



## VPN SITE TO SITE WITH SOPHOS

**Nombre Estudiante:** Alejandro Vilches Luna

**Ciclo Superior de Administración de Sistemas Informáticos en Redes**

**IES Medina Azahara**

**Fecha entrega:** 15/06/2023



Esta obra está sujeta a una licencia de Reconocimiento - No Comercial - Sin Obra Derivada [4.0 España de Creative Commons](https://creativecommons.org/licenses/by-nc-nd/4.0/es/)

## FICHA DEL PROYECTO FINAL

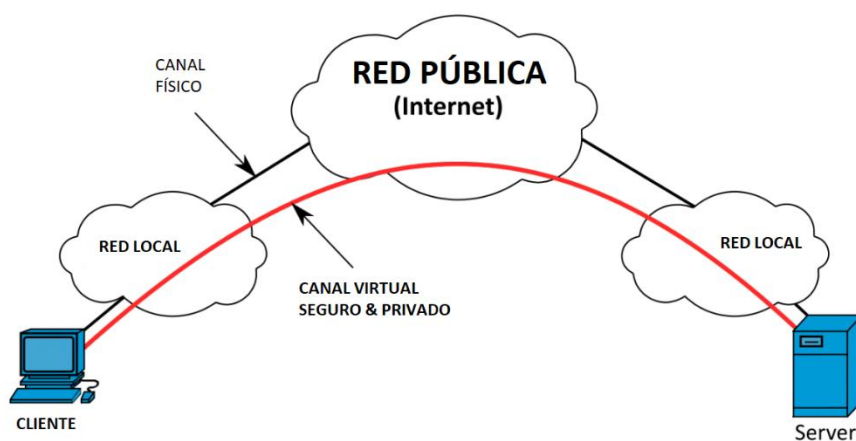
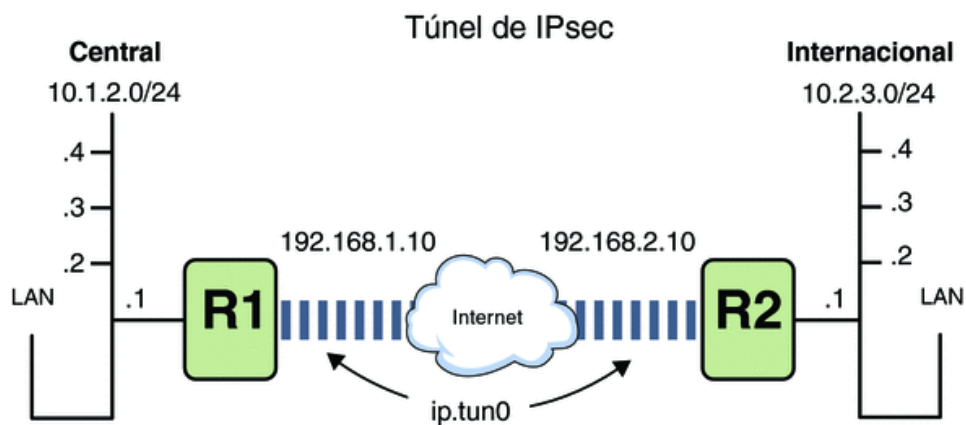
<b>Título del trabajo</b>	VPN-IPSEC SITE TO SITE WITH SOPHOS
<b>Nombre del autor</b>	Alejandro Vilches Luna
<b>Fecha de entrega (mm/aaaa)</b>	15/06/2023
<b>Área del Trabajo Final</b>	Seguridad en Redes.
<b>Ciclo Grado Superior</b>	Administración de Sistemas Informáticos en Red
<b>Resumen</b>	
<p>El presente proyecto trata sobre la implementación de dispositivos de seguridad en red mediante Sophos, mediante la creación de VPN o túneles IPSec para la interconexión de edificios, Gestionando así la realización de sus actividades de forma local entre edificios de forma segura, aumentando también la posibilidad de conexión tanto en la sucursal como de cualquier parte con la configuración de la VPN. Mediante la VPN con Sophos <b>segurizamos la información, ahorramos costes</b> de replicación de todos los servidores y garantizamos la <b>integridad en los datos</b> con la implementación del firewall de Sophos.</p>	

## Índice

1. Introducción.....	1
1.1 Contexto y justificación del Proyecto.....	1
1.2 Objetivos del Proyecto.....	3
1.3 Enfoque y método seguido.....	4
2. Propuesta de Solución .....	5
2.1 Análisis descriptivo.....	5
2.2 Análisis de requisitos.....	5
2.3 Limitaciones .....	6
2.4 Alcance.....	7
2.5 Marco de Referencia .....	7
2.6 Procedimientos.....	8
2.7 Descripción de las actividades .....	8
2.8 Análisis Final .....	10
3. Temporalización .....	11
3.1 Identificación de tareas.....	11
3.2 Secuenciación .....	12
4. Memoria Técnica.....	13
4.1 Especificaciones de implementación.....	13
4.1.1 Manual de instalación de Sophos XG.....	13
4.1.2 Manual de instrucciones de Sophos SD-RED.....	14
4.1.3 Realización de un túnel IPSec mediante Sophos.....	16
4.1.4 Realización de VPN SSL mediante Sophos .....	21
4.2 Seguimiento y control .....	28
5. Estudio Presupuestario .....	30
6. Conclusiones.....	31
6.1 Debilidades.....	31
6.2 Amenazas .....	32
6.3 Fortalezas.....	32
6.4 Oportunidades.....	32
6.5 Ampliaciones Futuras .....	33
6.6 Escalabilidad .....	33
7. Bibliografía y Referencias.....	34
8. Anexos .....	35
8.1 Lista de Acrónimos.....	35

## Lista de Imágenes

# SOPHOS



# 1. Introducción

## 1.1 Contexto y justificación del Proyecto

### 1.1.1 **Antecedentes.**

Una empresa privada ha crecido exponencialmente durante los últimos 2 años desde su creación, observando los resultados que han obtenido han decidido abrir una nueva sucursal con el objetivo de seguir expandiéndose. Esta empresa cuenta con la sucursal (central) y ha creado otra sucursal (nuevo). Donde van a necesitar compartir recursos entre las dos ubicaciones y a su vez que la conexión sea segura.

### 1.1.2 **Definición del Problema.**

Una empresa acaba de abrir una nueva sucursal, necesita compartir recursos y poder conectarse con la central para poder trabajar. Mediante la solución que ofrecemos pueden estar conectadas las dos sucursales para compartir recursos, trabajar de manera segura, implementar reglas a nivel de servidor firewall para crear un cortafuegos, garantizar la seguridad y la integridad de los datos.

Permitiendo a los empleados de las dos sucursales compartir recursos entre sí. Para conectar los dos edificios necesitamos dos dispositivos, en la sucursal central un firewall XG y en la sucursal nueva necesitamos un SD-RED.

Implementando esos dispositivos y una instalación acorde a la empresa, se garantiza que los datos sean protegidos y filtrados.

### 1.1.3 Justificación.

Mediante la solución que proponemos se podrá trabajar de forma local entre las dos sucursales compartiendo recursos con la seguridad de estar realizando una conexión remota securizado por la potencia de un cortafuegos, todas las conexiones se hacen sin tener que salir hacia internet mediante un túnel IPSec o mediante una conexión vía VPN SSL.

Esta implementación se potencia día a día gracias al cortafuegos con autoaprendizaje que tiene Sophos.

Debido al crecimiento de la empresa y la necesidad de centralización de ciertos procesos y flujos de trabajo para la mejora de la gestión y calidad.

Algunas de sus características principales:

- **Seguridad en la información:** ya que todo lo que vaya mediante la VPN estará cifrado de extremo a extremo y es mucho más difícil que un tercero se haga con la información.
- **Ahorrar costes:** ya que no hay que replicar los servidores ni las aplicaciones en el nuevo edificio.
- **Integridad en los datos:** Al implementar el firewall de Sophos vamos a proteger aún más las conexiones y sobre todo los datos.
- **Escalabilidad:** Mediante la VPN, si la empresa sigue creciendo se pueden agregar sitios, además, Sophos tiene una amplia gama de seguridad y redes para aumentar las necesidades si hay una evolución.

Se necesitará una infraestructura de red para poder soportar la conexión VPN y un dispositivo de firewall de Sophos con su respectiva licencia para garantizar que se implementen medidas adecuadas de autenticación, encriptación y protección de datos. Necesitaremos también un plan de políticas de seguridad para que la implantación de la VPN cumpla con dichas políticas.

Se tiene que tener en cuenta los recursos a necesitar para la realización de este proyecto, como puede ser el costo de los equipos de red, el personal necesario para configurar y mantener la VPN y el firewall de Sophos, el ancho de banda necesario para soportar la conexión y la licencia del Firewall de Sophos.

## 1.2 Objetivos del Proyecto

Los objetivos principales de nuestro proyecto a la hora de la realización de una VPN pueden ser:

- **Conexión Segura:** Establecer una conexión cifrada y segura entre las dos sucursales, lo que garantiza que estén protegidas de ataques y amenazas cibernéticas.
- **Compartir Recursos:** Compartir recursos entre las dos sucursales, puede incluir archivos, base de datos, aplicaciones y servicios en línea. Lo que permite trabajar de manera conjunta con mayor eficiencia y efectividad.
- **Redundancia de servicios:** Si una de las dos sucursales experimenta una pérdida de red por cualquier incidencia, la otra red puede continuar trabajando sin tener ningún tipo de problema, lo que garantiza la continuidad del negocio.
- **Mejora la colaboración:** La conexión entre las dos sucursales permiten a los empleados trabajar de forma conjunta para ser más eficientes y poder compartir información sobre algún tipo de proyecto y solucionar los problemas con mayor rapidez y facilidad.
- **Configurar Sophos:** Para garantizar la seguridad entre las dos sucursales a la hora de conectarse mediante la VPN, podemos crear reglas para la protección de datos durante la transmisión.
- **Copias de Seguridad:** Mediante el túnel IPSec podemos guardar todo tipo de archivos sin tener que realizar una conexión mediante internet hacia los servidores de copias de la empresa, es un gran factor al poder securizar la subida de archivos y directorios mediante red local.



## 1.3 Enfoque y método seguido

Tenemos dos posibles estrategias que llevar a cabo, mediante un dispositivo o mediante un fichero de configuración por cada usuario. Esta segunda no necesita el dispositivo para poder realizar la conexión con la sucursal.

**Túnel IPSec:** Mediante este método podemos tener una conexión de forma local sin tener que salir hacia internet con la implementación de un dispositivo [SD-RED](#), conectamos redes ubicadas en puntos geográficamente separados. Trae un asistente de configuración inicial para poder establecer conectividad con el Sophos XG y asegurarnos que el dispositivo está registrado correctamente.

Necesitamos configurar la dirección IP, la configuración del enlace VPN, la conexión con el Sophos XG. Una vez configurado, comprobamos la comunicación entre los sitios remotos y la red central esté establecida de manera adecuada.

Esta implementación permite tener una conectividad LAN entre las dos ubicaciones geográficamente separadas, con una buena seguridad y sistema de monitoreo para asegurarse de que funciona todo correctamente.

**VPN SSL:** Este método se puede implementar de dos formas.

1. **Mediante Túnel IPSec:** Sophos nos permite crear ficheros VPN para conectarnos mediante usuarios por el túnel IPSec realizado. Es decir, aparte de tener directamente acceso de forma local desde la sucursal nuestros usuarios podrán conectarse mediante VPN SSL con un programa llamado Sophos Client a la red de la sucursal para poder trabajar de forma local con la red del Sophos XG.
2. **Mediante Acceso Remoto:** Con este método no necesitamos un dispositivo SD-RED. Sin embargo, es más aparatoso porque tendremos que crear un usuario para cada trabajador que necesite conectarse con la sucursal central para utilizar los recursos en forma local.

La estrategia más apropiada para esta situación es la implementación mediante el dispositivo SD-RED. No necesitas estar creando usuarios cada vez que se necesite trabajar con recursos de otra sucursal y no se está abriendo el túnel mediante el programa. Con esta solución el túnel siempre está abierto para poder trabajar con los recursos de la otra sucursal sin tener que utilizar ningún programa ni crear usuarios. Con la seguridad de no tener que salir hacia internet para conectarte.

## 2. Propuesta de Solución

### 2.1 Análisis descriptivo

La solución que ofrecemos es un servicio remoto como si fuese local securizado por la potencia del cortafuegos con autoaprendizaje de sophos.

Usuarios de distintas sucursales puedan acceder a los servicios y datos centrales en condiciones de seguridad. Mediante instalación de un firewall central en la sucursal central y un dispositivo SD-RED en la sucursal nueva.

Con escalabilidad de poder abrir nuevas sucursales y ampliando el radio de conexión con las demás sucursales de una manera segura, rápida y eficaz.

Sophos ofrece unas subvenciones para empresas para no tener que correr todos los gastos la propia empresa.

### 2.2 Análisis de requisitos

Los requisitos que se necesitan para montar un sistema sophos en una empresa son:

- Router.
- Firewall XG de Sophos.
- Dispositivo SD-RED de Sophos (Un dispositivo por cada sucursal que no sea la central).
- Licencias de software.
- Personal cualificado.

La ventaja es que terminado la instalación la escalabilidad de sucursales es muy sencilla y bastante rápida.

## 2.3 Limitaciones

Para la realización de nuestro proyecto VPN estas son algunas de las limitaciones que tenemos que tener en cuenta:

- **Ancho de Banda:** La velocidad y el ancho de banda de las conexiones a internet pueden limitar la capacidad de la VPN para transmitir grandes cantidades de datos. Si la conexión es lenta o inestable, puede traer retrasos o interrupciones en la transmisión de datos, lo que puede afectar la calidad de la conexión VPN.
- **Seguridad:** La seguridad es la preocupación más importante al implementar una VPN punto a punto. La configuración incorrecta, la selección de protocolos de seguridad y la desactualización puede hacer que la conexión sea vulnerable a ataques. Es importante seleccionar cuidadosamente los protocolos de seguridad y mantener la configuración actualizada para proteger la información de la empresa.
- **Limitaciones del hardware:** Algunos dispositivos de red pueden tener una capacidad limitada para manejar grandes cantidades de tráfico de VPN, lo que puede afectar el rendimiento de la conexión.
- **Configuración de Sophos:** Hay que estar claro las reglas que se ponen en la configuración de Sophos y dejarlas en algún lado de guía para tenerlas de referencia. Porque si ponemos una regla mal, dejamos sin funcionamiento la VPN entre los dos edificios.
- **Corte de suministros:** Se debe implementar una prevención de riesgos a la hora de los suministros como puede ser un corte de luz, extintores de CO2, prevención contra incendios e inundaciones.

Estos factores son importantes tenerlos en cuenta antes de la elección para que cuando se realice la instalación sea segura, confiable y eficaz para la empresa.

## 2.4 Alcance

- Adquisición de hardware y software necesarios para la implementación del proyecto.
- Configuración y puesta en marcha de los equipos de la VPN y el Firewall de Sophos.
- Configuración y verificación de la conexión VPN y su rendimiento.
- Configuración y verificación del Firewall de Sophos para garantizar la seguridad de la conexión.
- Documentación detallada del proyecto para futuras referencias y mantenimiento.

## 2.5 Marco de Referencia

El marco de referencia debe incluir estas referencias:

- **Objetivos:** Debes definir los objetivos del proyecto, como establecer una conexión segura entre dos sitios remotos mediante una VPN, garantizar la confidencialidad y la integridad de los datos transmitidos a través de la conexión VPN, y proteger la red de tu organización contra amenazas externas.
- **Alcance:** Debes definir el alcance del proyecto, incluyendo los equipos, los recursos y los plazos necesarios para completar el proyecto con éxito. También debes incluir los límites de responsabilidad y autoridad de los equipos involucrados en el proyecto.
- **Requisitos:** Debes identificar los requisitos del proyecto, como las especificaciones técnicas de la conexión VPN, las políticas de seguridad de red que deben aplicarse, y los procedimientos para la configuración y el mantenimiento de la conexión VPN.
- **Procedimientos:** Debes describir los procedimientos para la configuración y el mantenimiento de la conexión VPN, incluyendo la configuración de los firewalls Sophos en ambos extremos de la conexión VPN, la configuración de las políticas de seguridad de red, y los procedimientos para la resolución de problemas.
- **Pruebas y verificación:** Debes describir los procedimientos para la realización de pruebas y verificación de la conexión VPN, incluyendo las pruebas de conectividad, pruebas de rendimiento y pruebas de seguridad.

## 2.6 Procedimientos

Para la realización de los procedimientos tenemos que tener instalado el sophos (**XG Firewall**) en el edificio central y acceso a internet desde el nuevo edificio que queremos conectarnos al central.

Existen dos formas de conectarnos con el edificio central. Mediante la **creación de usuarios y archivos VPN** o mediante los equipos **SD-RED**.

Las diferencias que tiene la **creación de usuarios** con los equipos de **SD-RED**. Sencillamente es que con la **creación de usuarios** tenemos que crear un **túnel** con la configuración de **un archivo VPN** mediante una **aplicación** donde necesitamos el **usuario y contraseña** para poder conectarnos al edificio central como si estuviéramos en local.

Con los equipos **SD-RED**, solo necesitamos conectarlos con el router del edificio nuevo, este se sincroniza con el central y aplicándole una configuración al Sophos XG del central para el **SD-RED** podremos conectar los dispositivos a los equipos **SD-RED** y ya estaríamos en local con el edificio central como si fuera una VPN sin tener que realizar ninguna configuración de archivos.

## 2.7 Descripción de las actividades

Las actividades a realizar principalmente es comprar un Sophos XG para el edificio central, este dispositivo conectarlo con el Router del edificio que a su vez está conectado con la ONT.

**El primer método** es configurar el Sophos XG y compramos las licencias necesarias para los usuarios de la empresa, podremos ajustar los parámetros para que los usuarios que necesiten puedan utilizar la VPN en cualquier edificio o en su casa.

**El segundo método** es comprar un dispositivo aparte para el nuevo edificio donde se crea una especie VPN con el edificio central que actúa como red local, es decir todos los usuarios que estén trabajando desde ese edificio pueden acceder al edificio central sin necesidad de configurar la VPN. Los dos procedimientos descritos arriba son los que vamos a utilizar para la realización de la VPN.

## 1. Creación de usuarios y Archivos VPN.

En esta solución solamente tendremos el dispositivo XG conectado en el edificio central. Debemos tener los siguientes apartados:

- **Rango de direcciones IP:** El rango al que los clientes se van a conectar.
- **Crear un grupo de usuarios:** Dejaremos todos los permisos guardados en este grupo para todos los usuarios que quieran conectarse mediante VPN.
- **Política de Acceso SSL:** Permitimos el acceso a los recursos de red especificados para los usuarios y grupos preconfigurados que seleccione.
- **Autenticación de usuarios:** Debemos crear los usuarios que se van a conectar mediante VPN para que se cree su configuración de archivo ovpn. Metiéndolo en el grupo que hemos creado antes para llevar todas las mismas políticas.

Una vez realizado todos los pasos, tenemos que entrar en el portal de cliente con el usuario y contraseña de cada usuario creado, descargar en cada dispositivo el archivo de configuración VPN y la aplicación para poder conectarnos al edificio central. Con eso estaría todo funcionando perfectamente.

## 2. Equipos SD-RED.

En esta solución tendremos que instalar en cada edificio que queramos conectar al central un dispositivo SD-RED.

Debemos conectar el SD-RED a la toma de corriente y al router del edificio para poder configurarse con el sophos del edificio central y una vez conectado realizará la configuración sola. Una vez estén todos los Leds encendidos solo tenemos que conectarnos con nuestros equipos al SD-RED para tener la conexión local con el edificio central. El firewall XG del edificio central es el que se encarga de darnos DHCP y rango de direcciones para poder tener conexión con internet.

## 2.8 Análisis Final

La implementación de una VPN con Sophos en una empresa ofrece numerosos beneficios y soluciones de seguridad para la conectividad remota.

- **Seguridad mejorada:** Proporciona una capa adicional de seguridad al establecer una conexión cifrada entre dos redes. Esto protege los datos confidenciales de la empresa durante la transmisión y evita el acceso no autorizado.
- **Conectividad flexible:** Permite la conexión segura y confiable entre las sucursales y oficinas remotas de la empresa. Esto brinda flexibilidad en el acceso a recursos compartidos, servicios de red y aplicaciones sin importar la ubicación geográfica.
- **Reducción de costos:** Al utilizar una VPN site-to-site, las empresas pueden evitar gastos adicionales en líneas dedicadas o servicios de conectividad especializados. La VPN utiliza la infraestructura de Internet existente, lo que ayuda a reducir los costos operativos.
- **Escalabilidad:** Como ya hemos nombrado antes, la implementación de una VPN con Sophos es altamente escalable. Puede adaptarse fácilmente a medida que la empresa crece y se expande, permitiendo agregar nuevas sucursales o conexiones sin dificultad.
- **Administración centralizada:** Sophos ofrece una interfaz de administración centralizada que simplifica la configuración y el monitoreo de las conexiones VPN. Esto permite una gestión eficiente y un control completo sobre la infraestructura de seguridad de red.
- **Cumplimiento normativo:** Ayuda a las empresas a cumplir con los requisitos normativos y de seguridad, ya que proporciona una capa adicional de protección para la transmisión de datos confidenciales.
- **Soporte técnico:** Sophos cuenta con un sólido equipo de soporte técnico que puede brindar asistencia y resolver cualquier problema o consulta relacionada con la VPN. Esto ayuda a garantizar un funcionamiento óptimo y una respuesta rápida en caso de problemas.

En resumen, la implementación de una VPN con Sophos en una empresa, proporciona una solución segura y escalable para la conectividad remota. Ofrece una mayor protección de datos, conectividad flexible, reducción de costos y una administración centralizada eficaz. Sophos, con su experiencia en seguridad de red, proporciona una sólida solución de VPN y un soporte técnico confiable.

## 3. Temporalización

### 3.1 Identificación de tareas

#### 1. Planificación y diseño:

- Identificar las sucursales o edificios que se conectarán mediante la VPN.
- Definir los objetivos y requisitos de la VPN, como los recursos que se compartirán y los protocolos de seguridad a utilizar.
- Determinar el tipo de VPN adecuada para las necesidades de la organización (VPN site-to-site o VPN SSL).

#### 2. Adquisición y configuración del hardware:

- Adquirir los dispositivos Sophos necesarios para la implementación de la VPN, como firewalls Sophos UTM/SG o dispositivos SD-WAN.
- Configurar los dispositivos Sophos según las especificaciones del fabricante y las necesidades de la red.

#### 3. Configuración de las políticas de seguridad:

- Establecer las políticas de seguridad para la VPN, como la autenticación de usuarios, la encriptación de datos y las reglas de firewall.
- Definir los permisos de acceso a los recursos compartidos y establecer las restricciones necesarias.

#### 4. Configuración de la conectividad:

- Configurar las interfaces de red y las direcciones IP en los dispositivos Sophos.
- Establecer las conexiones VPN entre las sucursales remotas, configurando los túneles VPN correspondientes.
- Configurar la conexión con Sophos Central Dashboard para administrar y monitorear la VPN de manera centralizada.

#### 5. Generación y configuración de certificados (en caso de utilizar VPN SSL):

- Generar o adquirir certificados SSL válidos para la autenticación y el cifrado de la conexión VPN SSL.
- Configurar los certificados en los dispositivos Sophos para su uso en la VPN SSL.



## 6. Pruebas y verificación:

- Realizar pruebas de conectividad y seguridad para garantizar que la VPN funcione correctamente.
- Verificar el acceso a los recursos compartidos y asegurarse de que los datos se transmitan de manera segura.

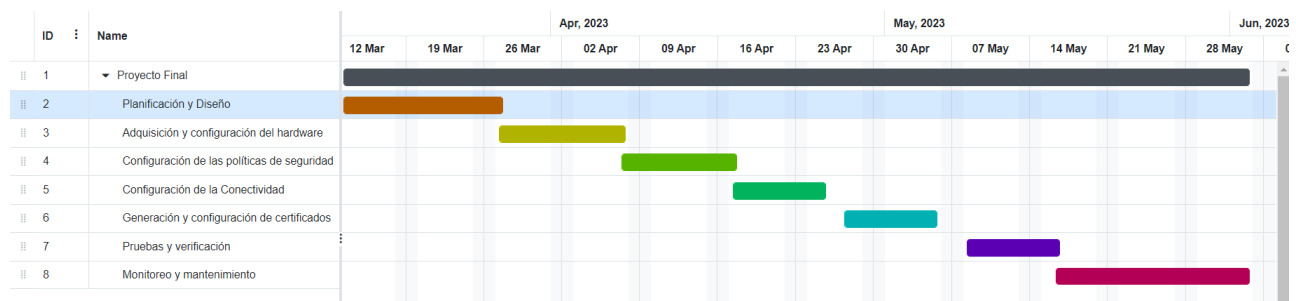
## 7. Monitoreo y mantenimiento:

- Establecer un sistema de monitoreo para supervisar el estado y el rendimiento de la VPN.
- Realizar actualizaciones de firmware y aplicar parches de seguridad según sea necesario.
- Realizar tareas de mantenimiento regulares para garantizar el buen funcionamiento y la seguridad de la VPN.

## 3.2 Secuenciación

Para la realización del cronograma vamos a realizar un diagrama de Gantt. De momento solo podemos poner el tiempo que hemos tardado en realizar el anteproyecto.

ID	Name	Start Date	End Date	Duration	Progress %	Dependency	Resources	Color
1	▼ Proyecto Final	Mar 13, 2023	Jun 02, 2023	60 days	100			
2	Planificación y Diseño	Mar 13, 2023	Mar 27, 2023	11 days	100			Orange
3	Adquisición y configuración del hardware	Mar 27, 2023	Apr 07, 2023	10 days	100			Yellow
4	Configuración de las políticas de seguridad	Apr 07, 2023	Apr 17, 2023	7 days	100			Light Green
5	Configuración de la Conectividad	Apr 17, 2023	Apr 25, 2023	7 days	100			Green
6	Generación y configuración de certificados	Apr 27, 2023	May 05, 2023	7 days	100			Cyan
7	Pruebas y verificación	May 08, 2023	May 16, 2023	7 days	100			Purple
8	Monitoreo y mantenimiento	May 16, 2023	Jun 02, 2023	14 days	100			Pink



## 4. Memoria Técnica

### 4.1 Especificaciones de implementación

#### 4.1.1 Manual de instalación de Sophos XG.



Los dispositivos XGS se envían con la siguiente configuración predeterminada.

<i>Ethernet Port</i>	<i>IP Address</i>	<i>Zone</i>
<i>1/LAN</i>	<i>172.16.16.16/255.255.255.0</i>	<i>LAN</i>
<i>2/WAN</i>	<i>DHCP</i>	<i>WAN</i>
<i>Admin Console Username</i>	<i>Admin Console Password</i>	<i>CLI Console Password</i>
<i>admin</i>	<i>admin</i>	<i>admin</i>
<i>Default Gateway</i>	<i>DNS</i>	<i>DHCP Service</i>
<i>DHCP</i>	<i>DHCP</i>	<i>Enabled</i>

#### **Encienda el dispositivo.**

Conecte el cable de alimentación y encienda el aparato. Conecte el aparato a la fuente de alimentación utilizando los cables de alimentación. Encienda el aparato. El interruptor de alimentación se encuentra en la parte posterior del aparato, cerca de la conexión de alimentación.

Durante el arranque, el LED de estado en la parte frontal parpadeará en verde. Una vez que el dispositivo haya arrancado por completo, el LED de estado se volverá verde fijo.

#### **Conecte su ordenador de Administración.**

Use la configuración a continuación para configurar su interfaz de red (PC/portátil):

- Dirección IP: 172.16.16.2
- Máscara de red: 255.255.255.0
- Puerta de enlace predeterminada: 172.16.16.16
- Servidor DNS: Habilitar esta opción y meter dirección de puerta de enlace.

## 4.1.2 Manual de instrucciones de Sophos SD-RED.



















Sophos SD-RED (dispositivo Ethernet remoto) es la solución ideal para extender fácilmente su red segura más allá de sus instalaciones principales a sucursales, tiendas minoristas y otras ubicaciones remotas.

















Los dispositivos SD-RED están contruidos sobre las últimas plataformas de red de alta velocidad de clase empresarial, que brindan tecnología de cifrado de datos de última generación para transportar de forma segura sus datos a través de Internet.

Toda la configuración y administración se realiza en un Sophos Firewall ubicado en sus instalaciones principales y no requiere conocimientos técnicos en el sitio remoto.

### LEDs de estado

Códigos de arranque LED				
Instantáneo	Router	Internet	Túnel	Descripción
				El dispositivo se está iniciando.
				El dispositivo ha terminado de iniciarse.
				El dispositivo se está conectando a la puerta de enlace/enrutador predeterminado.
				Se puede acceder a la puerta de enlace/enrutador predeterminados.
				El dispositivo se está conectando a Internet.
				Se ha establecido la conexión a Internet.
				El dispositivo se está conectando al cortafuegos.
				Se ha establecido la conexión con el cortafuegos.
				El dispositivo está instalando una nueva versión de firmware.

Códigos de error LED				
Instantáneo	Router	Internet	Túnel	Descripción
				La configuración de dirección estática o DHCP falló, no se puede acceder a la puerta de enlace predeterminada.
				Internet no accesible.
				Sin conexión con el cortafuegos.
				No hay configuración disponible o la actualización del firmware falló.

Códigos de conmutación por error LED 3G/4G				
Instantáneo	Router	Internet	Túnel	Descripción
				La conmutación por error 3G/4G está activa.
				Se puede acceder a la puerta de enlace/enrutador predeterminados.
				Se ha establecido la conexión a Internet.
				Se ha establecido la conexión con el cortafuegos.*

## Instalación

### Configuración del dispositivo SD-RED.

Configure el dispositivo SD-RED en su SG XG Firewall Central, una vez completada la configuración, se cargará en el servicio de agente de Sophos basado en la nube.

### Conexión del SD-RED en el sitio remoto.

Conecte el dispositivo SD-RED a su enrutador o cable en el sitio remoto y enciéndalo. Una vez que el sistema se haya iniciado, se conectará a internet para recuperar su configuración del servicio de agente de Sophos.

Los LED de estado “Sistema”, “Enrutador”, “Internet”, “Túnel” deben encenderse uno tras otro.

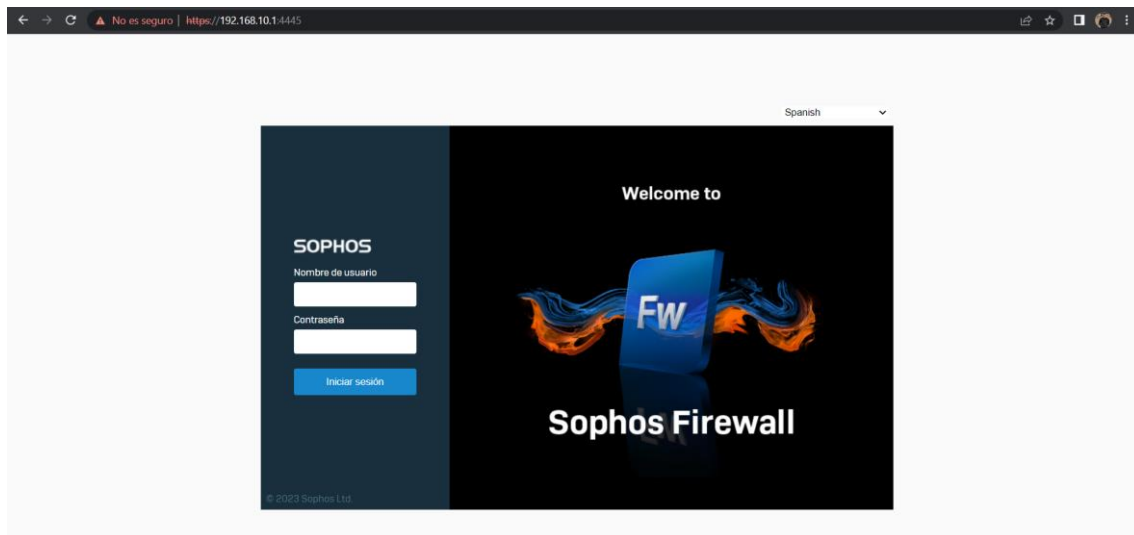
Si no ve los cuatro LED de estado encendidos o el LED de “Sistema” parpadea en rojo, mire la tabla para identificar los posibles estados de error y comuníquese con su administrador.

### 4.1.3 Realización de un túnel IPSec mediante Sophos

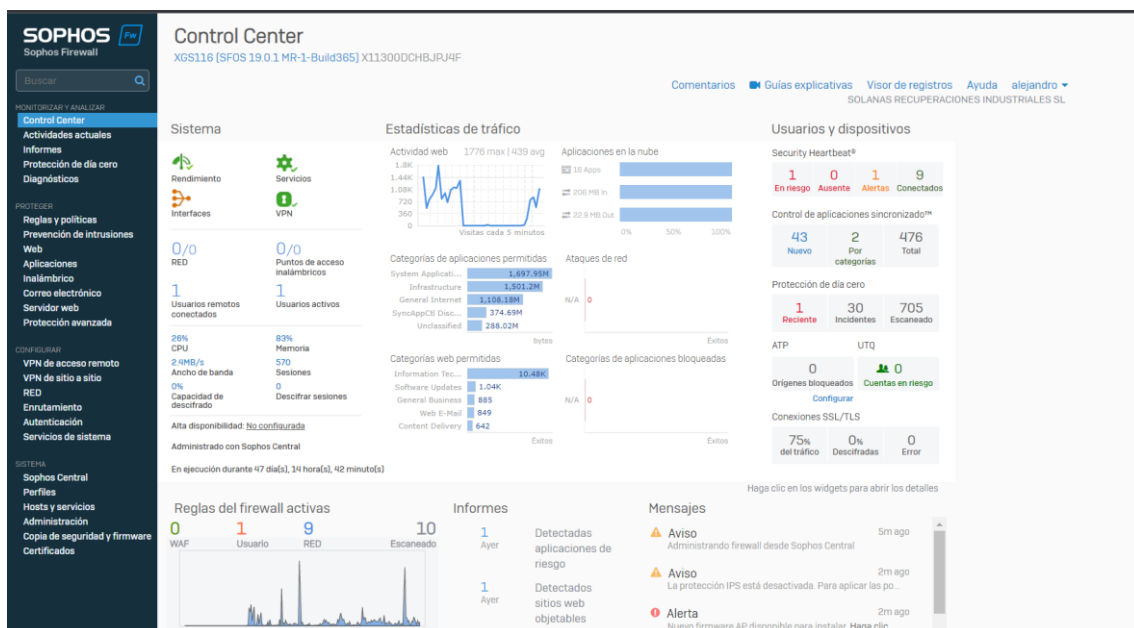
- Para la realización de un túnel IPSec debemos tener en la otra ubicación un dispositivo firewall Sophos.
- El manual que vamos a realizar deberá realizarse en los firewalls que se quieran conectar entre sí.

#### Acceso al firewall XG de Sophos.

Terminada la configuración del firewall XG. Accedemos mediante ip a la interfaz gráfica.



Accedemos y en la pantalla de inicio tenemos un resumen de todo el panel.



Añadimos la dirección local y la dirección remota.

Entramos en Hosts y Servicios > Host IP y Creamos dos LAN. Debemos saber el rango de local de cada sucursal para poder conectarlos.

La primera para el edificio central.

**SOPHOS** Firewall

Editar host IP

Comentarios Guías explicativas Visor de registros Ayuda alejandro SOLANAS RECUPERACIONES INDUSTRIALES SL

Host IP Grupo de hosts IP Host MAC Host FQDN Grupo de hosts FQDN Grupo de países Servicios Grupo de servicio

Nombre \* Rango\_Central

Versión IP \* IPv4

Tipo \* RED

Dirección IP \* 192.168.20.0 Subred /24 (255.255.255.0)

Grupo de hosts IP

Añadir nuevo elemento

Sophos Assistant

La segunda para el edificio nuevo.

**SOPHOS** Firewall

Añadir host IP

Comentarios Guías explicativas Visor de registros Ayuda alejandro SOLANAS RECUPERACIONES INDUSTRIALES SL

Host IP Grupo de hosts IP Host MAC Host FQDN Grupo de hosts FQDN Grupo de países Servicios Grupo de servicio

Nombre \* Rango\_Secun

Versión IP \* IPv4 IPv6

Tipo \* IP RED Rango IP Lista IP

Dirección IP \* 192.168.22.0 Subred /24 (255.255.255.0)

Grupo de hosts IP

Añadir nuevo elemento

Sophos Assistant

## Creación perfil de IPSec.

Tenemos dos posibilidades o escoger el perfil por defecto que trae para las conexiones IPSec o crear nosotros un perfil específico para nuestra conexión.

Para la creación de un perfil específico nos vamos a perfiles > Perfiles IPSec y añadimos un nuevo perfil.

Esta es la configuración para nuestro perfil.

The screenshot displays the Sophos Firewall configuration interface for creating an IPSec profile. The interface is divided into a left sidebar with navigation menus and a main content area with configuration tabs.

**Left Sidebar:**

- MONITOREO Y ANALISIS:** Control Center, Actividades actuales, Informes, Protección de día cero, Diagnósticos.
- PROTEGER:** Reglas y políticas, Prevención de intrusiones, Web, Aplicaciones, Inalámbrico, Correo electrónico, Servidor web, Protección avanzada.
- CONEXIONAR:** VPN de acceso remoto, VPN de sitio a sitio, RED, Enrutamiento, Autenticación, Servicios de sistema.
- SISTEMA:** Sophos Central, Perfiles, Hosts y servicios, Administración, Copia de seguridad y firmware, Certificados.

**Main Content Area:**

**Perfiles** (Tabs: Horario, Tiempo de acceso, Cuota de navegación, Cuota de tráfico de red, Perfiles de descifrado, **Perfiles IPSec**, Acceso de dispositivo)

**Configuración general**

Nombre: Central\_Secun Descripción: Perfil para la conexión de edificio central con el nuevo edificio.

Intercambio de claves: ☒ IKEv1 ☐ IKEv2 Intentos de negociación de clave: 0

Modo de autenticación: ☒ Modo principal ☐ Modo agresivo (Modo agresivo no es seguro)

☒ Conexión de regeneración de claves ☐ Ignorar datos en formato comprimido ☐ SHA2 con truncado de 96 bits

**Fase 1**

Vida de clave: 28800 Segundos Margen de regeneración de clave: 360 Segundos Aleatorizar margen de regeneración de clave en: 0 %

Grupo DH (grupo clave): 6 selected

**Perfiles** (Tabs: Horario, Tiempo de acceso, Cuota de navegación, Cuota de tráfico de red, Perfiles de descifrado, **Perfiles IPSec**, Acceso de dispositivo)

Cifrado: AES256 Autenticación: SHA2 256

☒ Puede añadir hasta 3 combinaciones distintas de algoritmos

**Fase 2**

Grupo PFS (grupo DH): Igual que fase 1 Vida de clave: 3600 Segundos

Cifrado: AES256 Autenticación: SHA2 256

☒ Puede añadir hasta 3 combinaciones distintas de algoritmos

**Detección de par muerto**

☒ Detección de par muerto

Comprobar pares después de cada: 30 Esperar respuesta hasta: 120 Cuando el par no es alcanzable: Reiniciar

**Buttons:** Guardar, Cancelar

Una vez terminado la creación de nuestro perfil le damos a guardar.

## Creación de Conexión VPN IPSec.

- La configuración en el otro firewall es exactamente igual, pero cambiando el local y el remoto.

Entramos en VPN de sitio a sitio > Ipsec.

Debajo de conexiones Ipsec, añadimos una nueva conexión.

El perfil que vamos a utilizar para la conexión IPSec es el por defecto, las claves para la conexión serían RSA, la clave local es la que aparece y la remota debemos cogerla de la conexión IPSEC del otro firewall de Sophos. En el otro firewall debemos poner como RSA remota la que aparece en este como local.

The first screenshot shows the 'VPN de sitio a sitio' configuration page for an IPSec connection. The 'Configuración general' section includes fields for 'Nombre' (IPSEC\_EDIFICIOS), 'Versión IP' (IPv4), 'Tipo de conexión' (La conexión de sitio a sitio), and 'Tipo de puerto de enlace' (Solo responder). The 'Cifrado' section shows 'Perfil' (Default Profile) and 'Tipo de autenticación' (Clave RSA). It displays two RSA keys: 'Clave RSA local' and 'Clave RSA remota'. The second screenshot shows the 'Configuración de puerto de enlace' section. It details the 'Puerta de enlace local' (Interface de escucha: Port2.20 - 85.51.55.71, ID local: 192.168.20.0, Subred local: Range\_Central) and the 'Puerta de enlace remota' (Dirección de puerta de enlace: \*, Tipo de ID remoto: Dirección IP, ID remoto: 192.168.22.0, Subred remota: Range\_Secun). A checkbox for 'Network Address Translation (NAT)' is also visible.

Activamos la conexión pulsando en el led, vemos como se activa y cambia a color verde pero el de la conexión sigue estando de color rojo.

The screenshot shows the 'Conexiones IPsec' table in the Sophos Firewall interface. The table lists two connections: 'IPSEC\_EDIFICIOS' and 'IPSEC\_TO\_OUT'. Both are in the 'Activo' state. The 'IPSEC\_EDIFICIOS' connection is highlighted with a green status indicator, while 'IPSEC\_TO\_OUT' remains red.

Nombre	Nombre del grupo	Perfil	Tipo de conexión	Estado	Conexión	Gestor
IPSEC_EDIFICIOS	-	Default Profile	La conexión de sitio a sitio	Activo	Conexión	[Iconos]
IPSEC_TO_OUT	-	Default Profile	La conexión de sitio a sitio	Activo	Conexión	[Iconos]



## Creación de reglas de Firewall para el tráfico VPN.

- *Tenemos que crear una regla en cada firewall.*

Necesitamos crear una regla para permitir el tráfico LAN y VPN entre las sucursales.

Entramos en **reglas y políticas** > **reglas de firewall** y seleccionamos **Ipv4**.  
Añadimos nueva regla de firewall.

Con esta configuración creamos una regla bidireccional donde permitimos la entrada y salida del tráfico entre las sucursales y permitimos el tráfico por conexión VPN SSL mediante el túnel IPSec.

**SOPHOS** Sophos Firewall

**Añadir regla de firewall**

Comentarios | Guías explicativas | Visor de registros | Ayuda | alejandro

SOLANAS RECUPERACIONES INDUSTRIALES SL

**Estado de la regla**

Nombre de regla \* Central\_Secun

Descripción Salida desde edificio Central al Secundario

Posición de regla Abajo

Acción Aceptar

Grupo de reglas Ninguna

☒ 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.

**Origen**

Seleccione las zonas, redes y dispositivos de origen. La regla se aplica al tráfico de estos orígenes durante el periodo de tiempo programado.

Zonas de origen \* LAN, VPN

Dispositivos y redes de origen \* Rango\_Central, Rango\_Secun

Durante la hora programada Siempre

**Destino y servicios**

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

Zonas de destino \* LAN, VPN

Redes de destino \* Rango\_Central, Rango\_Secun

Servicios \* CUALQUIERA

**Resumen Central\_Secun**

**Regla**

Accept any traffic going to "LAN" or "VPN" zones, when in "LAN" or "VPN" zones, and coming from "Rango\_Central" and "Rango\_Secun" networks, then apply log connections

**Origen y programación**

LAN/VPN

Dispositivos y redes de origen: Rango\_Central, Rango\_Secun

Durante la hora programada: Siempre

**Destino y servicios**

LAN/VPN

Redes de destino: Rango\_Central, Rango\_Secun

Servicios: CUALQUIERA

**Exclusiones**

Zonas de origen: Dispositivos y redes de origen: Red de destino: Red de destino: Servicios:

**Avanzado**

Reglas de firewall

Reglas NAT

Reglas de inspección SSL/TLS

Una vez creada la regla activamos la conexión en los dos firewalls y comprobamos que los leds están ambos en verde y ya está funcionando.

**SOPHOS** Sophos Firewall

**Reglas y políticas**

La regla de firewall "Central\_Secun" se ha añadido correctamente.

alejandro

SOLANAS RECUPERACIONES INDUSTRIALES SL

**Reglas de firewall**

Reglas NAT

Reglas de inspección SSL/TLS

IPv4 IPv6 Desactivar filtro

Añadir regla de firewall

Desactivar Eliminar

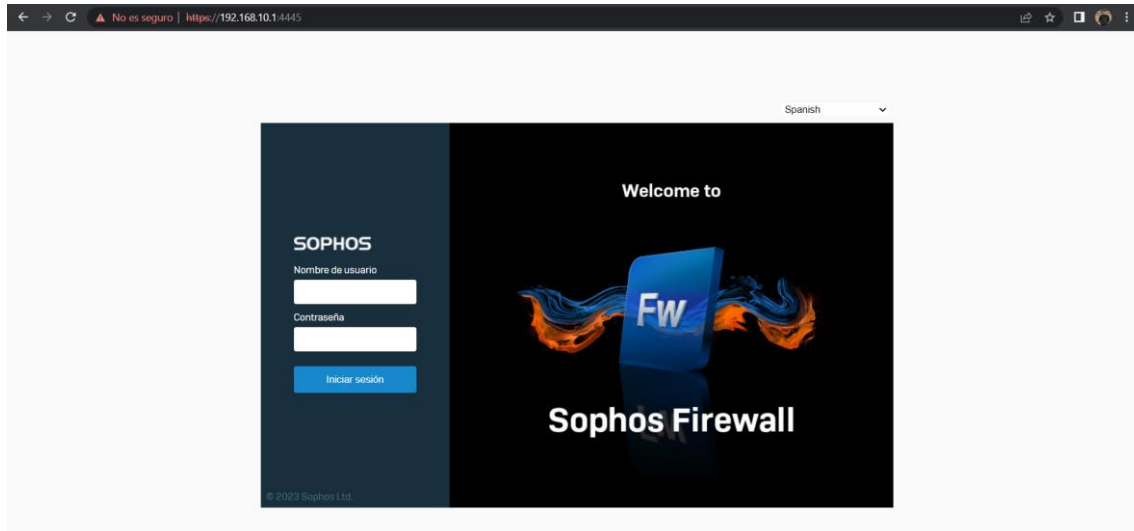
#	Nombre	Origen	Destino	Estado	ID de regla	Acción	Función y servicio
1	TRAFFIC_TO_VPN	entrada 1,23 TB, salida 10,53 GB					
2	Automatic VPN Rule...	entrada 12,34 GB, salida 146,18 GB					
3	TO_LAN	entrada 29,52 GB, salida 64,54 GB					
4	Traffic to WAN	entrada 768,86 GB, salida 931,28 GB					
5	Traffic to DMZ	entrada 0 B, salida 0 B					
10	Auto added firewall...	entrada 0 B, salida 30,17 KB	Cualquier zona, Cualquier host			SMTP: SMTP(S)	#1 Aceptar
11	Central_Secun	entrada 0 B, salida 0 B	LAN, VPN, Rango_Central, Rango...			Cualquier servicio	#11 Aceptar
12	Descartar todas	entrada 0 B, salida 0 B	Cualquier zona, Cualquier host			Cualquier servicio	#0 Descartar

Mostrando 12 de 12. Se ha seleccionado 0

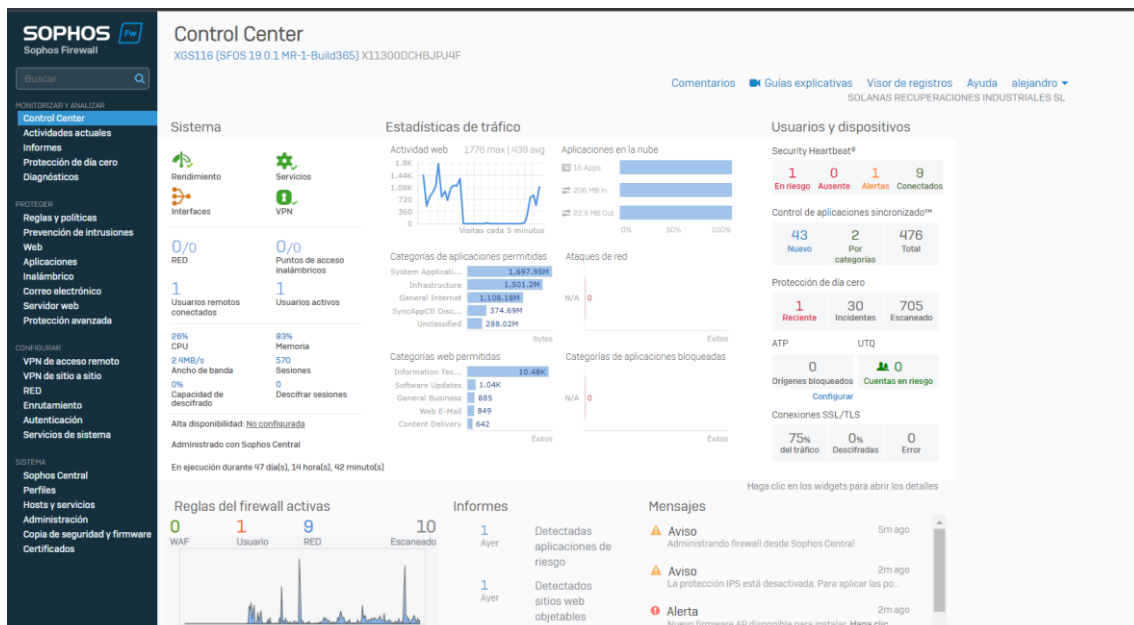
## 4.1.4 Realización de VPN SSL mediante Sophos

### Acceso al firewall XG de Sophos.

Terminada la configuración del firewall XG. Accedemos mediante ip a la interfaz gráfica.



Accedemos y en la pantalla de inicio tenemos un resumen de todo el panel.



## Creación de VPN SSL.

Tenemos que crear dos conexiones una para cada sucursal.  
Entramos en VPN de acceso remoto > VPN SSL y añadimos una nueva.

Esta conexión es para la sucursal central.

The screenshot shows the 'VPN de acceso remoto' configuration page in the Sophos Firewall interface. The 'VPN SSL' tab is selected. The configuration is for a central branch. The 'Configuración general' section shows the name 'Usuarios-VPN-SSL-Central' and the description 'Usuarios para acceso a la infraestructura de la sucursal central'. The 'Identidad' section shows the policy members. The 'Acceso túnel' section shows the tunnel type set to 'Usar como puerta de enlace predeterminada' and the resources set to 'Rango\_Central'.

**SOPHOS** Firewall  
SOLANAS RECUPERACIONES INDUSTRIALES SL

VPN de acceso remoto

Configuración general

Nombre \* Usuarios-VPN-SSL-Central

Descripción Usuarios para acceso a la infraestructura de la sucursal central

Identidad

Miembros de política

Añadir nuevo elemento

Acceso túnel

Usar como puerta de enlace predeterminada ☒

Recursos de red permitidos (IPv4) Rango\_Central

Añadir nuevo elemento

Recursos de red permitidos (IPv6)

Añadir nuevo elemento

Sophos Assistant

Esta conexión es para la sucursal nueva.

The screenshot shows the 'VPN de acceso remoto' configuration page in the Sophos Firewall interface. The 'VPN SSL' tab is selected. The configuration is for a new branch. The 'Configuración general' section shows the name 'Usuarios-VPN-SSL-Secun' and the description 'Usuarios para acceso a la infraestructura de la sucursal nueva'. The 'Identidad' section shows the policy members. The 'Acceso túnel' section shows the tunnel type set to 'Usar como puerta de enlace predeterminada' and the resources set to 'Rango\_Secun'.

**SOPHOS** Firewall  
SOLANAS RECUPERACIONES INDUSTRIALES SL

VPN de acceso remoto

Configuración general

Nombre \* Usuarios-VPN-SSL-Secun

Descripción Usuarios para acceso a la infraestructura de la sucursal nueva

Identidad

Miembros de política

Añadir nuevo elemento

Acceso túnel

Usar como puerta de enlace predeterminada ☒

Recursos de red permitidos (IPv4) Rango\_Secun

Añadir nuevo elemento

Recursos de red permitidos (IPv6)

Añadir nuevo elemento

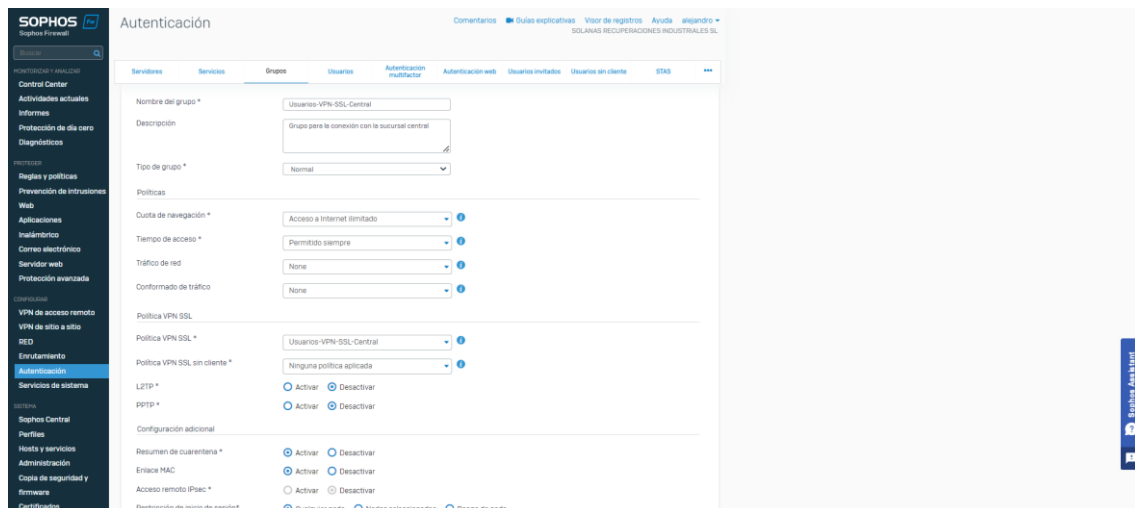
Sophos Assistant

## Creación de Grupo para usuarios VPN-SSL.

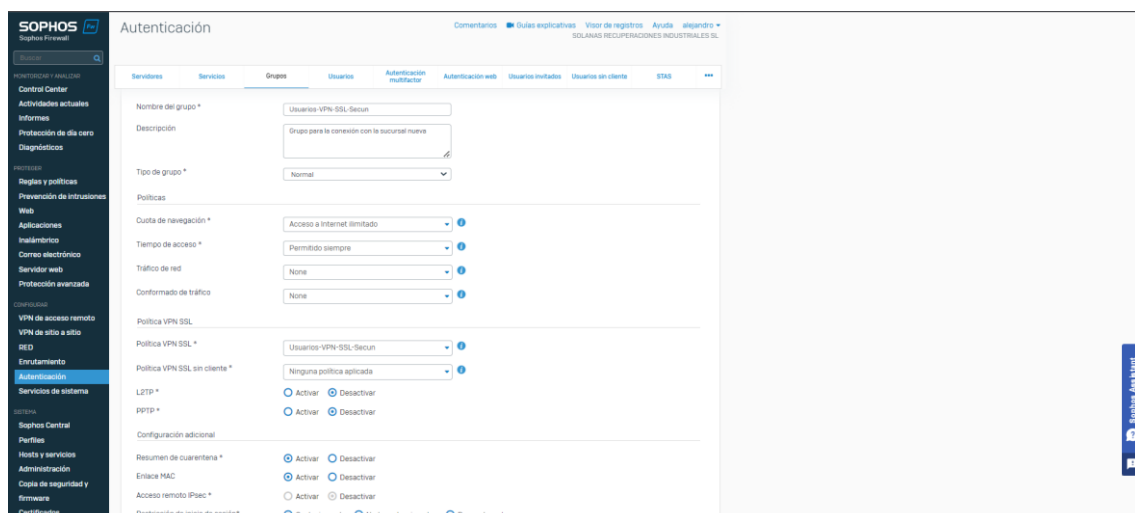
Entramos en **Autenticación** > **Grupos** y añadimos un nuevo **grupo**.

En cada grupo debemos de poner la conexión con la sucursal que va a realizar la conexión.

Esta es la configuración para nuestro grupo de la sucursal central.



Esta es la configuración para nuestro grupo de la sucursal nueva.



## Creación de usuarios para la conexión VPN-SSL.

Una vez tenemos ya la conexión y el grupo creado, solo necesitamos crear el usuario para conectarse con cualquiera de las dos sucursales. Solo debemos elegir la conexión a la que queremos conectarnos.

Entramos en **Autenticación > Usuarios** y añadimos un **usuario** nuevo.

En cada usuario debemos elegir a que sucursal quiere conectarse.

Este usuario se va a conectar con la sucursal central.

The screenshot displays the Sophos Firewall web interface. The left sidebar shows the navigation menu with 'Autenticación' (Authentication) selected. The main content area is titled 'Autenticación' and contains a sub-tab 'Usuarios'. The 'Añadir usuario' (Add user) form is visible, with the following fields and values:

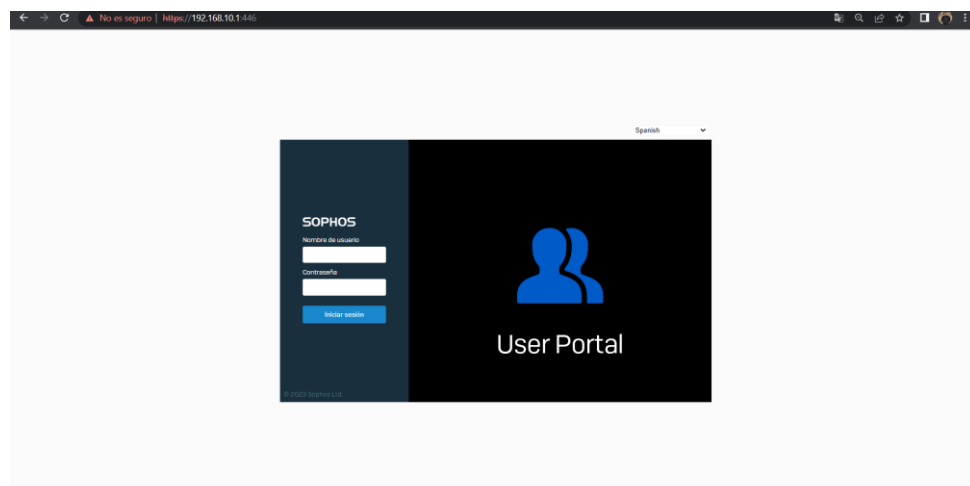
- Nombre de usuario \*: victor
- Nombre \*: victor
- Descripción: usuario que quiere conectar a la sucursal central
- Tipo de usuario \*: ☒ Usuario ☐ Administrador
- Perfil \*: Perfil
- Contraseña \*: [Redacted]
- Correo electrónico \*: aviliches@gmail.com
- Políticas:
  - Grupo \*: Usuarios-VPN-SSL-Central
  - Cuota de navegación \*: Acceso a Internet limitado
  - Tiempo de acceso \*: Permitido siempre
  - Tráfico de red: None
  - Conformado de tráfico: None
- Política VPN SSL:
  - Política VPN SSL \*: Usuarios-VPN-SSL-Central
  - Política VPN SSL sin cliente \*: Ninguna política aplicada
- Acceso remoto IPsec \*: ☐ Activar ☒ Desactivar Dirección IP: [Redacted]
- L2TP \*: ☐ Activar ☒ Desactivar Dirección IP: [Redacted]
- PPTP \*: ☐ Activar ☒ Desactivar Dirección IP: [Redacted]
- Configuración adicional:
  - Resumen de cuarentena \*: ☒ Activar ☐ Desactivar
  - Enlace MAC \*: ☒ Activar ☐ Desactivar
  - Lista de direcciones MAC: [Redacted]
  - Inicio de sesión simultáneos \*: ☒ Usar configuración global ☐ Ilimitado [1-99]
  - Restricción de inicio de sesión\*: ☐ Cualquier nodo ☒ Nodo(s) de grupo de usuario ☐ Nodos seleccionados ☐ Rango de nodo

Este usuario se va a conectar con la sucursal nueva.

## Conexión con el portal de usuario de Sophos.

En el portal de usuario de Sophos podremos descargarnos el fichero de configuración de VPN y el programa que lo ejecuta. La dirección es la misma, pero cambiando el puerto por el 446.

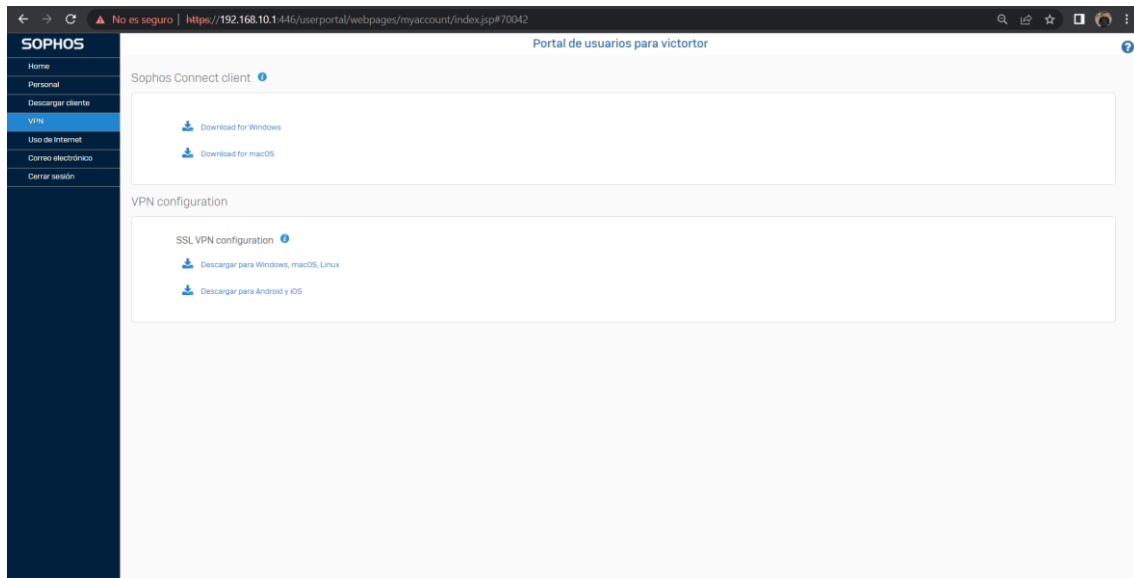
Para acceder debemos entrar con algún usuario creado en el Sophos, antes hemos creado dos usuarios uno para cada sucursal, vamos a entrar con uno de ellos para comprobar que funciona



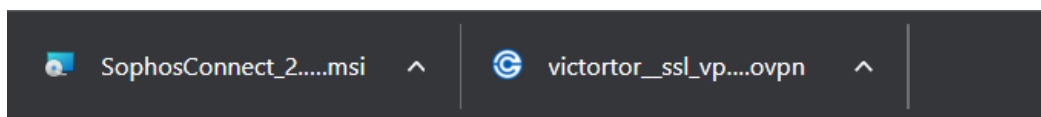
Una vez ingresamos en el portal podemos ver como directamente entra en el apartado de VPN.

Dentro de este apartado nos aparece dos cosas:

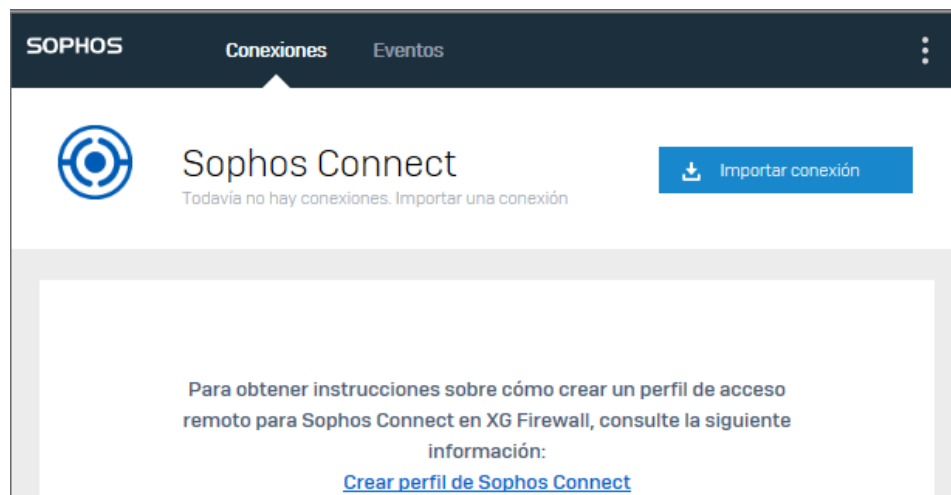
- El programa que debemos abrir para utilizar la VPN: **Sophos Connect client**.
- El fichero de configuración de nuestro usuario para la utilización de la VPN.



Descargamos para nuestro sistema operativo el programa y el fichero de configuración.



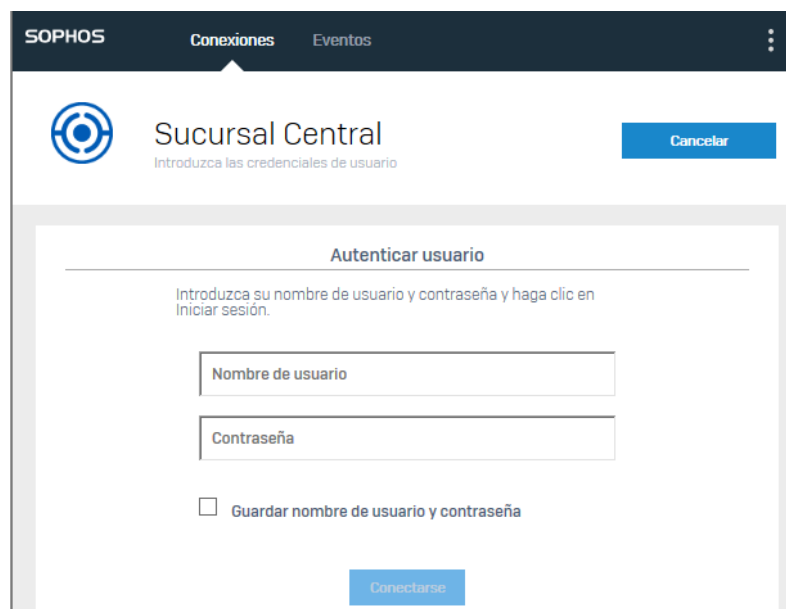
Instalamos la aplicación y ejecutamos la aplicación.



Importamos conexión y seleccionamos el fichero de configuración que nos hemos descargado, nos aparecerá para arrancar la conexión VPN pero primero le cambiamos el nombre para saber a qué sucursal nos estamos conectando.



Le ponemos el nombre de la sucursal que se va a conectar, una vez cambiado el nombre hacemos doble click y deberemos iniciar sesión con el usuario que hemos iniciado en el portal de usuario.



Una vez entrado con el usuario podemos ver que está funcionando.

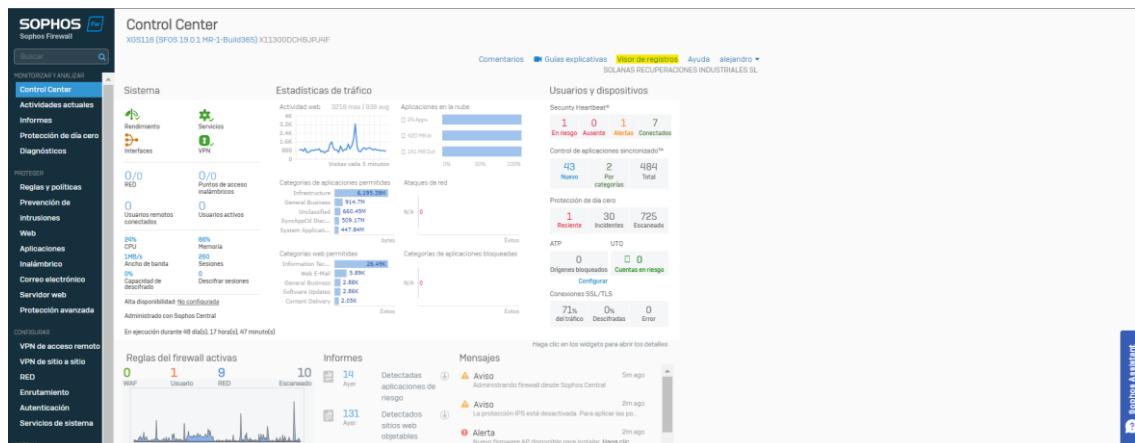




## 4.2 Seguimiento y control

### Visualización de Logs.

Dentro del panel de control del firewall tenemos arriba a la derecha un visor de registros.



Dentro del visor podemos visualizar logs de muchos tipos, pero podemos cambiar el tipo de filtro para visualizar solo los logs de VPN y mantener un control.

https://192.168.10.1:4445/webconsole/webpages/logging/EventViewer.js?selectedTab=log\_viewer&crf=90e1b0k2e17on3dhkhdgtn7 - Google Chrome

No es seguro https://192.168.10.1:4445/webconsole/webpages/logging/EventViewer.js?selectedTab=log\_viewer&crf=90e1b0k2e17on3dhkhdgtn7#65583

Visor de registros

Punto de política

Historial

Administrador

Protección avanzada contra amenazas

Filtro de aplicaciones

Autenticación

Correo electrónico

Firewall

IPS

Malware

Latido de seguridad

Inspección SSL/TLS

SD-WAN

Sistema

VPN

Política de contenido web

Filtro web

Protección de servidores web

Protección de día cero

Evento Dest. protocolo Tipo

2023-06-06 12:34:17	Firewall Rule	Allowed	5	LAN_TO_WAN	3	#NAT_Default_Net...	Port0	Port12.20	192.168.10.39		UDP	1		
2023-06-06 12:34:17	Firewall Rule	Allowed	5	LAN_TO_WAN	3	#NAT_Default_Net...	Port0	Port12.20	192.168.10.101		TCP	1		
2023-06-06 12:34:17	Firewall Rule	Allowed	5	LAN_TO_WAN	3	#NAT_Default_Net...	Port0	Port12.20	192.168.10.24		UDP	1		
2023-06-06 12:34:17	Firewall Rule	Allowed	5	LAN_TO_WAN	3	#NAT_Default_Net...	Port0	Port12.20	192.168.10.102		TCP	1		
2023-06-06 12:34:17	Firewall Rule	Allowed	5	LAN_TO_WAN	3	#NAT_Default_Net...	Port0	Port12.20	192.168.10.17		UDP	1		
2023-06-06 12:34:17	Firewall Rule	Allowed	5	LAN_TO_WAN	3	#NAT_Default_Net...	Port0	Port12.20	192.168.10.79		UDP	1		
2023-06-06 12:34:17	Firewall Rule	Allowed	5	LAN_TO_WAN	3	#NAT_Default_Net...	Port0	Port12.20	192.168.10.101		TCP	1		
2023-06-06 12:34:17	Firewall Rule	Allowed	5	LAN_TO_WAN	3	#NAT_Default_Net...	Port0	Port12.20	192.168.10.102	52.98.145.120	60398	443	TCP	1
2023-06-06 12:34:17	Firewall Rule	Allowed	5	LAN_TO_WAN	3	#NAT_Default_Net...	Port0	Port12.20	192.168.10.101	108.177.15.188	62060	5228	TCP	1
2023-06-06 12:34:16	Firewall Rule	Allowed	5	LAN_TO_WAN	3	#NAT_Default_Net...	Port0	Port12.20	192.168.10.19	52.114.77.98	57085	443	TCP	1
2023-06-06 12:34:16	Firewall Rule	Allowed	5	LAN_TO_WAN	3	#NAT_Default_Net...	Port0	Port12.20	192.168.10.102	52.98.145.120	60399	443	TCP	1
2023-06-06 12:34:16	Firewall Rule	Allowed	5	LAN_TO_WAN	3	#NAT_Default_Net...	Port0	Port12.20	192.168.10.70	142.250.200.138	63905	443	UDP	1
2023-06-06 12:34:16	Firewall Rule	Allowed	5	LAN_TO_WAN	3	#NAT_Default_Net...	Port0	Port12.20	192.168.10.70	142.250.184.170	54636	443	UDP	1

Elegido el filtro de VPN podemos visualizar todo tipo de logs.

Visualización de los logs de VPN. La interfaz muestra una pestaña 'Visual de registros' y una barra de búsqueda. El filtro seleccionado es 'VPN'. La tabla de logs contiene las siguientes columnas: Tiempo, Componente de registro, Estado, Nombre de usuario, Mensaje e ID de mensaje.

VPN	Tiempo	Componente de registro	Estado	Nombre de usuario	Mensaje	ID de mensaje
VPN	2023-06-06 12:28:52	IPSec	Deny		Received IKE message with invalid SPI (23306567) from the remote gateway.	18050
VPN	2023-06-06 10:35:36	IPSec	Deny		Received IKE message with invalid SPI (50534136) from the remote gateway.	18050
VPN	2023-06-06 08:41:42	IPSec	Deny		Received IKE message with invalid SPI (7EC004DC) from the remote gateway.	18050
VPN	2023-06-06 07:45:32	IPSec	Deny		Received IKE message with invalid SPI (8C0313AC) from the remote gateway.	18050
VPN	2023-06-06 06:48:58	IPSec	Deny		Received IKE message with invalid SPI (8779305) from the remote gateway.	18050
VPN	2023-06-06 04:55:34	IPSec	Deny		Received IKE message with invalid SPI (C37A5644) from the remote gateway.	18050

Dependiendo de lo que queramos buscar podemos añadir filtros y tiempo para buscar lo que necesitamos.

Interfaz para añadir un filtro. El diálogo 'Añadir filtro' permite configurar los criterios de búsqueda. Las opciones disponibles son:

- Campo:** Componente de registro
- Condición:** es
- Valor:** Regla de firewall

Se incluye un botón 'Add Filter' para confirmar la configuración.

Estas son las opciones de filtro que tenemos.

Interfaz para añadir un filtro. El diálogo 'Añadir filtro' muestra las opciones disponibles para el campo de filtro:

- Componente de registro
- Estado
- ID de mensaje
- Mensaje
- Nombre de usuario
- Regla de firewall

Se incluye un botón 'Add Filter' para confirmar la configuración.

Mediante este apartado podemos tener un control y un seguimiento específico de cualquier usuario que esté conectado a la VPN. Una vez realizado el seguimiento y el control podemos agregar una política para prohibirle o aceptarle lo que el usuario necesite.

## 5. Estudio Presupuestario

### Hardware:

Routers para la conexión VPN  
Firewall de Sophos  
Sophos SD-RED

### Software:

Licencias de Sophos XG Firewall

### Gastos operativos:

Costos de implementación y configuración  
Costos de mantenimiento y soporte

Presupuesto N° 001			
		Datos del cliente	
Clínica Parejo y Cañero		Nombre:	Sergio Lora Romero
14500 Puente Genil, Córdoba		Dirección	Santa Catalina N°9
32-20191209-3		CUIT-NIF:	25147652F
957 60 20 26		Teléfono:	652417562
<a href="mailto:atencioncliente@cañero.com">atencioncliente@cañero.com</a>		E-mail:	<a href="mailto:sergioromlo@gmail.com">sergioromlo@gmail.com</a>
Fecha	13/06/2023	Validez:	30 días
DESCRIPCIÓN	UNIDADES	PRECIO	TOTAL
Router Asus RT-AX82U	2,00	150,00	300,00 €
Sophos Firewall XG 116	1,00	600,00	600,00 €
Sophos SD-RED20	1,00	520,00	520,00 €
Licencia de Sophos XG Firewall	1,00	500,00	500,00 €
Costo de implementacion	1,00	1.500,00	1.500,00 €
Costo de mantenimiento y soporte	1,00	500,00	500,00 €
		SUB-TOTAL	3.920,00 €
		DESCUENTO	150,00 €
		IVA %	21%
TOTAL PRESUPUESTADO			4.561,70 €

## 6. Conclusiones

En conclusión, La creación de una VPN mediante Sophos ofrece soluciones de conectividad segura y confiable para la interconexión de edificios o sucursales en una organización.

La implementación de un dispositivo SD-RED proporciona una opción versátil para la conexión de sitios remotos. El enfoque de instalación del SD-RED de Sophos implica una planificación meticulosa, la adquisición del hardware adecuado, la configuración inicial y la configuración de la conectividad. Esto permite establecer una conexión segura y confiable entre las sucursales, aprovechando la infraestructura existente y reduciendo los costos de conectividad.

Por otro lado, la VPN SSL de Sophos ofrece una solución flexible y segura para conectar edificios a través de Internet. La implementación de una VPN SSL implica una planificación adecuada, la configuración del firewall Sophos SG, la generación de certificados SSL y la configuración de la conexión VPN SSL. Esto permite a los usuarios remotos conectarse de forma segura a la red central y acceder a los recursos necesarios.

Ambos enfoques tienen ventajas significativas. El SD-RED brinda una conectividad confiable y segura, especialmente en entornos con conexiones de Internet inestables o limitadas, utilizando una infraestructura de red dedicada. Por otro lado, la VPN SSL es una opción flexible y escalable que permite a los usuarios remotos acceder a la red central desde cualquier ubicación a través de Internet.

### 6.1 Debilidades

- **Configuración compleja:** Sophos puede requerir conocimientos técnicos avanzados para configurar y administrar correctamente, lo que podría dificultar su implementación para usuarios menos experimentados.
- **Dependencia de infraestructura externa:** El funcionamiento de la VPN Sophos puede depender de la infraestructura y recursos externos, como servidores y conexiones de red, lo que podría generar vulnerabilidades o fallas en el servicio si alguno de estos elementos falla.

## 6.2 Amenazas

- **Ataques cibernéticos:** Las VPN son objetivos atractivos para los ciberdelincuentes, ya que pueden intentar aprovechar las vulnerabilidades en el sistema para acceder a información confidencial o realizar ataques de denegación de servicio.
- **Pérdida de datos:** En caso de una configuración incorrecta o una falla en la VPN, existe el riesgo de que los datos transmitidos a través de la red sean interceptados o comprometidos, lo que podría tener consecuencias negativas para la seguridad y la privacidad de los usuarios.

## 6.3 Fortalezas

- **Seguridad:** Sophos es una reconocida empresa de seguridad cibernética y sus soluciones VPN suelen ofrecer altos niveles de cifrado y protección de datos, lo que contribuye a garantizar la confidencialidad y la integridad de la información transmitida.
- **Integración con otros productos:** Si ya utilizas productos de Sophos, como firewalls o soluciones de seguridad adicionales, la VPN puede integrarse fácilmente en tu infraestructura existente, lo que facilita la administración y el monitoreo centralizados.

## 6.4 Oportunidades

- **Colaboraciones estratégicas:** Buscar asociaciones con otras empresas o proveedores de servicios de seguridad cibernética podría ayudar a expandir la adopción de la VPN Sophos y aumentar su alcance en diferentes mercados o sectores específicos.
- **Mayor demanda de privacidad en línea:** Con el creciente interés en proteger la privacidad en línea, existe una creciente demanda de soluciones VPN seguras y confiables. Esto puede representar una oportunidad para promover y ofrecer la VPN de Sophos a un mercado en crecimiento.

## 6.5 Ampliaciones Futuras

- **Integración con sistemas de prevención de intrusiones (IPS):** Para detectar y prevenir intrusiones en la red, se puede considerar la integración de un sistema de prevención de intrusiones con la VPN. Un IPS monitoreará y analizará el tráfico de red en busca de patrones o comportamientos sospechosos, y tomará medidas para bloquear o mitigar posibles ataques antes de que puedan causar daño.
- **Implementación de políticas de acceso granulares:** Sophos permite implementar políticas de acceso granulares basadas en el usuario, dispositivo o ubicación. Esto puede ser útil para asegurar un acceso controlado y restringido a ciertos recursos de la red, lo que mejora la seguridad y la segmentación de la red.

## 6.6 Escalabilidad

- **Administración centralizada:** Sophos Central, la plataforma de administración unificada de Sophos, permite gestionar de manera centralizada y escalable múltiples instancias de Sophos VPN. Esto simplifica la administración y configuración de la VPN en diferentes ubicaciones y para un número creciente de usuarios.
- **Escalabilidad de usuarios:** Sophos puede admitir un número creciente de usuarios sin comprometer el rendimiento. Puede escalar verticalmente agregando más recursos de hardware a la infraestructura existente para manejar la carga adicional de usuarios. Sophos también ofrece la opción de implementar clústeres de VPN para equilibrar la carga entre varios servidores y garantizar un rendimiento óptimo.

## 7. Bibliografía y Referencias

1. Sophos. (2022). Configurar acceso VPN SSL mediante IPSec.
  - a. <https://doc.sophos.com/nsg/sophos-firewall/18.5/help/en-us/webhelp/onlinehelp/AdministratorHelp/VPN/RemoteAccessVPN/VPNIPsecSophosConnectClient/index.html>
2. Sophos. (2022). Acceso al portal de usuario.
  - b. <https://doc.sophos.com/nsg/sophos-firewall/18.5/help/en-us/webhelp/onlinehelp/UserPortalHelp/UserPortalIntro/index.html>
3. Cloudflare. (2022). Qué es IPSec.
  - c. <https://www.cloudflare.com/es-es/learning/network-layer/what-is-ipsec/>
4. Manual Plus. (2022). Manual de Instrucciones de SD-RED.
  - d. [https://es.manuals.plus/sophos/sd-red-20-remote-ethernet-device-manual#axzz8369pEnto?utm\\_content=cmp-true](https://es.manuals.plus/sophos/sd-red-20-remote-ethernet-device-manual#axzz8369pEnto?utm_content=cmp-true)
5. Mioficina. (2020). Manual de Instalación VPN SSL.
  - e. <https://www.mioficina.co/sites/default/files/2020-12/manual-mo-instalacion-vpn-ssl-sophos.pdf>
6. Sophos. (2022). Guía avanzada de inicio.
  - f. [https://docs.sophos.com/esg/enterprise-console/5-5/help/es-es/PDF/sec\\_55\\_asgesp.pdf](https://docs.sophos.com/esg/enterprise-console/5-5/help/es-es/PDF/sec_55_asgesp.pdf)
7. Sophos. (2022). Características de XG Firewall.
  - g. <https://www.sophos.com/es-es/products/next-gen-firewall/features>
8. Sophos. (2022). Guía de interfaz de admin en XG Firewall.
  - h. <https://docs.sophos.com/nsg/sophos-firewall/v17.0.0/PDF/Sophos%20XG%20Firewall%20Web%20Interface%20Reference%20Guide.pdf>

## 8. Anexos

### 8.1 Lista de Acrónimos

Acrónimo	Definición
VPN	Red Privada Virtual
IPSec	Protocolo de seguridad de internet
SSL/TLS	Capa de puertos seguros/Capa de transporte seguro
DES	Estándar de cifrado de datos
AES	Estándar de cifrado avanzado
SHA	Secure Hash Algorithm
MD5	Message-Digest Algorithm
PKI	Infraestructura de clave publica
ONT	Optical Network Terminal