

Ejercicio Bastionado Sophos FW



Índice

1. Análisis de riesgos	2
Configuración de las máquinas (fw/linux)	5
Configuración del fw (y un linux)	10
Copia de seguridad	31
Configuración Windows (12)	32
Configuración Windows Server (13)	35
Configuración debian (15)	41
Configuración de la VPN SSL	49
Añadir usuarios y grupos	57
Configuración de WAZU	58
Los correos llegan si te llega una alerta :	70
Creación de bot	71
Telegram	75

1. Análisis de riesgos

Riesgo	Descripción	Probabilidad	Impacto	Importancia
Exposición a ataques externos	Todos los dispositivos de la red están expuestos a ataques externos, ya que están directamente conectados a la Internet.	Alta	Alta	Muy alta
Dificultad de gestión de la seguridad	La gestión de la seguridad de la red es más difícil, ya que todos los dispositivos están en la misma red.	Alta	Media	Alta
Mayor impacto de un ataque	En caso de un ataque exitoso, el impacto sería mayor, ya que todos los dispositivos de la red estarían expuestos.	Alta	Alta	Muy alta
Incidentes internos	Los usuarios o empleados de la red pueden causar incidentes de seguridad, como introducir malware o cometer errores.	Media	Alta	Alta
Vulnerabilidades de seguridad	Los dispositivos de la red pueden tener vulnerabilidades de seguridad que pueden ser explotadas por los atacantes.	Media	Alta	Alta

Fallos de hardware o software	Los dispositivos de la red pueden fallar debido a fallos de hardware o software, lo que puede provocar una interrupción del servicio.	Media	Baja	Media
Errores humanos	Los usuarios o empleados de la red pueden cometer errores que pueden provocar incidentes de seguridad.	Alta	Baja	Media

Situación inicial

En la situación inicial, la red está configurada de la siguiente manera:

- Todos los dispositivos están conectados a la misma red.
- El router no tiene ningún firewall habilitado.
- El servidor web está expuesto directamente a la Internet.

Esta configuración presenta los siguientes riesgos:

- Exposición a ataques externos: Todos los dispositivos de la red están expuestos a ataques externos, ya que están directamente conectados a la Internet.
- Dificultad de gestión de la seguridad: La gestión de la seguridad de la red es más difícil, ya que todos los dispositivos están en la misma red.
- Mayor impacto de un ataque: En caso de un ataque exitoso, el impacto sería mayor, ya que todos los dispositivos de la red estarían expuestos.

Situación propuesta

En la situación propuesta, la red está configurada de la siguiente manera:

- Los dispositivos se dividen en dos redes: una red interna y una red DMZ.

- El router tiene un firewall habilitado para separar las dos redes.
- El servidor web se coloca en la red DMZ.

Esta configuración reduce los riesgos de la siguiente manera:

- Reduce la exposición a ataques externos: Los dispositivos internos están protegidos de ataques externos por el firewall del router.
- Facilita la gestión de la seguridad: La gestión de la seguridad de la red es más sencilla, ya que los dispositivos internos y externos están separados.
- Reduce el impacto de un ataque: En caso de un ataque exitoso, el impacto sería menor, ya que solo los dispositivos de la red DMZ estarían expuestos.

Conclusión

La transición de la situación inicial a la situación propuesta reduce los riesgos de la red de la siguiente manera:

- Reduce la exposición a ataques externos.
- Facilita la gestión de la seguridad.
- Reduce el impacto de un ataque.

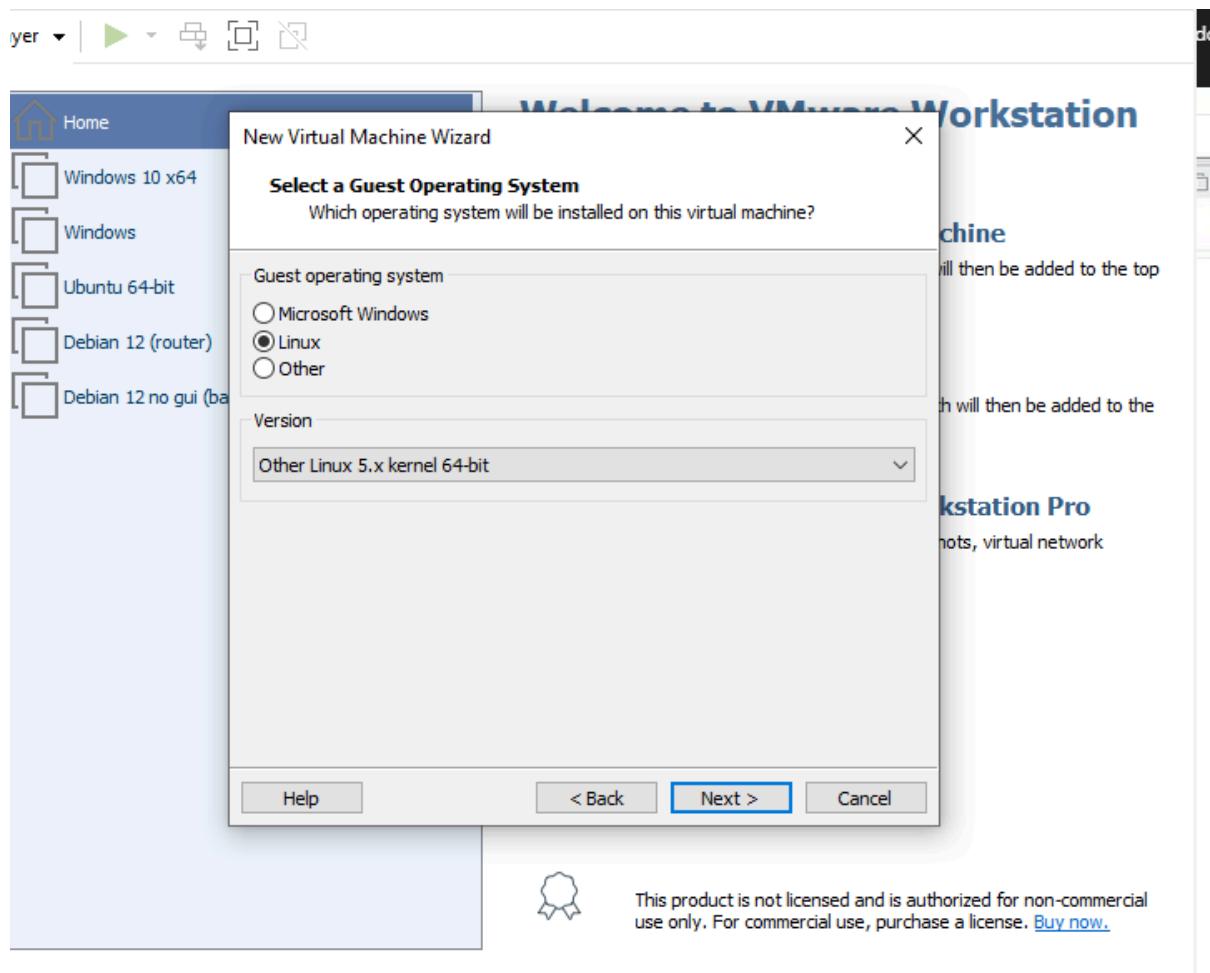
Por lo tanto, la transición de la situación inicial a la situación propuesta está justificada en términos de seguridad.

Configuración de las máquinas (fw/linux)

Primer paso

Para descargar el fw gratuito : [Sophos file download](#)

Creamos el fw de sophos con 6 puertos :



Hardware

The screenshot shows the 'Hardware' configuration screen for a virtual machine. On the left, a tree view lists various hardware components: Memory (selected), Processors, New CD/DVD (IDE), Network Adapter, Network Adapter 3, Network Adapter 2, Network Adapter 6, Network Adapter 4, Network Adapter 5, USB Controller, Sound Card, Printer, and Display. The 'Memory' section is expanded, showing a summary of 4 GB and a detailed configuration panel on the right.

Memory

Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.

Memory for this virtual machine: MB

Memory Size	Notes
128 GB	Maximum recommended memory (Memory swapping may occur beyond this size.)
64 GB	
32 GB	
16 GB	
8 GB	
4 GB	Recommended memory
2 GB	
1 GB	
512 MB	
256 MB	
128 MB	
64 MB	
32 MB	Guest OS recommended minimum
16 MB	
8 MB	
4 MB	

Cómo configurar :

Cómo configurar el firewall

1. Instale la imagen descargada en su hardware o entorno virtual.

Nota: La instalación sobrescribe el sistema operativo existente y todos los archivos.

2. Conecte la interfaz WAN (puerto 2) del firewall a la conexión a Internet.
3. Conecte una estación de trabajo a la interfaz LAN (puerto 1).
4. Para acceder al asistente de instalación, diríjase a la siguiente dirección IP desde la estación de trabajo: <https://172.16.16.16:4444>.

Nota: El asistente puede tardar varios minutos en iniciarse.

5. Siga los pasos del asistente de instalación.

Vea el [vídeo de registro y configuración](#).

Ahora necesitamos sacar la ip , para poder instalar nuestro fw dentro de nuestro linux . **Para sacar la ip dentro de nuestro FW**

La clave es **admin**

Escribimos "y" a los dos opciones

```
Installing firmware for application
Firmware Installed
Remove Installer disk
press y to reboot
y-
```

Ahora necesitamos saber la ip de nuestra máquina :

```
Sophos Firmware Version: SFOS 19.5.3 MR-3-Build652
Model: SF01U
Hostname:

Main Menu

AA. Device Activation
 1. Network Configuration
 2. System Configuration
 3. Route Configuration
 4. Device Console
 5. Device Management
 6. VPN Management
 7. Shutdown/Reboot Device
 8. Exit

Select Menu Number [0-7]: 1
```

```
Sophos Firmware Version: SFOS 19.5.3 MR-3-Build652
Model: SF01U
Hostname:

Network configuration Menu

 1. Interface Configuration
 2. DNS Configuration
 8. Exit

Select Menu Number [0-2]: 1
```

y nos saca nuestra ip que es :

```
Sophos Firmware Version: SFOS 19.5.3 MR-3-Build652
Model: SF01V
Hostname:

Network Settings
  Interface Name      : Port1 (Physical)
  Zone Name           : LAN

  IPv4/Netmask        : 172.16.16.16/255.255.255.0 (Static)
  IPv4 Gateway         : N.A.

  IPv6/Prefix          : Not Configured
  IPv6 Gateway          : N.A.

  Configured Aliases

  No Alias Configured

Press Enter to continue .....
```

```
Sophos Firmware Version: SFOS 19.5.3 MR-3-Build652
Model: SF01V
Hostname:

Network Settings
  Interface Name      : Port2 (Physical)
  Zone Name           : WAN

  IPv4/Netmask        : 192.168.139.139/255.255.255.0 (DHCP)
  IPv4 Gateway         : 192.168.139.2 (DHCP_Port2_GW)

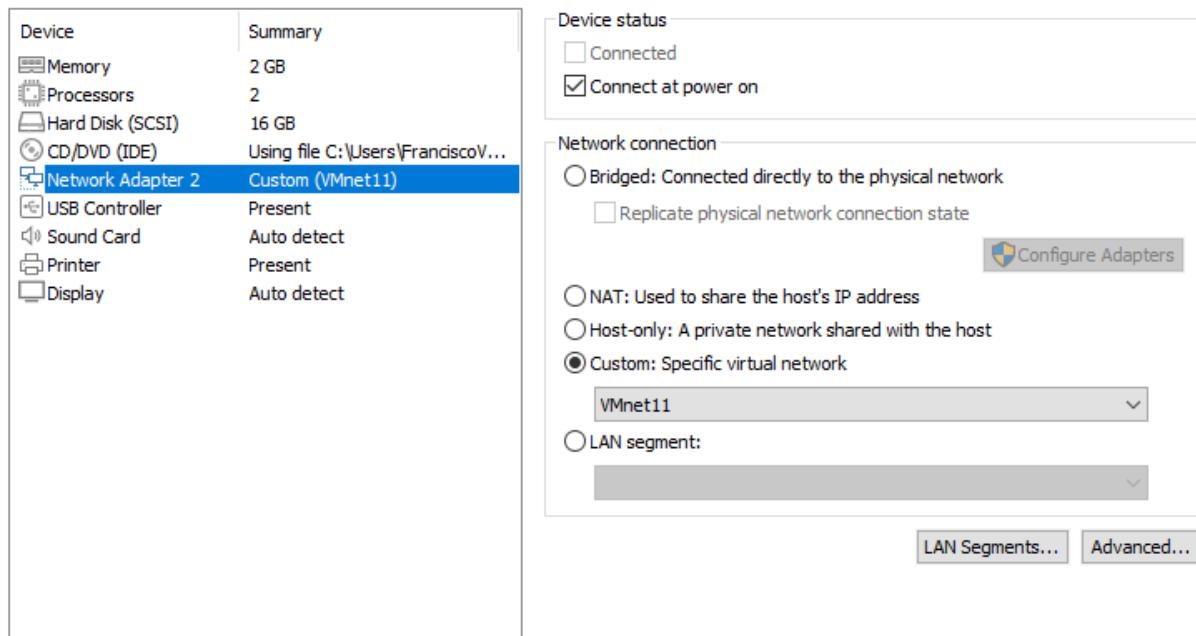
  IPv6/Prefix          : Not Configured
  IPv6 Gateway          : N.A.

  Configured Aliases

  No Alias Configured

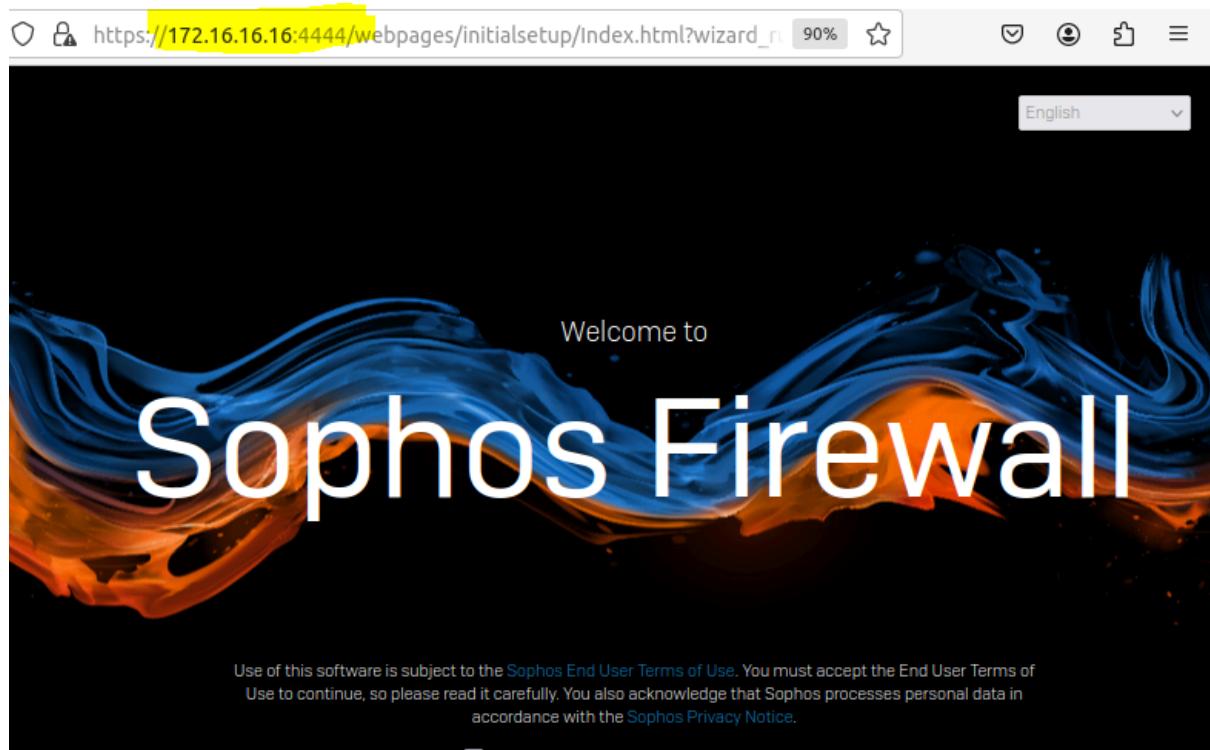
Press Enter to continue .....
```

Creamos un linux para interactuar



Configuración del fw (y un linux)

Para ello pondremos en el buscador de nuestro linux la ip de nuestro fw . En el caso de que no salga puede ser un error de que no está actualizado el linux . Una vez llegamos aquí , ya podemos empezar con nuestra configuración .



A screenshot of the 'Register your firewall' page from the Sophos website. The page features a blue 'S' logo and the heading 'Register your firewall'. It explains that every firewall must have a serial number and provides two options: 'I have an existing serial number' (selected) and 'I don't have a serial number [start a trial]'. The 'Serial Number' field contains the value 'V01001MJJKR7Q07'. To the right, a 'LICENSE SCHEDULE' window is displayed, showing a table with columns 'Serial Number', 'Activation Date', and 'Expiration Date'. A red arrow points to the 'Serial Number' column, highlighting the value 'C160703HBRQMRCE'. Other rows in the table are partially visible.

Network configuration (LAN)

Select the ports, the deployment mode, and how to assign IP addresses.
Currently, you're connected to "Port1".

Port

Port1 You can change the selected port.

Choose gateway

This firewall (route mode)

Gateway mode: The firewall acts as a router.
Bridge mode: The firewall acts as a bridge between your network and your internet gateway.
The firewall secures your network in both modes.

LAN IP address	Subnet mask
172.16.16.16	/24 (up to 254 client devices) <input type="button" value="▼"/>

Edit internet connection

Enable DHCP
Let the firewall assign IP addresses to your internal devices.

DHCP lease range

172.16.16.100	-	172.16.16.109
---------------	---	---------------

Enable TAP/discover mode

Network protection

You can configure permissions for users on wired and wireless networks to protect them when they access the internet.

-  Protect users from network threats
Protects users from network intrusion attempts. IPS protection is turned off by default. To turn it on, go to Intrusion prevention > IPS policies after you finish the setup.
-  Protect users from the suspicious and malicious websites
Protects users from clicking malicious links, and from visiting harmful sites. It does not scan the SSL traffic.
[Click here](#) to learn how to scan HTTPS traffic.
-  Scan files that were downloaded from the web for malware
Even reputed sites may contain malicious files. Scan files with Sophos malware detection engine to catch known malware and their variants.
-  Send suspicious files to zero-day protection
Protects users from undiscovered malware through advanced detection techniques that involve running applications, and viewing documents in a safe sandbox in the cloud, before letting users download files to their computers.



Notifications and backups

It is important to have quick access to backups. Enter the details to receive the latest backups and notifications by email.

Recipient's email address

pacocesurrr@gmail.com

Sender's email address

pacocesurrr@gmail.com

Send configuration backup every week

Use external mail server

[Previous](#)

[Continue](#)

Configuration summary

Please review your choices in the window. Click Finish. This will apply the settings that you have specified, install the latest firmware, and reboot the firewall. It will take approximately five minutes to complete.

Basic settings

Hostname: FW-clase

Time zone: Europe/Madrid

Network settings

Internet connection: DHCP on Port2

Local network: Port1

IP: 172.16.16.16/255.255.255.0

DHCP enabled

#Default_Network_Policy has been created with:

Scan HTTP: Enable

Use zero-day protection: Enable

Web policy: Default Policy

Intrusion prevention: lanitowan_general

Created linked NAT rule "#NAT_Default_Network_Policy" with source translated to MASQ.

Notifications and backups:

Send configuration backup every week: Disable

Built-in email server

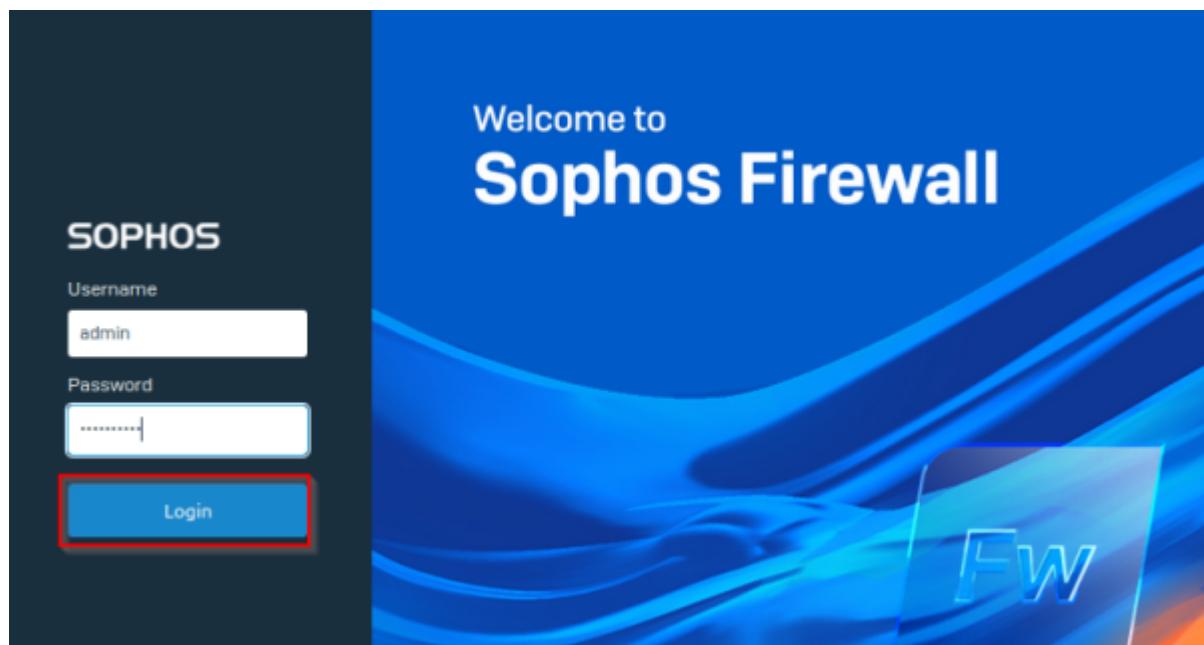
Recipient's email address: rafael.s275785@cesurformacion.com

[Copy to clipboard](#)

[Send as email](#)

[Previous](#)

[Finish](#)



Create the secure storage master key

Before you create the master key, ensure that you can store the master key in a password management system or another secure location.

⚠ If you lose the secure storage master key, you can't recover it.

Enter the secure storage master key

 eye icon

Key strength: **Strong**

Enter your key again to confirm

Complexity requirements:

- Minimum 12 characters
- An uppercase letter
- A lowercase letter
- A number (0-9)
- A special character

I have stored the master key in a password manager or another secure location

[Back](#)

[Create key](#)

Coquina@5656@

Vamos a añadir la wan (En este caso ya está añadida), para ello nos vamos a la derecha del todo y le damos a añadir

Esto se hace para que podamos configurarlo desde otras máquinas , por ejemplo hemos habilitado la red nat también y desde esta nat con esa ip también podremos entrar

The screenshot shows the Sophos XG Firewall configuration interface. On the left, a sidebar lists various sections: Zero-day protection, Diagnostics, PROTECT (Rules and policies, Intrusion prevention, Web, Applications, Wireless, Email, Web server, Active threat response), CONFIGURE (Remote access VPN, Site-to-site VPN, Network, Routing, Authentication, System services), SYSTEM (Sophos Central, Profiles, Hosts and services, Administration, Backup & firmware). The 'Administration' tab is selected. In the main area, a yellow box highlights the 'Local service ACL exception rule'. This section shows a table with one row: Rule name 'Acceso-WAN' and IP version 'IPv4'. Below this is another yellow box highlighting the 'Default admin's password settings' section, which contains fields for Username ('admin'), Current password (*redacted), New password (*redacted), Password (*redacted), and Confirm Password (*redacted). A blue 'Apply' button is at the bottom.

Destination host **puerto 2** , a mi no me deja pero si te dejá ponlo , la WAN tiene que ser 132 porque cuando nos vamos a nuestro cmd de nuestro pc la ip vmWare está dentro de su rango :

```
Adaptador de Ethernet VMware Network Adapter VMnet8:  
Sufijo DNS específico para la conexión. . . :  
Vínculo: dirección IPv6 local. . . : fe80::2d4f:b70e:7eb5:eb8b%9  
Dirección IPv4. . . . . : 192.168.132.1  
Máscara de subred . . . . . : 255.255.255.0  
Puerta de enlace predeterminada . . . . . :
```

The screenshot shows the 'Local service ACL exception rule' configuration page. At the top, there are links for How-to guides, Log viewer, Help, and admin@F. Below is a navigation bar with tabs: Licensing, Device access (selected), Admin and user settings, Time, and Notification settings. The 'Device access' tab has the following fields:

- Rule name *: Acceso-WAN
- Description: Acceso a mi red WAN 192.168.1.0/24 y 192.168.132.0/24
- IP version: IPv4 (radio button selected)
- Source zone: WAN (dropdown menu)
- Source Network / Host *:
 - WAN-192-168-132-0
 - WAN-192.168.1-0
 - Add new item
- Destination host *:
 - #Port2
 - Add new item

Services *

HTTPS	<input type="button" value="Delete"/>
SSL VPN	<input type="button" value="Delete"/>
VPN Portal	<input type="button" value="Delete"/>
Add new item	

Action Accept Drop

Save Cancel Sophos Assistant

Una vez hecho ya lo abrimos desde nuestro buscador con la ip que nos aparece en el puerto 2

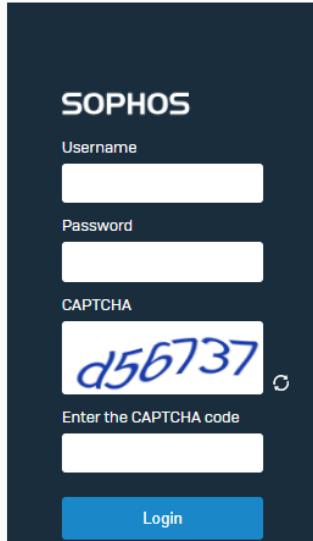
```
: Port2 (Physical)
: WAN

: 192.168.132.129/255.255.255.0 (DHCP)
: 192.168.132.2 (DHCP_Port2_GW)

: Not Configured
: N.A.
```

No es seguro <https://192.168.132.129:4444>

English



The login interface for Sophos Firewall. It features a dark blue header with the word "SOPHOS". Below it is a form with fields for "Username" and "Password", both represented by white input boxes. Underneath these is a "CAPTCHA" section with a CAPTCHA code "d56737" displayed in a blue box, followed by a text input field labeled "Enter the CAPTCHA code". At the bottom of the form is a blue "Login" button. To the right of the login form is a large blue background area with the text "Welcome to Sophos Firewall" and a stylized "FW" logo.

Podemos cambiar las modificaciones de seguridad , si queremos que a los 10 minutos sin actividad nos eche o el número de posibilidades de acertar la contraseña , lo podemos cambiar aquí .

Administration

How-to guides Log viewer Help admir

Licensing Device access Admin and user settings Time Notification settir

Login security

Logout admin session after Minutes of inactivity

Block login

After unsuccessful attempts from same IP in Seconds [1-120]

Block login access for Minutes [1-60]

Apply

Administrator password complexity settings

También podemos modificar el inicio de sesión

Login disclaimer settings

Enable login disclaimer

[Click here](#) to modify the disclaimer message [System > Administration > Messages]

[Click here](#) to preview the disclaimer message

Apply

He cambiado el mensaje para el tema de privacidad y ahora habilitamos la pestaña de arriba

Message key	Message
<input type="checkbox"/> Authentication	
<input type="checkbox"/> SMTP	
<input type="checkbox"/> Administration	
Disclaimer message	ACCESS WARNING Este dispositivo es de uso privado
<input type="checkbox"/> SMS customization	

ESTO SE HACE DESDE FUERA , DESDE INTERNET , PORQUE SI NO LINUXMINT PETA

Ahora vamos a editar la red wan1, para ello nos vamos a las 3 pestañas de la derecha y nos vamos a editar

Interface	Status	Speed & Duplex	IP Address
WiFi	Auto-negotiated	Static	172.16.16.16/255.255.255.0
Port1	Connected	1000 Mbps - Full Duplex	172.16.16.16/255.255.255.0
Port2	Connected	1000 Mbps - Full Duplex	192.168.132.131/255.255.0

General settings

Name * Port1

Hardware Port1

Network zone LAN

IPv4 configuration

IP assignment Static PPPoE [DSL] DHCP

IPv4/netmask * 192.168.11.1 /24 [255.255.255.0]

Gateway detail

Gateway name

Gateway IP

Save **Cancel** **Sophos Assistant**

Red

Interfaces Zones WAN link manager DNS DHCP IPv6 router advertisement Celular WAN IP tunnels Vecinos (ARP-NDP) DNS Dinámico

Servidor

Nombre	Interfaz	Detalle del arrendamiento	versión IP	Estado	Administrar
<input type="checkbox"/> Servidor_DHCP_predeterminado	Puerto1 - 192.168.11.1	172.16.16.100 - 172.16.16.199	-	IPv4 <input type="radio"/> OFF	
<input type="checkbox"/> Acceso_de_invitado_DHCP	InvitadoAP - 10.255.0.1	10.255.0.2 - 10.255.0.254	-	IPv4 <input type="radio"/> ON	

Configuración general

Nombre *	Default_DHCP_Server		
Interfaz	Puerto1 - 192.168.1.1		
<input type="checkbox"/> Aceptar solicitud del cliente vía retransmisión			
Arrendamiento de IP dinámica	Iniciar IP	IP final	+
	192.168.1.100	192.168.1.199	-
* Presione Tab para agregar una nueva fila			
Mapeo de IP MAC estática	Nombre de host	Dirección MAC	dirección IP
			+
			-
* Presione Tab para agregar una nueva fila			
Máscara de subred *	/24 (255.255.255.0)		
Nombre de dominio			
Puerta *	<input checked="" type="checkbox"/> Utilice la interfaz IP como puerta de enlace		
	192.168.1.1		
Tiempo de arrendamiento predeterminado *	1440	1-43200 minutos (30 días)	
Tiempo máximo de arrendamiento *	2880	1-43200 minutos (30 días)	
Detección de conflictos	<input checked="" type="checkbox"/> Permitir		

servidor DNS

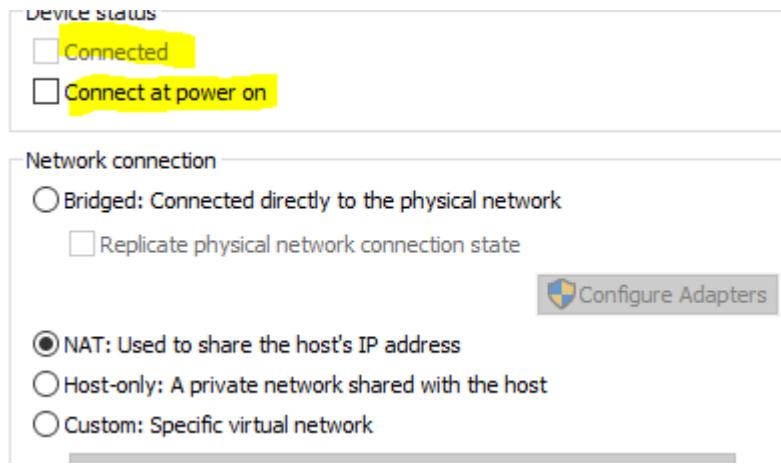
<input type="checkbox"/> Usar la configuración DNS del dispositivo	
DNS primario	192.168.1.2.1
DNS secundario	9.9.9.9

servidor GANA

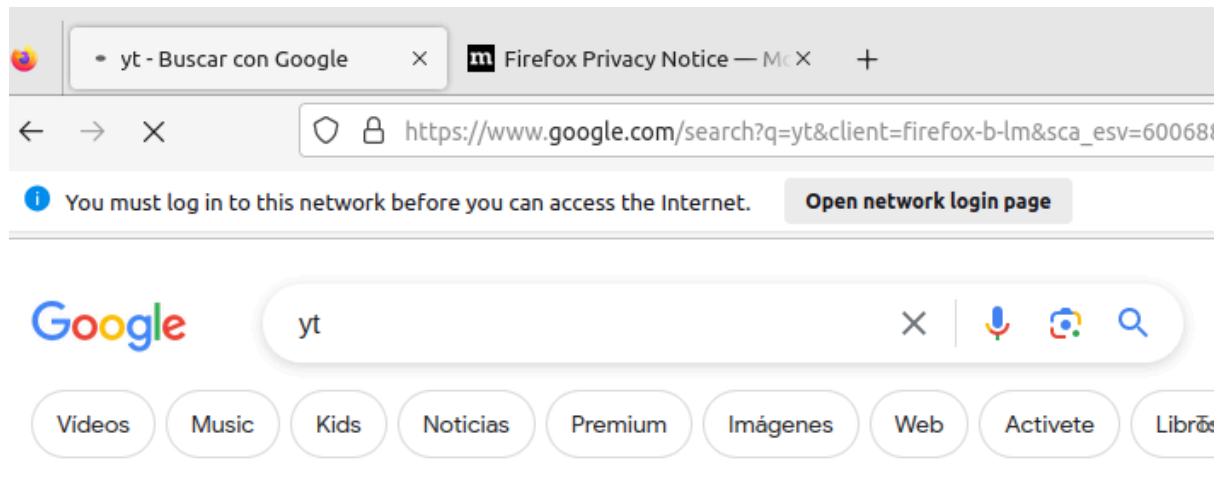
Servidor WINS primario	
Servidor WINS secundario	

Guardando los cambios

Y lo guardamos , ya tendremos configurado nuestro dhcp y ya lo ponemos en ON



Reiniciamos la máquina y comprobamos que tenemos conexión



Aproximadamente 2.370.000.000 resultados (0,25 segundos)



YouTube: Inicio

Pink Floyd - The Wall [Full Album] • Shorts • Compré una FÁBRICA de HELADOS || leo Study .

```
mint@mint:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group 0
    qlen 1000
        link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP
    qlen 1000
        link/ether 00:0c:29:20:89:e4 brd ff:ff:ff:ff:ff:ff
        altname enp2s1
        inet 192.168.11.100/24 brd 192.168.11.255 scope global dynamic noprefixroute
            ens33
```

Configuración de los puertos 3,4,5,6

Puerto 3

Si la de nuestro puerto 1 es la 11.1 esta es la 12.1 y así sucesivamente

Nombre *

Hardware Puerto3

Zona de red

configuración IPv4

asignación de IP Estático PPPoE [DSL] DHCP

IPv4/máscara de red *

Detalle de la puerta de enlace

Nombre de la puerta de enlace

Puerto 4

Nombre *

Hardware Puerto4

Zona de red

configuración IPv4

asignación de IP Estático PPPoE [DSL] DHCP

IPv4/máscara de red *

Detalle de la puerta de enlace

Nombre de la puerta de enlace

IP de acceso

Puerto 5

Nombre *

Hardware Puerto6

Zona de red

configuración IPv4

asignación de IP Estático PPPoE [DSL] DHCP

IPv4/máscara de red *

Detalle de la puerta de enlace

Nombre de la puerta de enlace

Puerto 6

Nombre *	<input type="text" value="Port6"/>																																																						
Hardware	<input type="text" value="Port6"/>																																																						
Zona de red	<input type="text" value="DMZ"/> <input type="button" value="▼"/>																																																						
<input checked="" type="checkbox"/> Configuración IPv4																																																							
Asignación IP																																																							
IPv4/máscara de red *	<input checked="" type="radio"/> Estática <input type="radio"/> PPPoE [DSL] <input type="radio"/> DHCP <input type="text" value="192.168.15.1"/> <input type="text" value="24 [255.255.255.0]"/> <input type="button" value="▼"/>																																																						
Detalle puerta de enlace																																																							
<table border="1"> <thead> <tr> <th colspan="6">Puertas de Enlace</th> </tr> <tr> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> </tr> </thead> <tbody> <tr> <td></td> <td>InvitadoAP Wifi Protección inalámbrica</td> <td>Desenchufado Negociado automáticamente</td> <td>10.255.0.1/255.255.255.0 Estático</td> <td colspan="2">Equipo: GuestAP</td> </tr> <tr> <td></td> <td>Puerto1 LAN Físico</td> <td>Conectado 1000 Mbps - Dúplex completo Negociado automáticamente</td> <td>192.168.11.1/255.255.255.0 Estático</td> <td colspan="2">Equipo: Puerto1</td> </tr> <tr> <td></td> <td>Puerto2 PÁLIDO Físico</td> <td>Conectado 1000 Mbps - Dúplex completo Negociado automáticamente</td> <td>192.168.132.129/255.255.255.0 DHCP</td> <td colspan="2">Hardware: Puerto 2</td> </tr> <tr> <td></td> <td>Puerto3 LAN Físico</td> <td>Conectado 1000 Mbps - Dúplex completo Negociado automáticamente</td> <td>192.168.12.1/255.255.255.0 Estático</td> <td colspan="2">Hardware: Puerto 3</td> </tr> <tr> <td></td> <td>Puerto4 LAN Físico</td> <td>Conectado 1000 Mbps - Dúplex completo Negociado automáticamente</td> <td>192.168.13.1/255.255.255.0 Estático</td> <td colspan="2">Hardware: Puerto 4</td> </tr> <tr> <td></td> <td>Puerto5 LAN Físico</td> <td>Conectado 1000 Mbps - Dúplex completo Negociado automáticamente</td> <td>192.168.14.1/255.255.255.0 Estático</td> <td colspan="2">Hardware: Puerto 5</td> </tr> <tr> <td></td> <td>Puerto6 LAN Físico</td> <td>Conectado 1000 Mbps - Dúplex completo Negociado automáticamente</td> <td>192.168.15.1/255.255.255.0 Estático</td> <td colspan="2">Hardware: Puerto 6</td> </tr> </tbody> </table>		Puertas de Enlace													InvitadoAP Wifi Protección inalámbrica	Desenchufado Negociado automáticamente	10.255.0.1/255.255.255.0 Estático	Equipo: GuestAP			Puerto1 LAN Físico	Conectado 1000 Mbps - Dúplex completo Negociado automáticamente	192.168.11.1/255.255.255.0 Estático	Equipo: Puerto1			Puerto2 PÁLIDO Físico	Conectado 1000 Mbps - Dúplex completo Negociado automáticamente	192.168.132.129/255.255.255.0 DHCP	Hardware: Puerto 2			Puerto3 LAN Físico	Conectado 1000 Mbps - Dúplex completo Negociado automáticamente	192.168.12.1/255.255.255.0 Estático	Hardware: Puerto 3			Puerto4 LAN Físico	Conectado 1000 Mbps - Dúplex completo Negociado automáticamente	192.168.13.1/255.255.255.0 Estático	Hardware: Puerto 4			Puerto5 LAN Físico	Conectado 1000 Mbps - Dúplex completo Negociado automáticamente	192.168.14.1/255.255.255.0 Estático	Hardware: Puerto 5			Puerto6 LAN Físico	Conectado 1000 Mbps - Dúplex completo Negociado automáticamente	192.168.15.1/255.255.255.0 Estático	Hardware: Puerto 6	
Puertas de Enlace																																																							
	InvitadoAP Wifi Protección inalámbrica	Desenchufado Negociado automáticamente	10.255.0.1/255.255.255.0 Estático	Equipo: GuestAP																																																			
	Puerto1 LAN Físico	Conectado 1000 Mbps - Dúplex completo Negociado automáticamente	192.168.11.1/255.255.255.0 Estático	Equipo: Puerto1																																																			
	Puerto2 PÁLIDO Físico	Conectado 1000 Mbps - Dúplex completo Negociado automáticamente	192.168.132.129/255.255.255.0 DHCP	Hardware: Puerto 2																																																			
	Puerto3 LAN Físico	Conectado 1000 Mbps - Dúplex completo Negociado automáticamente	192.168.12.1/255.255.255.0 Estático	Hardware: Puerto 3																																																			
	Puerto4 LAN Físico	Conectado 1000 Mbps - Dúplex completo Negociado automáticamente	192.168.13.1/255.255.255.0 Estático	Hardware: Puerto 4																																																			
	Puerto5 LAN Físico	Conectado 1000 Mbps - Dúplex completo Negociado automáticamente	192.168.14.1/255.255.255.0 Estático	Hardware: Puerto 5																																																			
	Puerto6 LAN Físico	Conectado 1000 Mbps - Dúplex completo Negociado automáticamente	192.168.15.1/255.255.255.0 Estático	Hardware: Puerto 6																																																			

Configuración de DHCP del puerto 3

Creamos una red nueva para este

DHCP	Anuncio de enrutador IPv6	WAN móvil	Túneles IP	Vecinos (ARP-NDP)	DNS dinámico

IPv4	IPv6														
Configuración general															
<p>Nombre * <input type="text" value="LAN12-dhcp"/></p> <p>Interfaz <input type="text" value="Port3 - 192.168.12.1"/></p> <p><input type="checkbox"/> Aceptar solicitud de cliente por retransmisión</p> <p>Concesión IP dinámica</p> <p style="text-align: center;"></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: center;">IP inicial</th> <th style="text-align: center;">IP final</th> <th style="text-align: right; vertical-align: bottom;"><small>+ </small></th> </tr> </thead> <tbody> <tr> <td style="text-align: center;">192.168.12.100</td> <td style="text-align: center;">192.168.12.254</td> <td style="text-align: right; vertical-align: bottom;"><small>- </small></td> </tr> </tbody> </table> <p style="text-align: center;"><small>* Presione Tab para añadir un fila nueva</small></p> <p>Asignación IP estática MAC</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: center;">Nombre de host</th> <th style="text-align: center;">Dirección MAC</th> <th style="text-align: center;">Dirección IP</th> <th style="text-align: right; vertical-align: bottom;"><small>+ </small></th> </tr> </thead> <tbody> <tr> <td style="text-align: center;"></td> <td style="text-align: center;"></td> <td style="text-align: center;"></td> <td style="text-align: right; vertical-align: bottom;"><small>- </small></td> </tr> </tbody> </table> <p style="text-align: center;"><small>* Presione Tab para añadir un fila nueva</small></p> <p>Máscara de subred * <input type="text" value="/24 [255.255.255.0]"/></p> <p>Nombre dominio <input type="text"/></p> <p>Puerta de enlace * <input checked="" type="checkbox"/> Usar IP de interfaz como puerta de enlace</p>		IP inicial	IP final	<small>+ </small>	192.168.12.100	192.168.12.254	<small>- </small>	Nombre de host	Dirección MAC	Dirección IP	<small>+ </small>				<small>- </small>
IP inicial	IP final	<small>+ </small>													
192.168.12.100	192.168.12.254	<small>- </small>													
Nombre de host	Dirección MAC	Dirección IP	<small>+ </small>												
			<small>- </small>												
<p>Puerta de enlace * <input checked="" type="checkbox"/> Usar IP de interfaz como puerta de enlace</p> <p>192.168.12.1</p> <p>Tiempo de concesión predeterminado * <input type="text" value="1440"/> 1-43200 minutos (30 días)</p> <p>Tiempo de concesión máx. * <input type="text" value="2880"/> 1-43200 minutos (30 días)</p> <p>Detección de conflictos <input checked="" type="checkbox"/> Activar</p>															
Servidor DNS															
<p><input type="checkbox"/> Usar configuración DNS de dispositivo</p> <p>DNS primario <input type="text" value="192.168.12.1"/></p> <p>DNS secundario <input type="text" value="9.9.9"/></p>															
Servidor WINS															
<p>Servidor WINS primario</p> <p style="background-color: #e0e0e0; padding: 5px; border-radius: 5px;"><input type="button" value="Guardar"/> <input type="button" value="Cancelar"/></p>															

Guardamos

Nombre	Interfaz	Detalles de concesión	Versión IP	Estado
		Dinámica	Estática	
Default_DHCP_Server	Port1 - 192.168.11.1	192.168.11.100 - 192.168.11.199	-	IPv4 <input checked="" type="checkbox"/>
GuestAccess_DHCP	GuestAP - 10.255.0.1	10.255.0.2 - 10.255.0.254	-	IPv4 <input checked="" type="checkbox"/>
LAN12-dhcp	Port3 - 192.168.12.1	192.168.12.100 - 192.168.12.254	-	IPv4 <input checked="" type="checkbox"/>

Reglas de FW

Reglas de inspección SSL/TLS

Añadir regla de firewall ▾

Desactivar Eliminar Restablecer filtro

Nueva regla de firewall

Asistente de acceso al servidor [DNAT]

Añadir regla de firewall

Estado de la regla

Nombre de regla *

Descripción

Acción

Aceptar

Registrar tráfico de firewall
Registra el tráfico que coincide con esta regla de firewall en el dispositivo (por defecto) o en el servidor syslog configurado.

Nombre de la regla *	lan-wan
----------------------	---------

Posición de regla

Arriba



Grupo de reglas

Traffic to WAN



ORIGEN

Añadimos dispositivos , para que solo se puedan conectar los dispositivos con esas características .

Fuente

Seleccione las zonas, redes y dispositivos de origen.

La regla se aplica al tráfico de estas fuentes durante el período de tiempo programado.

Zonas de origen *

LAN	
agregar ítem nuevo	

Redes y dispositivos de origen *

<input type="button" value="Agregar"/>
Todos los tipos
<input type="checkbox"/> Cualquier
<input type="checkbox"/> *.api.filepicker
<input type="checkbox"/> *.apple.com
<input type="checkbox"/> *.assist.com
<input type="checkbox"/> *.box.com
<input type="checkbox"/> *.box.net
<input type="checkbox"/> *.boxcdn.net
<input type="checkbox"/> *.boxcloud.co
<input type="checkbox"/> *.boxlocalhos
<input type="checkbox"/> *.citrixonline.c
<input type="checkbox"/> *.citrixonlinecl
Grupo de países
anfitrión FQDN
Grupo de host FQDN
Grupo anfitrión
IP
Lista de direcciones IP
rango de IP
Dirección MAC
lista de MAC
Red

Destino y servicios

Seleccione las zonas, redes, dispositivos y servicios de destino.

La regla se aplica al tráfico hacia estos destinos.

Zonas de destino *

agregar ítem nuevo

Emparejar usuarios conocidos

Editar red

Nombre *

LAN-11

versión IP *

IPv4

Tipo *

Red

dirección IP *

192.168.11.0

Subred

/24 [255.255.255.0]



grupo de hosts IP

agregar ítem nuevo

Guardar

cancelar

Nombre *

versión IP *

Tipo *

dirección IP * Subred

grupo de hosts IP

Guardar [cancelar](#)

Zonas de origen * [Añadir nuevo elemento](#)

Dispositivos y redes de origen * [Añadir nuevo elemento](#)

Durante la hora programada Seleccione para aplicar la regla a un período de tiempo y día de la semana específicos.

Destino y servicios
 Seleccione las zonas, redes, dispositivos y servicios de destino.
 La regla se aplica al tráfico hacia estos destinos.

Zonas de destino * [Añadir nuevo elemento](#)

Redes de destino * [Añadir nuevo elemento](#)

Servicios * [Añadir nuevo elemento](#)

Los servicios son tipos de tráfico basados en una combinación de protocolos y puertos.

Guardamos

y desactivamos esta regla , ya que está puesta para todos los host , por lo que por ahora no le vamos a dar uso

<input type="checkbox"/> <input type="button" value="+"/> <input type="file"/> 1 Traffic to DMZ in 0 B, out 0 B	Inbound traffic to DMZ. Firewall rules with the destination zone as DMZ would be added to this group on the first match basis if user selects automatic grouping option. This is the de...	<input type="checkbox"/> <input type="button" value="Edit"/> <input type="checkbox"/> <input type="button" value="Move to position"/> <input type="checkbox"/> <input type="button" value="Clone rule above"/> <input type="checkbox"/> <input type="button" value="Clone rule below"/> <input type="checkbox"/> <input type="button" value="Add rule above"/> <input type="checkbox"/> <input type="button" value="Add rule below"/> <input type="checkbox"/> <input type="button" value="Reset data transfer count"/> <input type="checkbox"/> <input type="button" value="LinkedNAT"/> <input type="checkbox"/> <input type="button" value="PRX LOG"/> <input type="checkbox"/> <input type="button" value="..."/>
<input type="checkbox"/> 5 <input type="button" value="Auto added firewall policy for MTA"/> 5 in 0 B, out 0 B	Any zone, Any host Any zone, Any host SMTP, SMTP(S) #1 Accept	<input type="checkbox"/> <input type="button" value="IPS"/> <input type="checkbox"/> <input type="button" value="AV"/> <input type="checkbox"/> <input type="button" value="WEB"/> <input type="checkbox"/> <input type="button" value="APP"/> <input type="checkbox"/> <input type="button" value="QoS"/> <input type="checkbox"/> <input type="button" value="HB"/> <input type="checkbox"/> <input type="button" value="LinkedNAT"/> <input type="checkbox"/> <input type="button" value="PRX LOG"/> <input type="checkbox"/> <input type="button" value="..."/>
<input type="checkbox"/> 6 <input type="button" value="#Default_Network_Policy"/> 6 in 6.6 KB, out 5.70 KB	LAN, Any host WAN, Any host Any service #5 Accept	<input type="checkbox"/> <input type="button" value="IPS"/> <input type="checkbox"/> <input type="button" value="AV"/> <input type="checkbox"/> <input type="button" value="WEB"/> <input type="checkbox"/> <input type="button" value="APP"/> <input type="checkbox"/> <input type="button" value="QoS"/> <input type="checkbox"/> <input type="button" value="HB"/> <input type="checkbox"/> <input type="button" value="LinkedNAT"/> <input type="checkbox"/> <input type="button" value="PRX LOG"/> <input type="checkbox"/> <input type="button" value="..."/>
<input type="checkbox"/> 7 <input type="button" value="Drop all"/> 7 in 0 B, out 0 B	Any zone, Any host Any zone, Any host Any service #0 Drop	<input type="checkbox"/> <input type="button" value="Edit"/> <input type="checkbox"/> <input type="button" value="Move to position"/> <input type="checkbox"/> <input type="button" value="Clone rule above"/> <input type="checkbox"/> <input type="button" value="Clone rule below"/> <input type="checkbox"/> <input type="button" value="Add rule above"/> <input type="checkbox"/> <input type="button" value="Add rule below"/> <input type="checkbox"/> <input type="button" value="Reset data transfer count"/> <input type="checkbox"/> <input type="button" value="LinkedNAT"/> <input type="checkbox"/> <input type="button" value="PRX LOG"/> <input type="checkbox"/> <input type="button" value="..."/>
Showing 7 of 7. Selected 0		
Sophos Assistant		

y activamos

#	Name	Source	Destination	What	ID	Action	Feature and service
<input type="checkbox"/> <input type="button" value="Traffic to Internal Zones"/> 1 in 0 B, out 0 B	To LAN, WiFi, VPN, DMZ. Firewall rules with the destination zone as LAN, WiFi, VPN, DMZ would be added to this group on the first match basis if user selects automatic grouping option...					<input type="checkbox"/> <input type="button" value="Edit"/> <input type="checkbox"/> <input type="button" value="Move to position"/> <input type="checkbox"/> <input type="button" value="Clone rule above"/> <input type="checkbox"/> <input type="button" value="Clone rule below"/> <input type="checkbox"/> <input type="button" value="Add rule above"/> <input type="checkbox"/> <input type="button" value="Add rule below"/> <input type="checkbox"/> <input type="button" value="Reset data transfer count"/> <input type="checkbox"/> <input type="button" value="LinkedNAT"/> <input type="checkbox"/> <input type="button" value="PRX LOG"/> <input type="checkbox"/> <input type="button" value="..."/>	
<input type="checkbox"/> <input type="button" value="Traffic to WAN"/> 2 in 0 B, out 0 B	Outbound traffic to WAN. Firewall rules with the destination zone as WAN would be added to this group on the first match basis if user selects automatic grouping option. This is the de...					<input type="checkbox"/> <input type="button" value="Edit"/> <input type="checkbox"/> <input type="button" value="Move to position"/> <input type="checkbox"/> <input type="button" value="Clone rule above"/> <input type="checkbox"/> <input type="button" value="Clone rule below"/> <input type="checkbox"/> <input type="button" value="Add rule above"/> <input type="checkbox"/> <input type="button" value="Add rule below"/> <input type="checkbox"/> <input type="button" value="Reset data transfer count"/> <input type="checkbox"/> <input type="button" value="LinkedNAT"/> <input type="checkbox"/> <input type="button" value="PRX LOG"/> <input type="checkbox"/> <input type="button" value="..."/>	
<input type="checkbox"/> 2 <input type="button" value="WAN-para-Linux"/> 2 in 0 B, out 0 B	LAN, LAN-11, LAN-12 WAN, Any host HTTP, HTTPS #6 Accept					<input type="checkbox"/> <input type="button" value="Edit"/> <input type="checkbox"/> <input type="button" value="Move to position"/> <input type="checkbox"/> <input type="button" value="Clone rule above"/> <input type="checkbox"/> <input type="button" value="Clone rule below"/> <input type="checkbox"/> <input type="button" value="Add rule above"/> <input type="checkbox"/> <input type="button" value="Add rule below"/> <input type="checkbox"/> <input type="button" value="Reset data transfer count"/> <input type="checkbox"/> <input type="button" value="LinkedNAT"/> <input type="checkbox"/> <input type="button" value="PRX LOG"/> <input type="checkbox"/> <input type="button" value="..."/>	
<input type="checkbox"/> 3 <input type="button" value="example) Traffic to WAN"/> 3 in 0 B, out 0 B	Any zone, Any host WAN, Any host Any service #3 Drop					<input type="checkbox"/> <input type="button" value="Edit"/> <input type="checkbox"/> <input type="button" value="Move to position"/> <input type="checkbox"/> <input type="button" value="Clone rule above"/> <input type="checkbox"/> <input type="button" value="Clone rule below"/> <input type="checkbox"/> <input type="button" value="Add rule above"/> <input type="checkbox"/> <input type="button" value="Add rule below"/> <input type="checkbox"/> <input type="button" value="Reset data transfer count"/> <input type="checkbox"/> <input type="button" value="LinkedNAT"/> <input type="checkbox"/> <input type="button" value="PRX LOG"/> <input type="checkbox"/> <input type="button" value="..."/>	
<input type="checkbox"/> <input type="button" value="Traffic to DMZ"/> 1 in 0 B, out 0 B	Inbound traffic to DMZ. Firewall rules with the destination zone as DMZ would be added to this group on the first match basis if user selects automatic grouping option. This is the de...					<input type="checkbox"/> <input type="button" value="Edit"/> <input type="checkbox"/> <input type="button" value="Move to position"/> <input type="checkbox"/> <input type="button" value="Clone rule above"/> <input type="checkbox"/> <input type="button" value="Clone rule below"/> <input type="checkbox"/> <input type="button" value="Add rule above"/> <input type="checkbox"/> <input type="button" value="Add rule below"/> <input type="checkbox"/> <input type="button" value="Reset data transfer count"/> <input type="checkbox"/> <input type="button" value="LinkedNAT"/> <input type="checkbox"/> <input type="button" value="PRX LOG"/> <input type="checkbox"/> <input type="button" value="..."/>	
<input type="checkbox"/> 5 <input type="button" value="Auto added firewall policy for MTA"/> 5 in 0 B, out 0 B	Any zone, Any host Any zone, Any host SMTP, SMTP(S) #1 Accept					<input type="checkbox"/> <input type="button" value="Edit"/> <input type="checkbox"/> <input type="button" value="Move to position"/> <input type="checkbox"/> <input type="button" value="Clone rule above"/> <input type="checkbox"/> <input type="button" value="Clone rule below"/> <input type="checkbox"/> <input type="button" value="Add rule above"/> <input type="checkbox"/> <input type="button" value="Add rule below"/> <input type="checkbox"/> <input type="button" value="Reset data transfer count"/> <input type="checkbox"/> <input type="button" value="LinkedNAT"/> <input type="checkbox"/> <input type="button" value="PRX LOG"/> <input type="checkbox"/> <input type="button" value="..."/>	

Dentro de esa regla (WAN-PARA-LINUX) vamos a cambiar y añadir

ON Rule status

Rule name * WAN-para-Lan1-2

Description Regla para acceder a internet desde LAN11-12

Action Accept

Log firewall traffic
Logs traffic, matching this firewall rule, on the appliance [by default] or on the configured syslog server.

Añadimos un grupo

Añadir grupo de servicio

Nombre * INTERNET-BASICO

Descripción PUERTOS DE INTERNET BASICOS POR DEFECTO

Seleccionar servicio *

POP3
POP3S
SMTP
SMTP(S)
SMTPS_465
SSH

Añadir nuevo elemento

Guardar Cancelar

Services *

DNS		
FTP		
HTTP		
HTTPS		
IMAP		
IMAPS		
NNTP		

Add new item

Services *

NNTP		
NTP		
PING		
POP3		
SMTP		
SMTP(S)		

SMTPS_465
Add new item
Services are traffic types based on a combination of protocols and ports.

PING
POP3
SMTP
SMTP[S]
SMTPS_465
SSH

Add new item

Services are traffic types based on a combination of protocol and ports.

Añadimos un servicio

Add service

Name * PLESK

Type * TCP/UDP IP ICMP ICMPv6

protocol	Source port	Destination port	
TCP	1:65535	8443	+

Save Cancel

Y lo guardamos

Configuración de dhcp

Nos vamos a nuestro linux , lo actualizamos y vemos la ip.

```
mint@mint:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    qlen 1000
        link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel
    qlen 1000
        link/ether 00:0c:29:20:89:e4 brd ff:ff:ff:ff:ff:ff
        altname enp2s1
        inet 192.168.11.100/24 brd 192.168.11.255 scope global dynamic
          ens33
            valid_lft 82862sec preferred_lft 82862sec
        inet6 fe80::e013:5f92:7a85:8960/64 scope link
           valid_lft forever preferred_lft forever
```

Ahora nos vamos al dhcp y añadimos

Name	Interface	Lease detail
<u>Default DHCP Server</u>	Port1 - 192.168.11.1	Dynamic 192.168.11.100 - 192.168.11.199 View detail
<u>GuestAccess DHCP</u>	GuestAP - 10.255.0.1	10.255.0.2 - 10.255.0.254 -
<u>LAN12-dhcp</u>	Port3 - 192.168.12.1	192.168.12.100 - 192.168.12.254 -

Start IP: 192.168.11.100 End IP: 192.168.11.199

Hostname: LINUX-PACO MAC address: 00:0c:29:20:89:E4 IP address: 192.168.11.99

```
mint@mint:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    qlen 1000
        link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel
    qlen 1000
        link/ether 00:0c:29:20:89:e4 brd ff:ff:ff:ff:ff:ff
        altname enp2s1
        inet 192.168.11.100/24 brd 192.168.11.255 scope global dynamic
          ens33
            valid_lft 82862sec preferred_lft 82862sec
        inet6 fe80::e013:5f92:7a85:8960/64 scope link
           valid_lft forever preferred_lft forever
mint@mint:~$
```

Ahora nos vamos a nuestro linux , hacemos un apt upgrade y update, una vez hecho ponemos el ethernet 12 y luego otra vez el 11 y ya tendria que aparecer esta ip .

```
mint@mint:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP
    link/ether 00:0c:29:20:89:e4 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.11.99/24 brd 192.168.11.255 scope global dynamic noprefixroute
        ens33
            valid_lft 86397sec preferred_lft 86397sec
        inet6 fe80::e013:5f92:7a85:8960/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
mint@mint:~$ apt update
```

Una vez actualizado hemos un :
apt autoclear
apt autoremove

Vamos a crear una regla para el windows Server

The screenshot shows a network management interface for creating a new firewall rule. The top navigation bar includes tabs for Firewall rules, NAT rules, and SSL/TLS inspection rules. Below the tabs, there are buttons for IPv4, IPv6, and Disable filter. A prominent 'Add firewall rule' button is located in the top right corner. A context menu is open over the 'Add firewall rule' button, with the option 'New firewall rule' highlighted.

Firewall rules

IPv4 **IPv6** **Disable filter**

Add firewall rule **Disable**

New firewall rule

Server access assistant (DNAT)

Rule type **Source zone** **Destination zone** **Status**

#	Name	Source	Destination	What
1	Traffic to Internal Zones in 0 B, out 0 B	To LAN, WiFi, VPN, DMZ.	Firewall rules with the destination zone as LAN, WiFi, VPN, DMZ would be added to this group on the first match basis if user selects automatic grouping option...	
2	Traffic to WAN in 0 B, out 0 B	Outbound traffic to WAN.	Firewall rules with the destination zone as WAN would be added to this group on the first match basis if user selects automatic grouping option. This is the d...	

Rule status **ON**

Rule name * **WAN-LAN13**

Action **Accept**

Description **INTERNET PARA LAN13 WINSERV**

Rule position **Bottom**

Rule group **Traffic to WAN**

Log firewall traffic Logs traffic, matching this firewall rule, on the appliance (by default) or on the configured syslog server.

Source
Select the source zones, networks, and devices.
The rule applies to traffic from these sources during the scheduled time period.

Source zones * **WAN**

Source networks and devices * **LAN13**

During scheduled time **All the time**

Source networks and devices :

The screenshot shows a 'Edit Network' dialog box. At the top left is a 'Save' button. The main area contains fields for Name, IP version, Type, IP address, and Subnet. The 'Name' field is set to 'LAN13'. The 'IP version' is 'IPv4'. The 'Type' is 'Network'. The 'IP address' is '192.168.13.0' and the 'Subnet' is '/24 (255.255.255.0)'. There is also a 'IP host group' section with an 'Add new item' button.

Edit Network

Name * **LAN13**

IP version * **IPv4**

Type * **Network**

IP address * **192.168.13.0** **Subnet** **/24 (255.255.255.0)**

IP host group

Add new item

Save **Cancel**

Destination and services

Select the destination zones, networks, devices, and services.

The rule applies to traffic to these destinations.

Destination zones *

WAN	
Add new item	

Destination networks *

Any	
Add new item	

Services *

Internet-Basico		
Add new item		

Services are traffic types based on a combination of protocols and ports.

Match known users

Y guardamos

Copia de seguridad

Es importante cada paso que vayamos haciendo hacer una copia

Reports
Zero-day protection
Diagnostics

PROTECT
Rules and policies
Intrusion prevention
Web
Applications
Wireless
Email
Web server
Active threat response

CONFIGURE
Remote access VPN
Site-to-site VPN
Network
Routing
Authentication
System services

SYSTEM
Sophos Central
Profiles
Hosts and services
Administration
Backup & firmware
Certificates

Backup

Backup mode
 Local FTP Email

Backup prefix
Cesur-23-24

Frequency
 Never Daily Weekly Monthly

Encryption password *

.....
.....

[Apply](#) **Backup now**

Backup restore

Restore configuration
 Seleccionar archivo | Ninguno archivo selec.

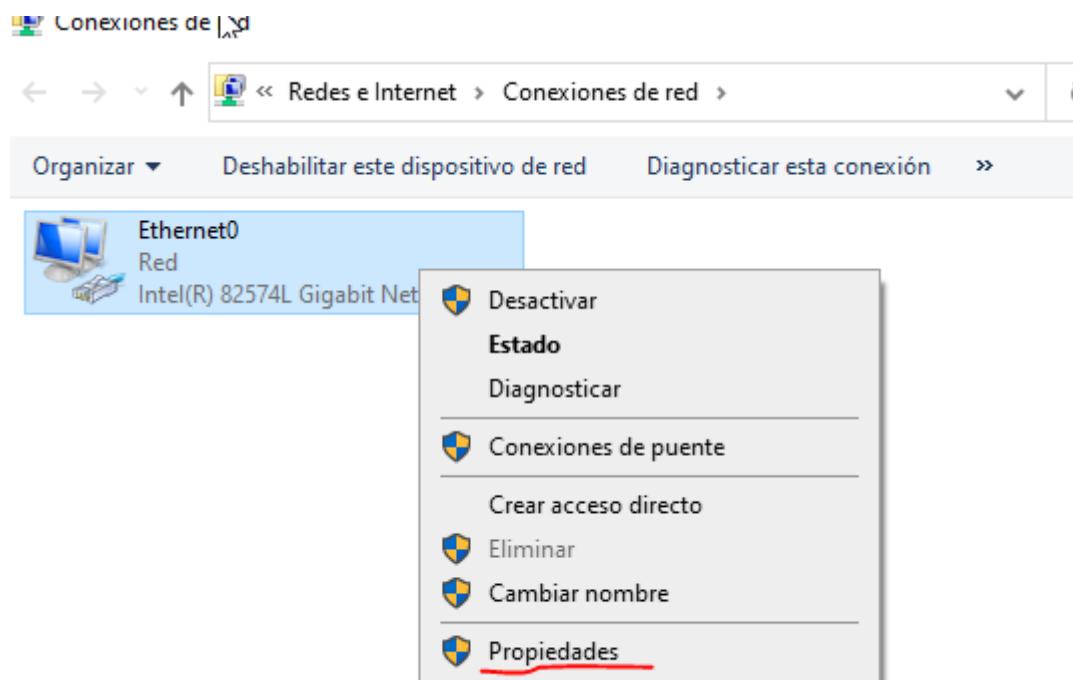
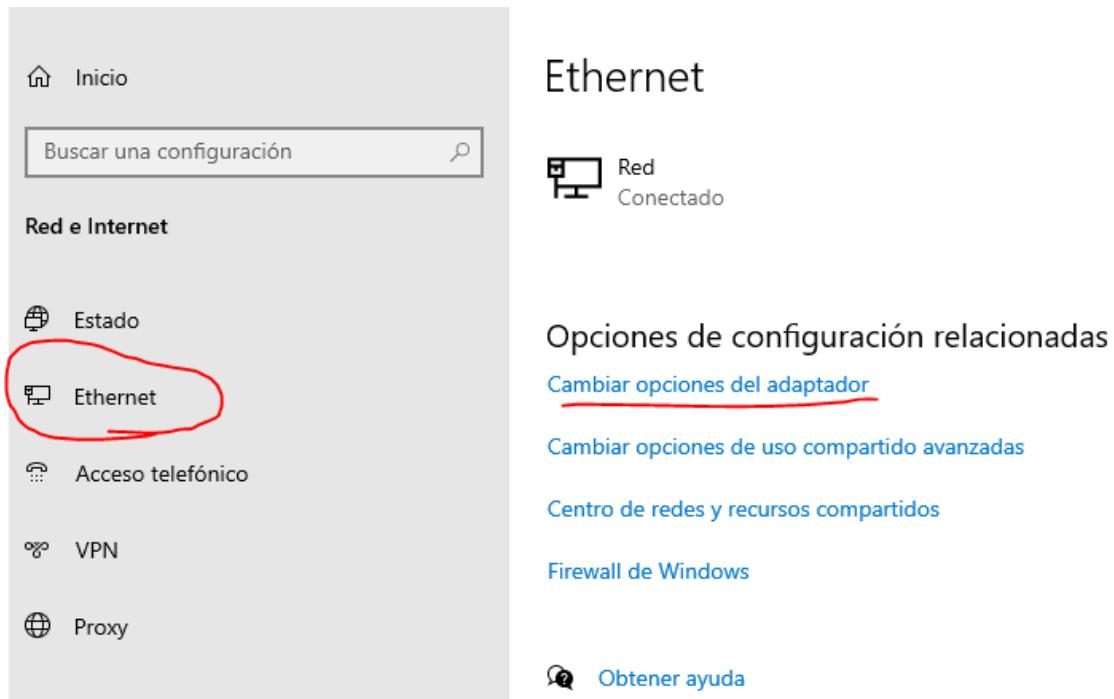
Encryption password

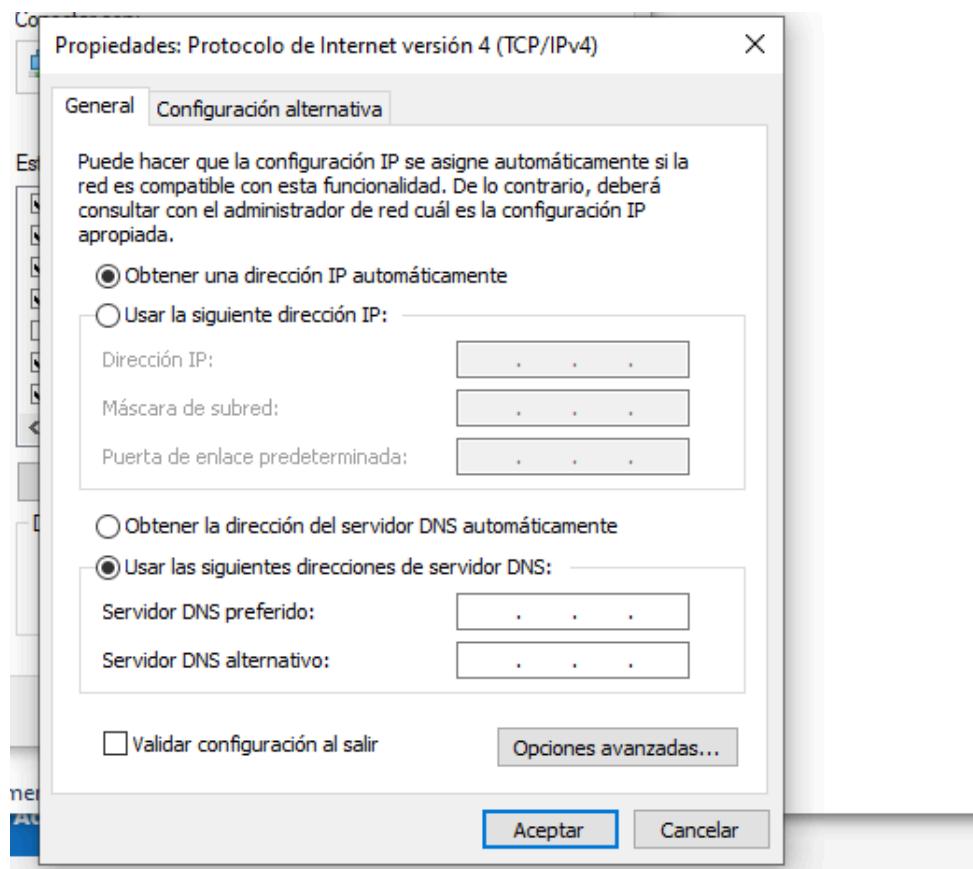
[Upload and restore](#)

Configuración Windows (12)

Vamos a levantar un windows

Nos vamos:





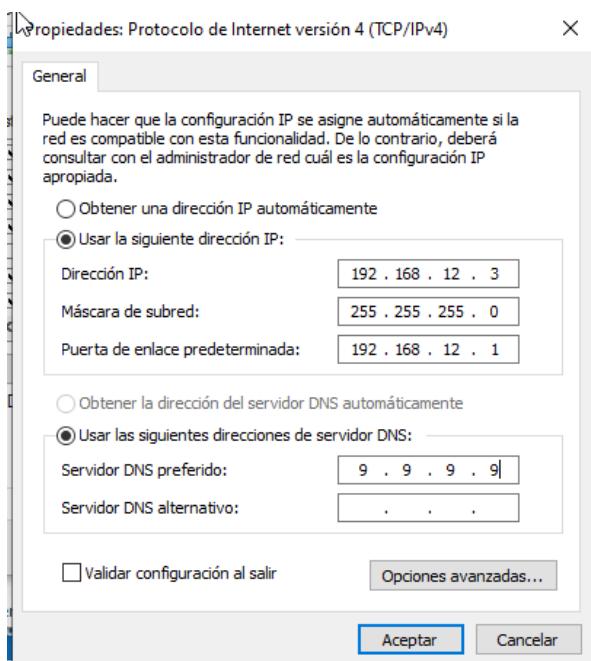
Puedes escoger una ip automática , en mi caso te dará la 192.168.12.100

```
C:\Users\paco>ipconfig
Configuración IP de Windows

Adaptador de Ethernet Ethernet0:
  Sufijo DNS específico para la conexión. . . :
  Vínculo: dirección IPv6 local. . . : fe80::ede4:697e:2db2:4abb%14
  Dirección IPv4. . . . . : 192.168.12.100
  Máscara de subred . . . . . : 255.255.255.0
  Puerta de enlace predeterminada . . . . : 192.168.12.1

C:\Users\paco>
```

Pero en mi caso prefiero meterla yo a mano y ponerme la 12.3



```
C:\Users\paco>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet0:

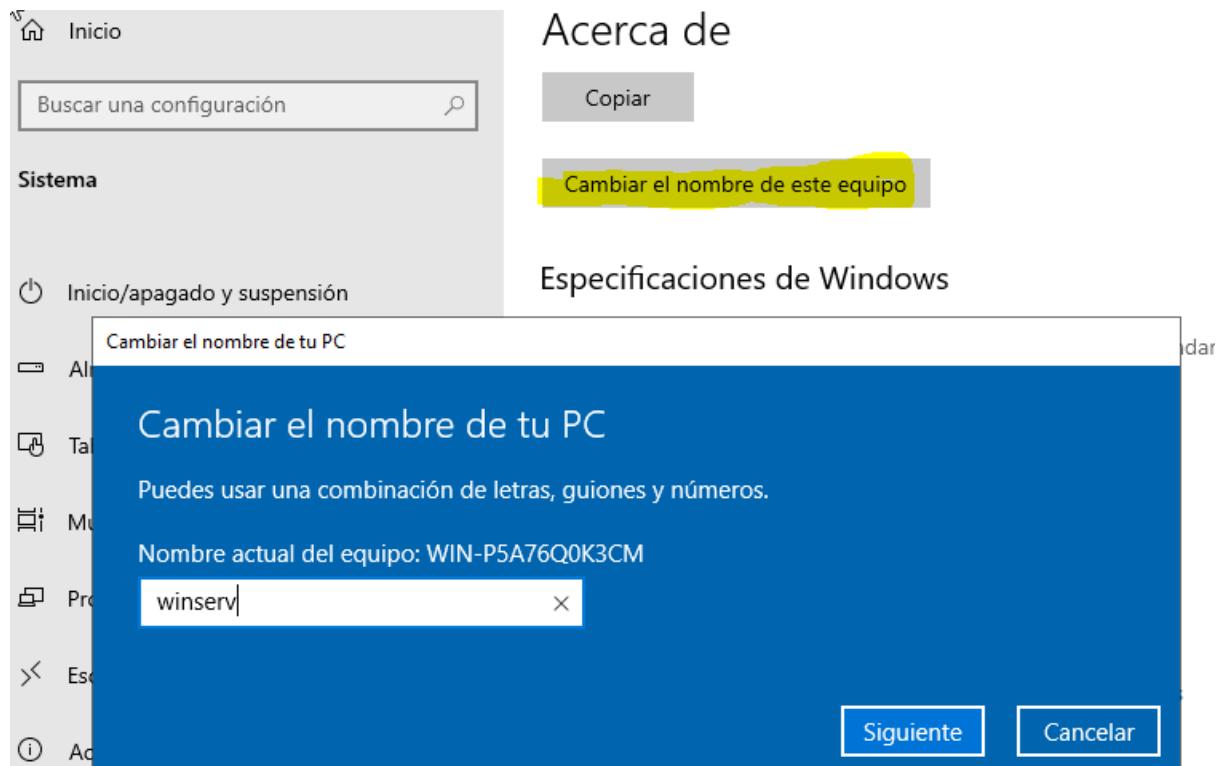
    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::ede4:697e:2db2:4abb%14
    Dirección IPv4. . . . . : 192.168.12.3
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . : 192.168.12.1

C:\Users\paco>
```

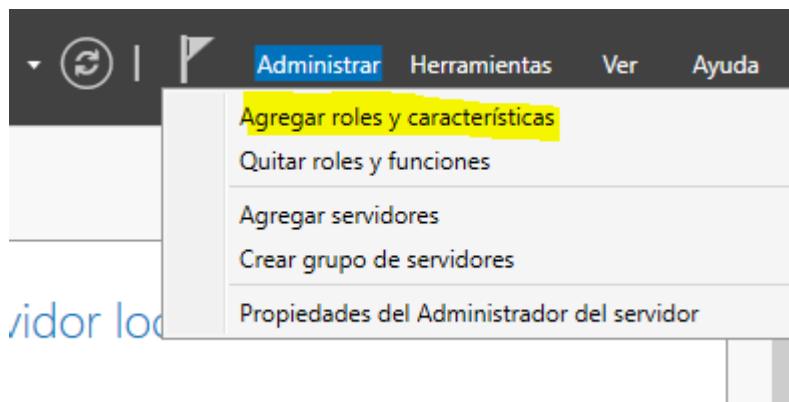
Comprueba si tienes internet (busca algo en google) si tienes ya lo tendrás configurado .

Configuración Windows Server (13)

Lo primero que hacemos es cambiar el nombre de nuestro pc para poder detectarlo .Reinicacionmos al cambiarlo



Ahora empezamos con la configuración de AD

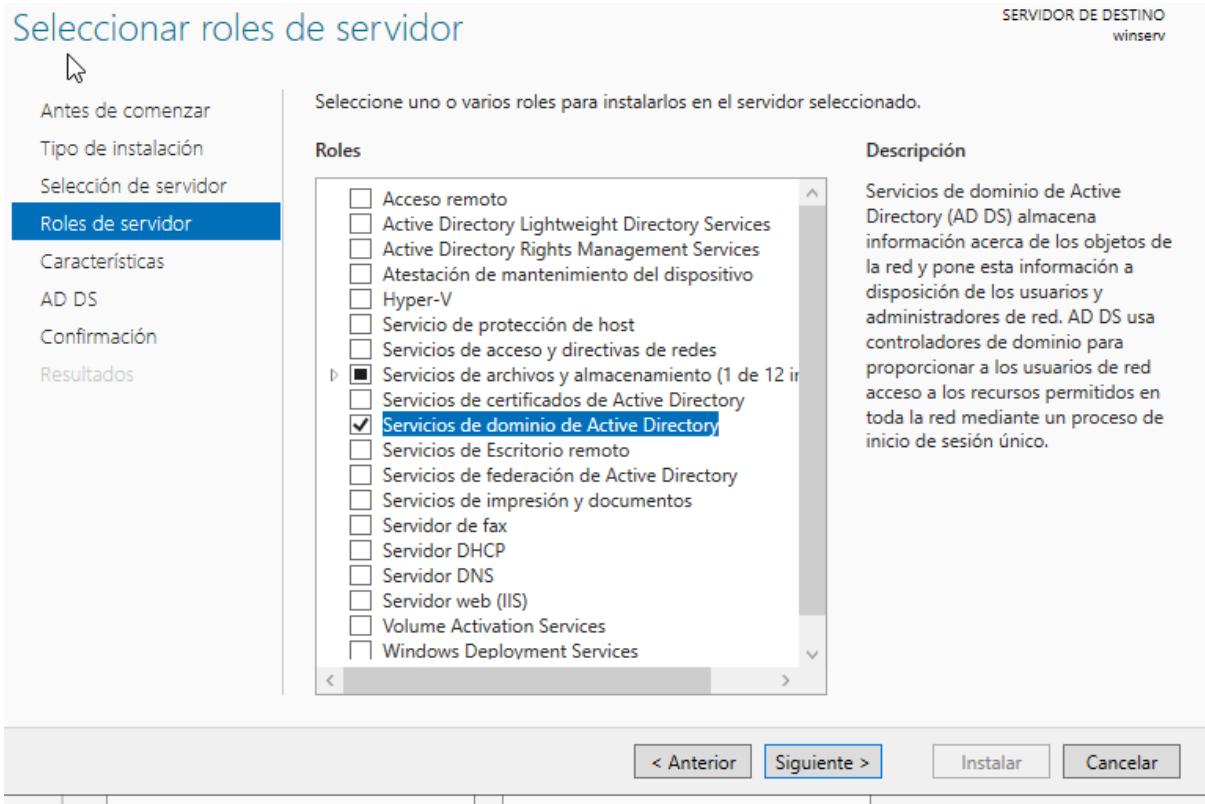


Antes de comenzar

SERVIDOR DE DESTINO
winserv

Antes de comenzar	<p>Este asistente le ayuda a instalar roles, servicios de rol o características. Podrá elegir qué roles, servicios de rol o características desea instalar según las necesidades de los equipos de la organización, como compartir documentos u hospedar un sitio web.</p> <p>Para quitar roles, servicios de rol o características: Iniciar el Asistente para quitar roles y características</p> <p>Antes de continuar, compruebe que se han completado las siguientes tareas:</p> <ul style="list-style-type: none">• La cuenta de administrador tiene una contraseña segura• Las opciones de red, como las direcciones IP estáticas, están configuradas• Las actualizaciones de seguridad más recientes de Windows Update están instaladas <p>Si debe comprobar que se ha completado cualquiera de los requisitos previos anteriores, cierre el asistente, complete los pasos y, después, ejecute de nuevo el asistente.</p> <p>Haga clic en Siguiente > para continuar.</p>
<input checked="" type="checkbox"/> Omitir esta página de manera predeterminada	
< Anterior Siguiente > Instalar Cancelar	

Dejamos los siguientes pasos por defecto , hasta



Aquí agregamos roles y características

Los demás pasos los dejamos por defecto y lo instalamos .

Luego acabamos de instalarlos lo .

Configuración

Lo primero comprobar en el sophos que la ip del puerto 4 (192.168.13.1) , que en mi caso es Static

IPv4 configuration

IP assignment Static PPPoE [DSL] DHCP

IPv4/netmask * /24 [255.255.255.0]

Gateway detail
Gateway name

Una vez comprobado nos vamos al winSerer a :



The screenshot shows the Windows Network and Sharing Center. On the left, there's a sidebar with icons for Estado, Ethernet, Acceso telefónico, VPN, and Proxy. The main area is titled "Red e Internet" and shows the "Ethernet" connection status: "Identificando..." and "Conectado". To the right, under "Opciones de configuración relacionadas", several links are listed: "Cambiar opciones del adaptador" (highlighted in yellow), "Cambiar opciones de uso compartido avanzadas", "Centro de redes y recursos compartidos", and "Firewall de Windows".

Ethernet

Identificando...
Conectado

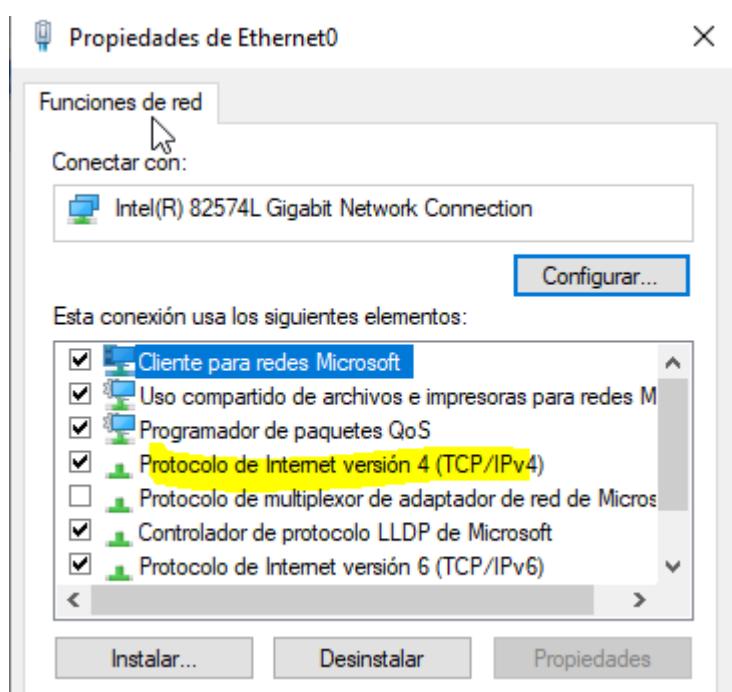
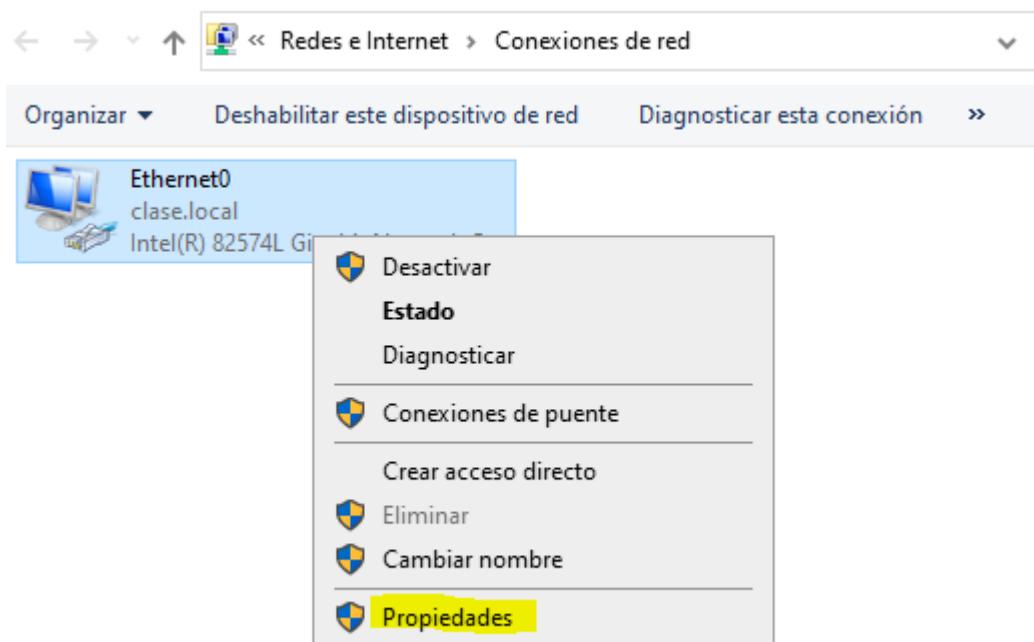
Opciones de configuración relacionadas

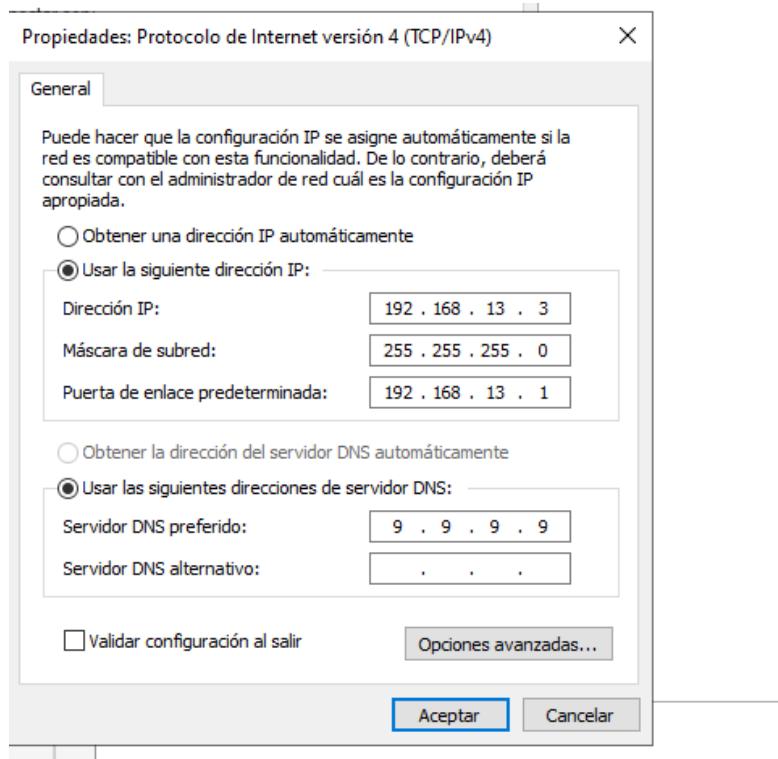
Cambiar opciones del adaptador

Cambiar opciones de uso compartido avanzadas

Centro de redes y recursos compartidos

Firewall de Windows





Aquí vamos a poner la dirección ip que queramos , dentro de nuestro rango , la puerta de enlace de nuestro puerto 1 y el dns , yo he puesto este porque he querido , podrías poner 1111.

Si nos ha salido bien : (metete en internet y comprueba si tienes)

Firewall de Microsoft Defender	Dominio: Activado	Antivirus de Microsoft Defender	Pro
Administración remota	Habilitado	Comentarios y diagnósticos	Cor
Escritorio remoto	Deshabilitado	Configuración de seguridad mejorada de IE	Act
Formación de equipos de NIC	Deshabilitado	Zona horaria	(UT
Ethernet0	192.168.13.3, IPv6 habilitado	Id. del producto	004

Versión del sistema operativo	Microsoft Windows Server 2022 Standard Evaluation	Procesadores	Inte
Información de hardware	VMware, Inc. VMware20,1	Memoria instalada (RAM)	4 G
		Espacio total en disco	59,3

EVENTOS

Todos los eventos | 41 en total

Nombre del servidor	Id.	Gravedad	Origen	Registro	Fecha y hora
WINSERV	12	Advertencia	Microsoft-Windows-Time-Service	Sistema	24/01/2024 9:31
WINSERV	5782	Advertencia	NETLOGON	Sistema	24/01/2024 9:31
WINSERV	27	Advertencia	e1i68x64	Sistema	24/01/2024 9:31

Configuración debian (15)

Primero vamos a crear una regla

ON Rule status

Rule name * DNAT to 192.168.15.10

Description Enter Description

Rule position Top

Action Accept

Log firewall traffic
Logs traffic, matching this firewall rule, on the appliance (by default) or on the configured syslog server.

Source zones * WAN Add new item

Source networks and devices * Any Add new item

During scheduled time All the time
Select to apply the rule to a specific time period and day of the week.

Destination and services
Select the destination zones, networks, devices, and services.
The rule applies to traffic to these destinations.

Destination zones * DMZ Add new item

Destination networks * #Port2 Add new item

Services * HTTP SSH Add new item
Services are traffic types based on a combination of protocols and ports.

Y esta regla también

ON Rule status

Rule name * DMZ-A-WAN

Description DMZ A WAN

Rule position Bottom

Action Accept

Log firewall traffic
Logs traffic, matching this firewall rule, on the appliance (by default) or on the configured syslog server.

Source zones * DMZ Add new item

Source networks and devices * DMZ-15 Add new item

During scheduled time All the time
Select to apply the rule to a specific time period and day of the w

Destination and services
Select the destination zones, networks, devices, and services.
The rule applies to traffic to these destinations.

Destination zones * WAN Add new item

Destination networks * Any Add new item

Services * Internet-DMZ Add new item
Services are traffic types based on a combination of protocols ar

Name *

Description

Select service * DNS FTP HTTP HTTPS NNTP NTP

Y también

NAT rules SSL/TLS inspection rules

Add firewall rule Disable

Status Rule ID

destination What New firewall rule

Server access assistant [DNAT]

Internal server IP address

Specify the private IP address of the internal server to access from the internet.

Select IP host

192.168.15.10 (Creates an IP host with the specified IP address ar

IP hostname

Server access assistant [DNAT]

Public IP address

Specify the public IP address through which users can access the server.

#Port2 - 192.168.132.129

Type IP [Creates an IP host with the specified IP address and name.]

[Cancel](#) [2 of 5](#) [Back](#) [Next](#)

Services

Users can access the selected services on the internal server.

HTTP	<input type="button" value="-"/>
HTTPS	<input type="button" value="-"/>
SSH	<input type="button" value="-"/>
Add new item	

External source networks and devices

Users can access the internal server from the selected source networks and devices.

Any	<input type="button" value="-"/>
Add new item	

[Cancel](#) [4 of 5](#) [Back](#) [Next](#)

Primero la montamos :

Hardware

The screenshot shows the 'Hardware' configuration window for a virtual machine. On the left, a list of device configurations is shown:

Device	Summary
Memory	1 GB
Processors	2
New CD/DVD (IDE)	Using file C:\Users\Francisco...
Network Adapter	Custom (VMnet15)
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

On the right, the 'Device status' section has the 'Connect at power on' checkbox checked. The 'Network connection' section shows 'Custom: Specific virtual network' selected, with 'VMnet15' chosen from a dropdown menu. Buttons for 'Configure Adapters', 'LAN Segments...', and 'Advanced...' are also present.

Configurar la red

Desde aquí puede intentar reintentar la configuración automática de la red a través de DHCP (lo que puede funcionar si su servidor de DHCP tarda mucho en responder) o configurar la red manualmente. Puede también reintentar la configuración automática de red introduciendo un nombre de máquina, algunos servidores exigen que el cliente de DHCP les envíe un nombre de máquina DHCP.

Método de configuración de red:

Reintentar la configuración automática de la red

Reintentar la configuración automática de red indicando un servidor DHCP

Configurar la red manualmente

No configurar la red en este momento

Configurar la red

La dirección IP es única para su ordenador y puede ser:

- * cuatro bloques de números separados por puntos (IPv4);
- * bloques de caracteres hexadecimales separados por dos puntos (IPv6).

También puede añadir una máscara de red CIDR al final (como por ejemplo «/24»).

Consulte con su administrador de red si no sabe qué escribir aquí.

Dirección IP:

192.168.15.10/24

Configurar la red

La pasarela es una dirección IP (cuatro números separados por puntos) que indica el encaminador de pasarela, también conocido como encaminador por omisión. Todo el tráfico que se envía fuera de su LAN (por ejemplo, hacia Internet) se envía a este encaminador. En algunas circunstancias anormales, puede no tener un encaminador; si es así lo puede dejar en blanco. Si no sabe la respuesta correcta a esta pregunta, consulte al administrador de red.

Pasarela:

192.168.15.1

Configurar la red

Los servidores de nombres se utilizan para buscar los nombres de las máquinas de la red. Por favor, introduzca la dirección IP (no el nombre de sistema) de hasta tres servidores de nombres, separados por espacios. No utilice comas. Se consultarán los servidores en el orden en que se introduzcan. Si no quiere utilizar ningún servidor de nombres deje este campo en blanco.

Direcciones de servidores de nombres:

1.1.1.1 8.8.8.8 9.9.9.9

Configurar la red

Por favor, introduzca el nombre de la máquina.

El nombre de máquina es una sola palabra que identifica el sistema en la red. Consulte al administrador de red si no sabe qué nombre debería tener. Si está configurando una red doméstica puede inventarse este nombre.

Nombre de la máquina:

Dbebian-FW

Particionado de discos

Este instalador puede guiarle en el particionado del disco (utilizando distintos esquemas estándar) o, si lo desea, puede hacerlo de forma manual. Si escoge el sistema de particionado guiado tendrá la oportunidad más adelante de revisar y adaptar los resultados.

Se le preguntará qué disco a utilizar si elige particionado guiado para un disco completo.

Método de particionado:

Guiado - utilizar todo el disco

Guiado - utilizar el disco completo y configurar LVM

Guiado - utilizar todo el disco y configurar LVM cifrado

Particionado de discos

Seleccionado para particionar:

SCSI3 (0,0,0) (sda) - VMware, VMware Virtual S: 42.9 GB

Este disco puede particionarse siguiendo uno o varios de los diferentes esquemas disponibles. Si no está seguro, escoja el primero de ellos.

Esquema de particionado:

Todos los ficheros en una partición (recomendado para novatos)

Separar la partición /home

Separar particiones /home, /var y /tmp

```
▽ SCS13 (0,0,0) (sda) - 42.9 GB VMware, VMware Virtual S
>   #1  primaria  41.9 GB    f  ext4      /
>   #5  lógica     1.0 GB    f  intercambio  intercambio

Deshacer los cambios realizados a las particiones
Finalizar el particionado y escribir los cambios en el disco
```

Capturar la pantalla Ayuda Retroceder Continuar

Configurar el gestor de paquetes

Escaneando el medio de instalación se encontró la etiqueta:

Debian GNU/Linux 12.2.0 _Bookworm_ - Official amd64 NETINST with firmware 20231007-10:28

Ahora tiene la opción de analizar medios de instalación adicionales para que los utilice el gestor de paquetes («apt»). Generalmente estos deberían ser del mismo conjunto de instalación que utilizó inicialmente. Puede omitir este paso si no dispone de más medios de instalación.

Inserte ahora otro medio de instalación si desea analizarlo.

¿Desea analizar medios de instalación adicionales?

- No
 Sí

Normalmente, deb.debian.org es una buena elección.

Réplica de Debian:

```
deb.debian.org
ftp.es.debian.org
ulises.hostalia.com
softlibre.unizar.es
debian.redparra.com
debian.grn.cat
ftp.udc.es
ftp.cica.es
ftp.calieu.cat
debian.redimadrid.es
debian.uvigo.es
mirror.librelabucm.org
repo.ifca.es
debian-archive.trafficmanager.net
```

Capturar la pantalla Retroceder Continuar

Si tiene que usar un proxy HTTP para acceder a la red, introduzca a continuación la información sobre el proxy. En caso contrario, déjelo en blanco.

La información del proxy debe estar en el formato estándar "http://[:user][:pass]@]host[:port]/".

Información de proxy HTTP (en blanco si no desea usar ninguno):

Capturar la pantalla

Retroceder

Continuar

Configuración de popularity-contest

Puede hacer que su sistema envíe anónimamente estadísticas a los desarrolladores sobre los paquetes más usa. Esta información tiene influencia sobre ciertas decisiones, como qué paquetes deben incluirse en primer CD de la distribución.

Si elige participar, el script de envío se ejecutará automáticamente una vez a la semana, mandando estadísticas a los desarrolladores. Las estadísticas se pueden consultar en <https://popcon.debian.org/>.

La elección siempre puede cambiar con la orden «`dpkg-reconfigure popularity-contest`»

¿Desea participar en la encuesta sobre el uso de los paquetes?

No

Sí

De momento sólo está instalado el sistema básico. Puede escoger la instalación de las siguientes colecciones predefinidas de programas para adaptar más la instalación a sus necesidades.

Elegir los programas a instalar:

Entorno de escritorio Debian

- ... GNOME
- ... Xfce
- ... GNOME Flashback
- ... KDE Plasma
- ... Cinnamon
- ... MATE
- ... LXDE
- ... LXQt
- web server
- SSH server
- Utilidades estándar del sistema

Capturar la pantalla

Continuar

Instalando el cargador de arranque GRUB

Ahora debe configurar el sistema recién instalado para que sea arrancable, instalando para ello el cargador GRUB en un dispositivo del que se pueda arrancar. La forma habitual de hacerlo es instalar GRUB en su unidad principal (partición UEFI o registro principal de arranque). Si lo prefiere, puede instalar GRUB en cualquier otra unidad (o partición), o incluso en un medio removible.

Dispositivo donde instalar el cargador de arranque:

Introducir el dispositivo manualmente

/dev/sda

Usuario ; coquina

Clave Coquina@56@

Configuración de la VPN SSL

Hay que crear dos , una para dentro de la empresa y otra para los usuarios de fuera

The screenshot shows the NetworkMiner interface with the 'SSL VPN global settings' tab highlighted. The left sidebar includes sections for MONITOR & ANALYZE (Control center, Current activities, Reports, Zero-day protection, Diagnostics), PROTECT (Rules and policies, Intrusion prevention, Web, Applications, Wireless, Email, Web server, Active threat response), and CONFIGURE (Remote access VPN, Site-to-site VPN, Network). The 'Remote access VPN' option is selected under CONFIGURE.

This screenshot displays the configuration options for the SSL VPN global settings. The fields include:

- Protocol: UDP (selected over TCP)
- SSL server certificate: ApplianceCertificate
- Override hostname: (empty field)
- Port: 8443
- Assign IPv4 addresses: 10.81.0.0 /16 (255.255.0.0)
- Assign IPv6 addresses: 2001:db8::1:0 / 64
- Lease mode: IPv4 only
- Use static IP addresses: (unchecked)
- IPv4 DNS: 8.8.8.8
- IPv4 WINS: Primary (Secondary is also listed)
- Domain name: clase.local
- Disconnect dead peer after: 180 seconds (60 - 1800)
- Disconnect idle peer after: 120 minutes (15 - 360)

Una vez ya tenemos hecha nuestra VPN genérica ya podemos empezar ha hacer la nuestra
Vamos a hacerla con ayudante .

Usuaris de la empresa

Comprobamos que todo esté bien

Remote access assistant [SSL VPN]

Global settings

These settings apply to all remote access SSL VPN connections.

Protocol	UDP
Override hostname	Not configured
Port	8443
Assign IPv4 addresses	10.81.0.0
Subnet mask	255.255.0.0
Lease mode	IPv4 only

You can change these settings on Remote access VPN > SSL VPN > SSL VPN global settings.

Cancel 1 of 9 Next

Remote access assistant [SSL VPN]

VPN name

Enter a name to identify the connection.

Name

vpn_clase

Description

Para conectar solo los de clase

[Cancel](#)

2 of 9

[Back](#)

[Next](#)

Remote access assistant [SSL VPN]

Users and groups

Select the users and groups that can connect using this policy.

[Open Group](#)



[Add new item](#)

You can configure users and groups on Authentication > Users or Groups.

[Cancel](#)

3 of 9

[Back](#)

[Next](#)

Authentication servers [global setting]

Select the servers you want to use to authenticate users.

- Same as VPN (IPsec, L2TP, PPTP)
- Same as firewall
- Set authentication method for SSL VPN

Authentication server list	Selected authentication server
<input type="text" value="type to search..."/>	Local
<input checked="" type="checkbox"/> Local	

drag to change priority

You can also change this global setting on Authentication > Services > SSL VPN authentication methods.

[Cancel](#)

4 of 9

[Back](#)

[Next](#)

Asistente de acceso remoto [VPN SSL]

Acceder a los recursos

Seleccione los hosts y las redes a los que desea permitir el acceso a los usuarios.

Recursos IPv4

DMZ-15



LAN13



Añadir nuevo elemento

[Cancelar](#)

5 de 9

[Atrás](#)

[Siguiente](#)

Remote access assistant [SSL VPN]

Tunnel mode

You can use VPN for all the users' traffic (to the resources you've specified and the internet) or only to the resources.

Use VPN for all traffic



Use VPN only for traffic to resources



[Cancel](#)

6 of 9

[Back](#)

[Next](#)

Remote access assistant [SSL VPN]

VPN portal access (global setting)

Users can download the SSL VPN client and configuration files from the VPN portal.

Select the zones from which users can access the VPN portal.

LAN



WAN



Add new item

You can also change these global settings on Administration > Device access.

[Cancel](#)

7 of 9

[Back](#)

[Next](#)

Remote access assistant [SSL VPN]

SSL VPN access [global setting]

Select the zones from which users can establish SSL VPN tunnels.

WAN



Add new item

You can also change these global settings on Administration > Device access.

[Cancel](#)

8 of 9

[Back](#)

[Next](#)

Remote access assistant [SSL VPN]

Review your settings

Click Finish to create the remote access SSL VPN policy and firewall rules automatically.

Name	vpn_clase
Users and groups	Open Group
Authentication servers	Local
IPv4 resources	LAN13
Tunnel mode	Use VPN only for traffic to resources
VPN portal access	LAN, WAN
SSL VPN access	WAN
Firewall rule group	Automatic VPN Rules
Firewall rules	SSLVPN_v4_vpnc clase

These firewall rules appear at the bottom of the firewall rule group and are turned on by default.

[Cancel](#)

9 of 9

[Back](#)

[Finish](#)

Usuarios de fuera

The screenshot shows a network configuration interface with several tabs at the top: SSL VPN, L2TP, PPTP, Clientless SSL VPN policy, and IPsec (legacy). The L2TP tab is currently selected. Below the tabs, there are two buttons: 'Assistant' (highlighted in yellow) and 'Add'. There is also a 'Delete' button. A table below these buttons has columns for 'Description' and 'Manage'. A small note at the bottom left says 'Use as default gateway' with a dropdown arrow.

Comprobamos que todo esté bien

Remote access assistant [SSL VPN]

Global settings

These settings apply to all remote access SSL VPN connections.

Protocol	UDP
Override hostname	Not configured
Port	8443
Assign IPv4 addresses	10.81.0.0
Subnet mask	255.255.0.0
Lease mode	IPv4 only

You can change these settings on Remote access VPN > SSL VPN > SSL VPN global settings.

Cancel 1 of 9 Next

Remote access assistant [SSL VPN]

VPN name

Enter a name to identify the connection.

Name
vpn_externos

Description
Usuarios externos

Next

Añadimos los usuarios , añadimos el grupo , para que solo los que añadamos a ese grupo se puedan conectar

Users and groups

Select the users and groups that can connect using this policy.

Open Group	
Add new item	

You can configure users and groups on Authentication > Users or Groups.

[Cancel](#)

3 of 9

[Back](#)

[Next](#)

La siguiente tiene que estar en local .

Solo a lan 13 ya que si vemos en el esquema del inicio lo importante es que llegue a esa lan 13

Remote access assistant (SSL VPN)

Access to resources

Select the hosts and networks you want to allow users to access.

IPv4 resources

LAN13			
Add new item			

[Cancel](#)

5 of 9

[Back](#)

[Next](#)

Remote access assistant (SSL VPN)

Tunnel mode

You can use VPN for all the users' traffic (to the resources you've specified and the internet) or only to the resources.

Use VPN for all traffic



Use VPN only for traffic to resources



[Cancel](#)

6 of 9

[Back](#)

[Next](#)

Remote access assistant [SSL VPN]

VPN portal access [global setting]

Users can download the SSL VPN client and configuration files from the VPN portal.

Select the zones from which users can access the VPN portal.

LAN	
WAN	
Add new item	

You can also change these global settings on Administration > Device access.

[Cancel](#)

7 of 9

[Back](#)

[Next](#)

Remote access assistant [SSL VPN]

SSL VPN access [global setting]

Select the zones from which users can establish SSL VPN tunnels.

WAN	
Add new item	

You can also change these global settings on Administration > Device access.

[Cancel](#)

8 of 9

[Back](#)

[Next](#)

Remote access assistant [SSL VPN]

Review your settings

Click Finish to create the remote access SSL VPN policy and firewall rules automatically.

Name	vpn_externos
Users and groups	Open Group
Authentication servers	Local
IPv4 resources	LAN13
Tunnel mode	Use VPN only for traffic to resources
VPN portal access	LAN, WAN
SSL VPN access	WAN
Firewall rule group	Automatic VPN Rules
Firewall rules	SSLVPN_v4_vpexternos

These firewall rules appear at the bottom of the firewall rule group and are turned on by default.

[Cancel](#)

9 of 9

[Back](#)

[Finish](#)

Ya estaría lista

Añadir usuarios y grupos

Vamos a crear un grupo nuevo , lo creamos para gente de fuera de la empresa que pueda trabajar .

Group name	Traffic shaping	Surfing quota
Open Group	No policy	Unlimited Internet Access
Clientless Open Group(C)	No policy	No policy
Guest Group	No policy	Unlimited Internet Access
Externos		

Lo rellenamos

Group name *	Externos
Description	Usuarios externos a la empresa
Group type *	Normal
Policies	
Surfing quota *	Unlimited Internet Access
Access time *	Allowed only during Work Hours
Network traffic	None
Traffic shaping	None

SSL VPN policy

SSL VPN policy *

vpn_externos

Clientless SSL VPN policy *

No policy applied

L2TP *

Enable Disable

PPTP *

Enable Disable

Other settings

Quarantine digest *

Enable Disable

MAC binding

Enable Disable

Save Cancel

Configuración de WAZU

Lo primero nos vamos a la red y creamos un nuevo protocolo DHCP para el WAZU

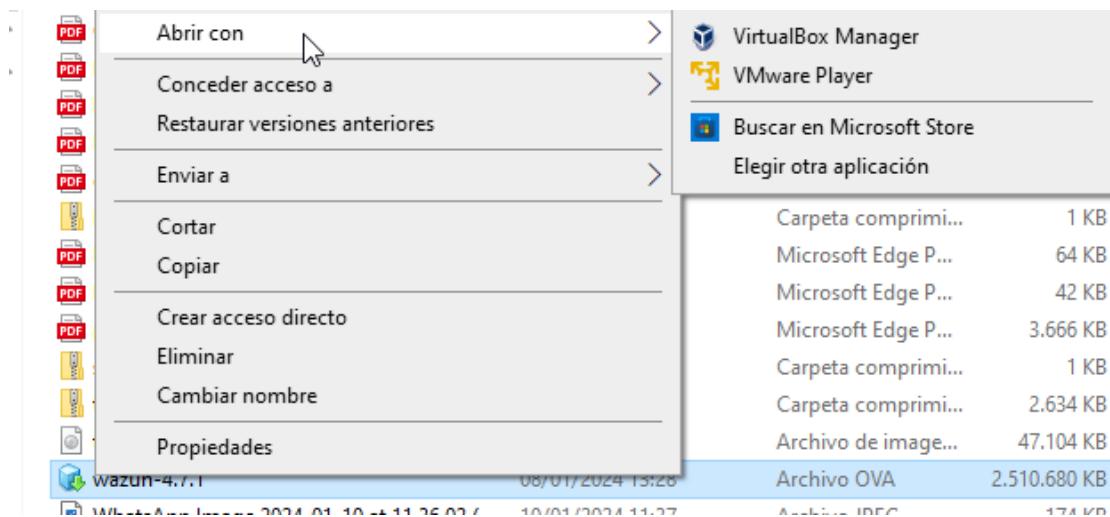
IPv4 | IPv6

General settings

Name *	dhcp-LAN14						
Interface	Select interface						
<input type="checkbox"/> Accept client request via relay							
Dynamic IP lease	<table border="1"> <thead> <tr> <th>Start IP</th> <th>End IP</th> </tr> </thead> <tbody> <tr> <td>192.168.14.100</td> <td>192.168.14.199</td> </tr> </tbody> </table> <small>* Press Tab to add a new row</small>	Start IP	End IP	192.168.14.100	192.168.14.199		
Start IP	End IP						
192.168.14.100	192.168.14.199						
Static IP MAC mapping	<table border="1"> <thead> <tr> <th>Hostname</th> <th>MAC address</th> <th>IP address</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> </tr> </tbody> </table> <small>* Press Tab to add a new row</small>	Hostname	MAC address	IP address			
Hostname	MAC address	IP address					
Subnet mask *	/24 (255.255.255.0)						
Domain name							

Nos bajamos wazu <https://wazuh.com/>

Y lo abrimos con VMware



Import Virtual Machine

Store the new Virtual Machine

Provide a name and local storage path for the new virtual machine.

Name for the new virtual machine:

Wazuh7-FW

Storage path for the new virtual machine:

C:\Users\FranciscoVasserotGon\Documents\Virtual Machines

[Browse...](#)

[Help](#)

[Import](#)

[Cancel](#)

Importante si lo haces con virtualbox

- [/ Installation alternatives / Virtual Machine \(OVA\)](#)
 - b. Click **Settings > Display**
 - c. In **Graphic controller**, select the **VMSVGA** option.
3. Start the machine.

Device	Summary
Memory	8 GB
Processors	4
Hard Disk (IDE)	50 GB
CD/DVD (IDE)	Using unknown backend
Floppy	Using drive A:
Network Adapter	NAT
Display	Auto detect

Memory
Specify the amount of memory allocated
size must be a multiple of 4 MB.

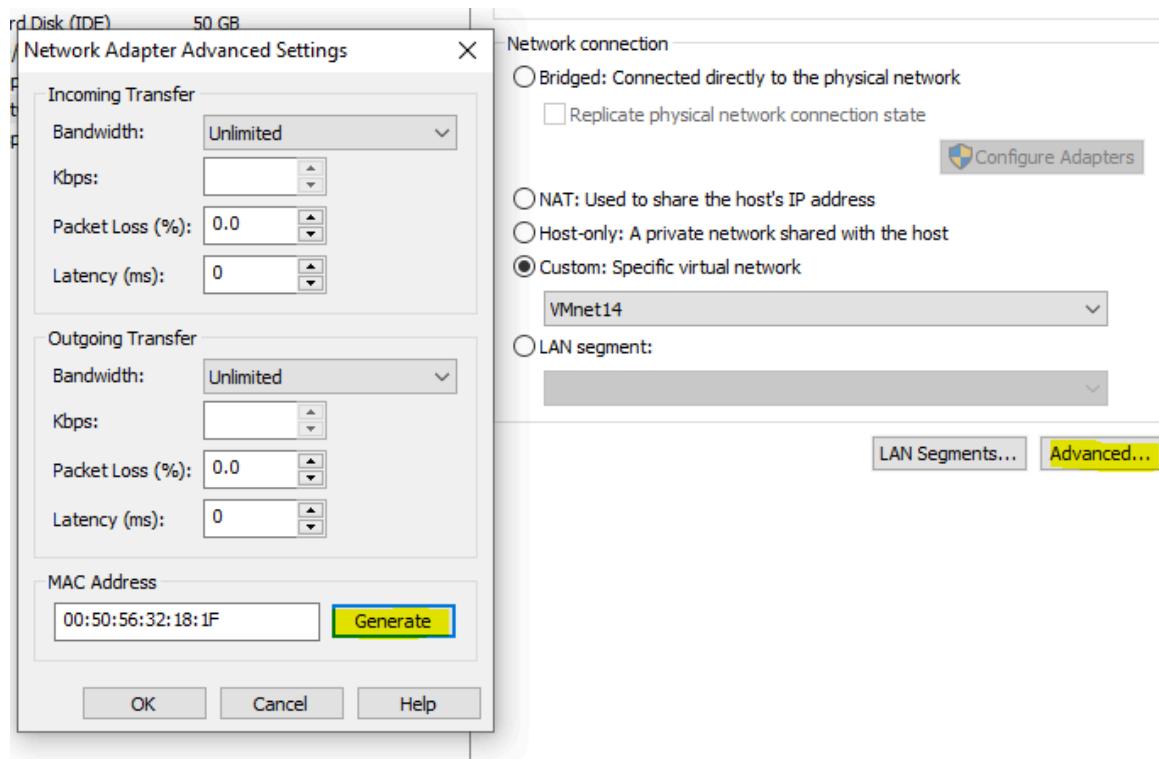
Memory for this virtual machine:

32 GB - ▲
16 GB - ▲
8 GB - ▶ **8 GB** ▲
4 GB - ▲

Esto es un paso muy importante

Apagamos la máquina y vamos a generar la mac

Es muy importante ya que tiene que tener una ip fija



Y ahora con esta mac volvemos a la configuración de la red que hemos hecho antes en la LAN 14 y le añadimos nuestra máscara .Y ya le ponemos la ip fija que queramos , que en nuestro caso es la 10

Name *	dhcp-LAN14		
Interface	Port5 - 192.168.14.1		
<input type="checkbox"/> Accept client request via relay			
Dynamic IP lease	Start IP	End IP	<input type="button" value="+"/>
	192.168.14.100	192.168.14.199	<input type="button" value="-"/>
* Press Tab to add a new row			
Static IP MAC mapping	Hostname	MAC address	IP address
	wazuh-server	00:50:56:32:18:1F	192.168.14.10
* Press Tab to add a new row			
Subnet mask *	/24 [255.255.255.0]		
Domain name	clase.local		
Gateway *	<input checked="" type="checkbox"/> Use interface IP as gateway		

Usuario = wazuh-server

Clave =wazuh

Primero vamos a ponerlo en Español , con los comandos :

```
[wazuh-user@wazuh-server ~]$ sudo -i  
[root@wazuh-server ~]# localectl set-keymap es  
[root@wazuh-server ~]#
```

Ahora hay que configurar nuestra red y nos vamos a instalar el mc , para ello nos iremos a :

```
[root@wazuh-server ~]# cd /etc/sysconfig/network-scripts
[root@wazuh-server network-scripts]#
[root@wazuh-server network-scripts]#
[root@wazuh-server network-scripts]# yum install mc
Loaded plugins: langpacks, priorities, update-motd
amzn2-core                                         | 3.6 kB     00:00
Package 1:mc-4.8.29-1.amzn2.x86_64 already installed and latest version
Nothing to do
[root@wazuh-server network-scripts]#
```

Dentro de mc nos interesa editar

Name	Size	Recently used	Name	Size
	UP--DIR	Dec 15 23:23		UP--DIR
ifcfg-eth0	120	Apr 20 2023	ifcfg-eth0	1
ifcfg-lo	254	Mar 29 2019	ifcfg-lo	2
@ifdown	24	Mar 8 2023	@ifdown	
*ifdown-Team	1621	Mar 17 2017	*ifdown-Team	16
*ifdown-TeamPort	1556	Mar 17 2017	*ifdown-TeamPort	15
*ifdown-bnep	654	Mar 29 2019	*ifdown-bnep	6
*ifdown-eth	6532	Mar 29 2019	*ifdown-eth	65
*ifdown-ippp	781	Mar 29 2019	*ifdown-ippp	7
*ifdown-ipv6	4540	Mar 29 2019	*ifdown-ipv6	45
@ifdown-isdn	11	Mar 8 2023	@ifdown-isdn	
*ifdown-post	2130	Mar 29 2019	*ifdown-post	21
*ifdown-ppp	1068	Mar 29 2019	*ifdown-ppp	10
*ifdown-routes	870	Mar 29 2019	*ifdown-routes	8
*ifdown-sit	1456	Mar 29 2019	*ifdown-sit	14
*ifdown-tunnel	1462	Mar 29 2019	*ifdown-tunnel	14
<hr/>				
ifcfg-eth0	45G / 50G (90%)			45

Ahora pulsamos F4 y nos tendría que llevar a

```
[root@rhel7 ~]# cat /etc/sysconfig/network-scripts/ifcfg-eth0
# Automatically generated by the vm import process
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
TYPE=Ethernet
NM_CONTROLLED=no
```

Esto se hace si es para virtualbox

Ahora aquí lo que vamos a editar es poner la ip estática y guardamos

```
ifcfg-eth0      [-M--]  0 L:[ 1+10 11/ 12]
# Automatically generated by the VM import process
DEVICE=eth0
ONBOOT=yes
#BOOTPROTO=dhcp
BOOTPROTO=none
TYPE=Ethernet
NM_CONTROLLED=no
PREFIX=24
IPADDR=192.168.1.222
GATEWAY=192.168.1.1
```

Esto se hace si es vmware

```
ifcfg-eth0      [----]  0 L:[ 1+ 0  1/  8] *
# Automatically generated by the VM import process
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=none
TYPE=Ethernet
NM_CONTROLLED=no
PREFIX=24
IPADDR=192.168.14.10
```

Y ahora reiniciamos el sistema con el comando : **systemctl reboot**

Vamos a cambiar el nombre del User:

```
[wazuh-user@wazuh-server ~]$ sudo -i
[root@wazuh-server ~]#
[root@wazuh-server ~]#
[root@wazuh-server ~]#
[root@wazuh-server ~]# cd /etc/
[root@wazuh-server etc]# cat hostname
wazuh-server
[root@wazuh-server etc]# mcedit
```

```
[root@wazuh-server etc]#
[root@wazuh-server etc]# mcedit hostname
```

Y reiniciamos el nombre

```
[root@wazuh-server etc]# hostname -b wazuh-FW
```

Ahora con esta configuración ya podríamos acceder a nuestro wazuh poniendo en internet la ip 192.168.14.10

Antes de meternos ya con el wazuh vamos a retocar algunas cosas .

Lo primero es tenerlo actualizado , por lo que hacemos un **yum update**

Puede que de error , es porque no tiene conexión , porque igual no le hemos dejado en sophos a que haya conexión , lo podemos poner en nat o autorizar el intercambio de paquetes .

Para ver los programas binarios de wazuh haríamos :

```
[wazuh-user@wazuh-demo ~]$ sudo -i
[root@wazuh-demo ~]#
[root@wazuh-demo ~]# cd /root/
[root@wazuh-demo ~]#
[root@wazuh-demo ~]#
[root@wazuh-demo ~]# ls -alh /var/ossec/bin/
total 24M
drwxr-x---  2 root wazuh 4.0K Dec 15 23:24 .
drwxr-x--- 19 root wazuh  242 Dec 15 23:25 ..
-rwxr-x---  1 root root  466K Dec 15 19:45 agent_control
-rwxr-x---  1 root wazuh 1.1K Dec 15 19:45 agent_groups
-rwxr-x---  1 root wazuh 1.1K Dec 15 19:45 agent_upgrade
-rwxr-x---  1 root root  114K Dec 15 19:45 clear_stats
-rwxr-x---  1 root wazuh 1.1K Dec 15 19:45 cluster_control
-rwxr-x---  1 root root  480K Dec 15 19:45 manage_agents
-rwxr-x---  1 root wazuh 1.1K Dec 15 19:45 rbac_control
-rwxr-x---  1 root wazuh 1.3M Dec 15 19:45 verify-agent-conf
-rwxr-x---  1 root root  1.3M Dec 15 19:45 wazuh-agentlessd
-rwxr-x---  1 root root  1.7M Dec 15 19:45 wazuh-analysisd
-rwxr-x---  1 root wazuh 1013 Dec 15 19:45 wazuh-anpid
```

Para añadir un agente :

```
[root@wazuh-server ~]# /var/ossec/bin/Manage_agents

*****
* Wazuh v4.7.1 Agent Manager.          *
* The following options are available: *
*****
(A)dd an agent (A).
(E)xtract key for an agent (E).
(L)ist already added agents (L).
(R)eMove an agent (R).
(Q)uit.

Choose your action: A,E,L,R or Q:
```

Vamos a crear una alias

para la carpeta de var ossec bin , apunte a una carpeta de root

Estas son las carpetas y documentos que encontramos en root

```
[root@wazuh-server ~]# ls -alh
total 28K
dr-xr-x---  6 root root  179 Jan 29 07:32 .
dr-xr-xr-x 18 root root  257 Apr 21 2023 ..
-rw-r--r--  1 root root  168 Jan 29 07:36 .bash_history
-rw-r--r--  1 root root   18 Oct 18 2017 .bash_logout
-rw-r--r--  1 root root  176 Oct 18 2017 .bash_profile
-rw-r--r--  1 root root  176 Oct 18 2017 .bashrc
drwx----- 3 root root   16 Jan 29 07:32 .cache
drwx----- 3 root root   16 Jan 29 07:32 .config
-rw-r--r--  1 root root  100 Oct 18 2017 .cshrc
drwx----- 3 root root   19 Jan 29 07:32 .local
-rw-------  1 root root 1.0K Dec 15 23:22 .rnd
drwx----- 2 root root    6 Apr 21 2023 .ssh
-rw-r--r--  1 root root 129 Oct 18 2017 .tcshrc
```

Cómo lo hacemos

```
[root@wazuh-demo ~]# ln -s --help
Usage: ln [OPTION]... [-T] TARGET [LINK NAME] (1st form)
      or: ln [OPTION]... TARGET (2nd form)
      or: ln [OPTION]... TARGET... DIRECTORY (3rd form)
      or: ln [OPTION]... -t DIRECTORY TARGET... (4th form)
In the 1st form, create a link to TARGET with the name LINK_NAME.
In the 2nd form, create a link to TARGET in the current directory.
In the 3rd and 4th forms, create links to each TARGET in DIRECTORY.
Create hard links by default, symbolic links with --symbolic.
By default, each destination (name of new link) should not already
```

Para crearla

```
[root@wazuh-server ~]#  
[root@wazuh-server ~]# ln -s /var/ossec/bin /root/ossecbin  
[root@wazuh-server ~]#
```

con ln - s , la creamos , lo siguiente sería el nombre y lo último donde queremos crearla , es decir la dirección .

Aquí se vería creada

```
[root@wazuh-server ~]# ls -alh  
total 28K  
dr-xr-x--- 6 root root 195 Jan 29 08:05 .  
dr-xr-xr-x 18 root root 257 Apr 21 2023 ..  
-rw-r--r-- 1 root root 168 Jan 29 07:36 .bash_history  
-rw-r--r-- 1 root root 18 Oct 18 2017 .bash_logout  
-rw-r--r-- 1 root root 176 Oct 18 2017 .bash_profile  
-rw-r--r-- 1 root root 176 Oct 18 2017 .bashrc  
drwx----- 3 root root 16 Jan 29 07:32 .cache  
drwx----- 3 root root 16 Jan 29 07:32 .config  
-rw-r--r-- 1 root root 100 Oct 18 2017 .cshrc  
drwx----- 3 root root 19 Jan 29 07:32 .local  
lrwxrwxrwx 1 root root 14 Jan 29 08:05 ossecbin -> /var/ossec/bin  
-rw----- 1 root root 1.0K Dec 15 23:22 .rnd  
drwx----- 2 root root 6 Apr 21 2023 .ssh  
-rw-r--r-- 1 root root 129 Oct 18 2017 .tcshrc  
[root@wazuh-server ~]#
```

Cambio de clave

El programa que cambia la clave de wazuh está en en mc y dentro en la ruta :

```
-rw-r--r-- 1 root root 133 ene 18 07:32 .tcshrc  
lrwxrwxrwx 1 root root 58 ene 18 16:27 tools -> /usr/share/wazuh-indexer/plugins/opensearch-security/tools  
[root@wazuh-server ~]#
```

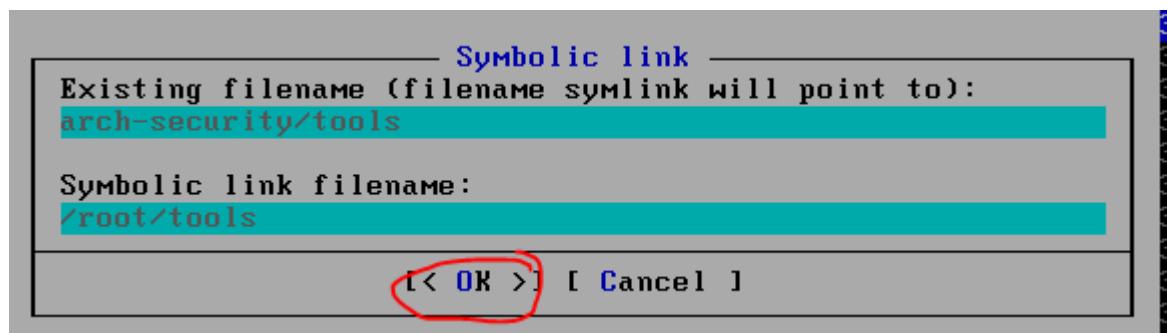
.n	Name	Size	Modify time
		UP--DIR	
/..			Dec 15 23:24
*SECURITY~ESTS.md	4013	Jun 3 2023	
*audit_co~ater.sh	1388	Jun 3 2023	
config.yml	636	Dec 15 19:54	
*hash.sh	1376	Jun 3 2023	
*securityadmin.sh	1417	Jun 3 2023	
*wazuh-ce~tool.sh	32077	Dec 15 19:54	
*wazuh-pa~tool.sh	39641	Dec 15 19:54	

Ahora vamos a crear el link entre root y la clave para ello tenemos que estar en el mc , en la parte de la izquierda en root y en la de la derecha en la que hemos llegado arriba pero nos quedamos antes de entrar en tools

.n	Name	Size	Modify time	.n	Name	Size	Modify time
		UP--DIR				UP--DIR	
/..			Apr 21 2023	/..			Dec 15 23:24
/.cache	16	Jan 29 07:32		/tools	184	Dec 15 23:24	
/.config	16	Jan 29 07:32		accessor~4.7.jar	29489	Jun 3 2023	
/.local	19	Jan 29 07:32		aggs-mat~8.0.jar	57359	Jun 3 2023	
/.ssh	6	Apr 21 2023		asm-9.1.jar	121790	Jun 3 2023	
~ossecbin	14	Jan 29 08:05		bcpkix-j~.70.jar	963713	Jun 3 2023	
.bash_history	168	Jan 29 07:36		bcprov-j~.67.jar	5961136	Jun 3 2023	
.bash_logout	18	Oct 18 2017		checker~5.0.jar	214381	Jun 3 2023	
.bash_profile	176	Oct 18 2017		commons~3.1.jar	52988	Jun 3 2023	
.bashrc	176	Oct 18 2017		commons~.14.jar	347669	Jun 3 2023	
.cshrc	100	Oct 18 2017		commons~2.2.jar	588337	Jun 3 2023	
.rnd	1024	Dec 15 23:22		commons~2.4.jar	261809	Jun 3 2023	
.tcshrc	129	Oct 18 2017		commons~3.4.jar	434678	Jun 3 2023	
				commons~1.2.jar	61829	Jun 3 2023	
				commons~0.0.jar	238400	Jun 3 2023	

ahora hacemos f9 sobre tools y nos vamos a :

Left	File	Command	Options	Right
-< ~			I>	<- ...ugins/c
.n N	View	F3	e	.n Name
/..	View file...		23	/..
/.cache	Filtered view	M-!	32	/tools
/.config	Edit	F4	32	accessor~4.7
/.local	Copy	F5	32	aggs-mat~8.6
/.ssh	Chmod	C-x c	23	asm-9.1.jar
~ossecbin	Link	C-x l	05	bcpkix-j~.70
.bash_h	Symlink	C-x s	36	bcprov-j~.67
.bash_l	Relative symlink	C-x v	17	checker~5.8
.bash_p	Edit symlink	C-x C-s	17	COMMONS~3.1
.bashrc	Chown	C-x o	17	COMMONS~.14
.cshrc	Advanced chown		17	COMMONS~2.2
.rnd	Chattr	C-x e	22	COMMONS~2.4
.tcshrc	Rename/Move	F6	17	COMMONS~3.4
	Mkdir	F7		COMMONS~1.2
	Delete	F8		COMMONS~2.0



Ahora no nos tendríamos que ir a buscar la carpeta de security , ya la tendríamos en root :

Left	Name	Size	Modify time	Right
-< ~			I>	<- .
.n	Name	UP--DIR	Apr 21 2023	.n
/..		16	Jan 29 07:32	/..
/.cache		16	Jan 29 07:32	/to
/.config		19	Jan 29 07:32	ac
/.local		6	Apr 21 2023	ag
/.ssh		14	Jan 29 08:05	as
~ossecbin		60	Jan 29 08:22	bc
~tools		168	Jan 29 07:36	bc
.bash_history		18	Oct 18 2017	ch
.bash_logout				co

Ahora vamos a retocar el archivo ossec

Se encuentra en :

`ls -l ~/ossec/bin`			`ls -l /var/ossec/etc`		
Name	Size	Modify time	Name	Size	Modify time
...	UP--DIR	Jan 29 08:22	...	UP--DIR	Dec 15 23:25
*agent_control	476967	Dec 15 19:45	/decoders	31	Dec 15 23:24
*agent_groups	1045	Dec 15 19:45	/lists	122	Dec 15 23:25
*agent_upgrade	1045	Dec 15 19:45	/rootcheck	4096	Dec 15 23:24
*clear_stats	115950	Dec 15 19:45	/rules	29	Dec 15 23:24
*cluster_control	1045	Dec 15 19:45	/shared	63	Dec 15 23:25
*manage_agents	490503	Dec 15 19:45	client.keys	0	Jan 29 08:28
*rbac_control	1045	Dec 15 19:45	internal_ns.conf	14163	Dec 15 19:45
*verify-a~nt-conf	1319781	Dec 15 19:45	local_in_ns.conf	320	Dec 15 19:45
*wazuh-agentlessd	1331427	Dec 15 19:45	localtime	127	Mar 30 2023
*wazuh-analysisd	1744745	Dec 15 19:45	ossec.conf	10708	Dec 15 23:25
*wazuh-apid	1013	Dec 15 19:45	sslmanager.cert	1192	Dec 15 23:25
wazuh-agent	1229452	Dec 15 19:45	wazuh-logstash	1784	Dec 15 23:25

Ahora dentro vamos a modificar (F4)

```
<ossec_config>
  <global>
    <jsonout_output>yes</jsonout_output>
    <alerts_log>yes</alerts_log>
    <logall>no</logall>
    <logall_json>no</logall_json>
    <email_notification>yes</email_notification>
    <smtp_server>localhost</smtp_server>
    <email_from>root@localhost</email_from>
    <email_to>wazuh-user@localhost</email_to>
    <email_maxperhour>12</email_maxperhour>
    <email_log_source>alerts.log</email_log_source>
    <agents_disconnection_time>10</agents_disconnection_time>
    <agents_disconnection_alert_time>0</agents_disconnection_alert_time>
  </global>
```

También vamos a modificar las alertas de 12 a 10

```
<alerts>
  <log_alert_level>3</log_alert_level>
  <email_alert_level>10</email_alert_level>
</alerts>
```

Una vez listo guardamos (F2) y salimos (F10).Reiniciamos

```
[root@wazuh-server etc]# systemctl restart wazuh-manager.service
```

Los correos llegan si te llega una alerta :

```
[root@wazuh-server etc]#  
[root@wazuh-server etc]# ls -alh /var/mail/  
total 4.0K  
drwxrwxr-x 2 root      mail   47 Dec 15 23:20 .  
drwxr-xr-x 9 root      root    97 Mar  8  2023 ..  
-rw----- 1 root      mail   931 Dec 15 23:20 root  
-rw-rw---- 1 rpc       mail    0 Mar  8  2023 rpc  
-rw-rw---- 1 wazuh-user mail    0 Apr 11  2023 wazuh-user  
[root@wazuh-server etc]#
```

Como vemos llegan a wazuh-user , por lo que vamos a crear un programa para que detecte la presencia de este

```
[root@wazuh-server etc]# cd /var/mail/  
[root@wazuh-server Mail]#  
[root@wazuh-server Mail]# mv wazuh-user wazuh-user.eml  
[root@wazuh-server Mail]# ls -alh  
total 4.0K  
drwxrwxr-x 2 root      mail   51 Jan 29 08:46 .  
drwxr-xr-x 9 root      root    97 Mar  8  2023 ..  
-rw----- 1 root      mail   931 Dec 15 23:20 root  
-rw-rw---- 1 rpc       mail    0 Mar  8  2023 rpc  
-rw-rw---- 1 wazuh-user mail    0 Apr 11  2023 wazuh-user.eml  
[root@wazuh-server Mail]#
```

Ahora nos vamos a instalar las prestaciones de mail :

Puede que de error , es porque no tiene conexión , porque igual no le hemos dejado en sophos a que haya conexión , lo podemos poner en nat o autorizar el intercambio de paquetes .

```
[root@wazuh-server Mail]#  
[root@wazuh-server Mail]#  
[root@wazuh-server Mail]# yum install mailx
```

Una vez instalado , si somos root podemos ver los mails

```
[root@wazuh-server Mail]#  
[root@wazuh-server Mail]#  
[root@wazuh-server Mail]# mail  
Heirloom Mail version 12.5 7/5/10. Type ? for help.  
"/var/spool/mail/root": 1 message 1 new  
>N 1 (Cron Daemon)           Fri Dec 15 23:20 25/931 "Cron <root@wazuh-serv>"  
&
```

Para mandar un correo de prueba

```
[root@wazuh-server mail]# echo "Hola" | mail -s "prueba de correo" wazuh-user@localhost
[root@wazuh-server mail]# ls -alh
total 8.0K
drwxrwxr-x 2 root      Mail    69 Jan 31 07:56 .
drwxr-xr-x 9 root      root    97 Mar  8  2023 ..
-rw----- 1 root      Mail   941 Jan 31 07:52 root
-rw-rw---- 1 rpc       Mail     0 Mar  8  2023 rpc
-rw----- 1 wazuh-user Mail  3.5K Jan 31 07:56 wazuh-user
-rw-rw---- 1 wazuh-user Mail     0 Apr 11  2023 wazuh-user.eml
[root@wazuh-server mail]#
```

Para verlo primero lo paso a mi con el comando ,en mc:

[<- /var/mail . [^I]>]		<- /			
.n	Name	Size	Modify time	.n	Name
/..		UP--DIR	Dec 15 23:27	~bin	
root		941	Jan 31 07:52	/boot	
rpc		0	Mar 8 2023	/dev	
wazuh-user		3525	Jan 31 07:56	/etc	
wazuh-user.eml		0	Apr 11 2023	/home	
				~lib	
				~lib64	

Creación de bot

Ahora vamos a crear el bot para controlar los parámetros

Para ello vamos a crear la carpeta bin dentro de root

```
[root@wazuh-server ~]# mkdir bin
[root@wazuh-server ~]# ls -alh
```

Y una vez creada le vamos a meter el alerbot y el botw , que los tenemos descargados

Ahora dentro de esa carpeta que hemos creado (bin) vamos con nano a crear dos archivos .

Alerbot

```
#!/bin/bash

while true;
do

if [[ -s /var/mail/wazuh-user ]]; then

    # Movemos correos a .eml
    mv -f /var/mail/wazuh-user /var/mail/wazuh-user.eml
    # Enviamos .eml por bot
    /root/bin/botw /var/mail/wazuh-user.eml
    # Y mandamos copia por email
    cat /var/mail/wazuh-user.eml | mail -s "Wazuh Alert de [$(hostname -f)]" wazuh-alert

fi

sleep 10

done
```

Una vez lo tenemos abierto escribimos y finalizamos guardando con control O

```
GNU nano 2.9.8                               alerbot

#!/bin/bash

while true;
do

if [[ -s /var/mail/wazuh-user ]]; then

    # Movemos correos a .eml
    mv -f /var/mail/wazuh-user /var/mail/wazuh-user.eml
    # Enviamos .eml por bot
    /root/bin/botw /var/mail/wazuh-user.eml
    # Y mandamos copia por email
    cat /var/mail/wazuh-user.eml | mail -s "Wazuh Alert de [$(hostname -f)]$"

fi
sleep 10

done
```

botw

```
#!/bin/bash

INFO=$1

. /root/bin/bot.conf

if [[ -z $1 ]]; then
    echo "Falta un parámetro!"
    exit 1
fi

for TOKEN in $TOKENS
do
    for ID in $IDS
    do
        if [[ -s $INFO ]]; then
            curl -s -o /dev/null -X POST https://api.telegram.org/bot$TOKEN/sendmessage -d chat_id="$ID" -d text="$INFO"
            curl -s -o /dev/null -X POST https://api.telegram.org/bot$TOKEN/sendDocument -F chat_id="$ID" -F document="@${INFO}"
        else
            curl -s -o /dev/null -X POST https://api.telegram.org/bot$TOKEN/sendmessage -d chat_id="$ID" -d text="$INFO"
        fi
    done
done

exit
```

GNU nano 2.9.8 botw

```
#!/bin/bash

INFO=$1

. /root/bin/bot.conf

if [[ -z $1 ]]; then
    echo "Falta un parametro!"
    exit 1
fi

for TOKEN in $TOKENS
do
    for ID in $IDS
    do
        if[[ -s $INFO ]]; then
            curl -s -o /dev/null -X POST https://api.telegram.org/bot$TOKEN/sendmessage
            curl -s -o /dev/null -X POST https://api.telegram.org/bot$TOKEN/sendDocument
        else
            curl -s -o /dev/null -X POST https://api.telegram.org/bot$TOKEN/sendmessage
        fi
    done
done

`G Get Help `O Write Out `W Where Is `E Cut Text `J Justify `C Cur Pos
```

Una vez creados los dos nos vamos a nuestro mc dentro de bin
Como vemos en el alerbot cuando hay algún fallo lo manda a wazuh alert , ahora qué es wazuh aler , tenemos que ir dentro de mc a esta ruta para poder poner nuestro correo o numero de telefono dentro para que cuando haya un Error nos lleve un mensaje .

Esto está dentro de **aliases**

Y cambiamos y guardamos

```
marketing:<----->postmaster  
sales:<----->postMASTER  
support:<----->postMASTER
```

```
# trap decode to catch security attacks
decode:>----->wazuh-alert
wazuh-alert:<-->pacocesurrr@gestionar.net
```

1Help **2**Save **3**Mark **4**Pen/Ink **5**PopUp **6**Mute **7**Search **8**De

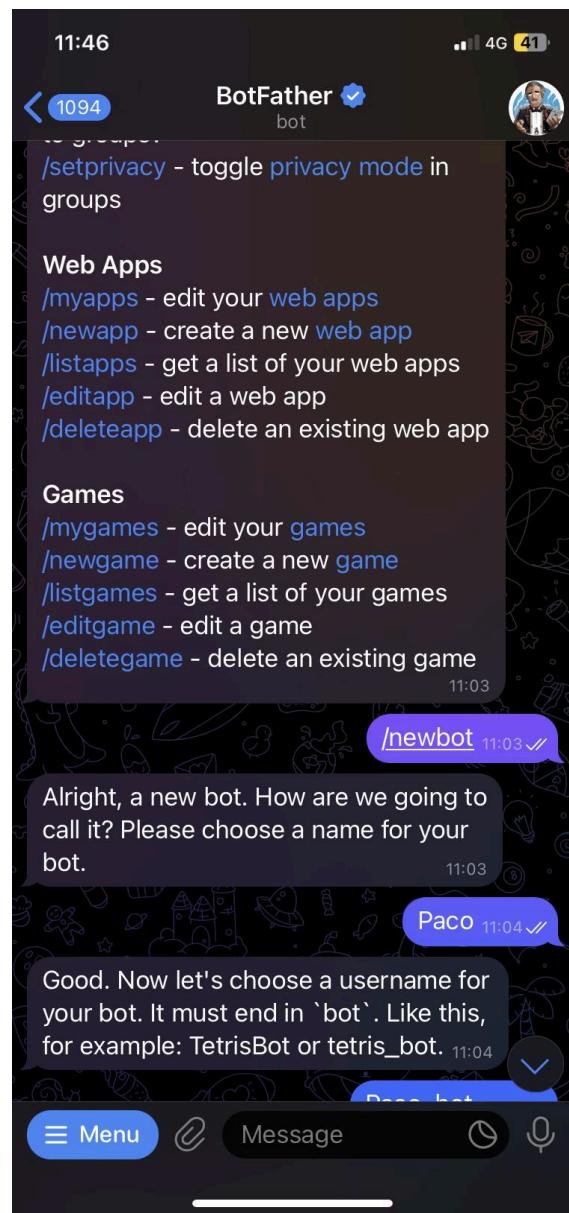
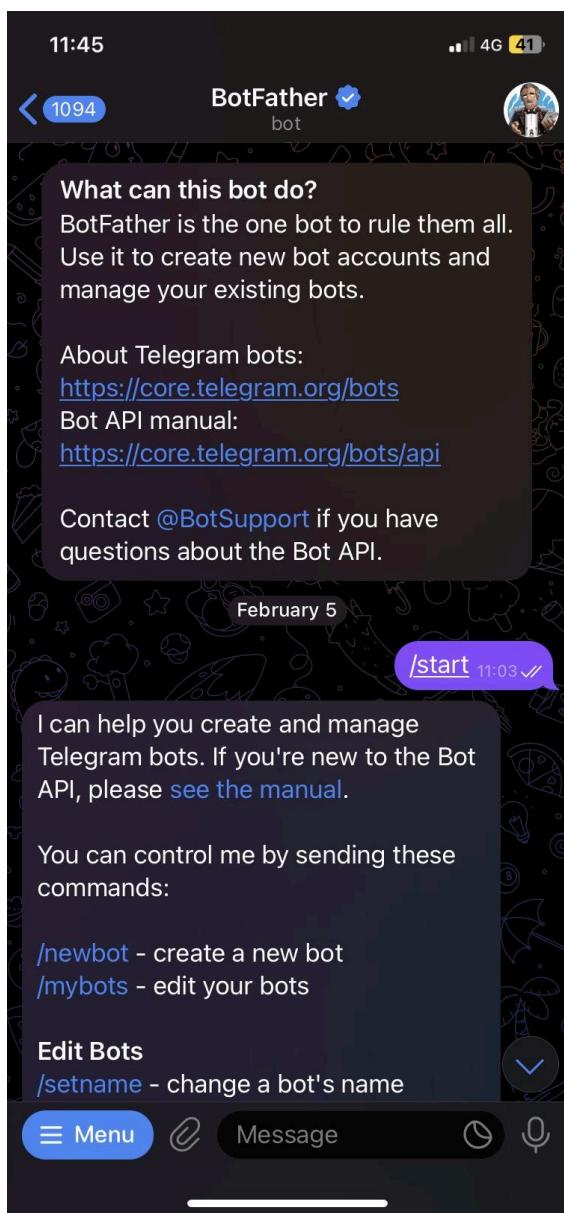
Ahora para probar que ha funcionando podemos hacer

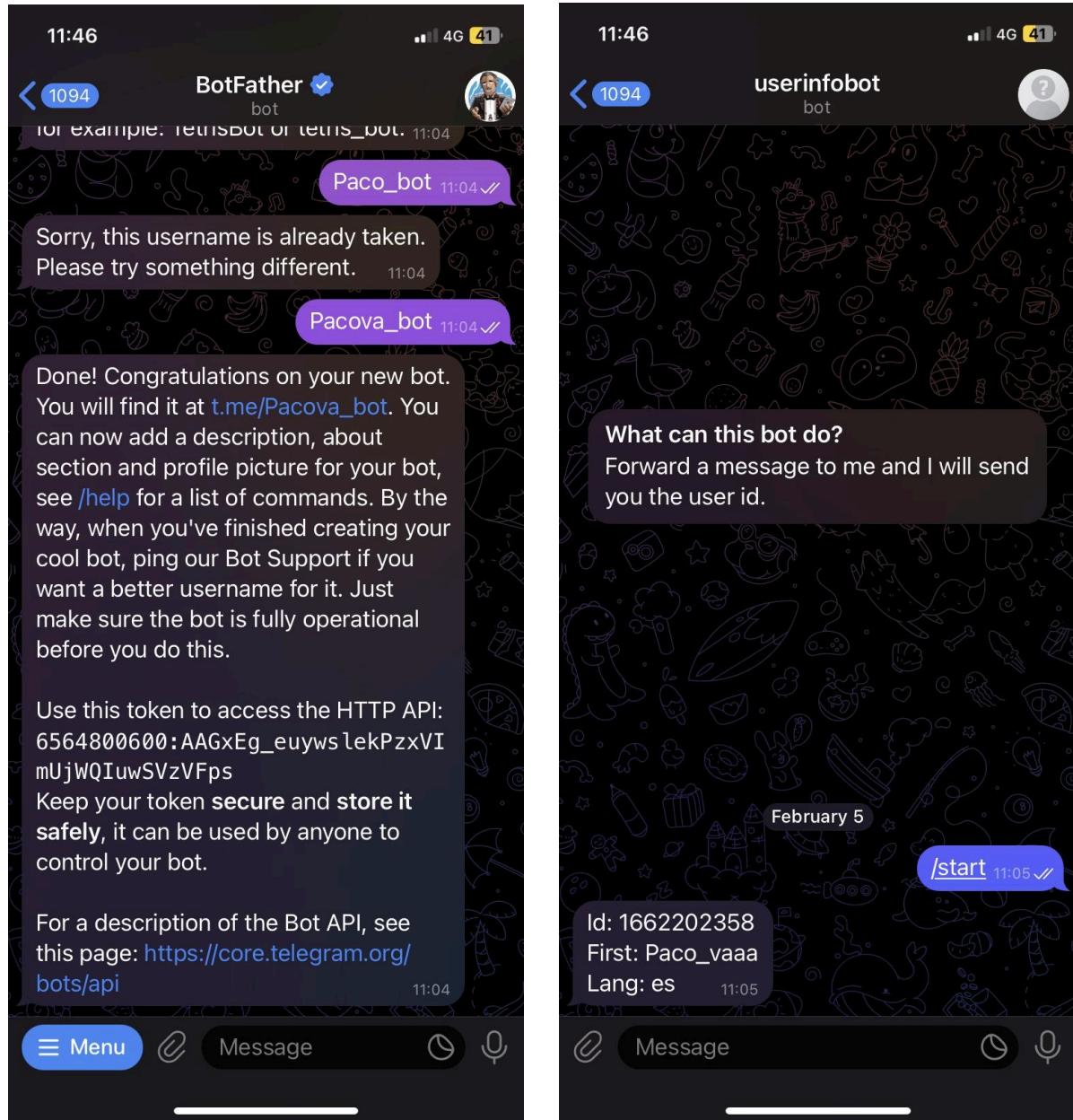
Primero hacemos un `cd /root/bin`, despues un `cd /var/mail/`

```
[root@wazuh-server Mail]#  
[root@wazuh-server Mail]#  
[root@wazuh-server Mail]# cat /root/bin/botw | mail -s "botw" wazuh-user  
[root@wazuh-server Mail]#  
[root@wazuh-server Mail]# cd /var/log  
[root@wazuh-server log]#  
[root@wazuh-server log]#  
[root@wazuh-server log]# cat maillog
```

Telegram

Esto son los pasos que hay que realizar para crearte tu cuenta para telegram





Ahora nos vamos a donde tenemos configurado el bot

```
< ~/bin
.
.
.
*alertbot.sh
bot.conf ←
*botw.sh
```

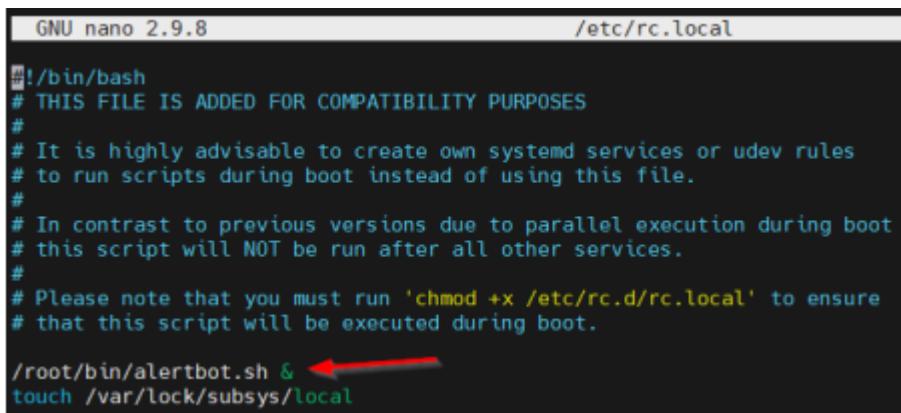
Pulsamos f4 para modificarlo

Habilitamos la ejecución del script en el arranque de Wazuh mediante modificaciones en /etc/rc.local.

#systemctl enable rc-local

```
[root@wazuh-fw bin]#  
[root@wazuh-fw bin]# systemctl enable rc-local  
[root@wazuh-fw bin]#
```

#nano /etc/rc.local



```
GNU nano 2.9.8                               /etc/rc.local  
  
#!/bin/bash  
# THIS FILE IS ADDED FOR COMPATIBILITY PURPOSES  
#  
# It is highly advisable to create own systemd services or udev rules  
# to run scripts during boot instead of using this file.  
#  
# In contrast to previous versions due to parallel execution during boot  
# this script will NOT be run after all other services.  
#  
# Please note that you must run 'chmod +x /etc/rc.d/rc.local' to ensure  
# that this script will be executed during boot.  
  
/root/bin/alertbot.sh & ←  
touch /var/lock/subsys/local
```

Añadir usuario wazuh-alert

adduser wazuh-alert

- El script y los bots deben ejecutarse como root con los permisos más restringidos posibles

Unicamente se dio permiso de ejecución a root a los script alertbot.sh, bot.sh y en Dentro de /etc/rc.local

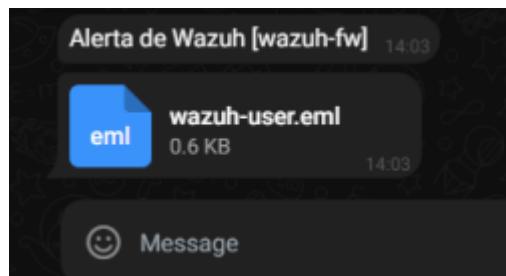
Daremos permiso de ejecución a root para el archivo rc.local

chmod 700 /etc/rc.d/rc.local

```
[root@wazuh-fw mail]# cd /root/bin/  
[root@wazuh-fw bin]# ls  
alertbot.sh  botw.sh  
[root@wazuh-fw bin]# ./alertbot.sh  
^C  
[root@wazuh-fw bin]# ./alertbot.sh &  
[1] 21204  
[root@wazuh-fw bin]# ps uxf  
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START    TIME COMMAND  
root     20783  0.0  0.2 239768  8716 pts/0      S  08:04  0:00 sudo su  
root     20784  0.0  0.1 190464  4172 pts/0      S  08:04  0:00  \_ su  
root     20785  0.0  0.1 125000  4444 pts/0      S  08:04  0:00  \_ bash  
root     21204  0.0  0.0 119856  2988 pts/0      S  08:35  0:00  \_ /bin/bash ./alertbot.sh  
root     21205  0.0  0.0 114640   724 pts/0      S  08:35  0:00  \_ \_ sleep 10  
root     21206  0.0  0.1 162456  4252 pts/0      R+ 08:35  0:00  \_ ps uxf  
root          2  0.0  0.0     0   0 ?      S  07:33  0:00 [kthreadd]
```

Se realizó una prueba de funcionamiento enviando un mensaje de correo electrónico de prueba a la cuenta de "wazuh-user" y verificando la recepción de la alerta a través del bot de Telegram.

sudo echo "Hola" | mail -s "prueba mail" wazuh-user@localhost



Conclusión

La configuración de Wazuh con Telegram para alertas ofrece notificaciones instantáneas y personalizables en una plataforma segura y multiplataforma. Esto mejora la capacidad de respuesta y eficacia de la gestión de seguridad al permitir que los usuarios reciben alertas en tiempo real en sus dispositivos móviles y computadoras, garantizando la confidencialidad de la información enviada. Además, su fácil configuración la hace accesible para una amplia gama de usuarios.