UNIVERSIDAD LUTERANA SALVADOREÑA
FACULTAD DE CIENCIAS DEL HOMBRE Y LA NATURALEZA
LICENCIATURA EN CIENCIAS DE LA COMPUTACIÓN
CÁTEDRA DE REDES II

NOMBRE DEL PROYECTO:

Firewall con Sophos XG

NOMBRE DE LOS INTEGRANTES:

Nombre del integrante	Carnet
José Cruz Zabaleta Ceren	ZC01135718
Anderson Fernando Argueta Jovel	AJ01135837
Raul Ernesto Mendoza Herrera	MH01133312
Miguel Alejandro Torres Garcia	TG01135889

ASIGNATURA:

Redes II.

DOCENTE:

Lic. Eduardo Chachagua Alfaro.

CICLO/AÑO:

Ciclo 2/2022

FECHA:

29 de noviembre del 2022.

ÍNDICE

ÍNDICE DE IMÁGENES

INTRODUCCIÓN

El presente proyecto está desarrollado con la finalidad de implementar un firewall usando Sophos XG, se busca profundizar en el uso adecuado de las herramientas físicas y digitales, para ello presentamos conceptos generales que consideramos que definen las funciones de Sophos XG, para así proceder con una implementación adecuada y segura del firewall.

Sophos XG Home Edition es una versión totalmente gratuita de Sophos XG, disponible sin coste alguno para usuarios particulares.

Sophos XG es un firewall que protege la red de amenazas, acelera el tráfico que es más importante de Saas. Elimina un enorme punto ciego con la inspección **TLS** inteligente que es rápida y efectiva y que admite los estándares más recientes con numerosas excepciones y herramientas de políticas muy sencillas para facilitarle el trabajo.

Las características más importantes de Sophos XG son: incrementa su ancho de banda de Internet, controla la navegación en Internet de sus familiares, accede a su red doméstica desde cualquier lugar, etc.

Se presenta el manual de instalación y configuraciones del firewall Sophos Home Edition.

OBJETIVOS

OBJETIVO GENERAL:

Instalar el firewall Sophos XG y aprender sobre funcionalidad, aplicando redes.

OBJETIVO ESPECÍFICO:

- Conocer acerca del funcionamiento del firewall
- Configuraciones de redes en el firewall versión ipv6
- Implementar el Firewall XG tipo Sophos Home Edition de forma correcta.

Descripción del proyecto:

Sophos XG firewall, es una distribución basada en linux de código propietario que se encuentra en la versión 10.8.14.1 VE3.85.1 Agosto 2022 actualmente. Diseñado para exponer riesgos ocultos, bloquear amenazas tanto conocidas como desconocidas y responder automáticamente a los incidentes.Sophos XG Firewall ofrece una visibilidad inigualable de los usuarios de riesgo, las aplicaciones desconocidas y no deseadas, las amenazas avanzadas, las cargas sospechosas, el tráfico cifrado y mucho más.Ofrece toda la tecnología avanzada más moderna que necesita para proteger su red contra ransomware y amenazas avanzadas, como IPS de primera categoría, protección contra amenazas avanzadas tal y como esperamos para un sistema que será crítico en nuestra empresa. Su administración se realiza vía web, por lo que podremos hacerlo desde cualquier equipo con conexión a la red.En este caso se realiza la demostración de instalación de Sophos XG con su tipo de clasificación, la Sophos Firewall Home Edition dedicada para operar en hogares. Como ya mencionamos anteriormente es un software privado, es necesario comprar una licencia, pero en este tipo de sophos hay una gratis, esta es la que se ha utilizado para la demostración del proyecto. Como primer paso se procede a llenar un formulario para que vía correo electrónico recibir un código “que seria la licencia” y poder descargar la ISO del software, la cual pesa menos de 1 GB. Por lo que respecta a la instalación, se trata de una instalación típica de cualquier distribución Linux, donde tendremos que ir definiendo las características que queremos instalar en el firewall, cabe destacar que la instalación del firewall sophos home edition se realizó en un hipervisor “en este caso se utilizó VirtualBox”, la memoria RAM tiene que ser mayor a 4Gb. Añadir lo que vayamos a usar y en caso de necesitar más lo vamos añadiendo posteriormente. En este caso el proyecto consiste en la configuración de tres redes 2 red LAN y WAN LAN como servidor y una como cliente, con rango de IP versión IPv6 y IPv4.En este caso necesitaremos que tenga dos tarjetas de red, puesto que la primera le conectará a la red externa, WAN y otra para su conexión a la red interna LAN. Posteriormente, tendremos que dar los parámetros a la red, interna y externa.

Recordar que para ingresar a la cli la contraseña es admin cuando ya se ha configurados las interfaces de red, Abrir un navegador escribir https://192.168.56.200:4444 para proceder a realizar las configuraciones para la instalación de Sophos, aparece ventanas en la cuales es de elegir el idioma, region, zona horario, aceptar terminos y condiciones, escribir un usuario y contraseña y esperar a que se instale. Ya instalado muestra la ventana de login para acceder a el dashboard en el cual está toda la funcionalidad de Sophos Home Edition

Dentro de las características que nos permite Sophos Firewall Home Edition dedicada para operar en hogares podemos citar las siguientes características.

Funciona de forma paralela a la protección antivirus existente

Acceda a la red doméstica desde cualquier lugar.

Supervise y controle la navegación por Internet de su familia para garantizar su seguridad.

Anti-malware, seguridad web, filtrado de URL, control de aplicaciones y mucho más. De igual manera permite el filtrado de contenidos a través del proxy de manera rápida y fácil. También podemos filtrar el tráfico por protocolos, denegando el servicio por ejemplo para p2p.

MARCO TEÓRICO

FIREWALL.

Un firewall, también llamado cortafuegos, es un sistema cuya función es prevenir y proteger a nuestra red privada, de intrusiones o ataques de otras redes, bloqueando el acceso.

Permite el tráfico entrante y saliente que hay entre redes u ordenadores de una misma red. Si este tráfico cumple con las reglas previamente especificadas podrá acceder y salir de nuestra red, si no las cumple este tráfico es bloqueado.

De esta manera impedimos que usuarios no autorizados accedan a nuestras redes privadas conectadas a internet.

Se puede implementar en forma de hardware, de software o en una combinación de ambos.

Firewall por software:

Los firewalls de software lo ayudan a mantenerse protegido en lugares públicos. Se ejecutan como un programa en su computadora o dispositivo y observan de cerca el tráfico de la red para ayudar a interceptar programas maliciosos antes de que lleguen a su computadora.

Firewall por Hardware:

Los firewall de hardware vienen incluidos en algunos enrutadores y requieren poca o ninguna configuración, ya que están incorporados en su hardware. Estos firewall monitorean el tráfico de todas las computadoras y dispositivos que están conectados a la red de dicho enrutador, lo que significa que usted puede filtrar el acceso a todos ellos solo con una pieza de equipo.

Funciones de un Firewall.

-Crear una barrera que permita o bloquee intentos para acceder a la información en su equipo.

-Evitar que usuarios no autorizados accedan a los equipos y las redes de la organización que se conectan a Internet.

-Supervisar la comunicación entre equipos y otros equipos en Internet.

-Visualizar y bloquear aplicaciones que puedan generar riesgo

-Advertir de intentos de conexión desde otros equipos.

-Advertir de intentos de conexión mediante las aplicaciones en su equipo que se conectan a otros equipos.

-Detectar aplicaciones y actualizar rutas para añadir futuras fuentes de información

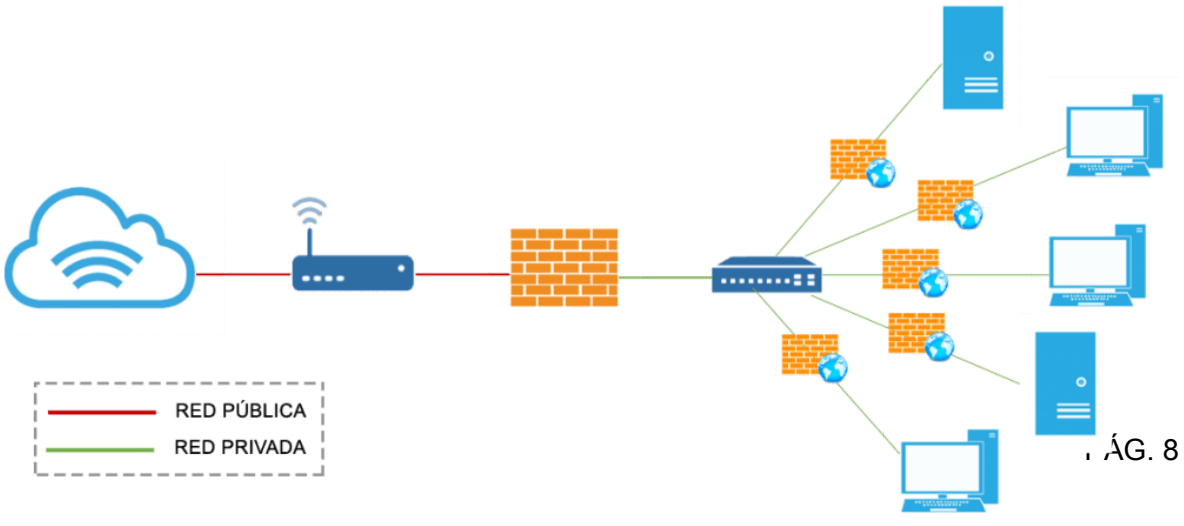
-Hacer frente a los cambios en las amenazas para la seguridad.

Métodos de filtración del tráfico.

Políticas de Firewall: Permiten bloquear o permitir determinados tipos de tráfico de red no especificados en una política de excepciones. El cortafuegos suspende cualquier petición de comunicación que no provenga de la red interna o del propio sistema de modo Nadie va a poder escanear la red, desde el exterior sólo se ve la dirección IP del cortafuegos, no se ven recursos internos dentro de la red.

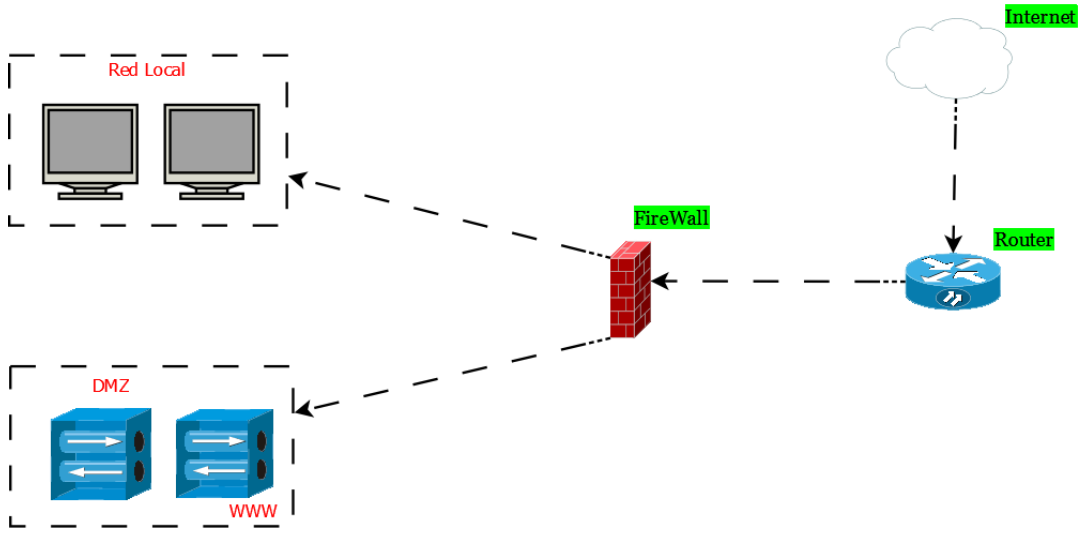
Antivirus Firewall: Servicio que incorporan algunos Firewall, es la primera línea de defensa para proteger la red interna contra ataques que provengan de Internet o enlace WAN.

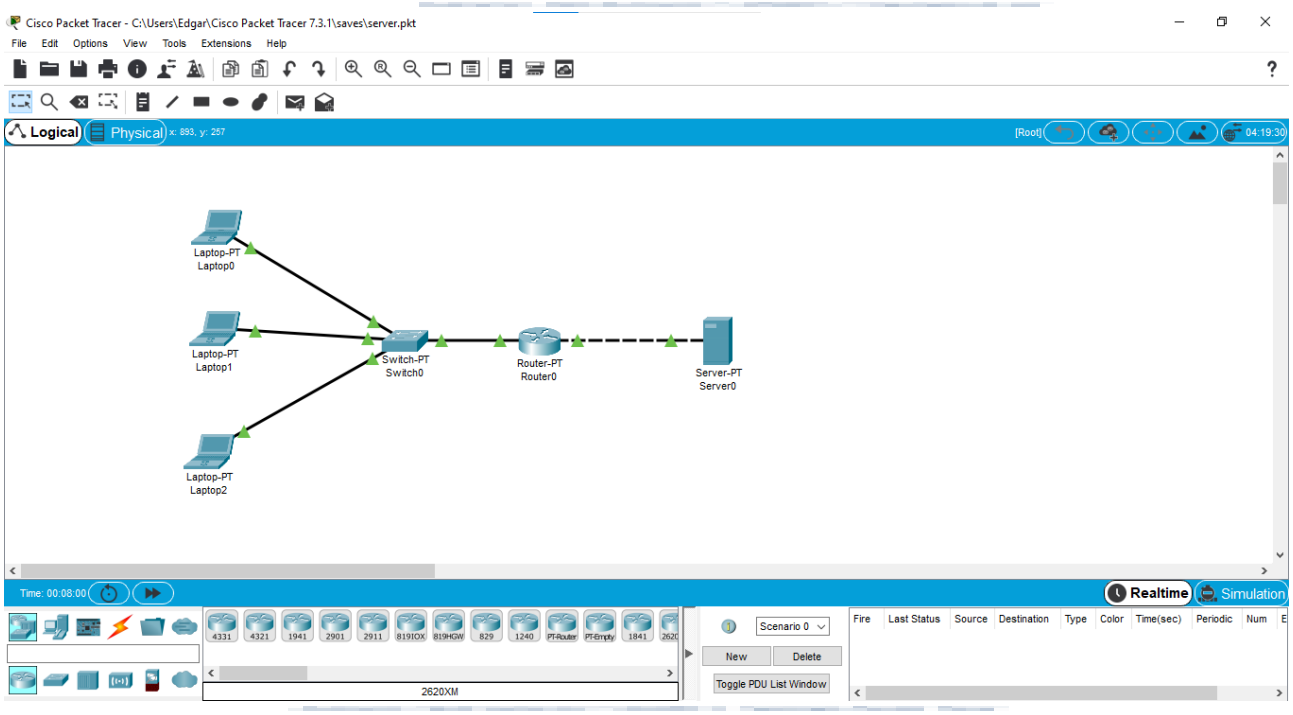
Servicios DPI: Se llama así a los procedimientos de Inspección Profunda de Paquetes (IPP o DPI por sus siglas en inglés: Deep Package Inspection). Permite al administrador controlar aplicaciones específicas conocidas como troyanos y aplicaciones de puerta trasera que pueden infiltrarse en su red interna.
Su función es añadir una segunda capa de seguridad al sistema, revisando el contenido profundo de los paquetes de información recibidos, proporcionando al administrador la flexibilidad para bloquear programas específicos que no están permitidos en la red.

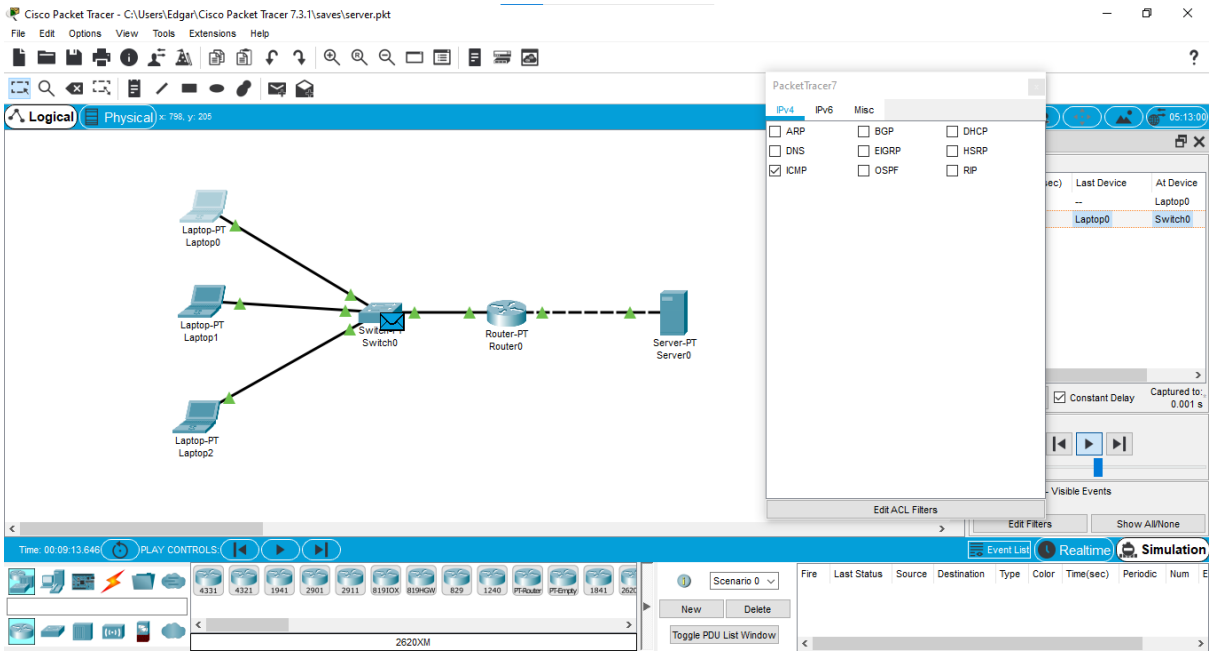


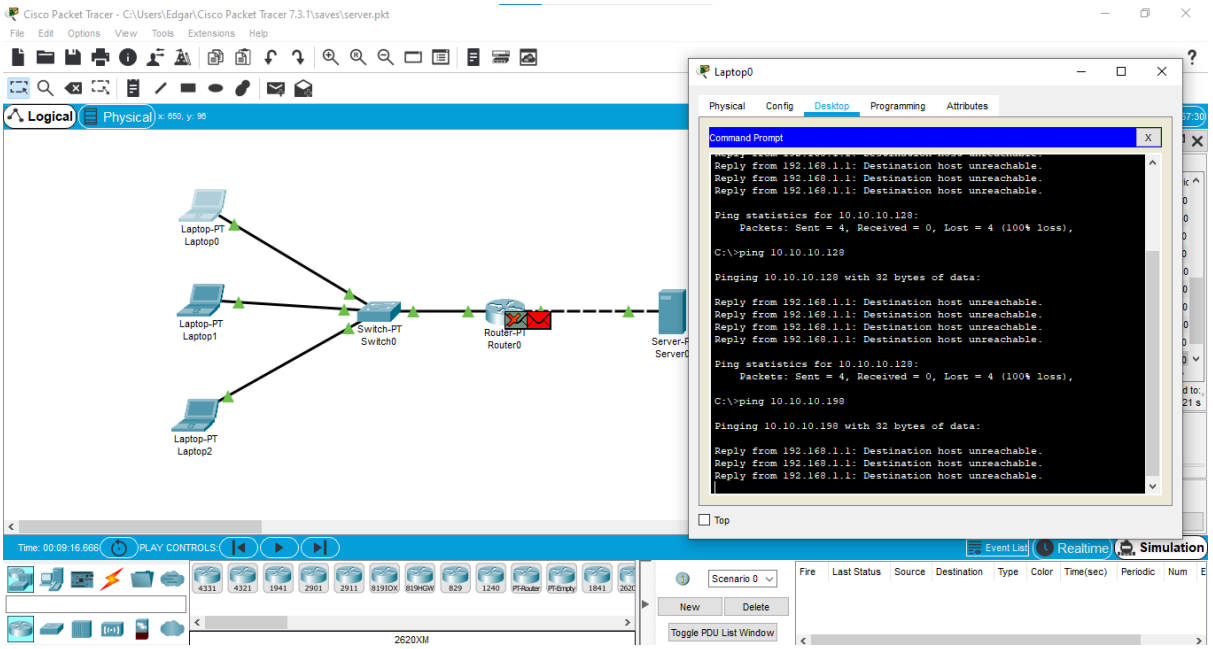
TOPOLOGÍA DE RED

Topología de Red Híbrida






Cisco Packet Tracer - C:\Users\Edgar\Cisco Packet Tracer 7.3.1\saves\server.pkt
File Edit Options View Tools Extensions Help
Logical
Physical
PacketTracer7
IPv4 IPv6 Misc
ARP
BGP
DHCP
DNS
EIGRP
HSRP
ICMP
OSPF
RIP
Edit ACL Filters
Laptop-PT Laptop0
Laptop-PT Laptop1
Laptop-PT Laptop2
Switch-PT Switch0
Router-PT Router0
Server-PT Server0
Constant Delay
Captured to: 0.001 s
Visible Events
Edit Filters
Show All/None
Event List
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
2620XM


Cisco Packet Tracer - C:\Users\Edgar\Cisco Packet Tracer 7.3.1\saves\server.pkt
Logical
Physical
Laptop0
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Ping statistics for 10.10.10.128:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 10.10.10.128
Pinging 10.10.10.128 with 32 bytes of data:
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Ping statistics for 10.10.10.198:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 10.10.10.198
Pinging 10.10.10.198 with 32 bytes of data:
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Top
Laptop-PT Laptop0
Laptop-PT Laptop1
Laptop-PT Laptop2
Switch-PT Switch0
Router-PT Router0
Event List
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
2620XM

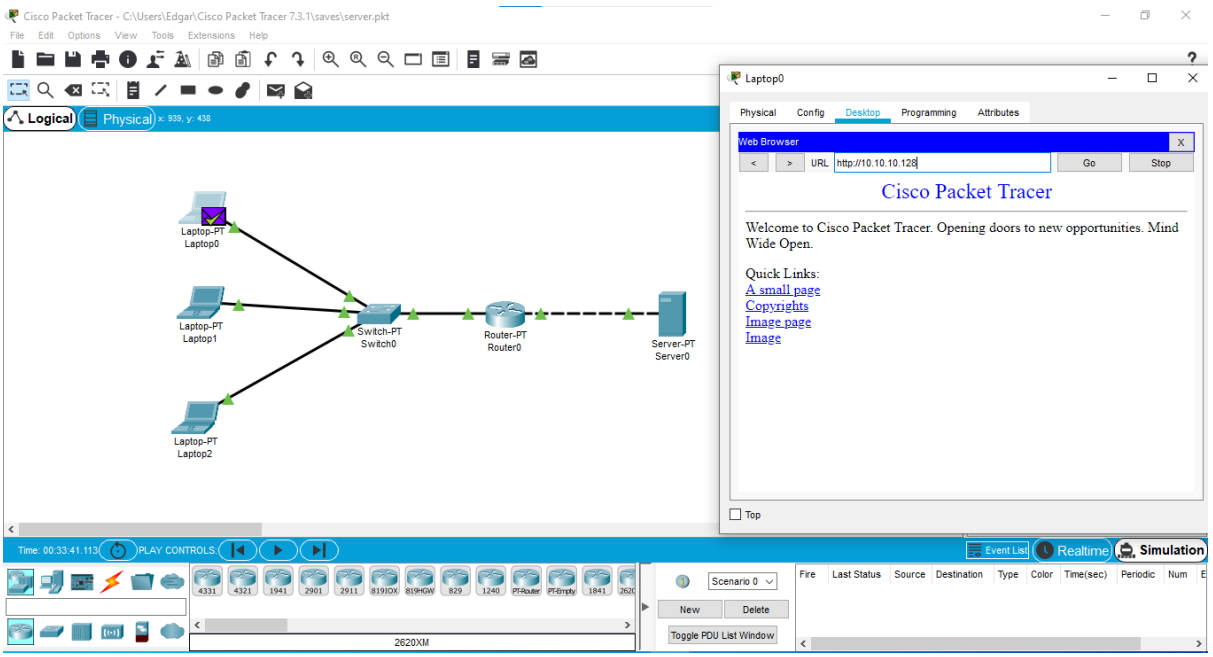


Ilustración 6: Carga de Firewall

Linux Firewall - Sophos XG

La aplicación de firewall de Linux permite a los administradores simplemente abrir puertos (o rangos de puertos) para los servicios que se ejecutan localmente en el servidor. Si un servicio requiere que se realicen conexiones desde fuera de su red (es decir, ejecutar un servicio web o de correo en un sistema configurado para puerta de enlace y servidor), será necesario agregar un puerto o rango de puertos correspondiente a través de esta aplicación.
Disponible en versión de 64 bits con interfaz gráfica de usuario web limpia y funcional, el firewall.
Sophos es una empresa de seguridad informática (tanto de software como de hardware) con sede en Abingdon - on-Thames, Inglaterra (Reino Unido). Ofrece productos de punto final de comunicación, cifrado, seguridad de red, seguridad de correo electrónico y seguridad móvil y también un producto de gestión de amenazas Unificado; se centra principalmente en proporcionar seguridad a organizaciones y empresas. SophosLabs es la red global de centros de desarrollo y análisis de amenazas cibernéticas de la compañía.

Sophos XG Firewall ofrece una visibilidad inigualable de los usuarios de riesgo, las aplicaciones desconocidas y no deseadas, las amenazas avanzadas, las cargas sospechosas, el tráfico cifrado y mucho más.

Sophos XG Firewall le ofrece toda la tecnología avanzada más moderna que necesita para proteger su red contra ransomware y amenazas avanzadas, como IPS de primera.

XG Firewall es la única solución de seguridad para redes que puede identificar totalmente el origen de una infección en la red y responder limitando el acceso a los otros recursos de red de forma automática.

Tiene diferentes características.

Inspección SSL de Xstream: Según las últimas estadísticas, aproximadamente el 80 % del tráfico web está cifrado, por lo que es invisible para la mayoría de firewalls. Una cantidad cada vez mayor de malware y aplicaciones no deseadas se aprovechan de que las empresas simplemente no utilizan la inspección SSL.

FastPath del flujo de red de Xstream: El tráfico que se sabe que es seguro puede descargarse a la ruta rápida FastPath del flujo de red de Xstream. Esta ruta acelerada para el tráfico de confianza potencia drásticamente el rendimiento al liberar recursos de las tareas de inspección de tráfico innecesarias.

Motor DPI de Xstream: Creemos que no debería tener que escoger nunca entre la seguridad y el rendimiento. XG Firewall incluye un motor de inspección detallada de paquetes (DPI) de alta velocidad para que pueda escanear su tráfico en busca de amenazas sin un proxy que ralentice el proceso.

Sophos Central es la base sobre la que se sustenta todo lo que hacemos. Nuestra plataforma de administración en la nube proporciona un único panel intuitivo para gestionar no solo sus firewalls, sino también toda su gama de soluciones de seguridad de Sophos.

Administración centralizada

Administrar fácilmente múltiples firewalls Sophos Central es la plataforma de gestión en la nube definitiva para todos sus productos Sophos. Facilita la configuración, supervisión y gestión diarias de XG Firewall.

- Configure cambios y aplíquese a un grupo de firewalls o gestione cada firewall individualmente.
- Administre todos sus dispositivos XG Firewall y demás productos de Sophos desde una única consola.
- Cree una programación de copia de seguridad y almacene hasta 5 copias en la nube.

Generación de informes de firewall en la nube

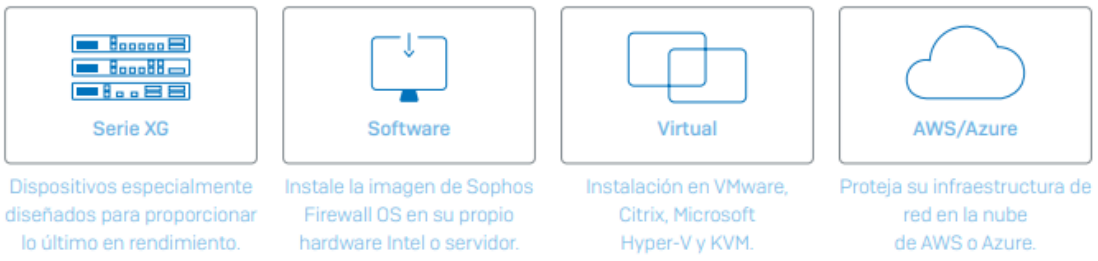
Sophos Central incluye potentes herramientas para la generación de informes que le permiten visualizar la actividad de la red, web y de las aplicaciones y la seguridad a lo largo del tiempo.

- Incremente su visibilidad de la actividad de la red a través de análisis.

- Analice datos para identificar carencias de seguridad, comportamientos sospechosos de los usuarios u otros eventos que requieran cambios en las políticas.

- Utilice los módulos predefinidos o personalizar cada informe para casos de uso específicos.

XG Firewall ofrece una amplia gama de dispositivos de hardware de alto rendimiento, soporte para todas las plataformas de virtualización más habituales y la nube pública y entornos híbridos de AWS y Azure, e incluso un dispositivo de software que se puede instalar en su propio hardware.



Datos Generales sobre este:

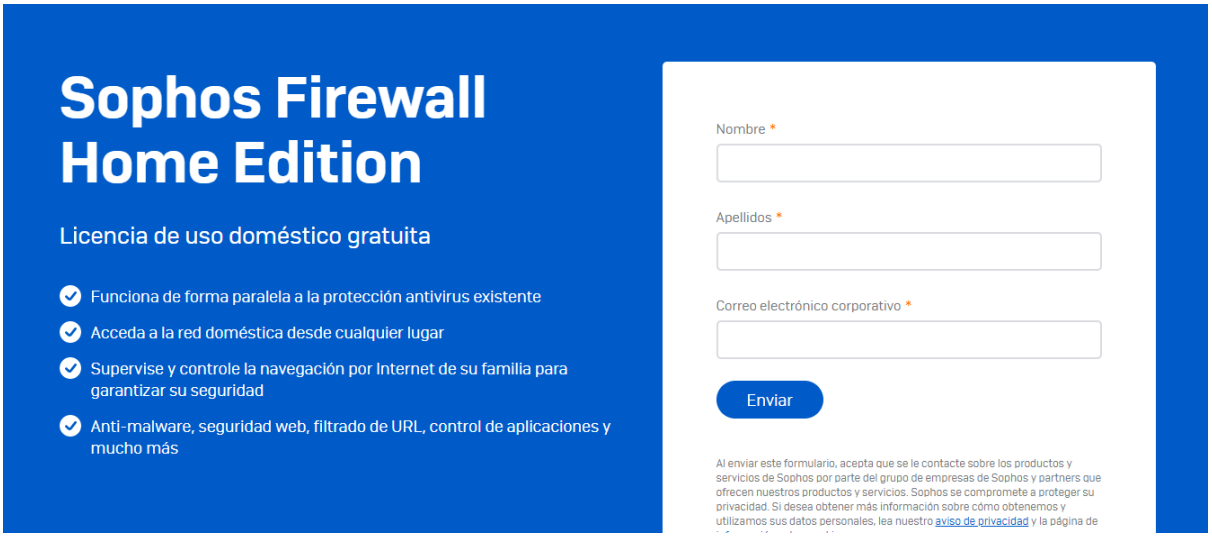
ÚLTIMA VERSIÓN:

10.8.14.

COSTO:

Privativo

En este caso utilizaremos la demostración del Sophos Home Edition.



Nuestro XG Firewall para uso doméstico gratuito es una versión de software totalmente equipada de Sophos XG Firewall, disponible sin costes para usuarios particulares y sin ningún compromiso. Incluye una protección completa para su red doméstica, incluidos antimalware, seguridad web y filtrado de URL, control de aplicaciones, IPS, conformado de tráfico, VPN, informes y control, y mucho más.

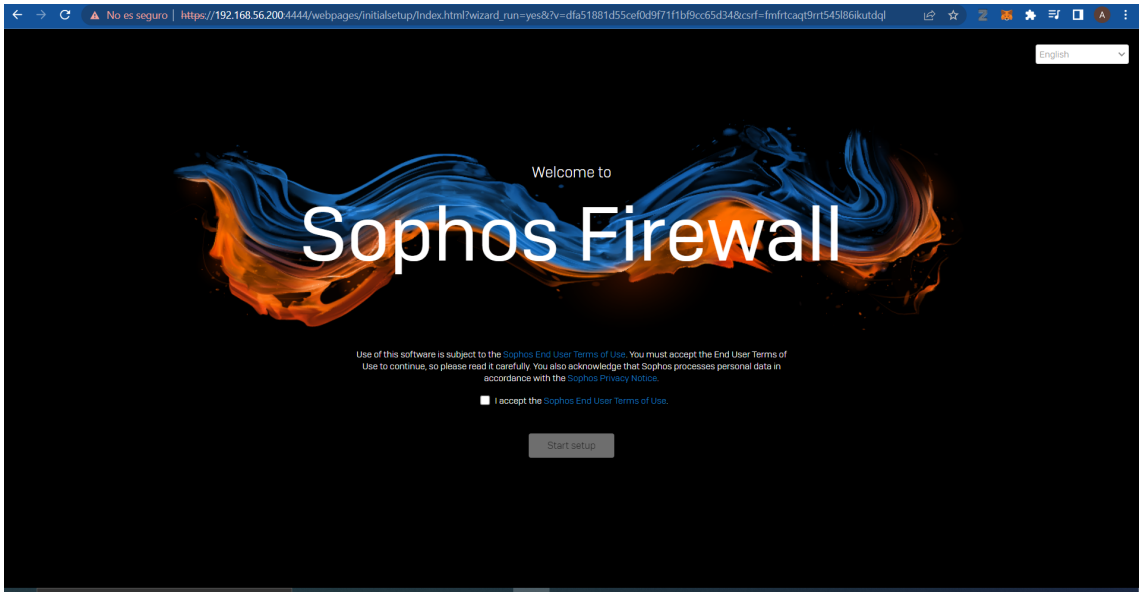
NOTA: El XG Firewall para uso doméstico gratuito de Sophos incluye su propio sistema operativo y sobrescribe todos los datos almacenados en el ordenador durante el proceso de instalación. Por lo tanto, es necesario un equipo independiente dedicado, que se convertirá en un dispositivo de seguridad totalmente funcional. ¡Perfecto para ese ordenador de más que tiene en un rincón!

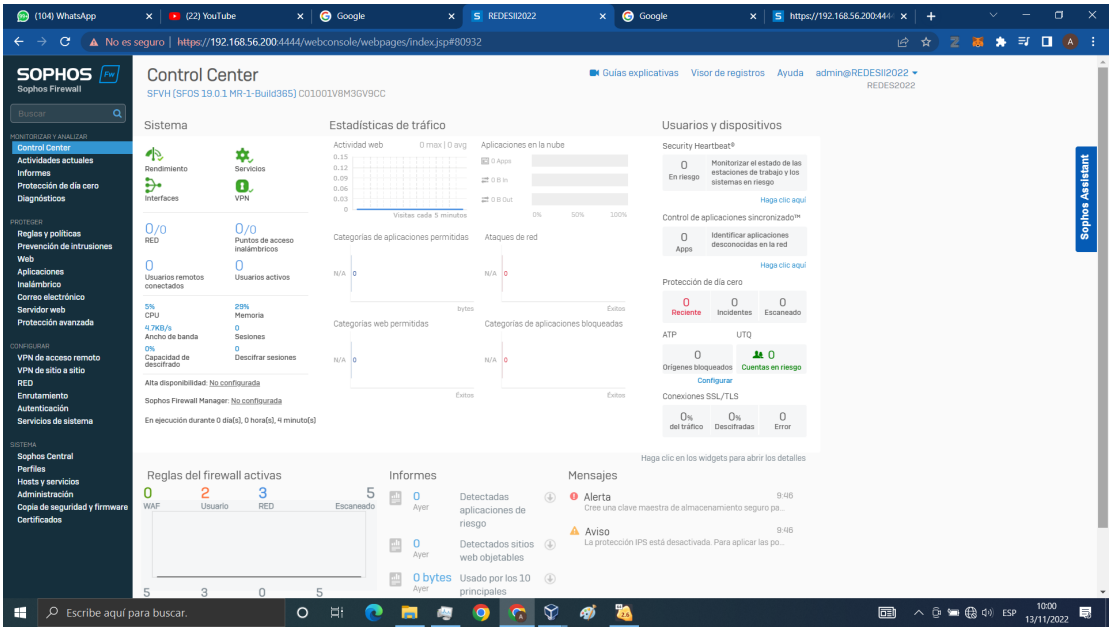
Características de Sophos Home Edition.

- Incremente su ancho de banda de Internet: puede utilizar fácilmente el conformado de tráfico para priorizar el tráfico de aplicaciones a través de su conexión a Internet e incluso suscribirse a múltiples conexiones ISP para conseguir más ancho de banda o resiliencia en el caso de que se produzca una interrupción en alguna de ellas.

- Supervise y controle la navegación en Internet de sus familiares: utilice el filtrado web para evitar que los sitios le infecten con virus y spyware, impedir que sus hijos accedan a sitios malintencionados y obtener informes completos sobre la actividad en su hogar. También puede establecer programaciones de acceso o cuotas de uso para miembros de su familia que estén pasando demasiado tiempo online.

- Acceda a su red doméstica desde cualquier lugar: utilice una VPN para acceder a su red de forma remota desde cualquier parte del mundo.




(104) WhatsApp
(22) YouTube
Google
REDESII2022
Google
https://192.168.56.200:444
No es seguro | https://192.168.56.200:4444/webconsole/webpages/index.jsp#80932
SOPHOS
Sophos Firewall
Control Center
SFVH (SFOS 19.0.1 MR-1-Build365) C01001V8M3GV9CC
Guías explicativas
Visor de registros
Ayuda
admin@REDESII2022
REDES2022
Sistema
Rendimiento
Servicios
Interfaces
VPN
0/0
RED
0/0
Puntos de acceso inalámbricos
0
Usuarios remotos conectados
0
Usuarios activos
5%
CPU
29%
Memoria
4.7KB/s
Ancho de banda
0
Sesiones
0%
Capacidad de descifrado
0
Descifrar sesiones
Alta disponibilidad: No configurada
Sophos Firewall Manager: No configurada
En ejecución durante 0 día(s), 0 hora(s), 4 minuto(s)
Estadísticas de tráfico
Actividad web
Aplicaciones en la nube
Categorías de aplicaciones permitidas
Ataques de red
Categorías web permitidas
Categorías de aplicaciones bloqueadas
Usuarios y dispositivos
Security Heartbeat®
0
En riesgo
Monitorizar el estado de las estaciones de trabajo y los sistemas en riesgo
Haga clic aquí
Control de aplicaciones sincronizado™
0
Apps
Identificar aplicaciones desconocidas en la red
Haga clic aquí
Protección de día cero
0
Reciente
0
Incidentes
0
Escaneado
ATP
UTQ
0
Orígenes bloqueados
0
Cuentas en riesgo
Configurar
Conexiones SSL/TLS
0%
del tráfico
0%
Descifradas
0
Error
Haga clic en los widgets para abrir los detalles
Sophos Assistant
Reglas del firewall activas
0
WAF
2
Usuario
3
RED
5
Escaneado
Informes
0
Ayer
Detectadas aplicaciones de riesgo
0
Ayer
Detectados sitios web objetables
0 bytes
Ayer
Usado por los 10 principales
Mensajes
Alerta
9:46
Cree una clave maestra de almacenamiento seguro pa...
Aviso
9:46
La protección IPS está desactivada. Para aplicar las po...
Escribe aquí para buscar.
ESP
10:00
13/11/2022

CRONOGRAMA DE ACTIVIDADES

Actividades	Meses (Semanas)															
	Agosto				Septiembre				Octubre				Noviembre			
Desarrollo de los objetivos del proyecto																
Recopilación de información para marco teórico																
Elección de topología de red																
Desarrollo de presupuesto general del proyecto																
Instalación y configuración de Sophos Home Edition																
Implementación de firewall Sophos Home Edition																
Pruebas generales del proyecto.																
Documentación, Demostración																

PRESUPUESTO

Tabla de presupuesto		
Cantidad-Material:	**Imagen:**	**Precio:**
1 Tarjeta de Red		$16.95
2 Cables de Red		$2.50
1 Computadora		$700

1 Router		$22.50

CONCLUSIONES

Para la realización del proyecto de instalación e investigación de Sophos XG, instalamos Sophos XG versión Home Edition es una versión que nos permite a los usuario tener seguridad de forma gratuita. Sophos XG nos permite configurar en IPv6 y IPv4.

Sophos XGs ofrece la mejor visibilidad, protección y rendimiento del sector, el XG firewall de uso doméstico gratuito de Sophos incluye su propio sistema operativo y sobreescribe todos los datos almacenados en el ordenador.

Bibliografía:

- Solís, A. I., Alvarado, P. V., Villaseñor, A. A., Camaré, L. J. M., Peláez, R. M., & Brust, A. M. O. (2018). EVALUACIÓN DE FIREWALLS BASADOS EN SOFTWARE LIBRE (FIREWALL EVALUATION BASED ON OPEN SOURCE SOFTWARE). Pistas Educativas, 40(130).

- Correa Bedoya, D. M., & Giraldo Echeverri, L. (2017). Diseño e implementación de políticas de seguridad a nivel de firewall perimetral y proxy en la red LAN del semillero OTM Bloque O Sede Fraternidad ITM.

SOPHOS. (s. f.). *Cybersecurity Delivered | Sophos Security Solutions*. Recuperado 29 de noviembre de 2022, de https://www.sophos.com/es-es/products/free-tools/sophos-xg-firewall-home-edition/software

Sophos XG Firewall. (s. f.). Sophos. Recuperado 29 de noviembre de 2022, de https://www.sophos.com/es-es/medialibrary/pdfs/factsheets/sophos-xg-series-appliances-brna.pdf

Sophos - Adquisiciones y asociaciones, Historia, Perfil | KripKit. (s. f.). https://kripkit.com/sophos/

AlbertoLopez TECH TIPS. (2020, 26 julio). 📌*[FIREWALL o CORTAFUEGOS] ¿Qué Es? y TIPOS de Firewalls ► Conocimientos BÁSICOS ESENCIALES* [Vídeo]. YouTube. https://www.youtube.com/watch?v=kH6oP6JUnHI

RECOMENDACIONES

-Como principal recomendación se daría tener los implementos necesarios para no parar los trabajos por falta de implementos.

-Trabajar necesariamente en una sola máquina para no tener problema de algún tipo por cambiar de máquina.

- Investigar sobre el tema antes de ponerse a implementar para evitar inconvenientes en el tiempo de realización de los trabajos.

Glosario:

Firewall:
El cortafuegos o firewall en inglés, en el mundo de la informática es un sistema de seguridad para bloquear accesos no autorizados a un ordenador mientras sigue permitiendo la comunicación de tu ordenador con otros servicios autorizados.

ClearOS:
Es una distribución GNU/Linux basada en CentOS y Red Hat; su creación proviene de ClearOS Enterprise, la cual creó la ClearFoundation organizadora y desarrolladora de esta distribución, donde su entorno de escritorio predeterminada puede ser KDE o GNOME Shell.

LAN:
Abreviatura para Local Area Network (Red de Area Local), es una red que cubre un área geográfica pequeña, como hogares, oficinas y grupos de edificios.

WAN:
Abreviada de Wide Area Network (Red de Area Amplia), es una red que cubre áreas geográficas más grandes que pueden abarcar todo el mundo.

Deep Packet Inspection o Inspección a fondo de los paquetes:
Es el acto de inspección realizado por cualquier equipo de red de paquetes que no sea punto final de comunicación, utilizando con algún propósito el contenido que no sea el encabezamiento del paquete.

ANEXOS

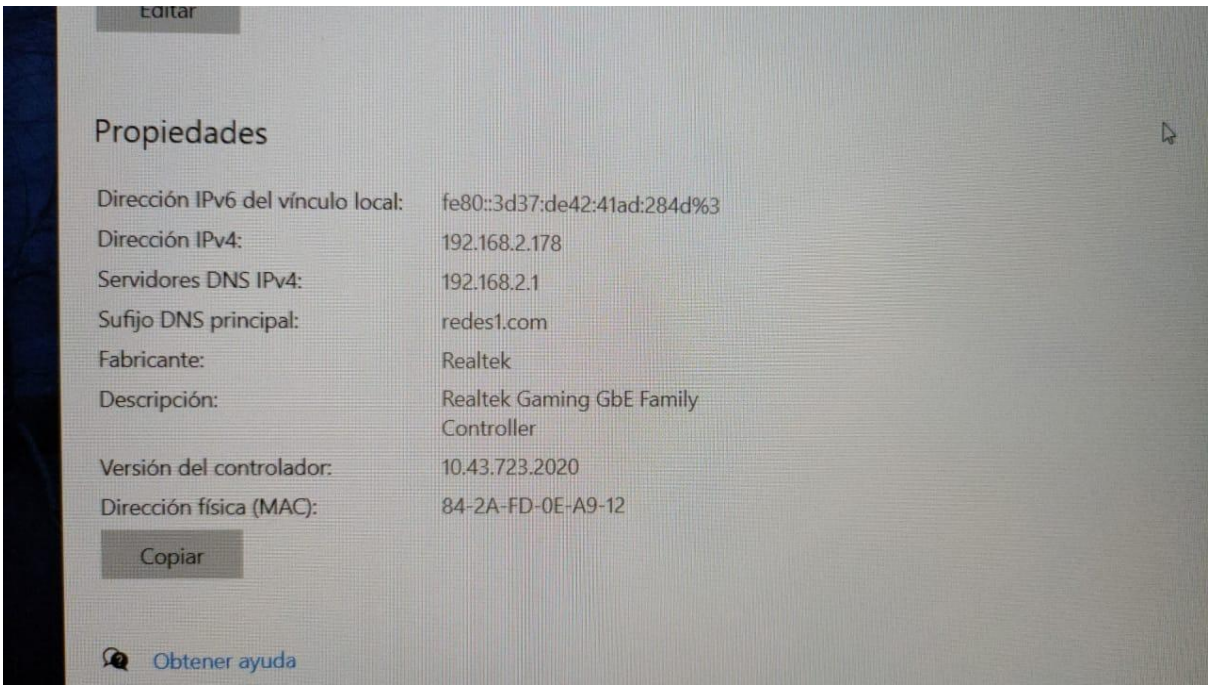


Ilustración 8: Conexión a Firewall desde computadora

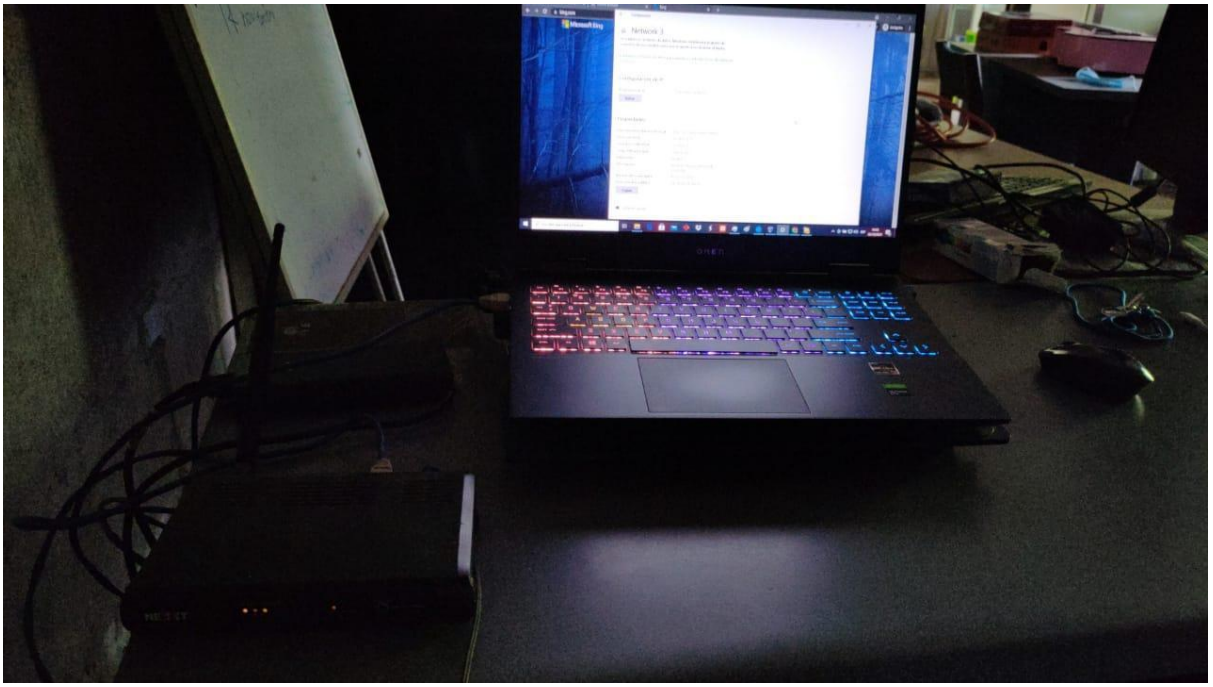


Ilustración 9: proyecto montado

Link de video demostrativo: https://www.youtube.com/watch?v=8mfuxndm7NU