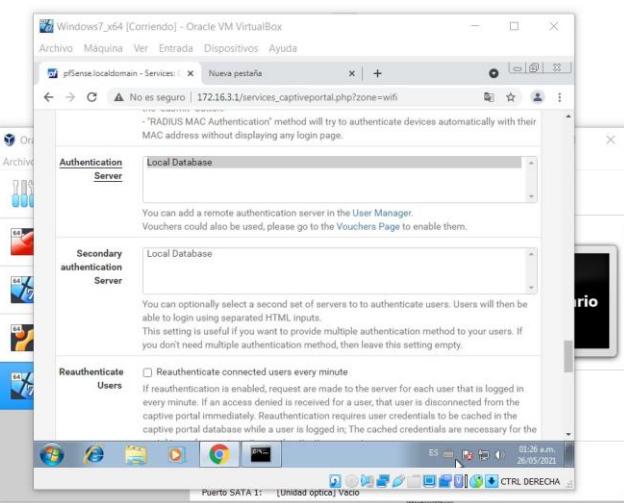
Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



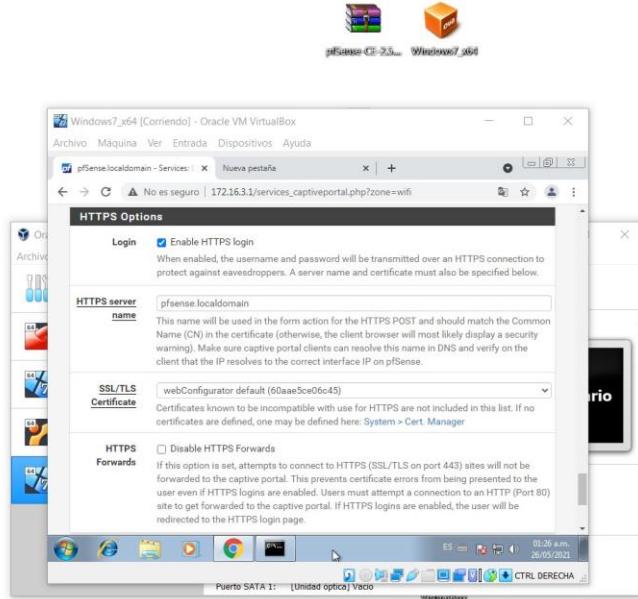
Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho

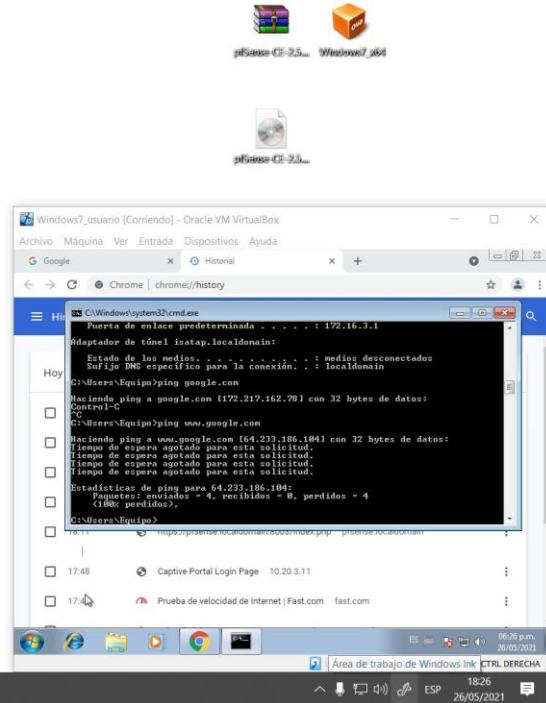


Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



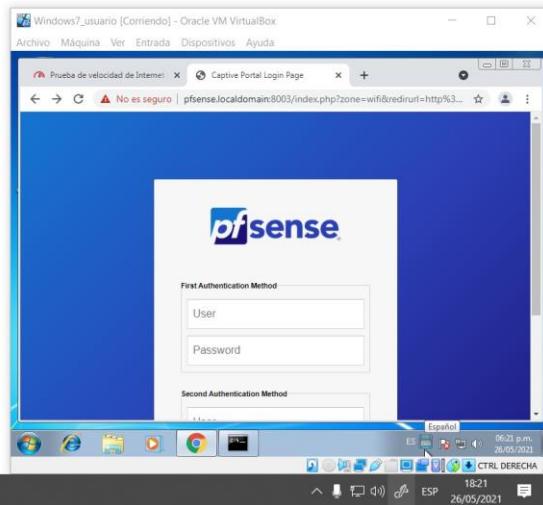
Una vez terminada todas las configuraciones podemos observar que al ingresar a la dirección apache no tendrá acceso a red

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



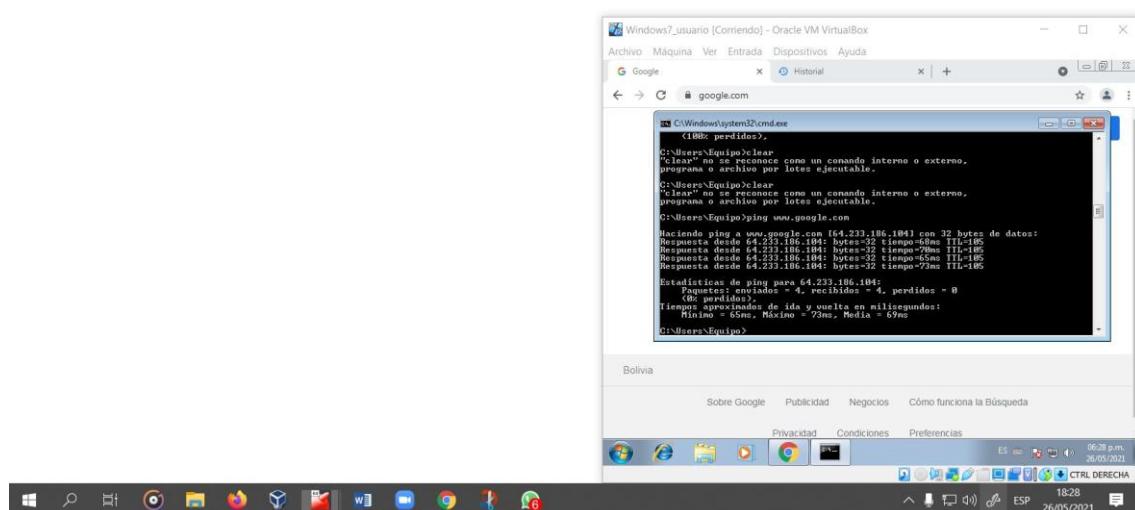
Y nos pedirá logear la cuenta user para poder tener internet

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



Una vez ingresada la cuenta aceptada por el usuario tendremos acceso a internet

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



LIMITAR EL ANCHO DE BANDA, ASIGNANDO DISTINTAS VELOCIDADES POR USUARIO PARA TENER NIVELES DE USUARIO CON RELACIÓN AL USO DEL INTERNET. UTILICE ALGUNA PAGINA PARA MEDIR EL ANCHO DE BANDA Y VERIFICAR QUE SE ESTÉ LIMITANDO EL BW.

Para poder limitar el ancho de banda debemos entrar al menú de Services elegimos Captive Portal y editamos el portal cautivo que ya habíamos configurado elegimos la pestaña de Allowed IP Addresses y presionamos en +Add

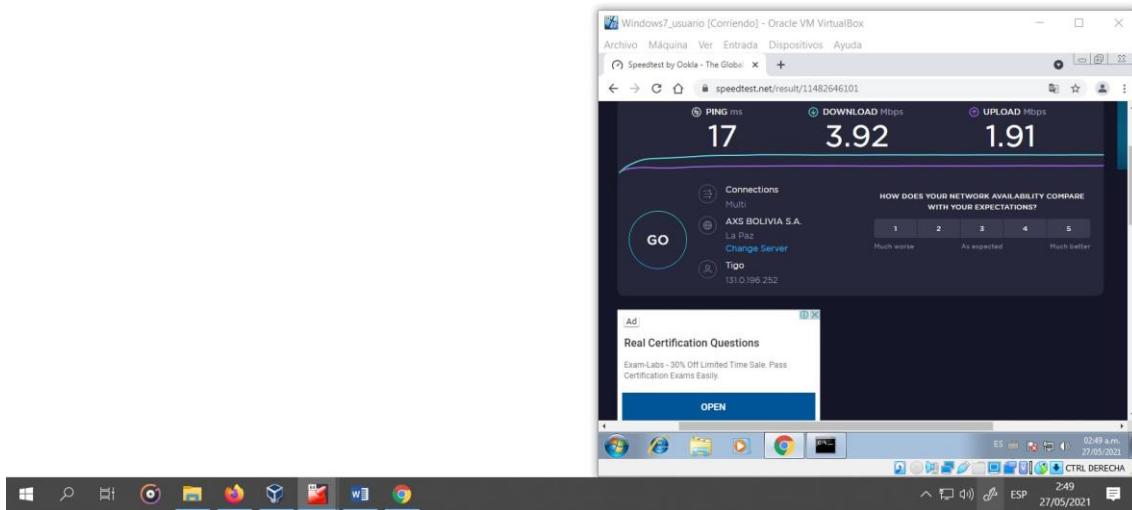
Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



A screenshot of a pfSense Community Edition interface running on a Windows 7 host. The window title is "Windows7_x64 [Corriendo] - Oracle VM VirtualBox". The URL in the address bar is "172.16.3.1/services_captiveportal_ip.php?zone=wifi". The pfSense logo is visible at the top. A warning message says: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, the navigation menu includes "Services / Captive Portal / WIFI / Allowed IP Addresses". The "Allowed IP Addresses" tab is selected. A table lists one IP address: "192.168.1.100" with a description "IP de la PC". A green "+ Add" button is visible. The pfSense logo is also present in the bottom right corner of the interface window.

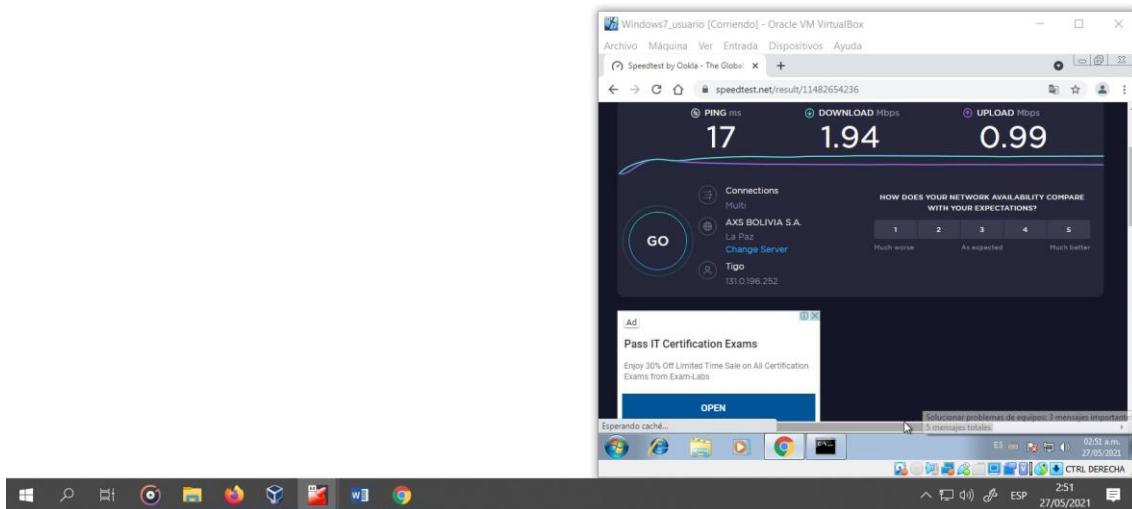
Antes de limitar el ancho de banda podemos hacer una verificación de velocidad de la máquina del usuario

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



Ingresamos la IP de la máquina del usuario la cual queremos limitar el ancho de banda en nuestro caso será la 172.16.3.13 limitaremos la subida en 1024kbps y la bajada en 2048kbps guardamos la configuración y verificamos la limitación de ancho de banda

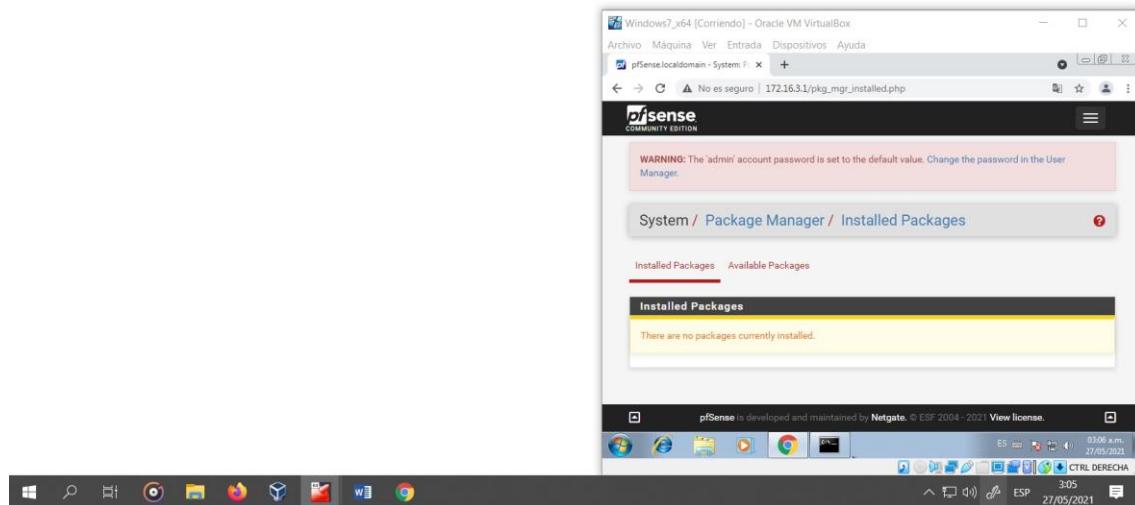
Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



Permisos en el firewall

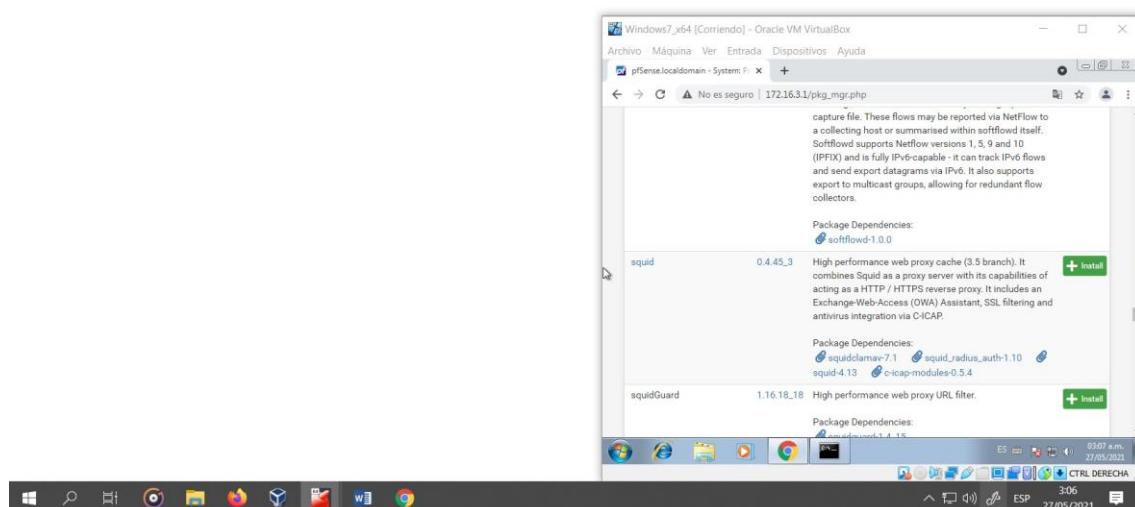
Para poder bloquear las páginas web para adultos de nuestra pc primeramente debemos descargar el paquete **squid** entrando al menú System y eligiendo Package Manager donde nos dirá que no tenemos ningún paquete descargado y entramos a la pestaña available packages

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho

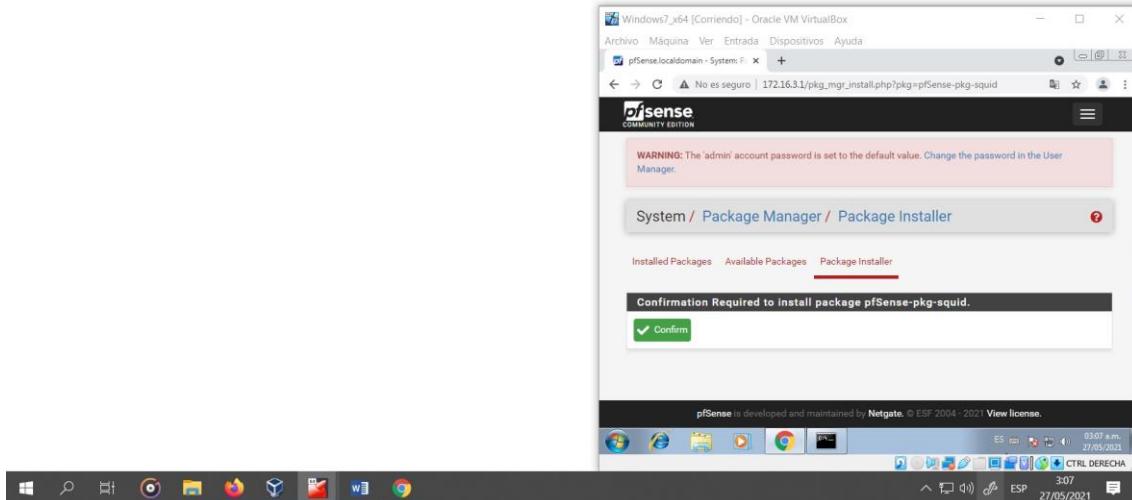


En esta pestaña buscaremos el paquete **squid** y le damos a instalar

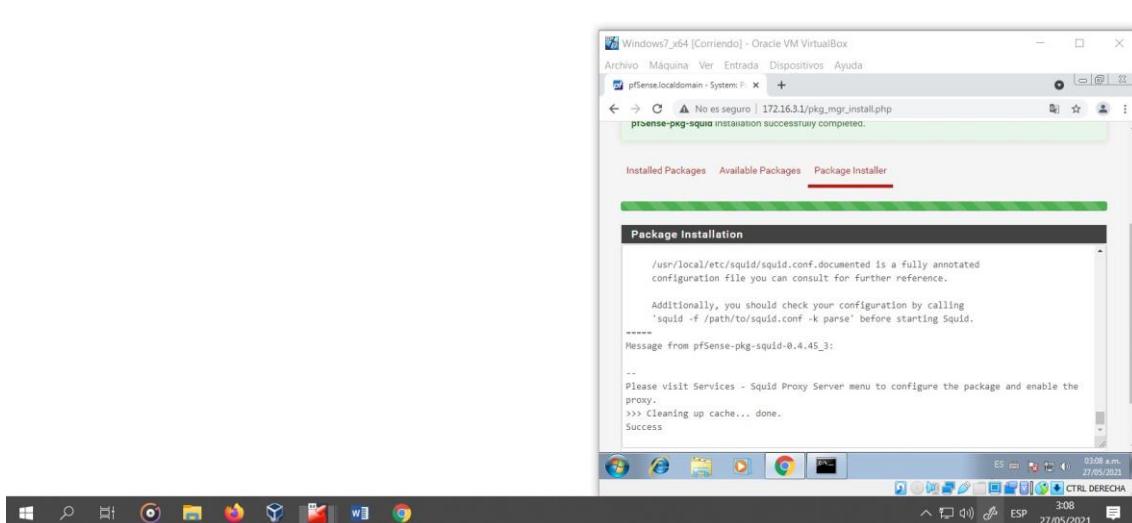
Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



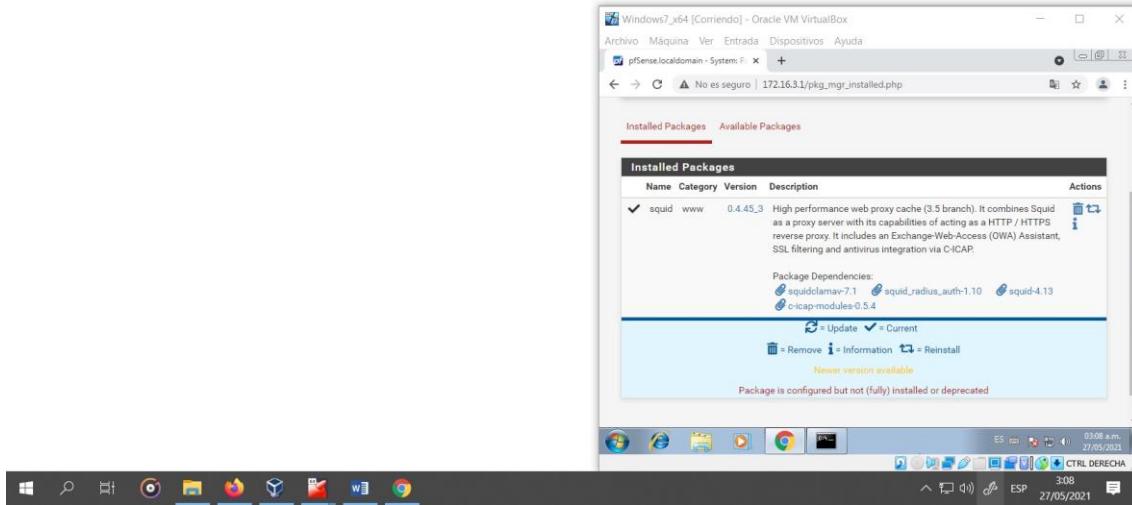
Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho

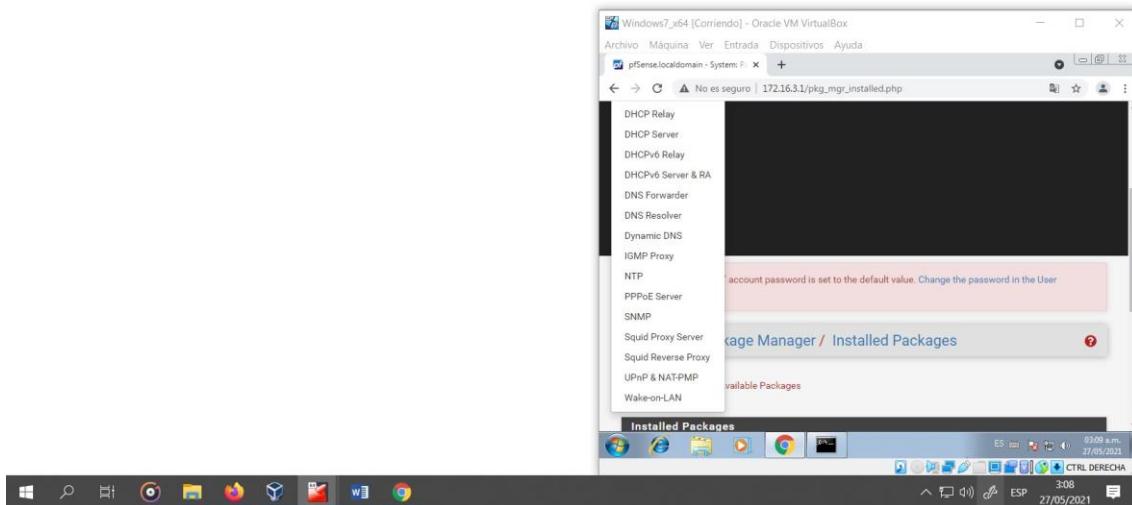


Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



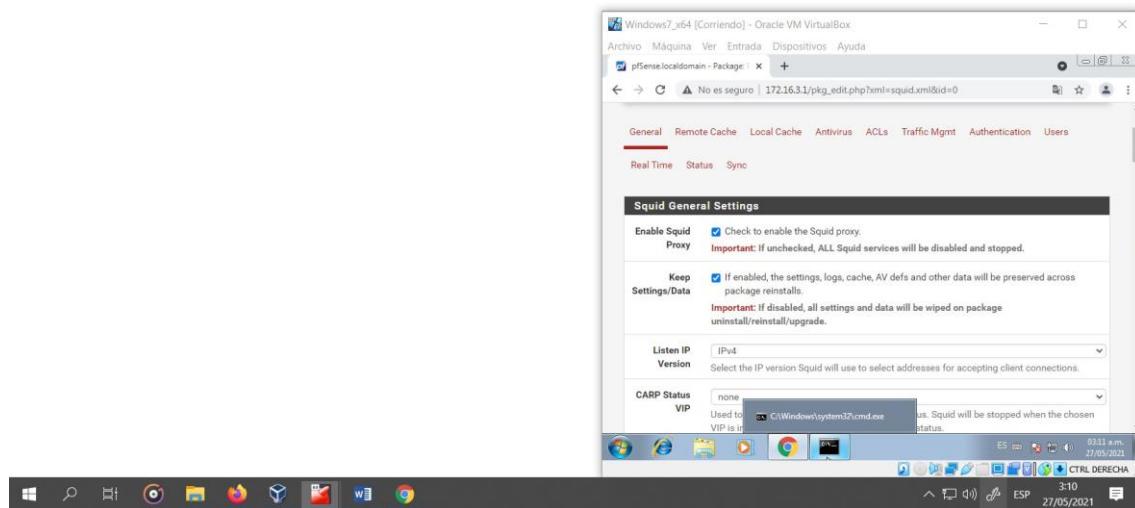
Ahora nos vamos al menú services donde encontraremos **squid proxy server**

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



Acá activaremos la opción de proxy

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



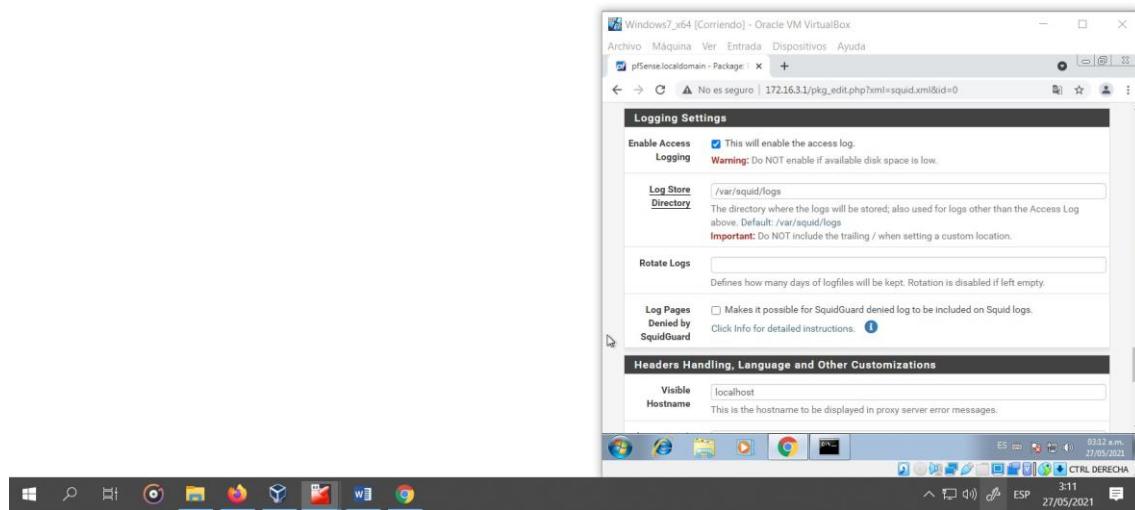
También la transparencia de proxy

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



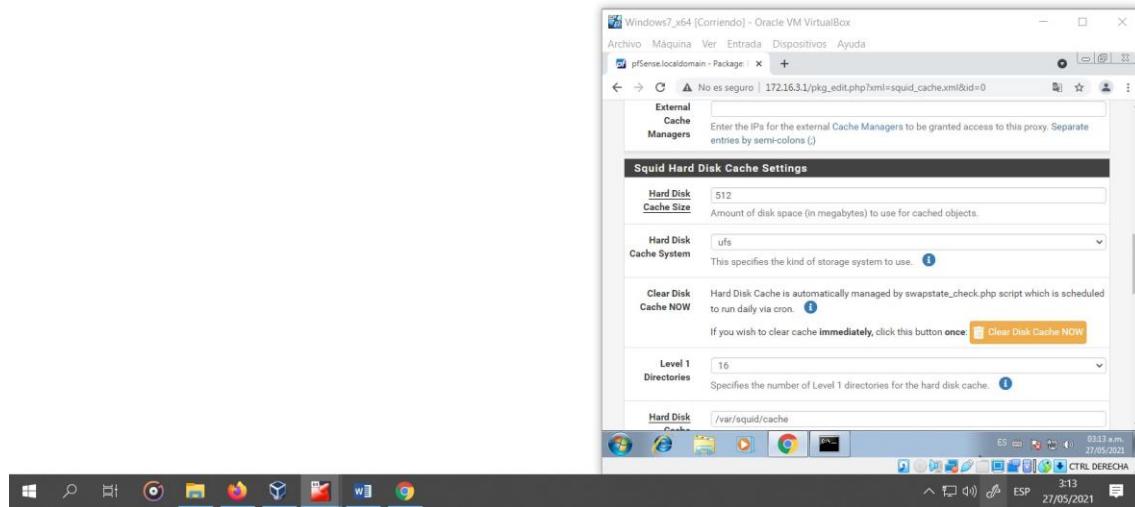
Y el acceso:

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



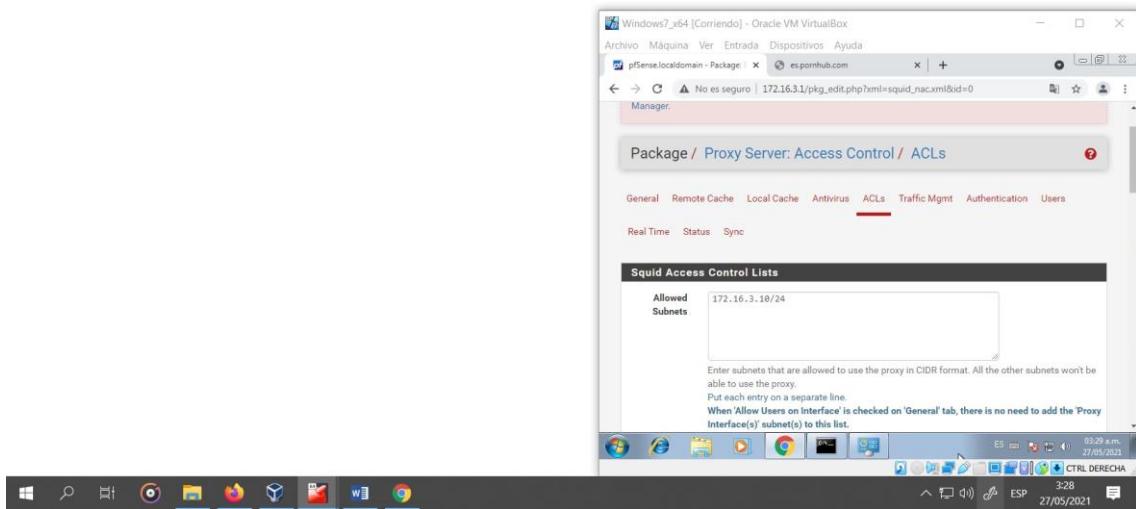
Ahora nos dirigimos a su pestaña Local Cache para darle una memoria de 512

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho

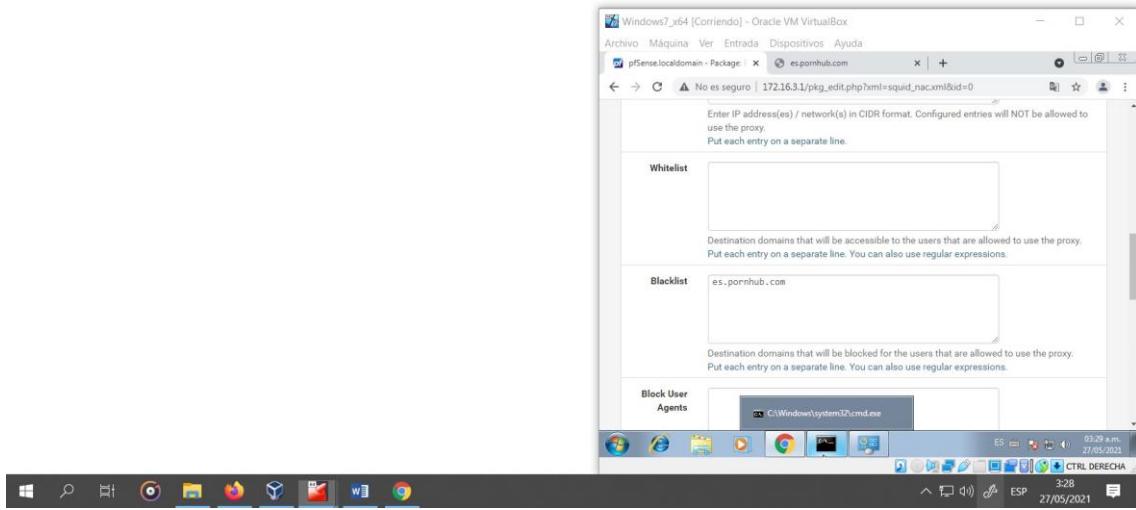


Ahora nos dirigimos a ACLs en Allowed Subnets pondremos la dirección LAN que controlaremos, en nuestro caso 172.16.3.10 nos dirigimos a blacklist donde pondremos todas las direcciones de páginas de adultos que querremos restringir

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho

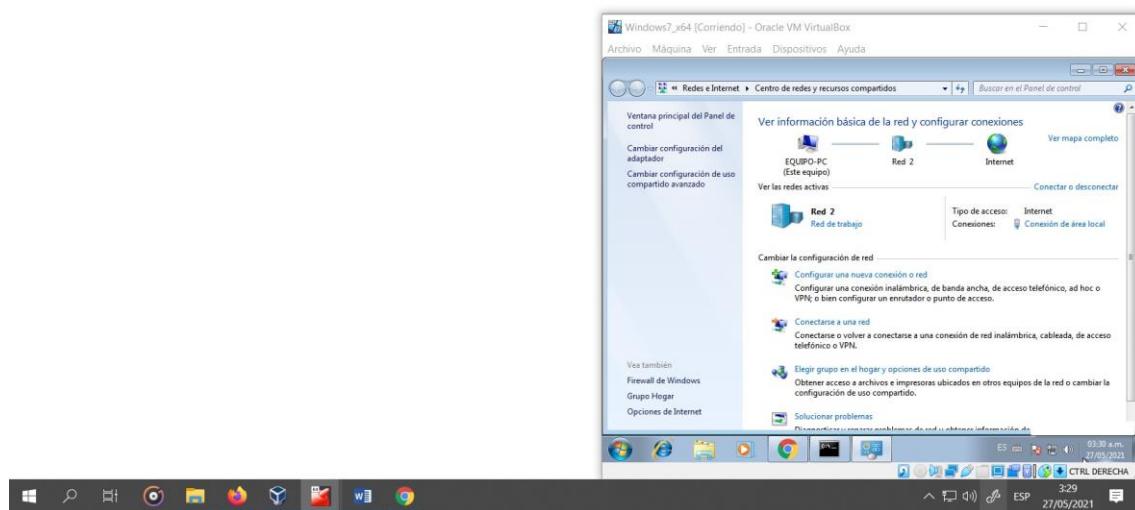


Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



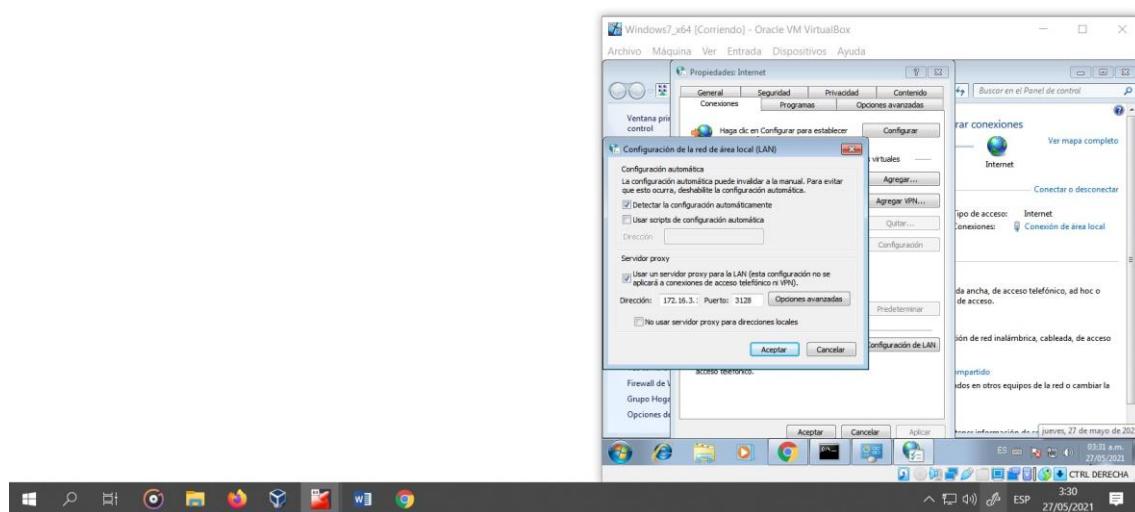
Abrimos el centro de redes y recursos compartidos elegimos opciones de internet

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho

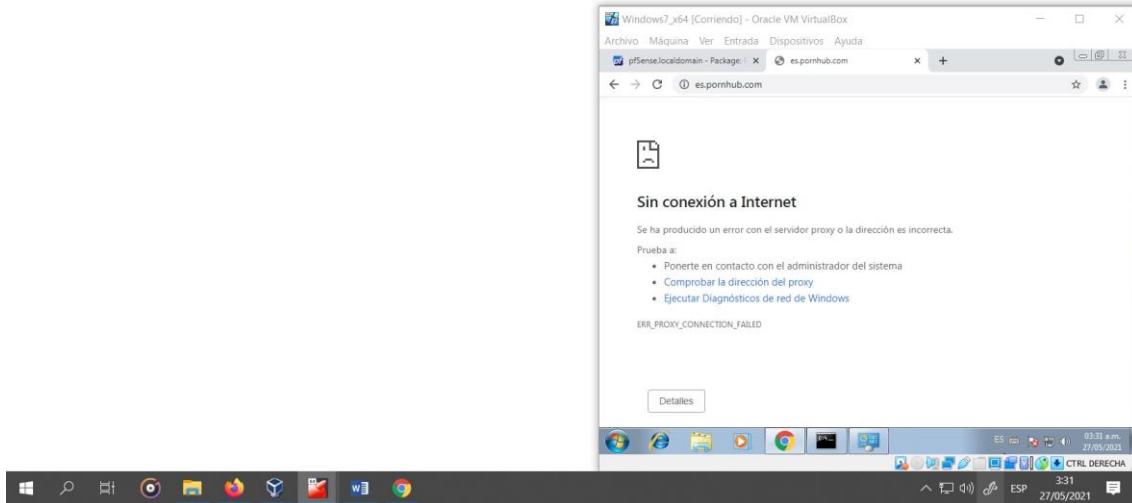


Entramos a la pestaña de conexiones y configuración de LAN activamos la casilla Usar un servidor proxy y le damos a la dirección de nuestra red LAN con puerto 3128 aceptamos las configuraciones y verificamos

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho

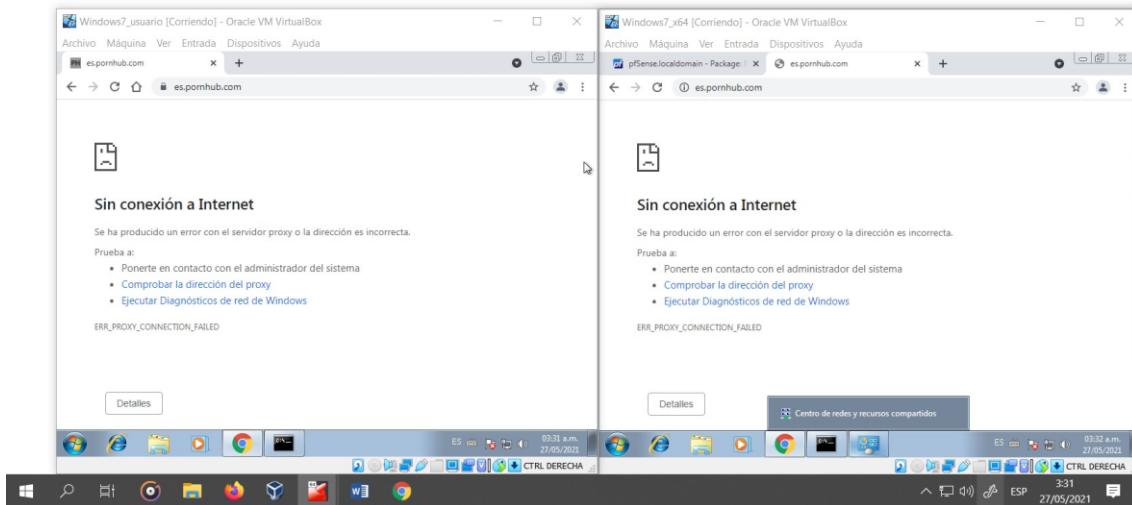


Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



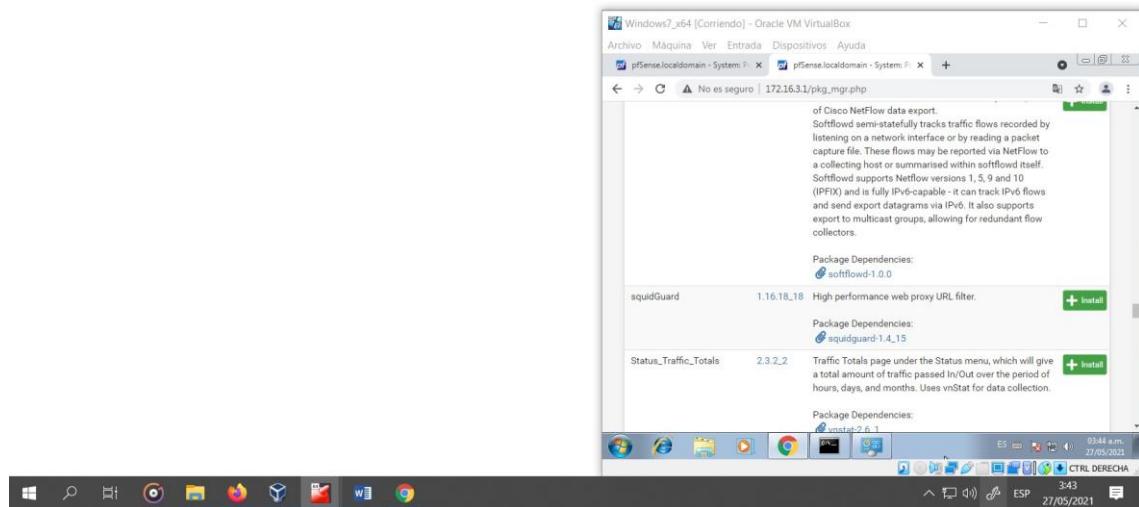
Como se puede observar en nuestros dos sistemas operativos el proxy ya está bloqueando la página que teníamos en nuestra lista negra

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



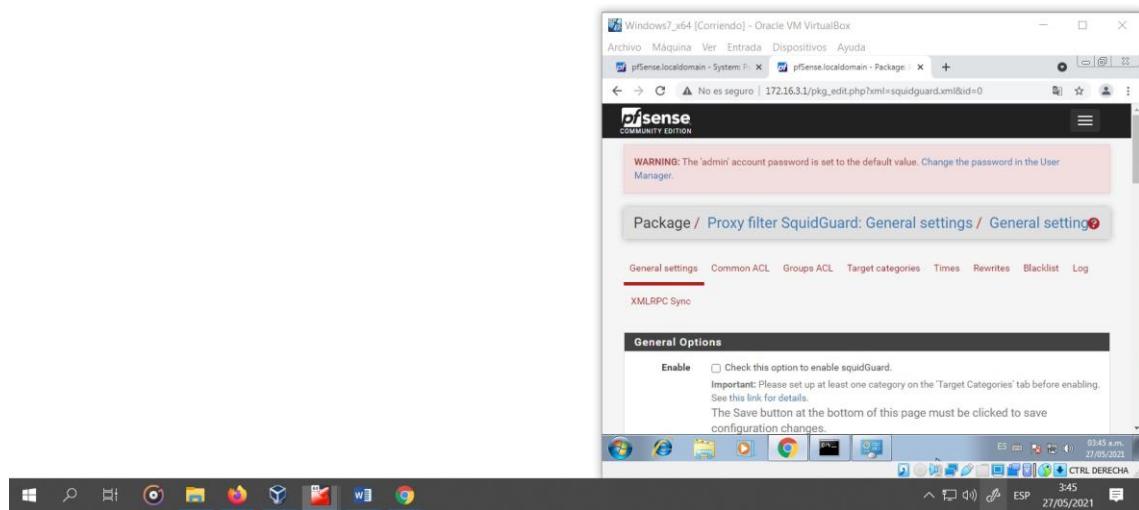
Este método para bloquear es más tardío ya que se debe poner la dirección de la página, otra manera de bloquear todas las páginas de adultos es mediante **SquidGuard** ya que esta nos ayuda a bloquear por contenido

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



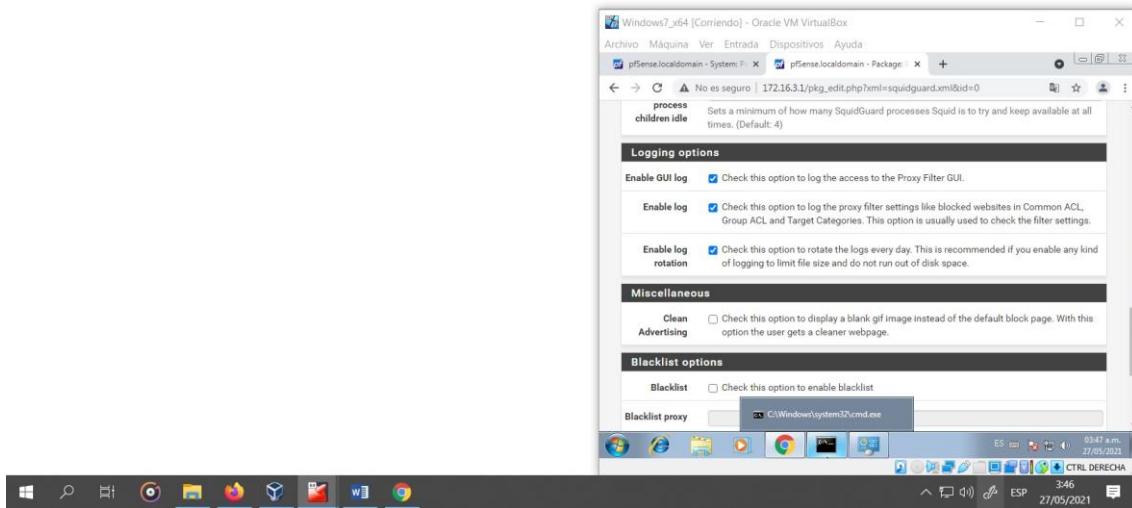
Para configurarlo nos vamos a Servises y elegimos la opción Proxy filter **squidGuard**

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



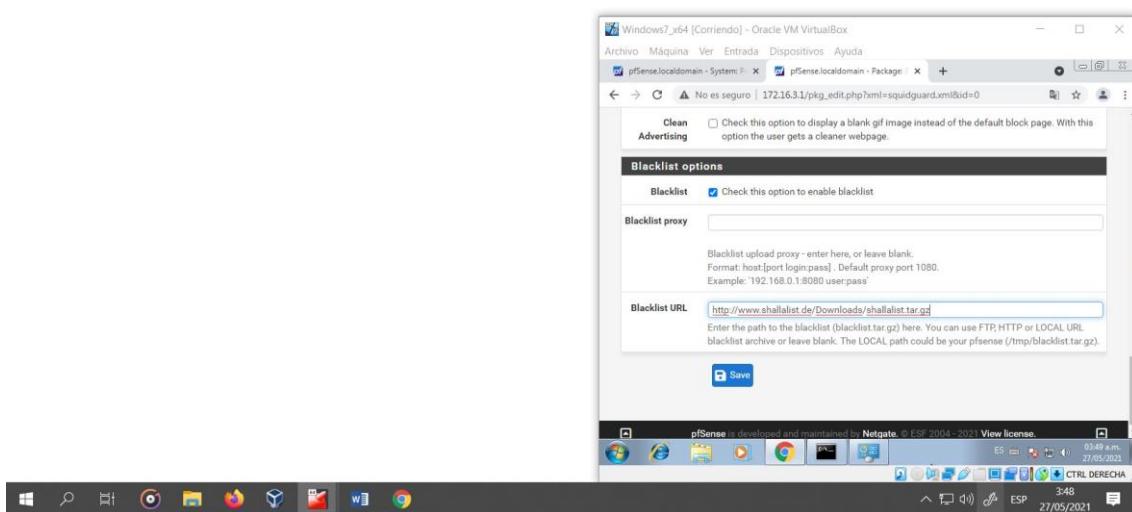
Donde marcaremos las opciones de enable y activamos los logging para tener un registro de lo que se haga

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



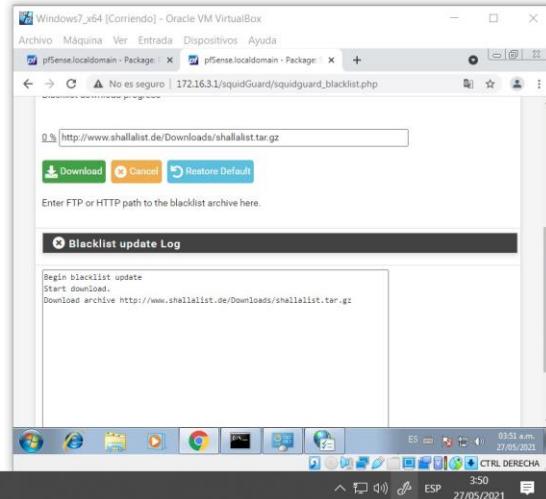
Nos dirigimos a la blacklist options donde la activaremos en un blacklist URL colocaremos la dirección <http://www.shallalist.de/Download/shallalist.tar.gz> y lo guardamos.

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



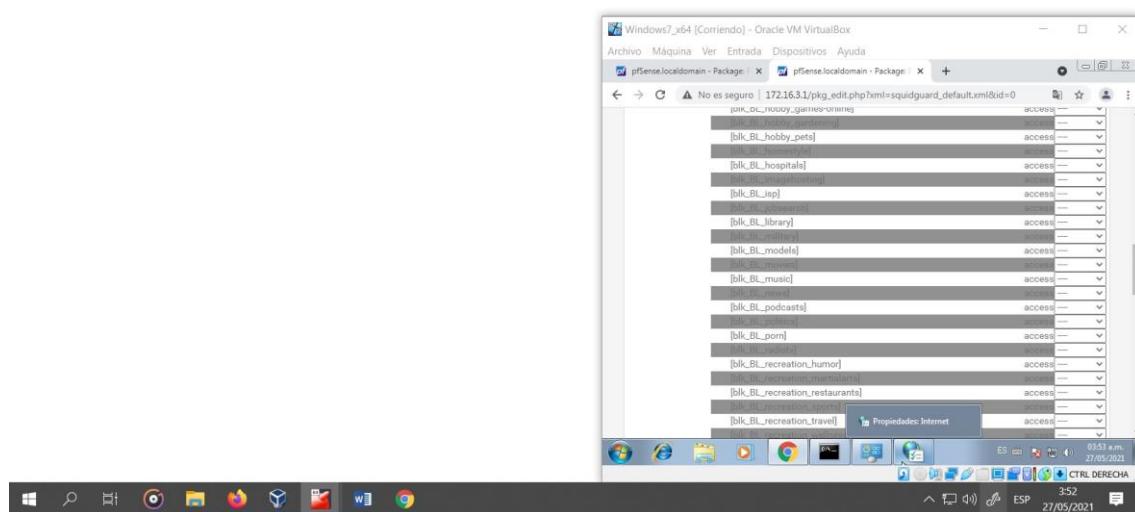
Nos dirigimos a la pantalla de blacklist y le damos a download para tener la lista de direcciones.

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



Una vez completa nos vamos a Common ACL extendemos la pestaña de target rules y veremos que nos bajó diferentes tipos de contenidos.

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



Donde bloquearemos “porn”

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



Y para evitar descargas con extensiones .exe .iso, etc denegamos downloads

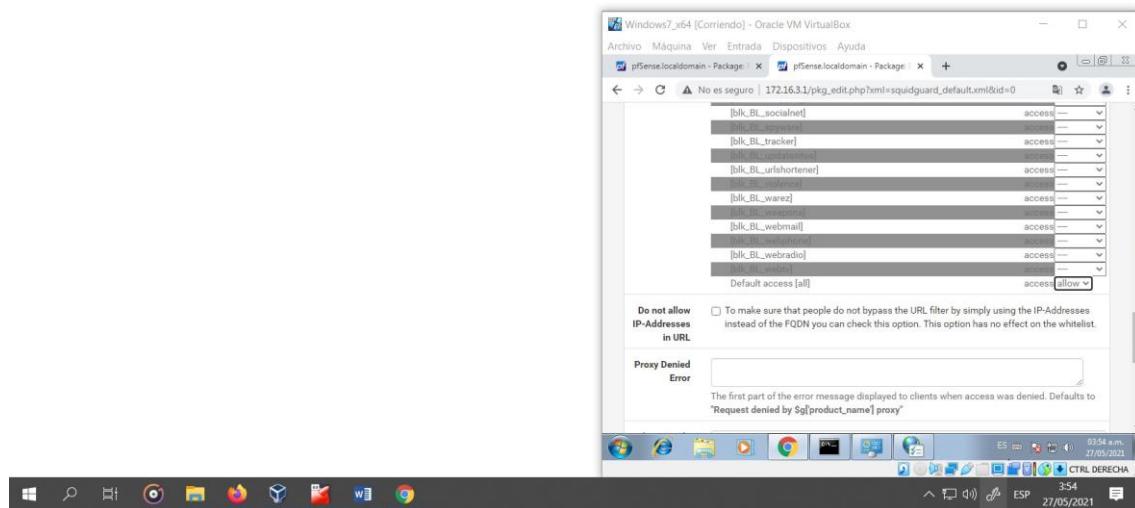
Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



Windows 7 desktop icons at the bottom.

Y permitimos default Access para que no se tenga todo bloqueado

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho

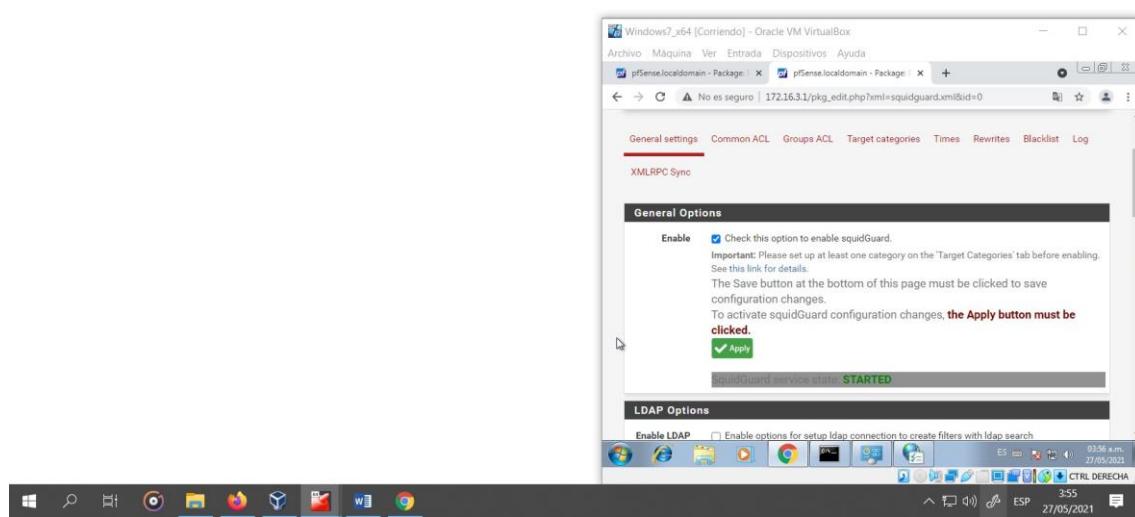


The screenshot shows a Windows 7 desktop environment with a pfSense VM running in Oracle VM VirtualBox. The pfSense interface is open, specifically the SquidGuard configuration page. In the 'Default access [all]' section, the 'access' dropdown is set to 'allow'. A tooltip below it states: 'Do not allow IP-Addresses in URL' and 'To make sure that people do not bypass the URL filter by simply using the IP-Addresses instead of the FQDN you can check this option. This option has no effect on the whitelist.' The 'Error' field displays the message 'The first part of the error message displayed to clients when access was denied. Defaults to "Request denied by Sg[product_name] proxy"'.

Activamos log para que se tengo una lista y guardamos nos dirigimos a general settings

Y damos en apply

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



The screenshot shows a Windows 7 desktop environment with a pfSense VM running in Oracle VM VirtualBox. The pfSense interface is open, specifically the SquidGuard configuration page. The 'General settings' tab is selected. The 'Enable' checkbox is checked, and the status bar at the bottom of the browser window shows 'squidGuardd service state: STARTED'. Other tabs visible include Common ACL, Groups ACL, Target categories, Times, Rewrites, Blacklist, and Log.

Ahora no se puede acceder a ninguna página con contenido adulto.

Para poder bloquear youtube.com entramos a package proxy server ACLs y ponemos la dirección de youtube.com

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



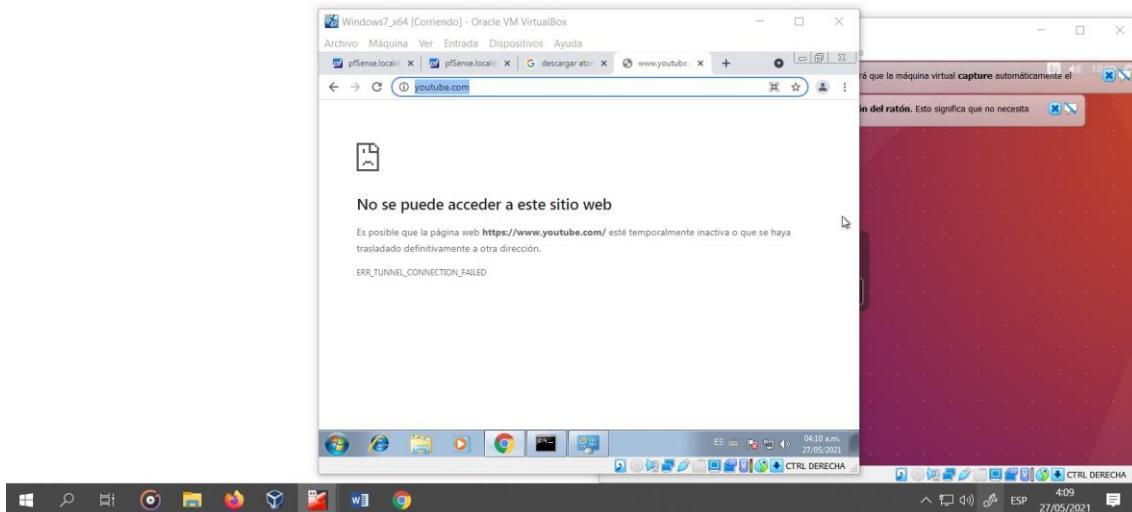
The screenshot shows the pfSense 2.5 General Settings page for the Squid proxy. It includes sections for enabling the proxy, keeping settings, and a note about preserving data during package reinstallation. The Squid General Settings section has two checked checkboxes: "Check to enable the Squid proxy" and "If enabled, the settings, logs, cache, AV defs and other data will be preserved across package reinstalls". Below this is a "Real Time" status bar.

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho

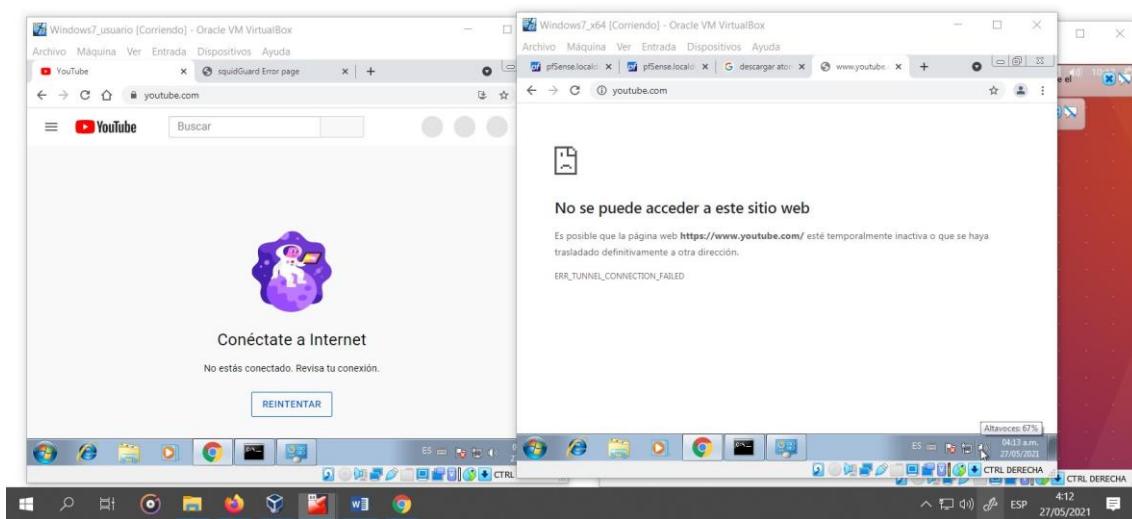


The screenshot shows the pfSense 2.5 ACLs page. It features sections for "Whitelist" and "Blacklist". In the "Whitelist" section, there is a text input field containing "www.youtube.com". In the "Blacklist" section, there is also a text input field containing "www.youtube.com". Below these sections is a "Block User Agents" section with an empty text input field. The bottom of the screen shows a taskbar with various icons and a system status bar indicating the date and time.

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho

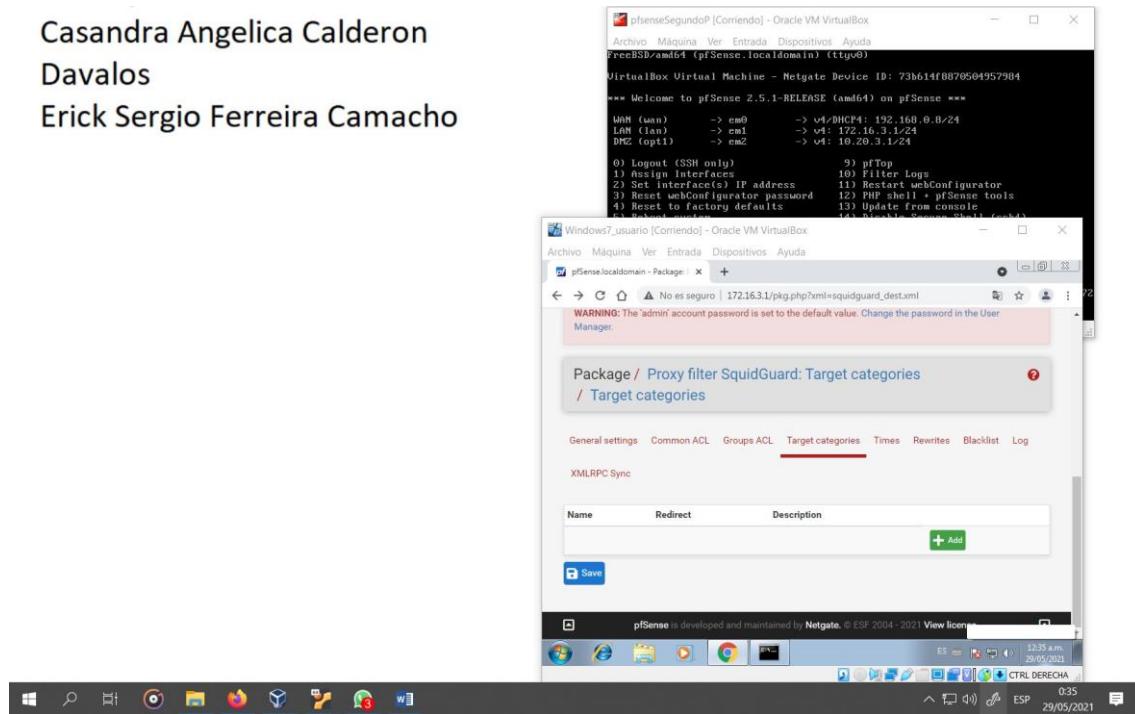


Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho

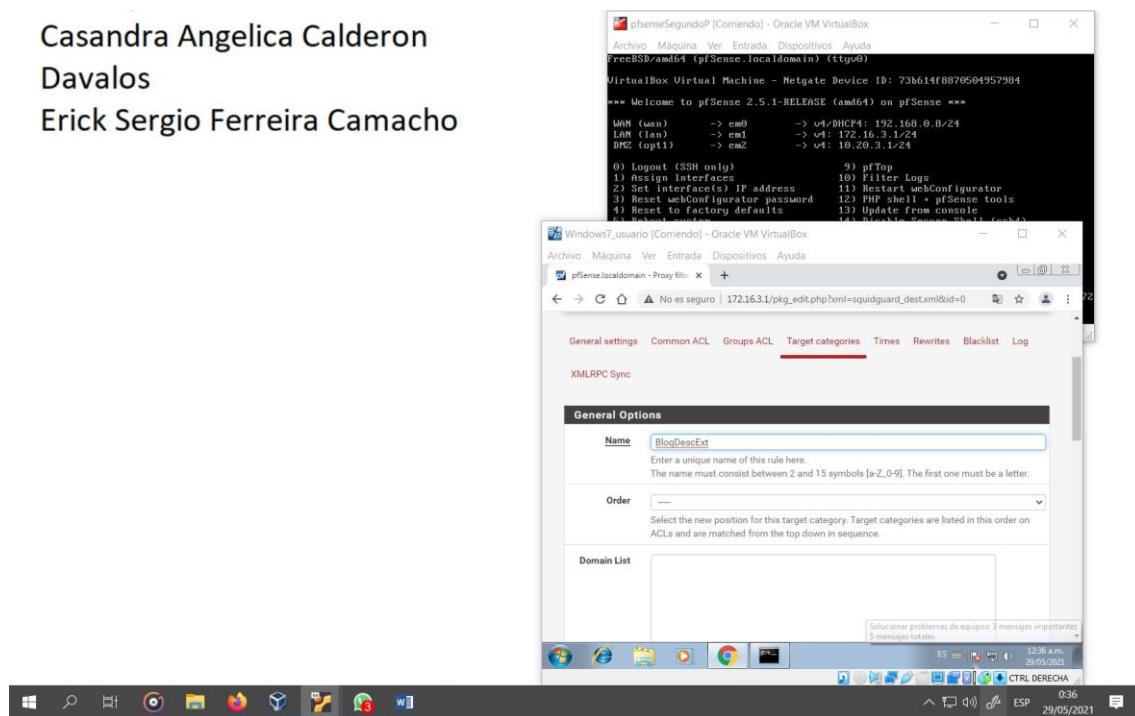


Para denegar descargar por extensiones nos vamos a services squiguard Proxy Filter y nos iremos a la pestaña de Target Categories

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho

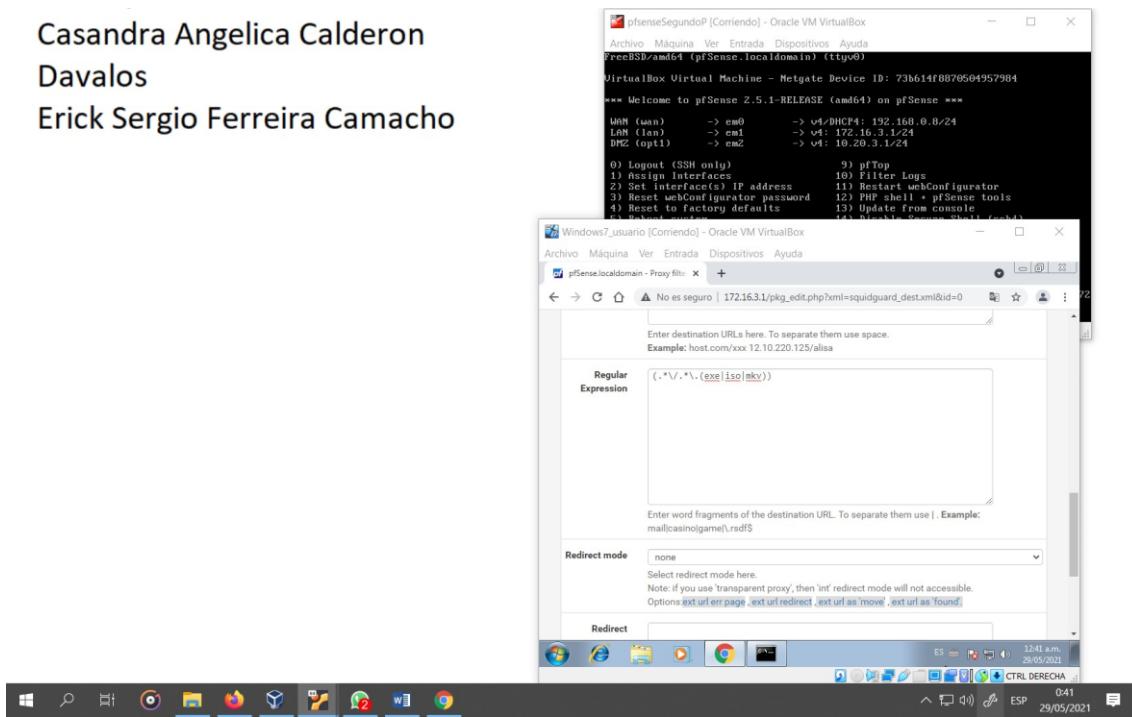


Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



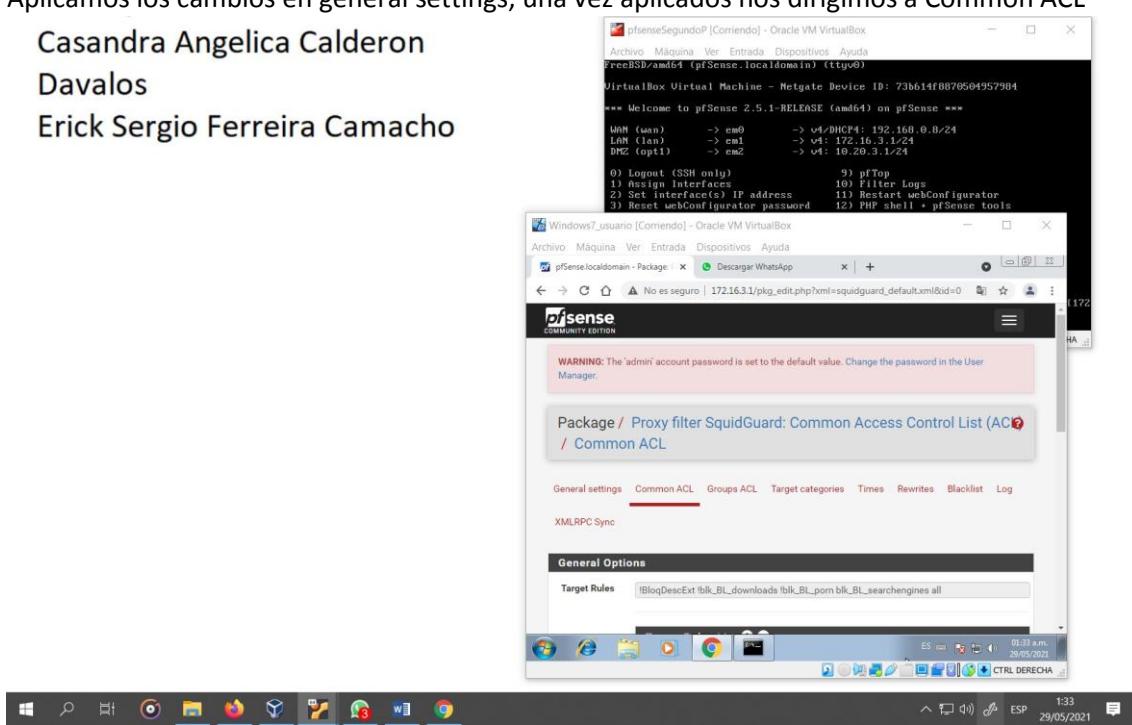
Nos dirigimos a Regular expresión donde pondremos lo siguiente (`.*\.*\mkv|iso|exe`) acá podemos agregar las extensiones que guste para denegar su descarga

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



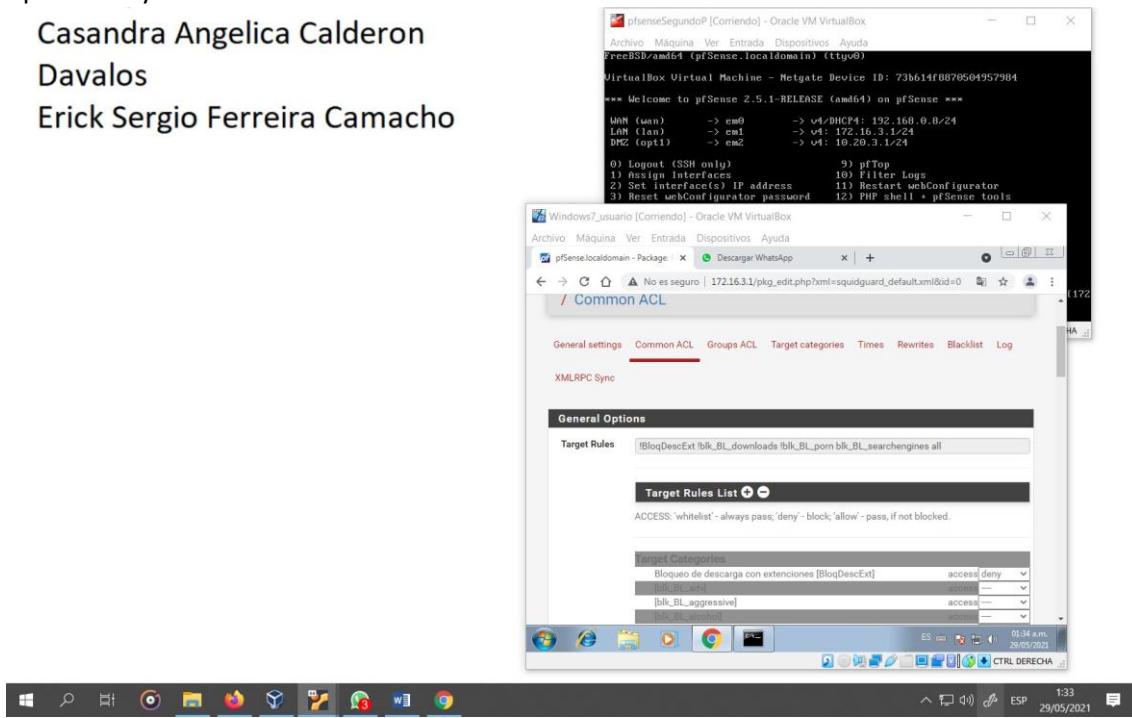
Aplicamos los cambios en general settings, una vez aplicados nos dirigimos a Common ACL

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



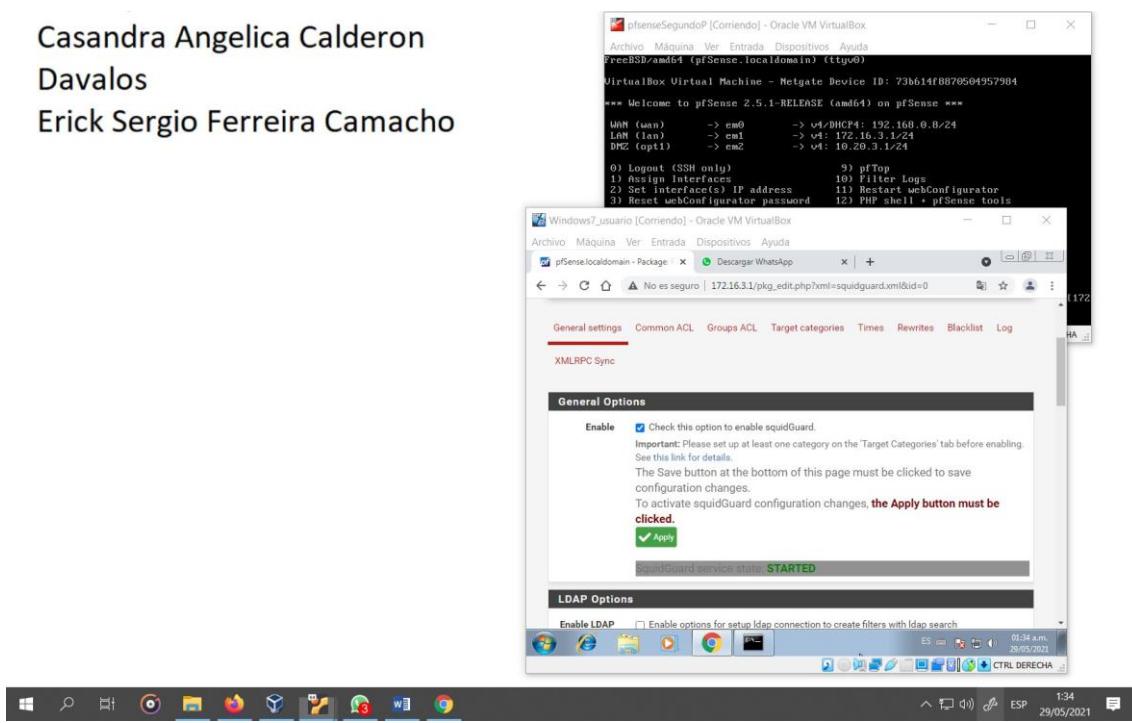
Veremos en Target Rules List que el Target que creamos nos aparece y le damos ponemos la opción deny

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



Salvamos y volvemos a aplicar los cambios

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho



Ahora podemos observar que no podremos descargar ningún archivo con extensión **iso** **exe** **mkv**.

Cassandra Angelica Calderon
Davalos
Erick Sergio Ferreira Camacho

