Universidad Nacional de Ingeniería

Área de Conocimiento de Tecnología de la Información y Comunicación

Desarrollo de propuesta técnica para la integración de Sophos Firewall como NGFW en redes Enterprise escalables

Trabajo Monográfico para optar al título de Ingeniero Electrónico

Elaborado por:

Br. Jafet Daniel Espinoza Chávez
Carnet: 2019-0437U

Br. María José Espinoza Abarca
Carnet: 2018-0031U

Br. Abiel Enrique Sequeira Robleto
Carnet: 2019-0172U

Tutor:

MSc. Jaime Alvarez Calero

14 de mayo de 2026
Managua, Nicaragua

Dedicatoria

A Dios y a la Santísima Virgen María, por iluminar mi camino, darme fortaleza en los momentos difíciles y permitirme culminar esta etapa tan importante de mi vida.

A mis padres y familia, por su amor, esfuerzo y apoyo incondicional; por estar presentes en cada paso, motivarme a seguir adelante y enseñarme que con fe, dedicación y perseverancia es posible alcanzar las metas. Con mucho cariño y gratitud, les dedico este logro, porque también es fruto de su apoyo y de todo lo que han hecho por mí.

A mis amigos y compañeros de trabajo, quienes en los peores días siempre han estado y han sido un gran apoyo anímico durante este camino.

María José Espinoza Abarca

Quiero agradecer especialmente a mis padres, Magda Patricia Chávez López y José Ariel Espinoza Salinas, por ser un ejemplo de dedicación y constancia, y por brindarme siempre su apoyo incondicional en cada reto y meta propuesta. Gracias por confiar en mí y acompañarme durante todo este proceso.

A mi hermano, Miguel Alejandro Espinoza Chávez, por acompañarme durante esta etapa y por cada momento compartido a lo largo de este proceso.

A mis mascotas, por acompañarme durante tantas horas de estudio y trabajo, haciendo este proceso más ameno.

Jafet Daniel Espinoza Chávez

A mí madre, María Isabel Robleto por ser el ejemplo más grande de constancia, esfuerzo y determinación en mi vida.

Este logro también le pertenece a usted, porque con su amor, dedicación y ejemplo me enseñó que la perseverancia siempre conduce a alcanzar las metas propuestas

Con profundo amor, respeto y gratitud, le dedico este trabajo

Abiel Enrique Sequeira Robleto

Resumen

El presente estudio analiza la integración de Sophos Firewall como solución de firewall de nueva generación (NGFW) dentro de una arquitectura de red empresarial escalable. El objetivo principal consiste en evaluar la viabilidad técnica y económica de implementar esta tecnología para mejorar la seguridad perimetral y el control del tráfico en entornos corporativos.

En primer lugar, se identifican los elementos técnicos de la infraestructura de red y los requerimientos necesarios para la incorporación del firewall, considerando aspectos como la segmentación de red, la topología existente y los riesgos asociados a la exposición de servicios hacia redes externas. A partir de este análisis, se establecen las condiciones necesarias para integrar el firewall como punto central de control del tráfico dentro de la arquitectura de red.

Posteriormente, se desarrollan políticas de seguridad orientadas a la protección perimetral de servidores web y al control de acceso basado en segmentación de red mediante VLAN. Estas políticas permiten implementar mecanismos de inspección profunda de tráfico, filtrado de aplicaciones, prevención de intrusiones y protección de aplicaciones web mediante el uso de funcionalidades avanzadas del firewall.

La evaluación funcional de la solución se realiza a través de un entorno de laboratorio emulado en la plataforma PNETLab, el cual permite validar el comportamiento del firewall dentro de un escenario Enterprise controlado. En este entorno se analizan diferentes mecanismos de seguridad implementados por el firewall y su capacidad para gestionar el tráfico entre distintas zonas de seguridad.

Finalmente, se realiza un análisis costo–beneficio basado en el modelo ROSI (Return on Security Investment) con el propósito de determinar la viabilidad económica de la solución. Los resultados obtenidos evidencian que la implementación de un firewall de nueva generación contribuye significativamente a fortalecer la postura de seguridad de la organización y puede generar beneficios económicos al reducir los riesgos asociados a incidentes de seguridad.

En conclusión, el estudio demuestra que la integración de Sophos Firewall dentro de una arquitectura Enterprise segmentada constituye una alternativa viable tanto desde el punto de vista técnico como financiero, permitiendo mejorar la protección de la infraestructura de red y facilitar la administración del tráfico en entornos empresariales.

Índice

I. INTRODUCCION 1

II. OBJETIVOS 3

2.1. Objetivo general 3

2.2. Objetivos específicos 3

III. JUSTIFICACIÓN 4

IV. MARCO TEÓRICO 5

4.1. Definición de Red de computadoras 5

4.2. Firewalls de nueva generación (NGFW) 9

4.3. Modelos de evaluación financiera en proyectos de ciberseguridad 18

V. DISEÑO METODOLOGICO 22

5.1. Paradigma de la investigación 22

5.2. Enfoque y tipo de investigación 22

5.3. Población y muestra 23

5.4. Diseño de la investigación 25

5.5. Técnicas e instrumentos de recolección de datos 25

5.6. Procedimiento para la validación técnica 29

5.7. Procedimiento para el dimensionamiento del Firewall 37

5.8. Procedimiento para el análisis de viabilidad económica 40

VI. DESARROLLO 45

6.2. Formulación de políticas de seguridad orientada a Sophos Firewall 49

6.3. Análisis de la efectividad funcional de Sophos Firewall en entorno emulado . 52

6.4. Procedimiento para el dimensionamiento del Firewall 80

6.5. Análisis de Viabilidad Económica mediante el Modelo ROSI 82

VII. CONCLUSIONES 94

VIII. RECOMENDACIONES 96
IX. BIBLIOGRAFÍA 97
X. ANEXOS 101

Índice de figuras

Figura 1: Topología Jerárquica de un diseño de red, adaptada de (Oppenheimer, 2010). 6
Figura 2: Topología con DMZ, tomada de (Oppenheimer, 2010). 8
Figura 3: Modelo Zero Trust Network Access, adaptada de (NGX Networks, 2022). 9
Figura 4: Proceso de inspección de paquetes, adaptado de (IR teams, s.f.). 11
Figura 5: Proceso de SSL forward proxy e inspección TLS, adaptado de (Cloud Google, s.f.). 12
Figura 6: Principios de diseño seguro en equipos Sophos, adaptado de (Sophos Firewall, 2025). 14
Figura 7: Procesador Xstream Flow en la serie XGS, adaptado de (McCormack, 2022). 17
Figura 8: Diagrama de Red PNETLab, elaboración propia. 58
Figura 9: Recursos SFOS, elaboración propia. 59
Figura 10: VLAN SFOS (elaboración propia, 2026), elaboración propia. 60
Figura 11: Interfaz WAN PortB, elaboración propia. 61
Figura 12: Interfaz WAN PortD, elaboración propia. 62
Figura 13: Interfaz MPLS PortE, elaboración propia. 62
Figura 14: Enrutamiento Sucursal 02, elaboración propia. 63
Figura 15: Configuración VPN TUNNEL INTERFACE, elaboración propia. 64
Figura 16: Configuración Phase 1 VPN, elaboración propia. 64
Figura 17: Configuración DH GROUP, elaboración propia. 65
Figura 18: Configuración DH GROUP, elaboración propia. 65
Figura 19: IPsec SINCRONIZACIÓN, elaboración propia. 65
Figura 20: Interfaz XFRM, elaboración propia. 66
Figura 21: Interfaz XFRM, elaboración propia. 67
Figura 22: Server AD Integration, elaboración propia. 68
Figura 23: Groups AD, elaboración propia. 69
Figura 24: Métodos de Autenticación, elaboración propia. 70
Figura 25: STAS Cuarentena, elaboración propia 71

Figura 26: Perfiles Web, elaboración propia. 72
Figura 27: Perfiles App, elaboración propia. 72
Figura 28:Perfiles App – Usuarios IT, elaboración propia. 73
Figura 29: Perfiles WEB – Usuarios IT, elaboración propia. 74
Figura 30: Perfiles WEB – Usuarios IT, elaboración propia. 75
Figura 31: Perfiles WEB Proxy, elaboración propia. 75
Figura 32: Perfiles IPS, elaboración propia. 76
Figura 33: FW-Rules, elaboración propia. 77
Figura 34: Diagrama de Red Casa Matriz, elaboración propia. 102
Figura 35: Diagrama de red sucursales, elaboración propia. 103
Figura 36: Repositorio de Imágenes en Pnetlab, elaboración propia. 108
Figura 38: Logs Bloqueos Application Control, elaboración propia. 110
Figura 39: Logs Bloqueos Web Filter, elaboración propia. 111
Figura 40: Logs Bloqueos WAF, elaboración propia. 111
Figura 41: Logs STAS, elaboración propia. 111
Figura 42: Logs VPN SSL, elaboración propia. 112
Figura 43: Logs VPN IPsec (Comunicación Sucursal01 a AD), elaboración propia. 112

Índice de tablas

Tabla 1: Distribución lógica de servicios y activos dentro de la infraestructura de red, elaboración propia. 53
Tabla 2: Distribución de flujos y puertos para activos críticos, elaboración propia. 54
Tabla 3: Estructura de comunicación, elaboración propia. 61
Tabla 4: Firewall WAF parte 1, elaboración propia. 78
Tabla 5: Firewall WAF parte 2, elaboración propia. 79
Tabla 6: Firewall WAF parte 3, elaboración propia. 79
Tabla 7: Inversión en Hardware y Licenciamiento (Periodo 36 meses), adaptada de (Grupo Intelector, 2026). 83
Tabla 8: Costos de servicios profesionales, adaptado de (Grupo Intelector, 2026). 83
Tabla 9: Consolidado de inversión total, adaptado de (Grupo Intelector, 2026). 84
Tabla 10: Identificación de escenarios de riesgos relevantes, adaptado de (Verizon DBIR, 2025). 85
Tabla 11: Cálculo de SLE por escenario, adaptado de (IBM Cost of a Data Breach Report ,2025). 87
Tabla 12: Estimación de annual rate of occurrence (ARO), adaptado de (IBM Cost of a Data Breach Report ,2025). 87
Tabla 13: Pérdida anual esperada - escenario actual (Sin NGFW), adaptado de (IBM Cost of a Data Breach Report ,2025). 88
Tabla 14: Eficacia de mitigación por escenario, adaptado de (Han,2024). 90
Tabla 15: Pérdida anual esperada - escenario con Sophos Firewall, elaboración propia. 90
Tabla 16: Aplicación de la fórmula ROSI, elaboración propia. 91
Tabla 17: Análisis de sensibilidad del ROSI, elaboración propia. 92
Tabla 18: Compra de equipos requeridos para la red, adaptado de (Grupo Intelector, 2026). 101
Tabla 19: Cotización, adaptado de (Grupo Intelector, 2026). 102
Tabla 20: Tabla VLSM, elaboración propia 104
Tabla 21: Matriz general de control de navegación, elaboración propia. 105

Tabla 22: Matriz general de control de navegación, elaboración propia. 106
Tabla 23: Matriz general de control de navegación, elaboración propia. 107
Tabla 24: Matriz de configuración VPN IPsec entre sucursal 1 y casa matriz, elaboración propia. 109
Tabla 25: Matriz de configuración VPN IPsec entre sucursal 1 y casa matriz, elaboración propia. 110

Anexos

Anexo A: Cotización y dimensionamiento de Sophos NGFW 101
Anexo B: Topología de red del escenario Enterprise 102
Anexo C: Segmentación lógica de la red 103
Anexo D: Repositorio de imágenes PnetLab. 108
Anexo E: Configuración de políticas en Sophos Firewall 108
Anexo F: Registros de Eventos y Resultados de Pruebas de Seguridad del Sophos Firewall 110

I. INTRODUCCION

Respecto al crecimiento acelerado de las tecnologías de la información y la comunicación ha transformado la forma en que las organizaciones diseñan, operan y protegen sus infraestructuras de red. En los entornos empresariales modernos, caracterizados por la interconexión de múltiples sedes, el uso intensivo de servicios digitales y la adopción de aplicaciones basadas en la nube, la seguridad de la información se ha convertido en un pilar fundamental para garantizar la continuidad operativa, la confidencialidad de los datos y el cumplimiento de los objetivos estratégicos institucionales. En este contexto, las redes Enterprise requieren soluciones de seguridad avanzadas que no solo controlen el tráfico, sino que también ofrezcan visibilidad, escalabilidad y protección integral frente a amenazas cada vez más sofisticadas.

Según; Cisco; 2024, p.78 afirme que, tradicionalmente, los firewalls convencionales han desempeñado un papel clave en la protección perimetral; sin embargo, su enfoque limitado a direcciones IP, puertos y protocolos resulta insuficiente frente a los vectores de ataque actuales, donde el tráfico cifrado, el malware avanzado, las amenazas internas y los ataques dirigidos representan riesgos significativos. Como respuesta a estas limitaciones, surgen los firewalls de nueva generación (NGFW), los cuales integran capacidades como inspección profunda de paquetes, control de aplicaciones, análisis de comportamiento, inspección de tráfico cifrado y mecanismos avanzados de prevención de intrusiones, permitiendo una defensa más eficaz y contextualizada.

Dentro de este marco tecnológico, Sophos Firewall se posiciona como una solución NGFW orientada a entornos empresariales escalables, incorporando la arquitectura Xstream, aceleración de tráfico mediante FastPath, inspección TLS 1.3, capacidades SD-WAN. Estas características lo convierten en una alternativa viable para organizaciones que buscan fortalecer su postura de seguridad sin comprometer el rendimiento ni la flexibilidad de su infraestructura de red.

El presente documento tiene como finalidad desarrollar una propuesta técnica para la integración de Sophos Firewall como firewall de nueva generación (NGFW) en redes Enterprise escalables, considerando los requerimientos de seguridad, desempeño y crecimiento propios de los entornos empresariales modernos. La propuesta se orienta a definir una arquitectura de protección perimetral capaz de ofrecer control de acceso granular, inspección avanzada del tráfico y mitigación efectiva de amenazas, sin comprometer la eficiencia operativa de la red.

El desarrollo del trabajo se fundamenta en el análisis técnico de las capacidades del Sophos Firewall y su aplicación dentro de un escenario empresarial escalable, evaluando su comportamiento frente a tráfico cifrado, segmentación de red, control de aplicaciones y políticas de seguridad avanzadas. Asimismo, se consideran criterios de rendimiento, flexibilidad y viabilidad económica que permiten determinar la pertinencia de su adopción como solución de seguridad perimetral en organizaciones con necesidades de crecimiento y modernización tecnológica.

De esta manera, el documento aporta una base técnica que facilita la toma de decisiones informadas para la implementación de soluciones NGFW en redes empresariales, contribuyendo al fortalecimiento de la seguridad perimetral y al diseño de infraestructuras de red más robustas, eficientes y preparadas para enfrentar los desafíos actuales y futuros en materia de ciberseguridad.

II. OBJETIVOS

2.1. Objetivo general

Desarrollar propuesta técnica para la integración de Sophos Firewall como NGFW en redes Enterprise escalables para el control de acceso granular y defensa integral contra amenazas cibernéticas.

2.2. Objetivos específicos

- Determinar los requerimientos técnicos, de tráfico y seguridad de la red, considerando la segmentación de la infraestructura y amenazas actuales
- Implementar políticas de seguridad para el control, inspección y protección del tráfico de red mediante Sophos firewall dentro del entorno emulado
- Analizar la efectividad funcional de Sophos Firewall en un escenario Enterprise escalable, definido como un caso de estudio lógico, mediante un entorno emulado controlado.
- Realizar un análisis costo–beneficio que determine la viabilidad económica y el retorno de inversión de la solución firewall mediante estimaciones económicas basadas en estándares e informes de la industria de ciberseguridad

III. JUSTIFICACIÓN

En cuanto a la propuesta de integración de un equipo Firewall de nueva generación (NGFW) surge debido a la constante evolución de las tecnologías de información y la evolución de vulnerabilidades en las infraestructuras de red, convirtiendo de esta forma la seguridad perimetral como un pilar estratégico para la continuidad de un negocio. Tradicionalmente, los firewalls tradicionales resultan limitados al basar su funcionamiento principalmente en el filtrado por direcciones IP, puertos y protocolos, sin ofrecer un análisis contextual del tráfico ni mecanismos avanzados de inspección.

Por esta razón, la selección de Sophos Firewall se fundamenta en sus capacidades técnicas orientadas a entornos empresariales. Entre estas destacan la arquitectura Xstream, el procesamiento optimizado del tráfico mediante FastPath y las capacidades de inspección TLS. Debido a la necesidad de proporcionar una referencia técnica sobre los criterios que deben considerarse durante el proceso de evaluación, dimensionamiento y cotización de soluciones de seguridad es que este trabajo también se realiza desde una perspectiva económica. Esto se realiza debido a que a diferencia de otros proyectos tecnológicos, la inversión en seguridad no puede analizarse únicamente bajo esquemas tradicionales de costo-beneficio, ya que su valor se relaciona principalmente con la reducción del riesgo y mitigación de incidentes.

En consecuencia, el presente estudio se justifica por la necesidad de evaluar e integrar mecanismos de seguridad avanzados capaces de responder a los requerimientos actuales de las redes empresariales. Asimismo, la propuesta aporta una referencia técnica y metodológica para futuras implementaciones de soluciones NGFW en entornos empresariales escalables, contribuyendo al fortalecimiento de la seguridad perimetral, la optimización de recursos y la toma de decisiones orientadas a la mejora continua de la infraestructura tecnológica.

IV. MARCO TEÓRICO

El presente Marco Teórico proporciona los fundamentos necesarios para entender la relevancia técnica y operativa de integrar un NGFW como Sophos Firewall en redes escalables, explorando desde la arquitectura de una red Enterprise hasta los elementos clave de seguridad, escalabilidad y protección perimetral avanzada.

4.1. Definición de Red de computadoras

Una red de computadoras es un conjunto de dispositivos interconectados que comparten recursos, servicios e información mediante protocolos de comunicación estandarizados. Su propósito es facilitar la transmisión de datos, mejorar la productividad y garantizar la disponibilidad de servicios tecnológicos esenciales.

4.1.1. Diseño jerárquico de red

El diseño de una red en orden jerárquico se realiza con el objetivo de brindar un enfoque que permita a la arquitectura poder ser escalable y eficiente a medida que se da un crecimiento en la institución. El modelo jerárquico se divide en tres capas, pensadas para que cada una desempeñe una función específica, permitiendo así una mayor facilidad en la realización de cambios dentro de la arquitectura. Las tres capas correspondientes al modelo jerárquico corresponden a la capa Core, capa de distribución y capa de acceso.

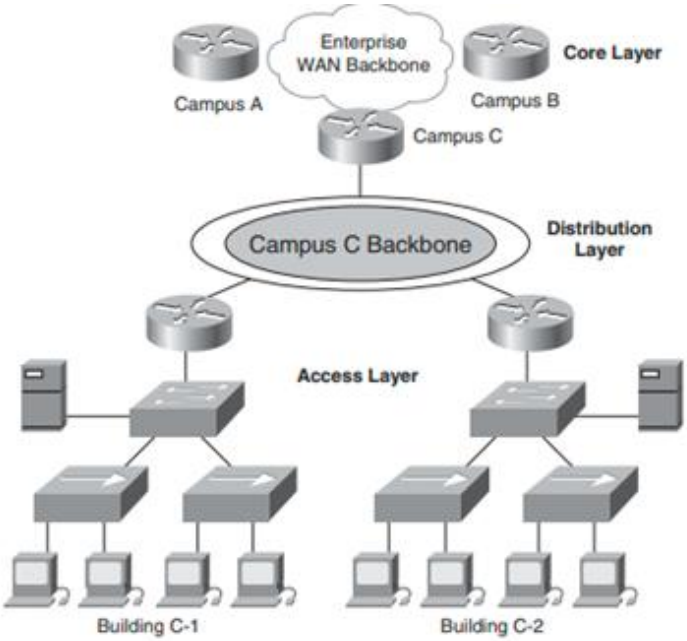


Figura 1: Topología Jerárquica de un diseño de red, adaptada de (Oppenheimer, 2010).

- Capa central (Core layer):

La capa central corresponde a la estructura principal de este sistema jerárquico, esta capa es crucial para la interconectividad rápida y confiable de grandes volúmenes de tráfico entre las capas de distribución y acceso. Al configurar enrutadores en la capa central, se deben utilizar funciones de enrutamiento que optimicen el rendimiento de los paquetes. Según Oppenheimer (2010, pág. 127) en Top-Down network design, se deben evitar el uso de filtros de paquetes u otras funciones que ralentizan la manipulación de paquetes.

- Capa de distribución (Distribution layer):

Dentro del modelo jerárquico de red, la capa de distribución corresponde al punto intermedio entre la capa de acceso y la capa central o core. El principal objetivo de

esta capa se basa en el control, enrutamiento y filtrado del tráfico antes de ser enviado al backbone. Una de las funciones de la capa de distribución se basa en permitir que la capa de acceso se pueda conectar a sitios con diferentes protocolos manteniendo un alto rendimiento. (Cisco, 2018) destaca la importancia de aplicar redundancia para garantizar alta disponibilidad, incluyendo enlaces redundantes entre los switches de capa distribución y acceso.

- Capa de acceso (Access layer):

(Oppenheimer, 2010, pág. 128) establece que la capa de acceso proporciona a los usuarios de segmentos locales acceso a la red, indicando que en esta capa se pueden incluir enrutadores, conmutadores, puentes, hubs y Access points, siendo los switches implementados a menudo para dividir dominios de ancho de banda para satisfacer altas demandas de ancho de banda.

4.1.2. Segmentación de redes y zonas de seguridad

El establecimiento de múltiples equipos dentro de una sola red plana genera congestión de tráfico y un aumento innecesario de dominio de broadcast, así como de brechas de seguridad. Si bien la segmentación de red es posible, resulta costosa y difícil de gestionar en infraestructuras modernas. En este contexto, las VLANs permiten una segmentación lógica eficiente que reduce dominios de broadcast, mejora el rendimiento y fortalece la seguridad de la red.

La forma en la que se decide segmentar una red se denomina política de seguridad, esto funciona bajo el control del tráfico entre las partes o segmentos, permitiendo la opción de bloquear el tráfico desde una zona a otra. Dentro del diseño de redes se tienen dos tipos de segmentación las cuales son: macrosegmentación y microsegmentación.

De acuerdo con (McCarthy, 2023, pág. 67), la macrosegmentación es una forma de dividir una red en redes virtuales más pequeñas, generalmente según los tipos de usuarios, dispositivos o aplicaciones. Esto permite que la macrosegmentación establezca límites de seguridad entre grandes dominios de red mediante la creación de segmentos lógicos con políticas diferenciadas.

4.1.3. ¿Qué es una zona desmilitarizada (DMZ)?

Una zona desmilitarizada o (DMZ) se considera un segmento de red el cuál alberga servicios que deben ser accesibles desde redes externas, pero mantiene una separación estricta con la red interna a la que pertenece. (Oppenheimer, 2010) menciona que, dentro del diseño de una red, los sistemas de gestión deben estar especialmente protegidos debido a su almacenamiento de información sensible por lo que, para disminuir riesgos, estos deben ubicarse en su propia DMZ protegidos por un firewall.

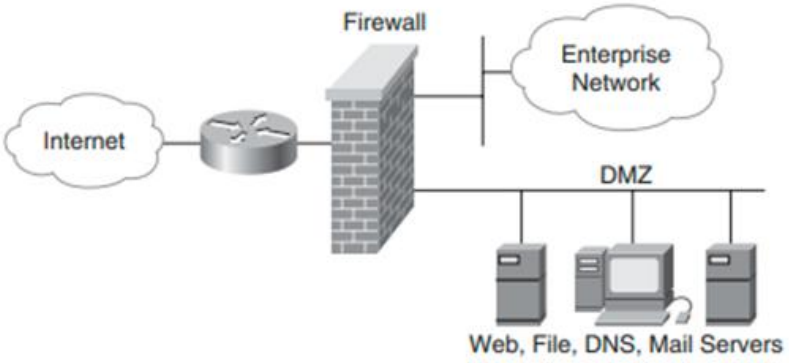


Figura 2: Topología con DMZ, tomada de (Oppenheimer, 2010).

Pese a que la DMZ representa un modelo tradicional y efectivo en cuanto a aislamiento perimetral, las arquitecturas modernas de seguridad han evolucionado de modo en el que no es suficiente solamente el enfoque de confianza que se deja implícito en la red interna. De este modo surge como modelo el Zero trust, modelo que redefine la forma en que se gestionan los accesos y las comunicaciones dentro de la infraestructura.

4.1.4. ¿Qué es una topología Zero Trust?

El modelo de confianza cero trabaja bajo el principio de establecer una verificación para cada usuario, dentro o fuera de la red. Siendo de esta forma que establece una estricta verificación de identidad y controles de acceso para cada usuario y dispositivo que quiera acceder a los recursos de la red, empleando de esta forma una supervisión continúa para detectar posibles riesgos durante las sesiones.

Para (Halley, Prajapati, Leza, & & Saini, 2025) el nacimiento de este modelo de confianza cero se debe a la constante evolución dentro del panorama de amenazas que pueden afectar a las organizaciones e individuos debido a la constante evolución de los avances tecnológicos. El modelo de confianza cero con respecto a cada acceso, inicia con una solicitud explicita a cada recurso, el cual es evaluado mediante controles de identidad y contexto antes de ser usado. Una vez se valida su identidad, se aplican políticas de acceso que restringen recursos innecesarios para la petición de acceso. Finalmente, establece una vigilancia continua del comportamiento, complementada con monitoreo e inspección del tráfico.

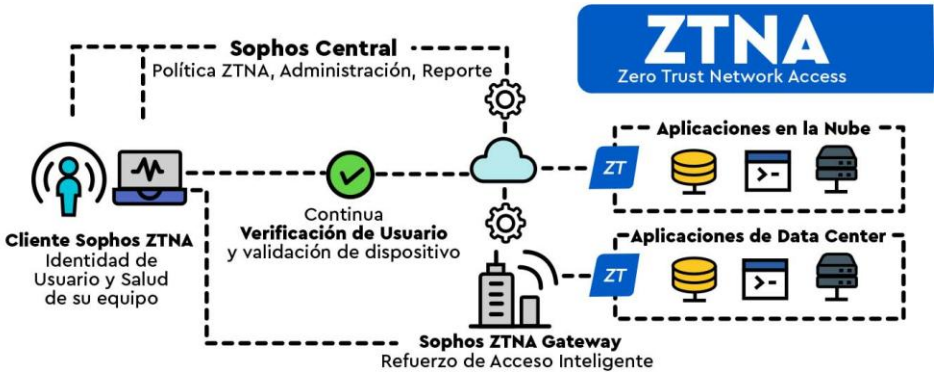


Figura 3: Modelo Zero Trust Network Access, adaptada de (NGX Networks, 2022).

4.2. Firewalls de nueva generación (NGFW)

Dentro del ámbito corporativo, el malware representa una amenaza significativa para la confidencialidad, integridad y disponibilidad de la información. (checkpoint, 2025) destaca que los ciber atacantes emplean este tipo de software con fines como: el robo de datos, la destrucción o cifrado de información, el espionaje digital, el control remoto de dispositivos, la participación en campañas delictivas a gran escala o la obtención de ingresos ilegales mediante actividades como la minería de criptomonedas sin autorización (cryptomining malware).

Es por esta razón y debido a la necesidad de garantizar un control de acceso sobre las redes confiables y no confiables, además de prevenir accesos no autorizados por lo que los firewalls fueron diseñados en principio.

4.2.1. Funcionalidades de un NGFW

Los firewalls de nueva generación (NGFW), contienen funcionalidades tales como IPS de nueva generación, control de aplicaciones, filtrado web avanzado, inspección TLS, protección contra amenazas “zero day” y sandboxing con análisis dinámico. Estas funciones proporcionan más capas de seguridad y control a nivel de aplicación en comparación con los firewalls tradicionales.

- Inspección profunda de paquetes (DPI): Los firewalls anteriores se enfocaban en realizar una inspección superficial de los paquetes ya que estos eran revisados mediante información de control como IP o puertos. DPI es integrado en firewalls de nueva generación para realizar una técnica avanzada de análisis de tráfico en donde esta no solo revisa los encabezados de los paquetes, sino que realiza inspección de la carga útil (payload) para identificar amenazas y comportamiento en la red.

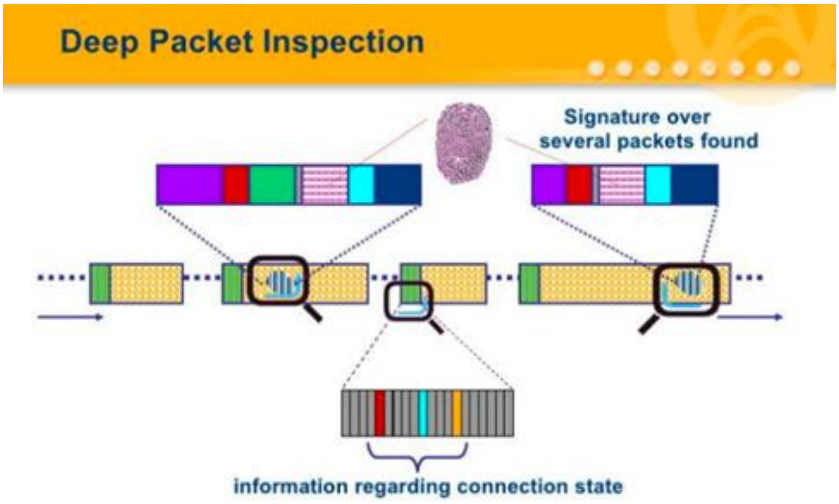


Figura 4: Proceso de inspección de paquetes, adaptado de (IR teams, s.f.).

- Filtrado web avanzado: Esta técnica permite clasificar y controlar el acceso a contenidos web basándose en categorías, reputación y comportamiento del usuario, abarcando incluso tráfico cifrado y políticas contextuales. A diferencia del filtrado básico de URLs, esta técnica integra inteligencia de amenazas y clasificación dinámica, proporcionando niveles superiores de seguridad para prevenir accesos a sitios maliciosos o no autorizados (Microsoft, s.f.).

- Amenazas zero day: Una amenaza del día cero es una de las formas más actuales por las que una empresa puede sufrir un ataque y comprometer la seguridad de la red. Este tipo de amenazas se basan en un fallo desconocido para el desarrollador de un sistema por lo que al momento de ser explotadas suponen un riesgo critico debido a que existe una gran brecha de tiempo desde que el atacante explota la vulnerabilidad hasta el momento en que se descubre.

- Inspección TLS: (Cloud Google) señala que la inspección TLS permite descifrar y analizar el tráfico cifrado para aplicar controles de seguridad avanzados. Esta técnica se encarga de desencriptar el tráfico cifrado de Internet (HTTPS/TLS), lo analiza internamente y luego lo vuelve a cifrar. Esto permite que se logren controles de seguridad avanzados para filtrado web, IPS y control de aplicaciones y políticas por contenido.

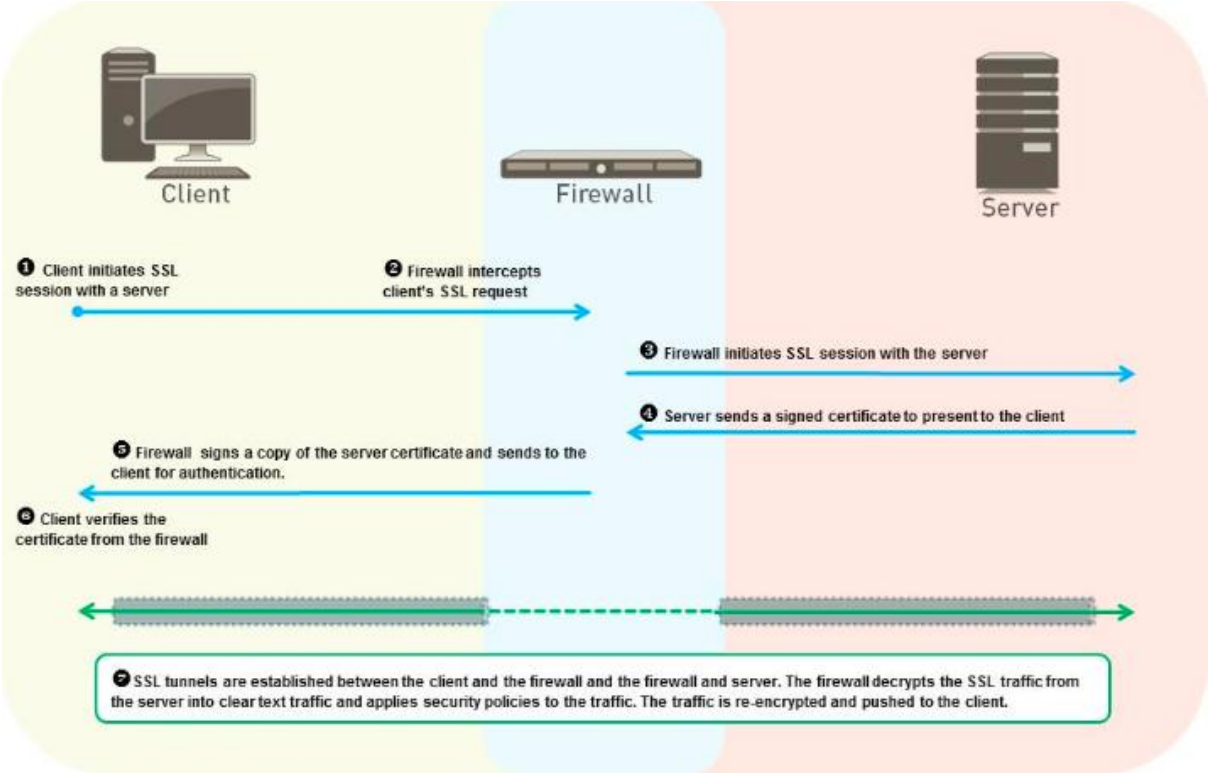


Figura 5: Proceso de SSL forward proxy e inspección TLS, adaptado de (Cloud Google, s.f.).

Se puede observar en la figura 5 como el flujo de tráfico desde el punto final del firewall al firewall de red inspecciona primero el paquete a través de un motor sin estado. Posterior si no hay coincidencias en el conjunto de reglas sin estado presentes y el tráfico está dentro del alcance de la configuración de cifrado TLS, el tráfico se reenvía para la operación de descifrado. Asimismo, después del descifrado, el tráfico se reenvía al motor con estado del firewall para su inspección en donde el firewall toma

una decisión en base a su conjunto de reglas de estado de entre las cuales están aprobar o desechar el tráfico. Si se aprueba, este procede a cifrar nuevamente el tráfico.

4.2.2. Sophos firewall como solución NGFW Enterprise

Sophos Firewall es un dispositivo de seguridad de red basado en zonas y políticas basadas en la identidad en su núcleo. Sophos incluye funciones diseñadas para diferentes entornos. Por ejemplo, tiene funciones específicamente para ayudar a las universidades y la educación superior. También incluyen potentes políticas de filtrado web y políticas integradas para la seguridad infantil y el cumplimiento normativo.

(Sophos Firewall, 2024) incorpora funciones de conectividad segura que permiten su implementación en arquitecturas empresariales distribuidas, facilitando la interconexión de sedes, sucursales y redes remotas mediante tecnologías como VPN y dispositivos de acceso remoto, manteniendo una aplicación coherente de las políticas de seguridad en toda la organización.

4.2.3. Arquitectura y funcionamiento de Sophos Firewall

Sophos Firewall es desarrollado usando los principios de “secure by design”, indicando de esta manera que sus productos están pensados desde el diseño en proteger la infraestructura de red. Uno de los primeros principios que emplea Sophos es el firewall health check, el cual consiste en la verificación de puntos de las configuraciones realizadas en el firewall y su comparación de mejores prácticas, informando de esta manera las áreas que podrían estar en riesgo. Posterior a esto integran como principio el monitoreo remoto de integridad el cuál consta de un sensor Linux Sophos XDR que permite la supervisión en tiempo real de la integridad del sistema (Sophos Firewall, 2025).

Asimismo, este incorpora la arquitectura next-gen Xstream la cual permite la modularización, aislamiento y contenedorización de los servicios. Los equipos Sophos cuentan con un kernel que les proporciona mayor seguridad y un aislamiento robusto en contra de ataques canal lateral y protección contra vulnerabilidades del CPU. Finalmente, Sophos incluye un sistema que permite incorporar actualizaciones de seguridad en caliente, lo cual permite actualizar los dispositivos de la marca sin necesidad de interrumpir las actividades y programar una ventana para ello.

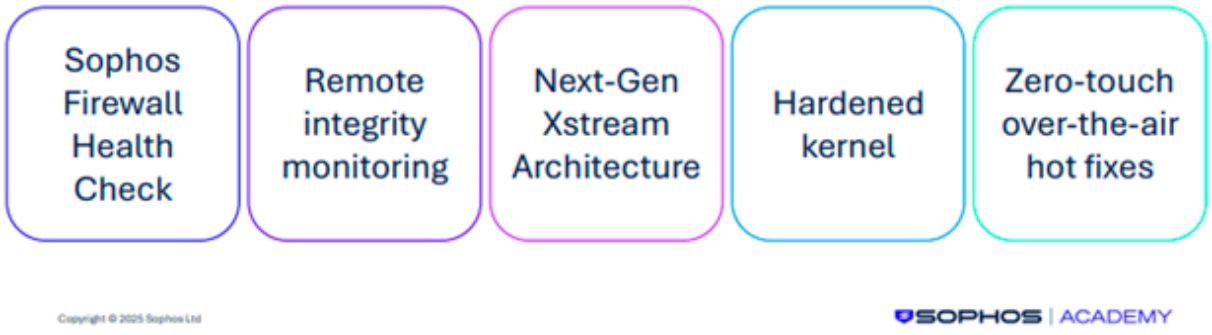


Figura 6: Principios de diseño seguro en equipos Sophos, adaptado de (Sophos Firewall, 2025).

La arquitectura de Sophos Firewall sigue el concepto del Attack kill chain, el cual describe las distintas etapas en las que se desarrolla un ataque desde su inicio hasta su impacto final. Esta clase de enfoque permite al firewall interrumpir un ataque en cualquiera de sus fases, en lugar de limitarse solamente al bloqueo perimetral. Sophos Firewall integra múltiples capacidades de seguridad que operan a lo largo del attack kill chain, incluyendo prevención de intrusiones, control de aplicaciones, filtrado web, inspección de tráfico cifrado y detección de amenazas avanzadas, con el fin de detener ataques antes de que comprometan los sistemas internos (Sophos Firewall, 2024).

4.2.4. Arquitectura Xstream: modelo de procesamiento del tráfico

Sophos Firewall, basado en arquitectura Xstream, es un NGFW diseñado para redes empresariales que requieren escalabilidad, visibilidad completa, alta eficiencia y seguridad sincronizada con endpoints y servidores. La arquitectura Xstream es uno de los elementos centrales en el funcionamiento de Sophos Firewall debido a que esta define el modo en que el tráfico es procesado y asegurado.

Asimismo, (Sophos Firewall, 2024) indica que esta arquitectura está diseñada para identificar rápidamente aplicaciones y flujos de tráfico confiables, permitiendo que estos sean acelerados, mientras que el tráfico sospechoso o desconocido es sometido a mecanismos de inspección avanzada, como análisis profundo de paquetes, prevención de intrusiones e inspección de tráfico cifrado.

4.2.5. Flujo de procesamiento del tráfico en Sophos Firewall

El flujo de procesamiento del tráfico que realiza Sophos Firewall es basado en un modelo secuencial de evaluación de reglas, donde cada paquete o sesión es comparado contra las reglas configuradas en el firewall siguiendo un orden especifico. De esta manera en este modelo, las reglas se procesan de arriba hacia abajo y la primera regla coincidente determina la acción aplicada al tráfico, ya sea permitirlo, bloquearlo o rechazarlo (Sophos Firewall, 2025).

Una característica distintiva del flujo de procesamiento en Firewalls de la marca Sophos es que las funciones avanzadas se integran directamente dentro de cada regla de firewall. Al permitir una conexión, la regla puede activar simultáneamente varias herramientas como DPI, control de aplicaciones, filtrado web, prevención de intrusiones y security Heartbeat. De esta forma el tráfico no es redirigido a motores externos, sino que es evaluado por múltiples controles de un único pipeline de inspección, alineado con la arquitectura Xstream (Sophos Firewall, 2025).

- Procesamiento mediante el motor DPI y aceleración del tráfico confiable

Dentro del procesamiento de tráfico que utiliza Sophos Firewall, se encuentra un motor de inspección profunda de paquetes (DPI) que permite analizar tráfico HTTP y HTTPS de forma independiente del puerto utilizado, identificando protocolos y aplicaciones mediante detección agnóstica de puertos. Este motor permite acelerar el tráfico considerado como “confiable” y derivarlo al mecanismo denominado como FastPath, lo que libera recursos del sistema para inspeccionar tráfico potencialmente riesgoso.

- Inspección de tráfico cifrado y control de contenido web

En relación flujo de procesamiento, cuando el contexto de la comunicación lo requiere, se incluye la inspección de tráfico cifrado TLS/SSL, permitiendo analizar sesiones HTTPS para detectar amenazas ocultas. Dependiendo de la configuración, el tráfico puede ser procesado directamente por el motor DPI o, en escenarios específicos, por el proxy web (Sophos Firewall, 2024).

En conjunto, el flujo de procesamiento del tráfico en Sophos Firewall se caracteriza por su evaluación secuencial de reglas, la integración de múltiples controles de seguridad dentro de un único flujo y la optimización del rendimiento mediante aceleración selectiva del tráfico confiable. De esta forma este diseño permite aplicar políticas de seguridad avanzadas sin introducir reprocesamientos innecesarios (Sophos Firewall, 2025).

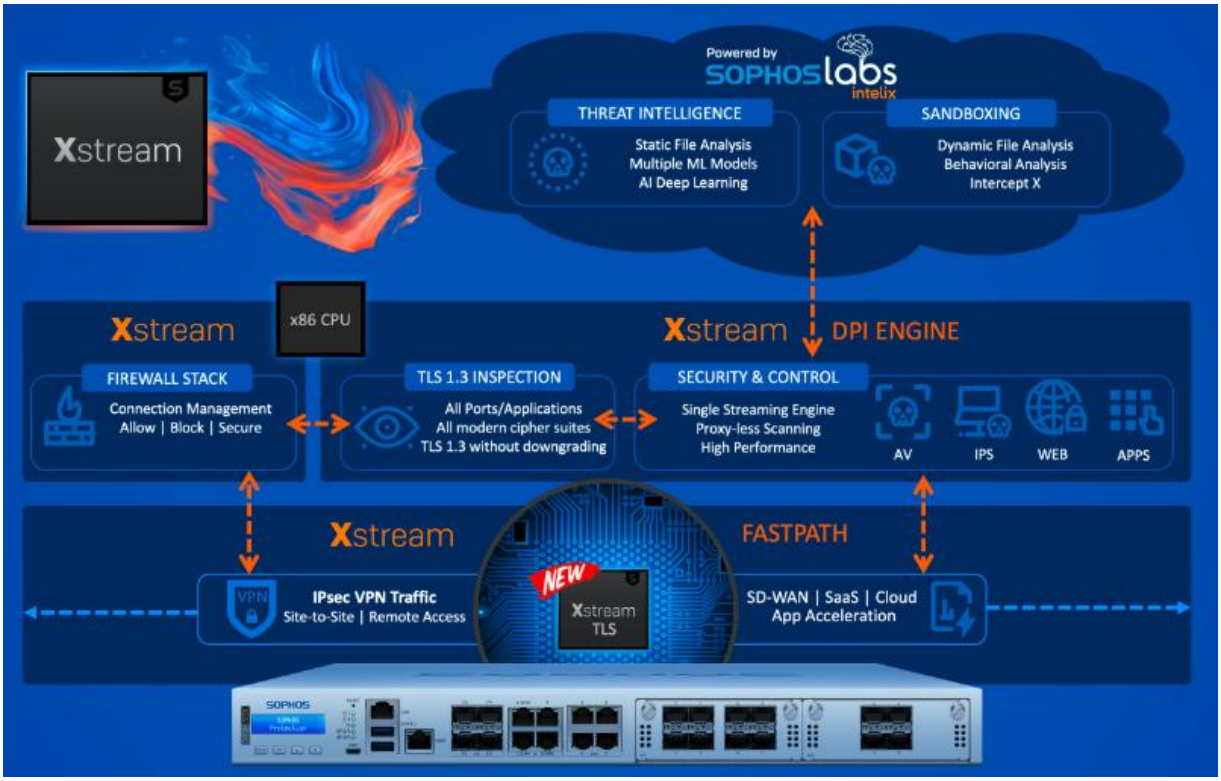


Figura 7: Procesador Xstream Flow en la serie XGS, adaptado de (McCormack, 2022).

De esta manera, la arquitectura Xstream representa el núcleo funcional del Sophos Firewall al establecer un modelo de procesamiento unificado del tráfico que integra varias funcionalidades de seguridad. Permitiendo así que este diseño pueda aplicar controles de forma eficiente, de modo que brinda un equilibrio entre rendimiento y protección que permite interrumpir un ataque en distintas fases. Siendo de esta forma que la arquitectura Xstream proporciona una base sólida para la implementación de políticas de seguridad avanzadas en entornos empresariales modernos.

4.3. Modelos de evaluación financiera en proyectos de ciberseguridad

4.3.1. La seguridad informática como inversión empresarial desde un enfoque económico

Dentro del entorno corporativo, la incorporación de sistemas de seguridad no solo contempla aspectos técnicos sino también financieros. De esta manera que para la ciberseguridad se toma el concepto de gestión del riesgo en donde se busca cuantificar el impacto económico potencial de incidentes y realizar una comparación con la inversión necesaria para mitigarlos. (Harkins, 2016) en su libro especializado sobre gestión del riesgo plantea cinco variables primarias las cuales se dividen en costo y mantenimiento, productividad y experiencia del usuario, objetivos del mercado, necesidades del cliente y finalmente el riesgo y cumplimiento. Este enfoque permite articular no solo cuáles son los riesgos tecnológicos, sino también cuál es la repercusión económica potencial de su materialización y, por ende, cómo justificar de manera cuantitativa la inversión en controles de seguridad.

De esta manera, los modelos de evaluación financiera como el Annual Loss Expectancy (ALE) y el Return on Security Investment (ROSI) proporcionan herramientas metodológicas para estimar el impacto económico de amenazas y ponderar la rentabilidad de las decisiones de inversión en ciberseguridad

4.3.2. Annual Loss Expectancy (ALE)

Dentro del estudio de análisis de riesgo, el análisis cuantitativo de riesgo se basa en el empleo de fórmulas que permiten expresar el riesgo en términos numéricos y financieros. Dentro de este enfoque, destacan tres formulas clásicas de análisis cuantitativo. Las cuales son el Annual Loss Expectancy (ALE), Single Loss Expectancy (SLE) y Safeguard Value.

(Landoll, 2011) parte del concepto de pérdida esperada, señalando que en el campo de la seguridad no se trabaja con certezas sino con probabilidades. Lo que implica que el riesgo debe calcularse considerando:

- Probabilidad de ocurrencia
- Impacto económico del evento

Estos principios estadísticos son los que funcionan como base conceptual sobre la cual se construyen SLE y ALE

El single Loss Expectancy (SLE) se puede definir como la pérdida esperada resultante de un solo incidente. Dicha pérdida esperada se puede representar por la siguiente fórmula:

$$SLE = ASSET\ VALUE\ X\ \text{EXPOSURE FACTOR}$$

Donde:

- **Asset Value (AV):** Valor económico del activo
- **Exposure Factor (EF):** Porcentaje promedio de pérdida en caso de incidente.

Se puede concluir que, para el factor de perdida en caso incidente, se puede ejemplificar con el caso de que, si un almacén se incendia y en promedio pierde la mitad de su valor, entonces el EF sería de 0.5.

De este modo, para los eventos de seguridad que ocurren varias veces al año y debido a que los presupuestos empresariales se manejan anualmente, es necesario calcular la pérdida esperada dentro de un ciclo anual con la siguiente formula:

$$ALE = SLE\ X\ ANNUAL\ RATE\ OF\ OCCURRENCE$$

Donde:

- **Annual Rateo of Occurrence (ARO):** Frecuencia estimada en la que ocurre un evento en el año.

Nota. Fórmula SLE y ALE tomada de The Security Risk Assessment Book (Landoll, 2011).

Finalmente, (Landoll, 2011) indica que el objetivo final no es solo calcular pérdidas, sino determinar cuánto debería invertirse en contramedidas. Introduciendo de este modo el concepto de Safeguard Value que permite evaluar si una medida de seguridad es económicamente justificable y se expresa como:

$$Safeguard\ Value = (ALE\ before\ - ALE\ after) - Annual\ Cost$$

Siendo de esta forma que el modelo Annual Loss expectancy expresa el riesgo de seguridad en términos financieros anuales, integrando el impacto económico de un incidente con su frecuencia estimada. De esta manera, el análisis cuantitativo no solo permite estimar perdidas esperadas, sino también fundamentar decisiones de inversión en controles de seguridad.

4.3.3. Retorno de la inversión en seguridad (ROSI)

El retorno de la inversión (ROI) es un indicador financiero utilizado para medir la rentabilidad de una inversión mediante la comparación entre los beneficios obtenidos y los costos asociados. En el ámbito de la seguridad informática, su aplicación presenta limitaciones, ya que este tipo de inversiones no genera ingresos directos, sino que busca prevenir pérdidas derivadas de incidentes de seguridad.

Para abordar esta particularidad surge el retorno de la inversión en seguridad (ROSI), la cuál es una adaptación del ROI diseñada para evaluar económicamente las inversiones en ciberseguridad. El calculo del ROSI se basa en comparar las pérdidas esperadas antes y después de implementar una solución de seguridad, tomando en cuenta factores como la frecuencia de incidentes, el costo promedio de cada evento y el nivel de mitigación proporcionado por la solución. De manera general se expresa de la siguiente manera:

$$ROSI = \frac{BENEFICIO\ DE\ SEGURIDAD - COSTO\ DE\ SOLUCIÓN}{COSTO\ DE\ LA\ SOLUCIÓN}$$

Nota. Fórmulas Safeguard Value y ROSI tomadas de The Security Risk Assessment Book (Landoll, 2011).

Donde:

- **Beneficio de la seguridad:** corresponde al valor económico de las perdidas evitadas
- **Costo de solución:** corresponde a aspectos de adquisición de tecnología, implementación, mantenimiento o capacitación personal.

De este modo, además de los beneficios cuantificables, el ROSI también considera factores estratégicos como la protección de la reputación corporativa, el cumplimiento normativo, la confianza de clientes y la continuidad operativa

V. DISEÑO METODOLOGICO

En este capítulo, se establecen el paradigma, tipo y diseño de la investigación; la técnica, validez y confiabilidad del instrumento para la recolección de datos; y las técnicas y procedimientos para interpretar los resultados.

5.1. Paradigma de la investigación

La metodología del presente proyecto se enmarca dentro del paradigma positivo, ya que busca comprobar la efectividad técnica y económica de una solución de seguridad (Sophos Firewall) mediante datos observables y medibles (tráfico de red, logs, bloqueos, costos, porcentajes de mitigación) en un entorno controlado.

Este paradigma resulta adecuado dado que posibilita analizar el comportamiento funcional del Sophos Firewall y determinar si sus capacidades técnicas son suficientes para cubrir los requerimientos de seguridad, segmentación y control de acceso en un entorno Enterprise, sin comprometer infraestructuras productivas reales.

5.2. Enfoque y tipo de investigación

5.2.1. Enfoque de la investigación

La presente investigación adopta un enfoque mixto, integrando métodos cuantitativos y cualitativos para abordar de manera integral el problema de seguridad en la infraestructura Enterprise objeto de estudio.

El componente cuantitativo se manifiesta en:

- El análisis financiero mediante el modelo ROSI con cálculos numéricos (inversión, ALE, SLE, ARO, porcentajes de retorno).

- La estimación de costos basada en cotización real de proveedor autorizado.
- La medición de eficacia de mitigación expresada en porcentajes.
- El análisis de sensibilidad con escenarios numéricos.

El componente cualitativo se manifiesta en:

- El diseño de la arquitectura de seguridad y segmentación de red.
- La formulación de políticas de seguridad por zona y perfil de usuario.
- La identificación de escenarios de riesgo mediante juicio experto.
- La evaluación de beneficios intangibles (reputación, confianza, cumplimiento normativo).
- La validación técnica en entorno emulado (PNETLab).

5.2.2. Tipo de investigación

De acuerdo con los objetivos planteados, la investigación es tipo descriptiva ya que se analizan y describen las características de la infraestructura de red actual, los flujos de tráfico críticos y los requisitos de seguridad del entorno Enterprise; tipo proyectiva ya que se diseña una propuesta técnica de integración de Sophos Firewall como NGFW que da solución a una necesidad específica de seguridad perimetral e interna.

5.3. Población y muestra

En el contexto del presente documento, los conceptos de población y muestra se adaptan al estudio de infraestructuras de red y escenarios de seguridad.

- Población

La población objeto de estudio está constituida por el universo de elementos técnicos y escenarios operativos que conforman una infraestructura de red Enterprise escalable, susceptible de ser protegida mediante un firewall de nueva generación.

Dicha población incluye: activos de red como servidores (internos y expuestos), estaciones de trabajo, dispositivos de infraestructura (switches, routers), enlaces WAN/LAN; flujos de tráfico como comunicaciones internas, tráfico perimetral, acceso remoto, tráfico cifrado y no cifrado; escenarios de riesgo como amenazas externas (malware, intrusión), amenazas internas (movimiento lateral), exposición de servicios web, filtración de datos; controles de seguridad con políticas de acceso, segmentación lógica, inspección de tráfico, filtrado de contenido, protección contra intrusiones.

Dado que la propuesta se desarrolla en un entorno emulado, la población se define de forma lógica y representativa, basada en estándares de arquitectura Enterprise y buenas prácticas de seguridad (NIST, ISO 27001), sin corresponder a una infraestructura productiva específica.

- Muestra

La muestra corresponde al subconjunto seleccionado de elementos y escenarios de la población, que fueron considerados para el diseño, implementación y validación de la propuesta técnica.

La selección se realizó mediante un muestreo intencional técnico, considerando criterios de criticidad, representatividad y viabilidad de emulación. En cuanto a la criticidad operativa, se incluyeron servidores AD, web públicos y enlaces WAN principales. Para la representatividad de tráfico, se consideraron flujos usuario-servidor, acceso a Internet y comunicaciones inter-VLAN. En términos de relevancia para seguridad, se seleccionaron escenarios de ransomware, filtración de datos, ataque a aplicación web y movimiento lateral. Finalmente, para la viabilidad de

emulación, se tomó una topología replicable en PNETLab con los recursos disponibles.

La composición de la muestra se estructura en cinco elementos fundamentales. Primero, la topología emulada corresponde a una arquitectura jerárquica. Segundo, los segmentos de red se organizan en cinco dominios lógicos que incluyen Usuarios, Servidores Internos, DMZ, Gestión y WAN. Tercero, los escenarios de prueba comprenden cuatro vectores de amenaza priorizados identificados como E1 a E4. Cuarto, las políticas validadas incluyen reglas de acceso, filtrado web, inspección SSL e IPS. Quinto, los parámetros financieros consideran los costos de la solución Sophos XGS 2100 más el licenciamiento por 36 meses.

5.4. Diseño de la investigación

El diseño es no experimental de campo simulado, ya que no se manipulan variables deliberadamente, los datos se obtienen de fuentes primarias (cotizaciones, especificaciones técnicas); la validación se realiza en entorno emulado (PNETLab) que replica las condiciones de una infraestructura Enterprise real.

5.5. Técnicas e instrumentos de recolección de datos

5.5.1. Técnicas empleadas

Para el desarrollo del presente proyecto se emplearon las siguientes técnicas:

Simulación en redes: mediante la plataforma PNETLab para validar la funcionalidad del firewall en entorno controlado.

Análisis documental: revisión de especificaciones técnicas, cotizaciones y documentación del fabricante (Sophos, 2025).

Juicio experto: evaluación técnica de requerimientos de seguridad basada en conocimiento especializado en redes Enterprise.

5.5.2. Identificación de elementos técnicos y requerimientos de red

Se establece una metodología de análisis técnico basada en preguntas estructuradas, orientada a identificar los elementos de una infraestructura de red empresarial y los requerimientos necesarios para la integración de un firewall de nueva generación, considerando de forma explícita las capacidades, alcances y limitaciones del Sophos Firewall como tecnología seleccionada.

Esta metodología se concibe como un marco de análisis orientado a una solución específica, en el cual las preguntas formuladas permiten evaluar si la infraestructura existente es compatible con las funcionalidades ofrecidas por Sophos Firewall y si dicha solución puede cubrir las necesidades de seguridad identificadas.

El análisis se organiza en cuatro dimensiones, cada una compuesta por un conjunto de preguntas técnicas que guían la recolección y evaluación de información relevante, tomando en cuenta los mecanismos de inspección, segmentación, control de tráfico y protección perimetral disponibles en Sophos Firewall.

- Análisis de la arquitectura general de la red

Este inciso tiene como objetivo comprender la estructura global de la red empresarial y su organización funcional, sin considerar aún dispositivos o topologías específicas.

Preguntas metodológicas:

1. ¿Qué tipo de arquitectura de red utiliza la organización (jerárquica, colapsada, distribuida o híbrida)?
2. ¿Existen puntos únicos de falla en la arquitectura actual?
3. ¿Cómo se gestiona el enrutamiento interno entre distintos segmentos de red?

4. ¿La arquitectura permite escalar en número de usuarios, servicios o sedes?
5. ¿Qué grado de centralización o descentralización presenta la red?
6. ¿Qué limitaciones arquitectónicas podrían afectar la integración de un NGFW?

- Identificación de la segmentación lógica y dominios de red

En esta fase se analiza la forma en que la red está segmentada lógicamente y cómo dicha segmentación puede ser controlada y reforzada mediante las capacidades de políticas y zonas de seguridad del Sophos Firewall.

Preguntas metodológicas:

1. ¿Qué criterios se utilizan para segmentar la red (usuarios, servicios, dispositivos, nivel de confianza)?
2. ¿Existen dominios que requieren aislamiento estricto que deba ser reforzado por políticas del firewall?
3. ¿Qué segmentos contienen información o servicios críticos?
4. ¿Existen flujos de tráfico innecesarios que Sophos Firewall debería restringir?
5. ¿La segmentación actual reduce efectivamente la superficie de ataque o requiere controles adicionales?
6. ¿Qué segmentos deberían ser considerados zonas de baja confianza dentro del firewall?
7. ¿La infraestructura permite aplicar políticas diferenciadas utilizando las capacidades de Sophos Firewall?
8. ¿Qué desafíos de control y visibilidad pueden abordarse mediante el uso del firewall?

- Evaluación de conectividad externa y exposición de la red

Este inciso se enfoca en identificar cómo la red se conecta con entornos externos y qué riesgos se derivan de dicha conectividad.

Preguntas metodológicas:

1. ¿Qué tipos de enlaces externos utiliza la red (Internet, VPN, MPLS, enlaces dedicados)?
2. ¿Existen enlaces redundantes que puedan ser gestionados por el firewall?
3. ¿Qué servicios o recursos internos están expuestos hacia redes externas?
4. ¿Cómo se gestiona el acceso a aplicaciones publicadas desde el punto de vista del firewall?
5. ¿Qué tipos de tráfico entrante y saliente predominan?
6. ¿Qué riesgos se asocian a la falta de inspección del tráfico externo?
7. ¿Cómo se controla el acceso desde ubicaciones remotas?
8. ¿Qué capacidades de control y monitoreo del Sophos Firewall son necesarias en el perímetro?

- Identificación de necesidades de seguridad previas a la integración del NGFW

En esta etapa se determinan las capacidades de seguridad requeridas antes de definir políticas o configuraciones específicas del firewall.

Preguntas metodológicas:

1. ¿Qué tipo de amenazas representan mayor riesgo para la organización?
2. ¿Se requiere control de aplicaciones basado en usuarios o roles soportado por Sophos Firewall?
3. ¿Es necesario implementar filtrado de contenido web mediante el firewall?
4. ¿Cómo se deben proteger los servicios críticos y aplicaciones expuestas?
5. ¿Qué mecanismos de detección y prevención de intrusiones son necesarios?
6. ¿Es necesario integrar Sophos Firewall con otros sistemas de seguridad?
7. ¿Qué requerimientos existen para el acceso remoto seguro?
8. ¿Cómo se debe garantizar la trazabilidad y visibilidad del tráfico desde el firewall?

La identificación de los elementos técnicos de la red y de los requerimientos previos para la integración del Sophos Firewall se realiza a partir de un escenario empresarial simulado, representativo de una red escalable.

5.6. Procedimiento para la validación técnica

5.6.1. Metodología para el diseño de políticas de seguridad

La formulación de políticas de seguridad en un firewall de nueva generación se aborda en este proyecto mediante una metodología técnica estructurada, orientada a traducir los requerimientos de seguridad de una red empresarial en políticas lógicas coherentes, consistentes y verificables, tomando como referencia las capacidades funcionales del Sophos Firewall.

Esta metodología no describe configuraciones específicas, sino que define cómo deben diseñarse las políticas, bajo qué criterios, con qué nivel de restricción y sobre qué activos, garantizando alineación con buenas prácticas de seguridad

El enfoque metodológico se fundamenta en cuatro pilares técnicos:

clasificación de activos, principio de mínimo privilegio, definición de perfiles de seguridad y control explícito del tráfico permitido.

- Clasificación de activos y definición del nivel de criticidad

Como primer paso metodológico, se establece la necesidad de clasificar los activos protegidos según su función y criticidad dentro de la infraestructura. Esta clasificación permite determinar el nivel de exposición aceptable y el grado de restricción que deben aplicar las políticas de seguridad.

Los activos se agrupan, de forma metodológica, en categorías tales como:

- Servidores expuestos (por ejemplo, servidores web),

- Servidores internos críticos,
- Usuarios finales
- Servicios de infraestructura
- Redes de acceso restringido.

Cada categoría se asocia a un nivel de criticidad (alto, medio o bajo), el cual condiciona directamente el tipo de tráfico permitido, el nivel de inspección requerido y las restricciones aplicables. Este enfoque permite que las políticas no sean uniformes, sino proporcionales al riesgo asociado a cada activo.

- Aplicación del principio de mínimo privilegio en el diseño de políticas

Una vez clasificados los activos, la metodología establece la aplicación sistemática del principio de mínimo privilegio como eje central del diseño de políticas. Bajo este principio, toda comunicación es considerada no permitida por defecto, y únicamente se habilitan aquellos flujos de tráfico que estén claramente justificados por una necesidad operativa.

En términos metodológicos, esto implica que:

- Las políticas se diseñan de forma explícita, evitando reglas permisivas generales;
- Cada permiso otorgado debe estar asociado a un servicio, usuario o función específica;
- Cualquier acceso no identificado o no requerido queda bloqueado.

Este enfoque reduce la superficie de ataque, limita el impacto de incidentes de seguridad y facilita la auditoría de las políticas definidas.

- Definición de perfiles de seguridad basados en riesgo

Para la definición de los controles de seguridad, se establece previamente el concepto de riesgo como la probabilidad de que una amenaza se materialice y el impacto que esta tendría sobre los activos de información, los servicios críticos y la operación del negocio. No obstante, la presente metodología adopta el principio de mínimo privilegio, bajo el cual todo acceso se considera potencialmente riesgoso y debe limitarse únicamente a lo estrictamente necesario para el cumplimiento de las funciones operativas.

Bajo este enfoque, el objetivo es mantener la menor exposición posible de los recursos de red, reduciendo la superficie de ataque mediante la habilitación controlada de servicios y aplicaciones. Para facilitar la administración de estos controles, las políticas de seguridad se organizan en grupos de usuarios o áreas operativas que requieren un nivel de exposición similar, permitiendo aplicar reglas de acceso coherentes y consistentes según las necesidades funcionales de cada área. Este modelo permite una gestión más eficiente de las políticas de seguridad, manteniendo un enfoque de control granular y alineado con las mejores prácticas de seguridad.

- Control de acceso interno mediante segmentación y políticas explícitas

La metodología establece que la segmentación lógica de la red debe ser reforzada mediante políticas de control de acceso explícitas entre dominios. En este contexto, la comunicación entre segmentos se permite únicamente cuando existe una relación funcional definida, evitando accesos transversales innecesarios.

Desde el punto de vista metodológico:

- Los segmentos críticos no deben iniciar ni aceptar comunicaciones sin justificación.
- Los accesos entre usuarios y servidores se restringen según perfil y función.
- El movimiento lateral entre segmentos se limita de forma deliberada.

Este enfoque fortalece la seguridad interna y complementa la protección perimetral, reduciendo el riesgo de propagación de amenazas.

- Regulación del acceso a Internet y control de tráfico saliente

La metodología contempla de forma específica la regulación del acceso a Internet, diferenciando claramente entre usuarios finales y servidores. En el caso de los servidores y servicios críticos, se adopta un modelo de acceso saliente restringido, en el cual solo se permiten conexiones externas estrictamente necesarias para su operación.

Para los usuarios, el acceso a Internet se regula mediante perfiles de filtrado de contenido y control de aplicaciones, alineados con su rol y nivel de riesgo. Este control metodológico permite:

- Reducir la exposición a amenazas externas.
- Limitar el uso de aplicaciones no autorizadas.
- Garantizar que el acceso a recursos externos no comprometa la seguridad de la red.

5.6.2. Análisis de la efectividad funcional de Sophos Firewall en entorno emulado.

El análisis de la efectividad funcional de un firewall de nueva generación en un entorno Enterprise requiere un escenario controlado que permita observar y validar el comportamiento de la solución frente a los requerimientos de seguridad definidos, sin introducir variables propias de una infraestructura productiva. La utilización de un entorno controlado posibilita centrar el análisis exclusivamente en la funcionalidad, el flujo de tráfico y la aplicación de políticas, evitando interferencias externas que puedan distorsionar los resultados.

En este proyecto, la metodología se apoya en un entorno emulado mediante la plataforma PNETLab, sobre el cual se implementa un escenario Enterprise escalable definido como caso de estudio lógico. Este entorno permite reproducir las condiciones necesarias para evaluar la integración y operación del firewall, asegurando que las pruebas realizadas se limiten a las capacidades requeridas de la solución, tales como control de acceso, segmentación, inspección de tráfico y protección perimetral, sin depender de una infraestructura productiva real ni afectar su operación.

Para la ejecución de las pruebas, se emplea Sophos Firewall con licencia trial, la cual habilita el conjunto completo de funcionalidades de la solución, permitiendo evaluar de forma integral los mecanismos de seguridad disponibles sin restricciones funcionales. Este enfoque garantiza que la evaluación realizada se centre en la efectividad funcional de la tecnología y no en limitaciones derivadas del licenciamiento.

La metodología no tiene como objetivo medir rendimiento absoluto ni capacidad máxima de procesamiento, sino analizar el comportamiento funcional del firewall, su capacidad para aplicar políticas de seguridad, inspeccionar tráfico y mantener la coherencia operativa dentro de un entorno Enterprise emulado.

A continuación, se presenta el diagrama de la topología de red de la casa matriz, el cual representa la arquitectura base del entorno empresarial considerado en el presente estudio. La topología ilustra la organización jerárquica de la red por capas, la segmentación lógica de los distintos dominios de usuarios y servicios, así como los elementos de conectividad hacia Internet.

Este diagrama sirve como referencia estructural para el análisis de los elementos técnicos de la red y la definición de los requerimientos necesarios para la integración de un firewall de nueva generación, permitiendo visualizar de manera clara la relación entre los componentes internos, los enlaces WAN y las zonas de seguridad contempladas.

- Definición del entorno emulado y escenario de prueba

El análisis de la efectividad funcional del Sophos Firewall se realiza sobre una topología de red Enterprise previamente definida, la cual constituye la base lógica del caso de estudio propuesto en el presente proyecto. Dicha topología representa una infraestructura empresarial escalable que contempla segmentación de red, servicios internos, acceso a redes externas y dominios con distintos niveles de confianza, y sobre la cual se proyecta la integración de un firewall de nueva generación como elemento central de seguridad.

Esta topología no corresponde a una red productiva real, sino a un modelo lógico representativo diseñado para cubrir las necesidades más comunes de conectividad, control de acceso y protección perimetral presentes en entornos Enterprise. A partir de este diseño lógico, se procede a su despliegue en un entorno emulado mediante la plataforma PNETLab, con el objetivo de validar el comportamiento funcional del firewall dentro de la arquitectura previamente planteada.

- Integración del firewall dentro de la topología existente

Desde el punto de vista metodológico, el Sophos Firewall no se introduce como un elemento aislado, sino como un componente integrado dentro de la topología Enterprise definida. Su ubicación y función dentro del entorno emulado responden al diseño previo de la red además de cubrir los requerimientos de la infraestructura, en el cual el firewall actúa como punto de control del tráfico perimetral y de las comunicaciones entre segmentos con diferentes niveles de confianza.

Este enfoque permite evaluar la efectividad funcional del firewall en el contexto realista de una red ya estructurada, observando su interacción con los distintos dominios de red y servicios contemplados en el diseño original.

- Materialización del diseño lógico en PNETLab

La implementación de la topología en PNETLab se realiza respetando la estructura lógica previamente definida, de manera que el entorno emulado reproduzca las relaciones funcionales entre los distintos componentes de la red. Esta materialización permite:

- Validar la integración del firewall dentro de la arquitectura propuesta,
- Aplicar políticas de seguridad sobre segmentos ya establecidos,
- Generar tráfico representativo entre los distintos dominios de red.

El uso de PNETLab facilita la recreación controlada de este escenario, permitiendo realizar ajustes y repetir pruebas sin alterar el diseño conceptual de la topología.

Condiciones metodológicas del entorno de prueba

Para asegurar la coherencia entre el diseño lógico y el entorno emulado, se establecen las siguientes condiciones:

- La topología implementada en PNETLab debe corresponder al diagrama de red definido como caso de estudio.
- El firewall debe operar con licencia trial, garantizando la disponibilidad de todas las funcionalidades requeridas para la evaluación.
- El entorno debe permitir la observación del comportamiento del firewall ante tráfico legítimo y no autorizado, de acuerdo con las políticas definidas.

Estas condiciones aseguran que la evaluación se centre en la efectividad funcional del Sophos Firewall dentro de la arquitectura propuesta.

Es importante destacar que el entorno Enterprise definido como caso de estudio no pretende replicar de forma exacta una infraestructura productiva real, sino representar de manera lógica las necesidades de conectividad, segmentación y seguridad más comunes en organizaciones empresariales. En consecuencia, los resultados obtenidos se interpretan dentro del alcance del entorno emulado, sirviendo como base

para analizar la efectividad funcional del Sophos Firewall y no como indicadores de rendimiento absoluto en producción.

5.6.3. Criterios de Evaluación

La evaluación se basa en la observación sistemática del comportamiento del Sophos Firewall frente a los requerimientos de seguridad identificados en el entorno Enterprise emulado.

Criterios fundamentales:

- Aplicación adecuada de políticas de seguridad: Se evalúa que el firewall permita o restrinja el tráfico conforme a las reglas establecidas para cada dominio de red (usuarios, servidores internos, DMZ, redes restringidas).
- Aislamiento efectivo entre segmentos: Se verifica que la segmentación lógica se mantenga en la práctica, sin comunicaciones laterales no autorizadas entre redes internas, reduciendo el riesgo de propagación de incidentes.
- Protección de servicios expuestos: Se observa que solo los servicios previamente definidos sean accesibles desde el exterior y que las comunicaciones entre servidores expuestos e internos respondan a los criterios de seguridad.
- Gestión coherente del tráfico de enlaces externos: Se verifica la aplicación consistente de políticas sobre comunicaciones que ingresan o salen de la infraestructura.
- Control de acceso a Internet: Se evalúa el comportamiento del firewall frente a políticas de filtrado web y control de aplicaciones, aplicando restricciones diferenciadas por perfil.

Determinación de efectividad: Se considera satisfactorio cuando el firewall aplica correctamente los controles, mantiene el aislamiento entre dominios y gestiona el tráfico coherentemente, sin impactos operativos no deseados.

5.6.4. Interpretación de los resultados dentro del entorno emulado

Los resultados se analizan de forma cualitativa y técnica, contrastando el comportamiento observado con el esperado según las políticas y criterios definidos.

Elementos clave de interpretación:

- Consistencia en la aplicación de políticas
- Preservación del aislamiento lógico entre dominios de red
- Gestión adecuada del flujo de tráfico

Los resultados se valoran según la alineación con los objetivos funcionales del proyecto, sin extrapolar a métricas de rendimiento absoluto ni a condiciones de infraestructuras productivas reales.

Los resultados constituyen un insumo analítico para valorar la pertinencia de la solución NGFW en un entorno Enterprise escalable. La interpretación se mantiene estrictamente dentro del marco del entorno emulado, garantizando coherencia metodológica y delimitando claramente el alcance del análisis.

5.7. Procedimiento para el dimensionamiento del Firewall

Para la selección del modelo de Sophos Firewall en el escenario Enterprise definido, se toman como referencia los parámetros de dimensionamiento establecidos por el fabricante, los cuales permiten estimar técnicamente el equipo más adecuado según las características del entorno analizado. Estos parámetros se utilizan como insumo metodológico para alinear el modelo de firewall con las necesidades operativas y de

seguridad del escenario propuesto. El dimensionamiento considera variables relacionadas con el uso del enlace WAN, entre las que se incluyen:

- Ancho de banda WAN total, correspondiente a la capacidad contratada para la salida y entrada de tráfico hacia Internet.
- Consumo promedio de ancho de banda, representativo del uso habitual del enlace en condiciones normales de operación.
- Crecimiento anticipado del tráfico WAN, proyectado a un horizonte de tres años, con el fin de contemplar la escalabilidad del entorno.
- Crecimiento esperado en picos de tráfico, considerando incrementos temporales de demanda.
- Crecimiento promedio estimado, utilizado para evaluar la evolución progresiva del consumo de ancho de banda.

Estos valores permiten estimar el volumen de tráfico que el firewall debe procesar dentro del escenario modelado, considerando tanto condiciones normales como escenarios de mayor demanda.

5.7.1. Parámetros de protección WAN y funcionalidades de seguridad

El proceso de selección del modelo incorpora la habilitación de mecanismos avanzados de seguridad, los cuales influyen directamente en el dimensionamiento del equipo. Dentro del alcance del caso de estudio, se consideran funcionalidades tales como:

- Protección contra amenazas (IPS, control de aplicaciones y antimalware);
- Inspección y control del tráfico web;
- Descifrado SSL/TLS para inspección de tráfico cifrado;
- Funcionalidades avanzadas de protección incluidas en Xstream Protection;
- Protección de aplicaciones web mediante Web Application Firewall (WAF).

La activación de estos servicios incrementa la carga de procesamiento del firewall, por lo que su inclusión es un factor determinante en la estimación del modelo adecuado para el escenario Enterprise planteado.

5.7.2. Parámetros de conectividad VPN

Asimismo, el dimensionamiento contempla los requerimientos de conectividad segura mediante redes privadas virtuales, considerando:

- Número de túneles IPsec concurrentes.
- Número de conexiones simultáneas de SSL VPN.
- Requerimientos de throughput para tráfico IPsec en condiciones de mayor demanda.

Estos parámetros permiten estimar la capacidad del firewall para soportar comunicaciones seguras entre sitios, usuarios remotos o entornos híbridos, de acuerdo con el diseño del escenario de estudio.

5.7.3. Parámetros de autenticación y usuarios

Finalmente, se considera la cantidad estimada de usuarios, la cual influye en el número de sesiones concurrentes, procesos de autenticación y aplicación de políticas de seguridad. Este valor es relevante para dimensionar el firewall de forma coherente con el tamaño del entorno Enterprise representado en el caso de estudio.

5.7.4. Integración de los parámetros en la selección del modelo

La combinación de los parámetros de throughput, funcionalidades de seguridad, conectividad VPN y cantidad de usuarios permite estimar el modelo de Sophos Firewall más adecuado para el escenario analizado. Este proceso se apoya en la herramienta oficial de dimensionamiento de Sophos (Firewall Sizing Calculator), la cual

correlaciona dichas variables con los modelos disponibles de la serie XGS, proporcionando una referencia técnica para la selección del equipo dentro del contexto de propuestas reales y procesos de cotización alineados a las necesidades del entorno analizado.

5.8. Procedimiento para el análisis de viabilidad económica

El análisis se desarrolló con el objetivo de establecer las condiciones bajo las cuales la inversión en seguridad resultaría justificable dentro del entorno Enterprise definido. Este análisis se enfoca en la relación entre el costo de la solución y la reducción del riesgo asociado a los escenarios identificados.

Dado que el escenario de estudio corresponde a un entorno emulado y no cuenta con registros históricos de incidentes ni con datos económicos reales, el análisis evita la estimación directa de impactos monetarios absolutos. En su lugar, se adopta un enfoque condicional, utilizando estándares de la industria para estimar pérdidas potenciales.

La metodología parte de una cotización real de la solución NGFW utilizada para determinar el costo anual de la inversión. A partir de este costo, se identifican las condiciones de reducción de riesgo que la solución debe cumplir para que el valor de la mitigación sea equivalente o superior al costo de la inversión, conforme al marco ROSI definido en el capítulo 4.

5.8.1. Fuente de datos para el cálculo

Para la determinación de los costos de la solución, se utilizó una cotización formal de referencia correspondiente al modelo Sophos Firewall XGS 2100**,** cuyos valores se presentan en el Anexo B. La fuente específica que generó la cotización no se menciona en el presente documento con el fin de evitar la divulgación de información comercial sensible.

Para la estimación de las pérdidas (ALE), y considerando que el entorno evaluado corresponde a un laboratorio emulado sin históricos reales de incidentes, se utilizaron referencias y estimaciones basadas en estándares de la industria (IBM Security, 2024), ajustadas al contexto de una infraestructura empresarial.

5.8.2. Criterios de viabilidad económica

En ausencia de datos históricos reales, el ROSI se emplea como herramienta analítica que, en este estudio emulado, permite estimar condiciones de viabilidad mediante valores proyectados fundamentados en estándares de la industria. Bajo este enfoque, la inversión en seguridad se considera económicamente justificable cuando la reducción del riesgo atribuible a la solución NGFW es suficiente para compensar el costo anual de la inversión.

Este marco permite evaluar la propuesta en función de variables estructurales del entorno, como la cantidad de usuarios, la criticidad de los servicios, la superficie de ataque y la concentración de controles de seguridad en una única plataforma.

5.8.3. Definición de impactos económicos

Para el análisis de viabilidad económica bajo el enfoque ROSI, se seleccionaron impactos económicos potenciales asociados a incidentes de seguridad que podrían materializarse en el entorno Enterprise definido como caso estimado, utilizados como referencia para evaluar el valor de la mitigación que puede aportar la solución NGFW.

Bajo este criterio metodológico, se determinó estimar los impactos económicos basándose en cuatro categorías principales derivadas de la topología de red propuesta de estudio. Estos impactos no se interpretan como pérdidas reales ocurridas, sino como escenarios de impacto Indisponibilidad operativa: Costos asociados a la interrupción de servicios críticos (ej. servidores AD, DNS) y pérdida de productividad por horas de inactividad.

- Compromiso de información: Costos estimados por filtración de datos sensibles, incluyendo notificación a clientes y asesoría legal.
- Interrupción de servicios web: Impacto por la indisponibilidad del portal público y pérdida de confianza del cliente.
- Esfuerzos de recuperación: Costos técnicos asociados a la investigación forense, reconfiguración de políticas y capacitación de refuerzo tras un incidente.

Dado que el proyecto no dispone de datos históricos ni de métricas financieras reales, estos impactos no se cuantifican como pérdidas absolutas en esta etapa metodológica, sino como rangos de impacto económico potencial definidos a partir de variables observables del entorno (cantidad de usuarios, criticidad de los servicios). Este enfoque permite construir escenarios conservadores y razonables para su posterior cálculo en el capítulo de Resultados.

➢ Condición de viabilidad económica bajo el enfoque ROSI

Dado que el objetivo del proyecto no es obtener un valor numérico de ROSI, sino establecer condiciones de viabilidad, la ecuación se reinterpreta de forma condicional, considerando que la inversión resulta económicamente justificable cuando el valor de las pérdidas mitigadas es igual o superior al costo anual de la solución.

Esta condición expresa que la reducción del impacto económico potencial atribuible a la solución NGFW debe ser, al menos, equivalente al costo anual de la inversión en seguridad.

En el presente estudio, los términos de las ecuaciones anteriores no se utilizan para calcular pérdidas reales ni retornos financieros exactos, sino para estructurar el análisis económico y definir los umbrales bajo los cuales la solución NGFW sería viable dentro de un entorno Enterprise emulado. La evaluación se basa en escenarios de impacto económico potencial y en la capacidad funcional del NGFW para reducir

dichos impactos, manteniendo coherencia con el alcance metodológico y las limitaciones del proyecto.

5.8.4. Criterios de estimación de riesgos

La frecuencia de incidentes (ARO) y el impacto (SLE) se estimaron mediante un enfoque conservador, considerando la superficie de ataque expuesta en la topología definida (servicios web en DMZ, tráfico cifrado sin inspección). No se calcularon pérdidas absolutas reales, sino escenarios de impacto potencial para validar la condición de viabilidad.

5.8.5. Alcances y limitaciones del análisis

El análisis de viabilidad económica desarrollado bajo el enfoque ROSI se encuentra delimitado por el alcance metodológico del proyecto y por las características del entorno definido como caso de estudio. En este sentido, el análisis se orienta a establecer condiciones de viabilidad económica, y no a calcular retornos financieros exactos ni a estimar pérdidas reales asociadas a incidentes de seguridad ocurridos en producción.

Como alcance principal, el análisis permite relacionar el costo anual de la solución NGFW con los impactos económicos potenciales derivados de incidentes de seguridad relevantes para un entorno Enterprise, considerando variables estructurales como la cantidad de usuarios, la criticidad de los servicios y la exposición de la infraestructura. Asimismo, el enfoque adoptado permite evaluar la pertinencia económica de la solución a partir de la reducción del riesgo esperada, sin recurrir a supuestos financieros no verificables.

Dado que el proyecto se valida en un entorno emulado (PNETLab), los resultados económicos representan una proyección teórica de viabilidad y no un retorno

financiero contabilizado. Los beneficios intangibles (reputación, confianza) se consideran cualitativamente.

Entre las limitaciones del análisis, se reconoce que la evaluación se realiza sobre un entorno emulado, por lo que no se dispone de registros históricos de incidentes, métricas reales de pérdidas económicas ni datos estadísticos propios de una infraestructura productiva. En consecuencia, los impactos económicos considerados se expresan como escenarios de referencia y rangos estimados, y no como valores absolutos o resultados financieros medibles.

Adicionalmente, el análisis no contempla variaciones específicas asociadas a normativas regulatorias particulares, contratos comerciales o políticas internas propias de una organización real, las cuales podrían influir en la magnitud del impacto económico ante ciertos tipos de incidentes. Tampoco se incluyen costos indirectos difíciles de cuantificar, como efectos a largo plazo sobre la reputación o la confianza de los clientes.

En este contexto, los resultados del análisis deben interpretarse como un marco de evaluación aplicable a entornos Enterprise con características similares al escenario de estudio, y no como una proyección financiera universal. Las conclusiones obtenidas permiten valorar la viabilidad económica de la solución NGFW desde una perspectiva metodológica y condicional, sirviendo como base para la toma de decisiones informadas, pero requiriendo un análisis específico y contextualizado para su aplicación en entornos productivos reales.

VI. DESARROLLO

El análisis de la arquitectura general de la red es un paso crucial para entender la estructura funcional actual antes de integrar un firewall de nueva generación (NGFW). La topología actual se basa en segmentación lógica, enrutamiento centralizado y diferenciación de dominios de confianza. Se concluye que, aunque la segmentación actual es funcional en términos de conectividad, necesita mecanismos de control más granulares para regular la interacción entre dominios y proteger mejor los servicios en la DMZ.

Tipo de arquitectura

Se implementó una arquitectura jerárquica por capas con núcleo colapsado (core/distribución). El núcleo absorbe las funciones de distribución para simplificar la administración. La distribución funcional es:

- Núcleo (Core): Dos equipos que actúan como gateway principal, centralizan el enrutamiento inter-VLAN y gestionan la salida a Internet.
- Distribución: Funciones absorbidas por el núcleo.
- Acceso: Switches de Capa 2 para conectividad de usuarios y dispositivos finales.

Flujos de tráfico y puntos únicos de falla

Los flujos principales se centralizan en el núcleo de la casa matriz. Existen puntos únicos de falla críticos: el Core centralizado (su fallo interrumpe toda la operación) y los servicios esenciales centralizados (DNS en un solo servidor Windows).

Gestión del enrutamiento interno

El enrutamiento interno es gestionado por el core mediante enrutamiento inter-VLAN en capa 3, sin seguridad granular, lo que justifica integrar un firewall.

Grado de centralización

La red presenta un modelo predominantemente centralizado. La sucursal 02 envía todo su tráfico (incluido Internet) vía MPLS a la casa matriz. La sucursal 01 es parcialmente descentralizada, con salida local a Internet y VPN solo para tráfico corporativo.

Limitaciones arquitectónicas para integrar un NGFW

- Centralización del Gateway en el core: Integrar un NGFW obliga a redefinir el tránsito del tráfico.
- Exposición de servicios en la DMZ: Requiere políticas estrictas por ser un dominio de alto riesgo.
- Dependencia de servicios críticos internos: El DNS centralizado debe preservar su acceso controlado.
- Segmentación lógica y dominios de red

La segmentación actual usa VLANs y subredes IP con enrutamiento capa 3 en el core, sin políticas avanzadas por nivel de riesgo. Se requiere reforzar el aislamiento de múltiples flujos innecesarios (comunicación lateral entre departamentos, acceso excesivo a servidores, tráfico no regulado de sucursales, conexiones desde DMZ, riesgos en móviles e invitados, y tráfico de videovigilancia).

Control actual entre segmentos

El control se realiza exclusivamente mediante el Core, que realiza enrutamiento inter-VLAN sin inspección, sin control por aplicaciones ni por usuario.

Segmentación y superficie de ataque

La segmentación actual proporciona separación lógica pero no reduce efectivamente la superficie de ataque, ya que carece de controles avanzados, permitiendo movimiento lateral ante incidentes.

Zonas de baja confianza

Bajo el principio de desconfianza implícita, se consideran de baja confianza: WAN, DMZ, WIFI (invitados), MOVILES y VPN. Incluso las zonas LAN, SERVIDORES y MGMT no gozan de confianza absoluta.

Políticas diferenciadas con Sophos Firewall

Sí, pero requiere que el firewall actúe como gateway en zonas críticas (DMZ y servidores) y reciba todas las conexiones externas (WAN, MPLS, VPN) en lugar del Core.

Desafíos de control y visibilidad resueltos por el firewall

Sophos Firewall permite: inspeccionar tráfico cifrado SSL/TLS, aplicar mínimo privilegio entre zonas, incorporar IPS y control de aplicaciones por capa 7, integrarse con Active Directory para políticas por identidad, y centralizar la inspección del tráfico de sucursales desde VPN y MPLS.

6.1.1. Evaluación de conectividad externa y exposición de la red

La evaluación de la conectividad externa analiza cómo la infraestructura interactúa con entornos fuera de su dominio, identificando recursos expuestos, tráfico cifrado predominante y visibilidad sobre comunicaciones VPN y MPLS. Esto permite definir la superficie de ataque y justificar la integración de Sophos Firewall para implementar publicación segura, inspección SSL/TLS y protección de aplicaciones web.

¿Qué servicios o recursos internos están expuestos hacia redes externas?

El único recurso interno expuesto es el servidor en la DMZ (IP 10.0.21.4/28), que aloja dos servicios: página web institucional y portal de autenticación para clientes. Solo se permite acceso a través del puerto 80 (HTTP). No se exponen servicios críticos como AD o DNS, y el servidor DMZ no debe permitir conexiones entrantes distintas a las necesarias.

¿Cómo se gestiona el acceso a aplicaciones publicadas desde el punto de vista del firewall?

El acceso se gestiona con el módulo Web Application Firewall (WAF) en modo Reverse Proxy, actuando el firewall como intermediario entre el cliente externo y el servidor interno. La conexión HTTPS se establece contra el firewall, valida, inspecciona y filtra la solicitud, reenviando solo el tráfico legítimo al servidor en la DMZ. La dirección IP interna no se expone directamente a Internet.

6.1.2. Identificación de necesidades de seguridad previas a la integración del NGFW

Antes de configurar el firewall, es imperativo traducir los riesgos detectados en requerimientos técnicos que el NGFW debe cubrir. En este escenario, factores como la exposición de servicios web, el predominio de tráfico cifrado y la segmentación sin controles granulares obligan a definir capacidades mínimas de protección e inspección.

Se desarrollan las siguientes preguntas que han sido extraídas y adaptadas de la metodología:

¿Qué tipo de amenazas representan mayor riesgo para la organización?

Ataques a aplicaciones web (SQL injection, fuerza bruta), malware en tráfico cifrado HTTPS sin inspección, ransomware y movimiento lateral hacia AD/DNS, y exfiltración de datos mediante conexiones cifradas.

¿Se requiere control de aplicaciones basado en usuarios o roles?

Sí. La segmentación por VLAN e IP es insuficiente. La integración con Active Directory permitirá controles por departamento, restringir aplicaciones no productivas e identificar servicios en puerto 443 para evitar que aplicaciones no autorizadas se oculten en HTTPS.

¿Es necesario implementar filtrado de contenido web?

Sí. Es indispensable para gestionar la navegación HTTPS saliente, bloqueando sitios de phishing, malware y categorías no operativas, fortaleciendo la productividad y mitigando riesgos.

¿Qué nivel de inspección del tráfico cifrado es requerido?

Inspección profunda con descifrado controlado (SSL/TLS Decryption) mediante proxy. Para la DMZ, terminación SSL en el módulo WAF. En servidores críticos (AD/DNS): mínimo privilegio. En aplicaciones DMZ: publicación con WAF en modo Reverse Proxy para proteger contra SQLi y XSS.

¿Qué mecanismos de detección y prevención de intrusiones son necesarios?

IPS para detectar ataques y escaneos en tiempo real, WAF para bloquear ataques a aplicaciones web, y reputación de amenazas para identificar dominios maliciosos, botnets y servidores C2.

¿Qué requerimientos existen para el acceso remoto seguro?

VPN cifradas (IPsec o SSL), autenticación fuerte con AD y MFA, y segmentación para que cada usuario acceda solo a sus recursos bajo monitoreo continuo con IPS.

¿Qué limitaciones actuales mitiga Sophos Firewall?

Mitiga la falta de visibilidad (inspección de tráfico cifrado HTTPS), la ausencia de control granular (políticas de mínimo privilegio e inspección capa 7), y la debilidad en gobernanza (monitoreo centralizado, trazabilidad de usuarios y gestión de enlaces WAN).

6.2. Formulación de políticas de seguridad orientada a Sophos Firewall

La formulación de políticas de seguridad en este proyecto parte de la infraestructura y segmentación lógica de la red, organizada en múltiples VLAN que incluyen DMZ, servidores internos, usuarios, móviles, invitados y videovigilancia. Actualmente, el

enrutamiento InterVLAN permite la comunicación entre segmentos, pero sin controles de seguridad avanzados, lo que genera tráfico sin restricciones suficientes entre dominios de distinta confianza. Por ello, las políticas se orientan a regular explícitamente la interacción entre segmentos, integrando el firewall como punto central de control. Esto requiere identificar los activos críticos y establecer su nivel de criticidad para priorizar la protección de los recursos más sensibles.

6.2.1. Clasificación de activos y definición del nivel de criticidad.

La clasificación de activos se realiza según su función en la arquitectura: servidores expuestos (DMZ), servidores internos críticos, usuarios finales, servicios de infraestructura y redes de acceso restringido. Se aplican criterios de nivel de exposición, relevancia operativa y nivel de confianza. Los servidores expuestos en la DMZ tienen alta exposición a Internet. Los servidores internos críticos almacenan recursos clave para los usuarios. Los servicios de infraestructura (enrutamiento y conectividad) también tienen criticidad alta. En cambio, los usuarios finales y las redes de acceso restringido (invitados, dispositivos específicos) representan menor nivel de confianza. Esta diferenciación permite priorizar la protección de los recursos más sensibles.

6.2.2. Aplicación del principio de mínimo privilegio en el diseño de políticas

Por Una vez clasificados los activos, se aplicó el principio de mínimo privilegio como criterio fundamental para el diseño de políticas de seguridad. Bajo este enfoque, la comunicación entre segmentos se restringe por defecto, permitiendo solo los flujos necesarios para el funcionamiento de los servicios. El diseño controla explícitamente la comunicación entre dominios, evitando configuraciones permisivas. Por ejemplo, el acceso desde usuarios finales a servidores internos se limita a servicios operativos esenciales, y el tráfico externo solo a los servicios publicados en la DMZ. Este principio

se eligió porque reduce la superficie de ataque y limita el movimiento lateral ante un posible compromiso.

6.2.3. Definición de perfiles de seguridad basados en riesgo

A partir de la clasificación de activos y la segmentación lógica, se establecen perfiles de seguridad según el nivel de riesgo de cada dominio de red. Los segmentos (servidores internos, DMZ, usuarios corporativos, móviles, invitados, videovigilancia) se agrupan en zonas gestionadas por el firewall: WAN, DMZ, servidores, LAN, VPN, móviles, wifi y MGMT.

Alto riesgo: servidores (recursos críticos) y zona de management (administración de infraestructura). Requieren políticas restrictivas, inspección profunda y controles estrictos.

- Riesgo medio: zona LAN (usuarios corporativos) y zona VPN (conexiones de otras sedes).
- Bajo riesgo: zonas móviles y wifi (dispositivos móviles e invitados), con menor confianza y acceso limitado.
- DMZ: perfil específico para exposición controlada de servicios desde la WAN hacia Internet, limitando la interacción con segmentos internos.

6.2.4. Definición de controles de seguridad y aplicación de políticas del firewall

Con base en la criticidad de los activos y el riesgo de cada zona, se definen los siguientes controles de seguridad:

- El tráfico desde la zona WAN se restringe exclusivamente a los servicios publicados en la DMZ (servidores web accesibles desde Internet).

- El acceso a la zona de servidores (recursos corporativos y servicios críticos) se limita a conexiones desde la zona LAN o desde accesos remotos autorizados vía zona VPN.
- Las zonas móviles y wifi (dispositivos móviles e invitados) tienen acceso restringido a recursos internos, permitiendo solo comunicaciones específicas o acceso controlado a servicios externos.

Además de las restricciones de comunicación entre zonas, el firewall aplica mecanismos de inspección y control como: filtrado de contenido web, control de aplicaciones, inspección de tráfico cifrado, y detección y prevención de intrusiones.

6.3. Análisis de la efectividad funcional de Sophos Firewall en entorno emulado

Esta sección se centra en las configuraciones y validaciones del Sophos Firewall en un entorno PNETLab, operando como gateway principal entre la red interna, la DMZ y el enlace externo. La casa matriz tiene una arquitectura jerárquica por capas con dos enlaces WAN (ENATREL principal, CLARO respaldo). La segmentación incluye VLAN para TI, contabilidad, RRHH, gerencia, ventas, operaciones, servidores, móviles, invitados y MGMT, con un servidor Windows (DNS) y una DMZ con servidores web.

Las sucursales comparten arquitectura interna, pero difieren en conectividad: Sucursal 01 tiene Internet local y VPN IPsec (solo tráfico corporativo); Sucursal 02 se conecta vía MPLS (todo el tráfico hacia casa matriz).

La segmentación asigna una red independiente por área con bloques CIDR (/28 usuarios, /26 móviles). El Gateway está en el core, gestionando el enrutamiento inter-VLAN con funciones de capa 3 tradicionales (sin inspección avanzada). Por ello, la integración del firewall requiere reubicar el punto de control sin alterar el direccionamiento existente. La tabla 20 (Anexo C) es la base técnica para migrar el gateway.

Elemento	Función / Servicio	Dirección IP	Ubicación Lógica	Propósito / Criticidad
Servidor de Infraestructura	Active Directory / DNS	10.0.20.5/27	Segmento servidores internos	Alta: Centraliza autenticación y resolución interna.
Servidores Web	Publicación de servicios web	10.0.21.4/28	Zona Desmilitarizada (DMZ)	Exposición controlada y aislamiento de la red interna.

Tabla 1: Distribución lógica de servicios y activos dentro de la infraestructura de red, elaboración propia.

Definición de flujos y puertos requeridos para activos críticos

Con base en la identificación de los activos definidos en la infraestructura, se establecen los flujos de comunicación estrictamente necesarios para garantizar la operación del entorno, limitando la exposición de servicios únicamente a los puertos indispensable

Comunicación entrante hacia el servidor Windows (AD + DNS): IP: 10.0.20.5/27

Los usuarios internos deben poder autenticarse en el dominio y resolver nombres mediante el servicio DNS. Para ello, se requiere habilitar los siguientes puertos desde los segmentos autorizados hacia el servidor:

Origen	Destino	Servicio	Puerto / Protocolo	Dirección
Segmentos Internos Autorizados	Servidor AD/DNS (10.0.20.5/27)	DNS	TCP/UDP 53	Entrante
Segmentos Internos Autorizados	Servidor AD/DNS (10.0.20.5/27)	Kerberos	TCP/UDP 88	Entrante
Segmentos Internos Autorizados	Servidor AD/DNS (10.0.20.5/27)	LDAP(S)	TCP/UDP 389, TCP 636	Entrante
Segmentos Internos Autorizados	Servidor AD/DNS (10.0.20.5/27)	RPC Mapper	TCP 135	Entrante
Segmentos Internos Autorizados	Servidor AD/DNS (10.0.20.5/27)	SMB	TCP 445	Entrante
Segmentos Internos Autorizados	Servidor AD/DNS (10.0.20.5/27)	RPC Dinámico	TCP 49152–65535	Entrante
Redes Externas Autorizadas	Servidor Web DMZ (10.0.21.4/28)	HTTP	TCP 80	Entrante
Segmento Usuarios IT	Servidor Web DMZ (10.0.21.4/28)	RDP	TCP 3389	Entrante
Servidor Web DMZ (10.0.21.4/28)	Servidor AD/DNS (10.0.20.5/27)	AD Services	Puertos AD/DNS detallados arriba*	**Saliente**

Tabla 2: Distribución de flujos y puertos para activos críticos, elaboración propia.

Estos puertos deberán permitirse únicamente desde los segmentos internos autorizados. No se permitirá comunicación desde la DMZ hacia otros segmentos internos fuera de este alcance específico.

6.3.1. Control de navegación y autenticación para segmentos de usuarios

Los segmentos de usuarios serán controlados centralizadamente por el Sophos Firewall como gateway principal, permitiendo autenticación obligatoria contra Active Directory, trazabilidad, políticas diferenciadas y control granular mediante un modelo de inspección proxy (filtrado web, control de aplicaciones y registro detallado).

Sucursal 01 (Internet local): su tráfico de navegación no es inspeccionado por el firewall central; solo el acceso a recursos internos atraviesa la VPN. No se recomienda redirigir todo el tráfico sin análisis previo por consumo de ancho de banda y dependencia operativa.

Sucursal 02 (MPLS centralizado): todo su tráfico (incluido Internet) atraviesa el firewall central, permitiendo autenticación, inspección proxy y aplicación uniforme de políticas.

Segmentación basada en identidad: los perfiles se aplican según el grupo de Active Directory (Ventas, Operaciones, etc.), no por la red de origen, manteniendo las mismas políticas independientemente de la ubicación física del usuario

6.3.2. Consideraciones sobre el control intersegmento y el rol del firewall como gateway

Para aplicar políticas de bloqueo y control entre segmentos de usuarios, el firewall debe estar en el camino del tráfico, operando como gateway de las redes que se desea controlar. En el esquema actual, el core realiza el enrutamiento inter-VLAN sin inspección avanzada, lo que impide controles granulares.

Decisión arquitectónica: en entornos de gran escala se recomienda un firewall de segmentación interna independiente del perimetral. Sin embargo, el entorno de este estudio es de escala reducida (pocos usuarios, tráfico moderado), por lo que resulta viable que el Sophos Firewall perimetral asuma también el rol de gateway de los segmentos de usuarios, centralizando el control norte a sur (perimetral) y este a oeste

(intersegmento). Esto responde a criterios de eficiencia en costos, simplificación del diseño, capacidad suficiente y escala limitada.

6.3.2.1. Implementación de acceso remoto mediante SSL VPN

Se implementará como mecanismo de acceso remoto seguro con autenticación integrada contra Active Directory, asignación de IP virtual desde un segmento definido para VPN, restricción a recursos internos específicos y registro de eventos. El acceso se produce exclusivamente a través del túnel SSL autenticado, sin exponer el servidor AD directamente a Internet.

- Sistema de Prevención de Intrusiones (IPS)

El módulo IPS se habilita en las reglas que gestionan:

- Tráfico de usuarios autenticados hacia Internet
- Tráfico entrante hacia servidores en la DMZ
- Comunicación proveniente de conexiones SSL VPN
- Flujos intersegmento que atraviesen el firewall

El IPS opera mediante firmas actualizadas y detección basada en patrones conocidos, identificando escaneo de puertos, intentos de explotación de servicios vulnerables, ataques a aplicaciones web, tráfico malformado o sospechoso, e intentos de ejecución remota.

Dado que el firewall está configurado como gateway de los segmentos de usuarios, todo el tráfico interzonal (norte-sur y este-oeste) atraviesa el dispositivo, permitiendo al IPS inspeccionar ambos flujos.

- Implementación de políticas de Web Application Firewall (WAF) para publicaciones HTTPS

Se incorpora la protección de aplicaciones web mediante el Web Application Firewall (WAF) para los servidores publicados en la DMZ, mitigando amenazas como SQL Injection, XSS, CSRF, exploración de rutas y manipulación de parámetros HTTP.

Controles implementados: detección de inyecciones SQL, análisis de scripts embebidos (XSS), restricción de métodos HTTP, URL Hardening, Form Hardening y Cookie Signing (detección de modificaciones en cookies de sesión).

Consideración técnica: la correcta implementación en entornos productivos requiere un conocimiento detallado del comportamiento del aplicativo (métodos HTTP, rutas, parámetros, autenticación), ya que la activación indiscriminada puede generar falsos positivos o afectar el servicio.

En el contexto del laboratorio (entorno emulado con servidores web de estructura básica sin lógica transaccional compleja), los mecanismos configurados resultan adecuados para validar el funcionamiento del módulo WAF de Sophos Firewall, demostrando su capacidad para reforzar la seguridad de servicios web expuestos.

6.3.3. Desarrollo del entorno de pruebas en PNETLab

En esta sección se desarrolla el entorno de laboratorio utilizado para evaluar el Sophos Firewall como solución de firewall de nueva generación dentro de una arquitectura de red empresarial. El objetivo de esta fase consiste en implementar el diseño de red definido previamente, con el fin de realizar pruebas controladas sobre los mecanismos de seguridad del firewall.

Para la construcción del laboratorio se utiliza la plataforma de virtualización PNETLab, la cual permite emular infraestructuras de red mediante dispositivos virtuales como routers, switches y servidores. Este entorno facilita la reproducción de escenarios

empresariales dentro de un ambiente controlado, permitiendo validar configuraciones de red y mecanismos de seguridad sin afectar infraestructuras reales.

Aunque la topología incluye distintos componentes de red, el enfoque principal del desarrollo se centra en la integración, configuración y validación funcional del Sophos Firewall, evaluando su capacidad para gestionar el tráfico entre diferentes segmentos de red y aplicar mecanismos de seguridad como inspección profunda de paquetes, control de aplicaciones y filtrado de tráfico.

Dentro de esta arquitectura, el firewall se integra como el gateway principal, reemplazando al dispositivo de core como puerta de enlace de las redes internas. Esta decisión se adopta con el objetivo de centralizar el control del tráfico en el Sophos Firewall y demostrar sus capacidades de control y bloqueo de comunicaciones tanto a nivel interzona como entre distintos segmentos de usuarios.

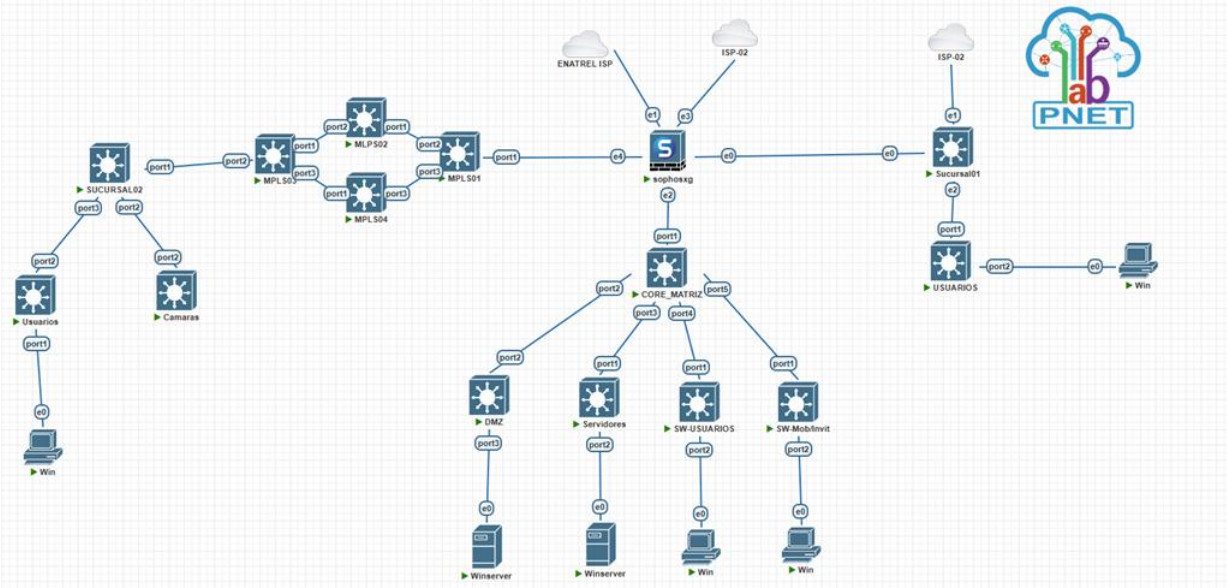


Figura 8: Diagrama de Red PNETLab, elaboración propia.

Como resultado del análisis arquitectónico, se propone eliminar la dependencia del Core como puerta de enlace principal y asignar dicha función al Sophos Firewall, constituyéndolo como el gateway central de la infraestructura. Bajo este esquema, el firewall gestiona y controla todas las comunicaciones que entran o salen de cada

segmento, permitiendo aplicar políticas de seguridad, inspección profunda de tráfico y control de acceso entre zonas.

El despliegue del firewall se realiza en PNETLab utilizando la imagen virtual SFOS 21.5.1 MR-1 Build 261 en formato qcow2. Se crea el nodo correspondiente dentro de la topología del laboratorio, permitiendo su interconexión con los demás dispositivos emulados.

Los recursos asignados para el laboratorio son: 10 núcleos de CPU, 8192 MB de RAM, 8 interfaces de red, disco primario de 16 GB y disco auxiliar de 80 GB. Esta asignación no corresponde a un dimensionamiento definitivo, sino a una configuración suficiente para garantizar la operatividad durante las pruebas. El dimensionamiento adecuado será abordado posteriormente en una sección dedicada a la evaluación de capacidad y requerimientos técnicos.



Figura 9: Recursos SFOS, elaboración propia.

En esta etapa se realizan las configuraciones iniciales del equipo perimetral con el objetivo de que el Sophos Firewall asuma la función de gateway principal de la red. Con base en la tabla de segmentación definida previamente (Tabla 1 – VLSM), se procede a configurar en el firewall la dirección IP que anteriormente estaba asignada al Core. Para evitar conflictos o duplicidad de direcciones IP dentro de la red, dicha dirección es eliminada previamente de la interfaz correspondiente del Core antes de ser configurada en el Sophos Firewall. Se asigna de la siguiente forma en Sophos Firewall:



DMZ DMZ VLAN	N/A N/A	10.0.21.1/255.255.255.240 Static	Hardware: PortC.30 VLAN ID: 30
GESTION_MGMT LAN VLAN	N/A N/A	10.0.22.1/255.255.255.240 Static	Hardware: PortC.40 VLAN ID: 40
Invitados_WiFi WiFi VLAN	N/A N/A	10.0.30.1/255.255.255.192 Static	Hardware: PortC.120 VLAN ID: 120
MOBILES LAN VLAN	N/A N/A	10.0.10.129/255.255.255.192 Static	Hardware: PortC.110 VLAN ID: 110
Servidores Servidores VLAN	N/A N/A	10.0.20.1/255.255.255.224 Static	Hardware: PortC.20 VLAN ID: 20
Usuarios_Contabili... LAN VLAN	N/A N/A	10.0.10.17/255.255.255.240 Static	Hardware: PortC.60 VLAN ID: 60
Usuarios_Gerencia LAN VLAN	N/A N/A	10.0.10.81/255.255.255.240 Static	Hardware: PortC.100 VLAN ID: 100
Usuarios_IT LAN VLAN	N/A N/A	10.0.10.1/255.255.255.240 Static	Hardware: PortC.50 VLAN ID: 50
Usuarios_Operacio... LAN VLAN	N/A N/A	10.0.10.65/255.255.255.0 Static	Hardware: PortC.90 VLAN ID: 90
Usuarios-RRHH LAN VLAN	N/A N/A	10.0.10.33/255.255.255.240 Static	Hardware: PortC.70 VLAN ID: 70
Usuarios_Ventas_C... LAN VLAN	N/A N/A	10.0.10.49/255.255.255.240 Static	Hardware: PortC.80 VLAN ID: 80

Figura 10: VLAN SFOS (elaboración propia, 2026), elaboración propia.

Una vez realizadas las configuraciones de las VLAN en el Sophos Firewall, estas se asignan sobre la interfaz PortC del equipo. Para permitir la comunicación entre los diferentes segmentos de red y el firewall, se configura un enlace troncal (trunk) entre el Core y el Sophos Firewall. Este enlace permite transportar las distintas VLAN definidas en la red, facilitando que el firewall pueda gestionar el tráfico proveniente de los usuarios y de los demás segmentos ubicados detrás del Core.

Una vez definida la estructura de la comunicación de casa Matriz incluyendo ser GW el Sophos Firewall para todos los segmentos procedemos con la integración de los enlaces externos tanto para el MPLS como para Internet y por ende comunicación por medio de VPN a la Sucursal01.

Sitio	MPLS	Comentario	Sophos FW	GW
Casa Matriz		Comunicaciones Sucursal02	172.31.255.0/30	172.31.255.2
ISP01		Interfaz externa Internet	10.0.10.16/28	10.0.137.1
ISP02		Interfaz externa Internet	X.X.X.X/X	X.X.X.X

Tabla 3: Estructura de comunicación, elaboración propia.

Nota: La dirección IP pública configurada en la interfaz externa del firewall no se detalla en este documento por motivos de confidencialidad. Si bien se cuenta con autorización para su uso dentro del entorno de pruebas, no se dispone de autorización para su divulgación, ya que este direccionamiento podría ser reutilizado para otros fines en el futuro.

Una vez declarada la anterior tabla de enlaces externo se procede a realizar las configuraciones en el Sophos Firewall y se realizan pruebas de conectividad.

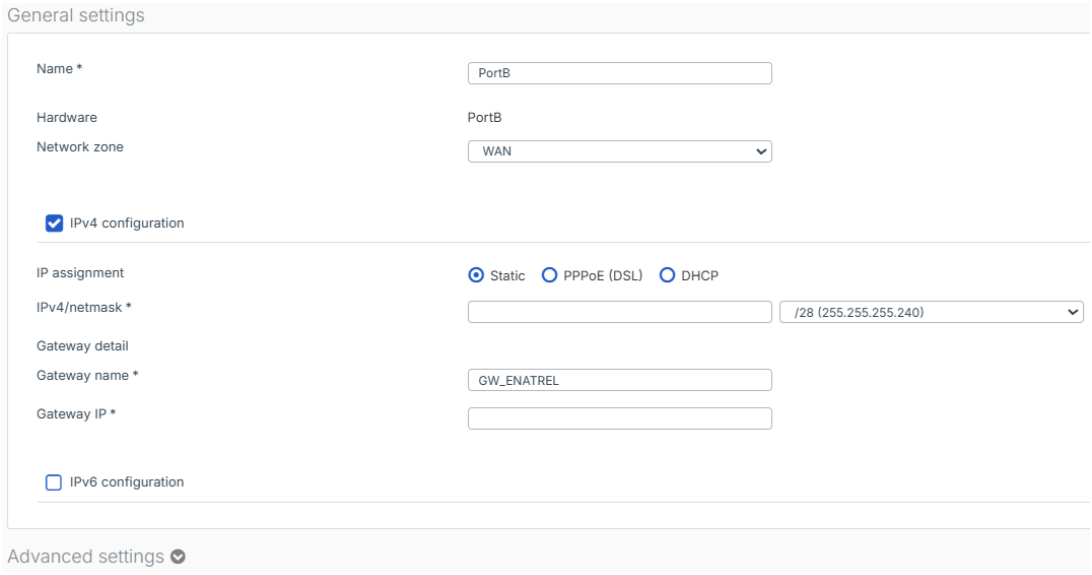


Figura 11: Interfaz WAN PortB, elaboración propia.

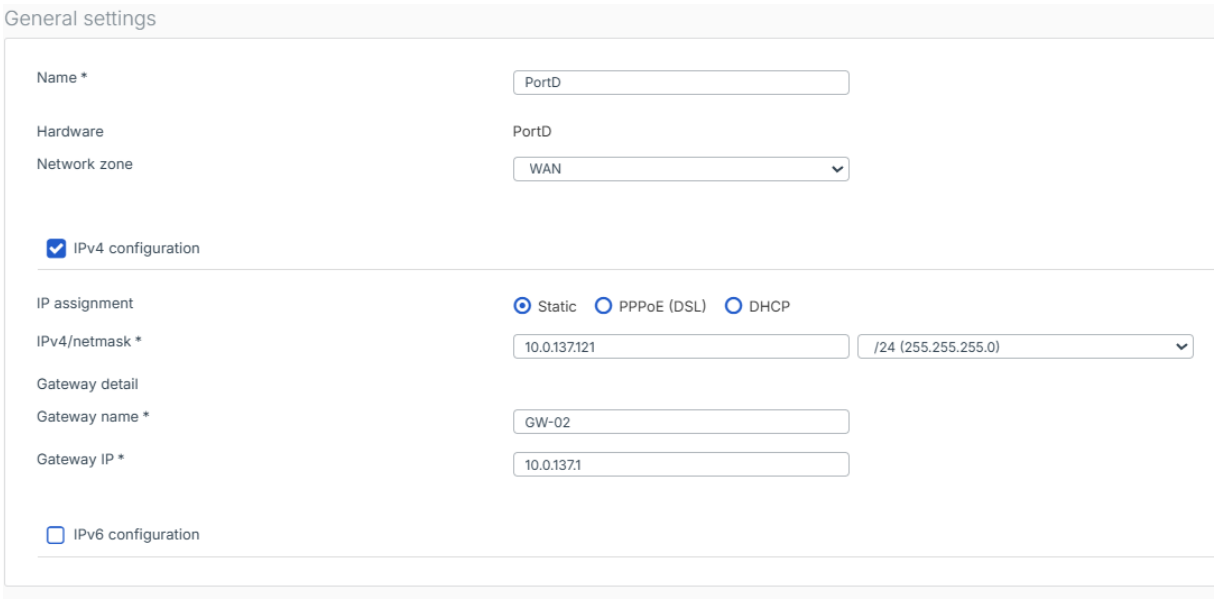


Figura 12: Interfaz WAN PortD, elaboración propia.

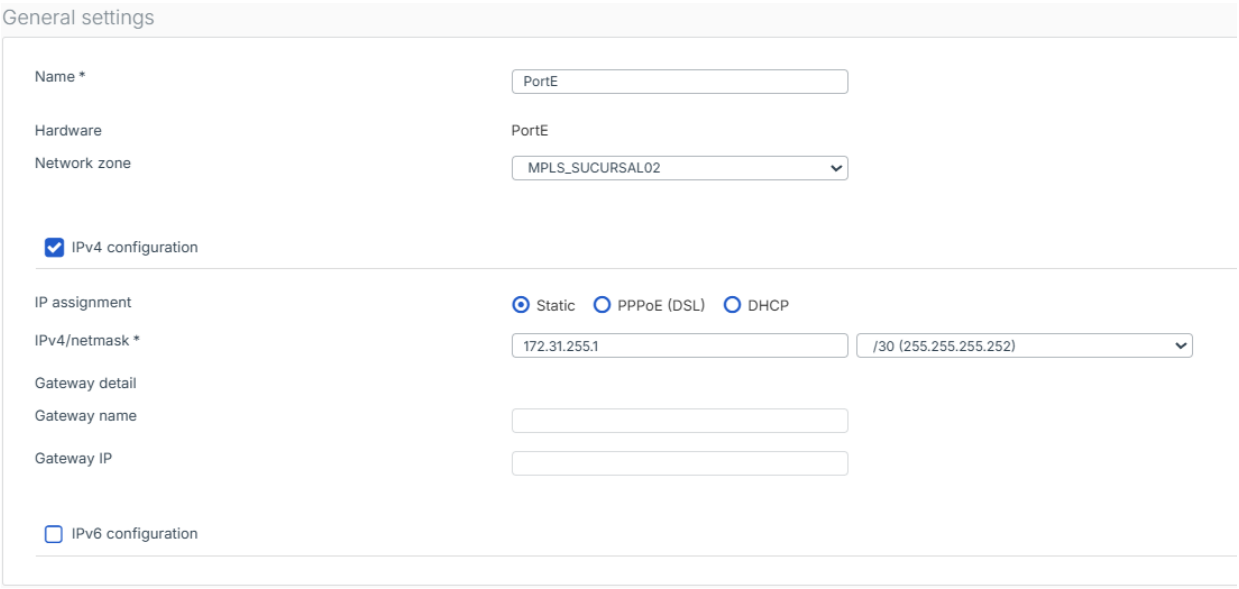
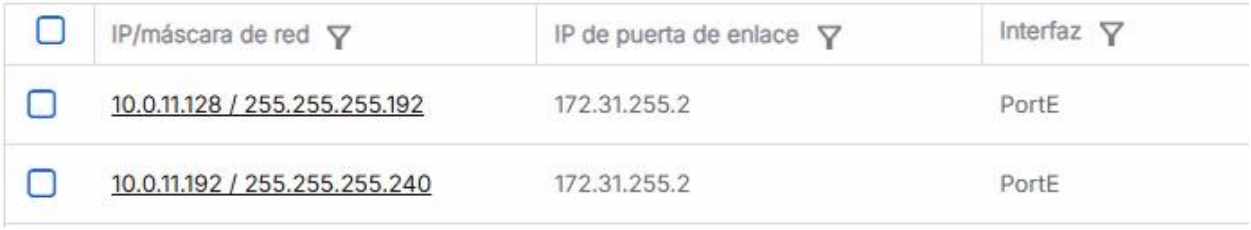


Figura 13: Interfaz MPLS PortE, elaboración propia.

En la figura 13 se muestra la configuración de múltiples VLAN asociadas a zonas de seguridad en el Sophos Firewall. La zona DMZ aísla servicios publicados (como servidores web) para evitar que un compromiso se propague a la red interna. La zona LAN agrupa las VLAN de usuarios internos: GESTION_MGMT, MOBILES,

Contabilidad, Gerencia, IT, Operaciones, RRHH y Ventas, permitiendo controles entre departamentos y reduciendo movimientos laterales. La zona WiFi aísla a invitados, permitiendo solo acceso a Internet. La zona Servidores aloja sistemas críticos con políticas estrictas. La zona WAN es la interfaz de salida a Internet y actúa como ruta por defecto. La zona MPLS_SUCURSAL02 (interfaz PortE) conecta con una sucursal remota vía MPLS. Una aclaración clave: pertenecer a una misma zona no implica comunicación directa entre VLAN; el tráfico solo se permite si existe una regla explícita que lo autorice.



	IP/máscara de red	IP de puerta de enlace	Interfaz
☐	10.0.11.128 / 255.255.255.192	172.31.255.2	PortE
☐	10.0.11.192 / 255.255.255.240	172.31.255.2	PortE

Figura 14: Enrutamiento Sucursal 02, elaboración propia.

En esta etapa se configuraron las VLAN de la casa matriz sobre la interfaz PortC del Sophos Firewall mediante un enlace troncal (trunk) con el Core, asociándolas a diferentes zonas de seguridad y estableciendo al firewall como gateway principal. Posteriormente, se configuraron las interfaces externas para conectividad a Internet y al enlace MPLS con Sucursal02. La comunicación con Sucursal01 se realizará mediante una VPN IPsec Tunnel Interface basada en rutas con IKEv2. Los parámetros criptográficos de Phase 1 y Phase 2 (cifrado, autenticación, grupos Diffie-Hellman y tiempos de vida) deben coincidir en ambos extremos. Los detalles completos se presentan en el anexo D.

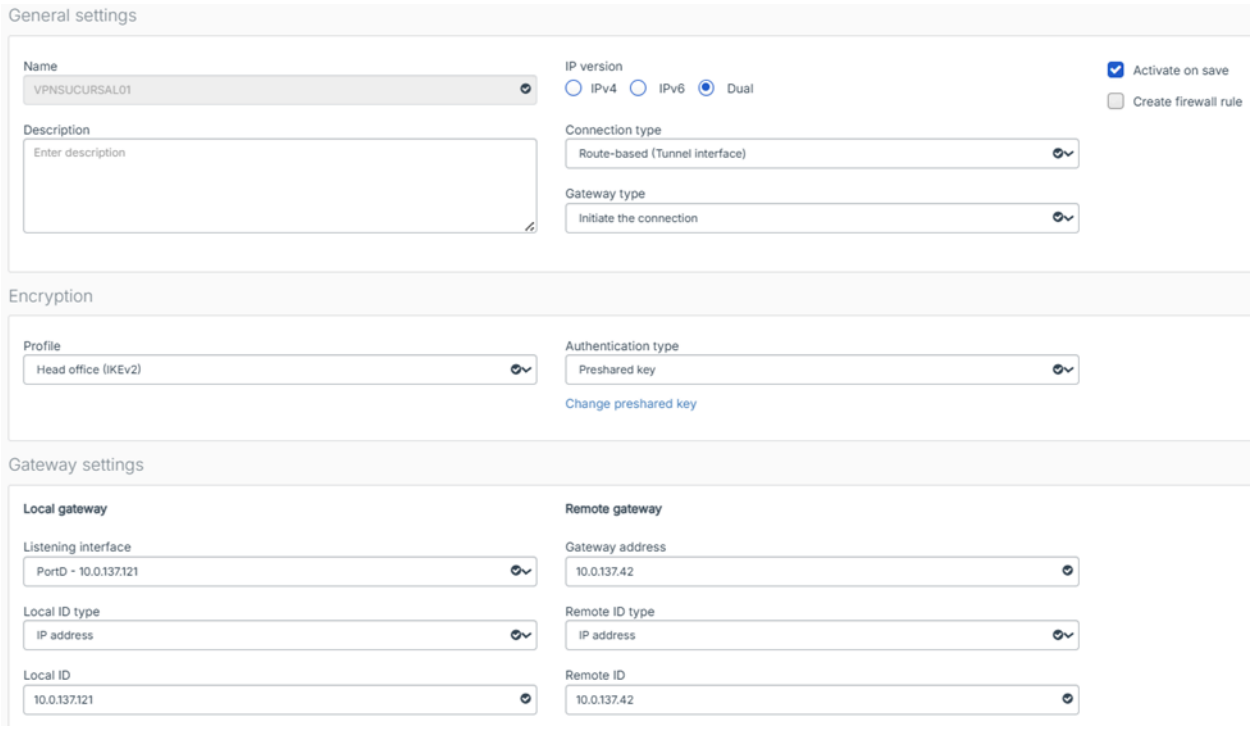


Figura 15: Configuración VPN TUNNEL INTERFACE, elaboración propia.

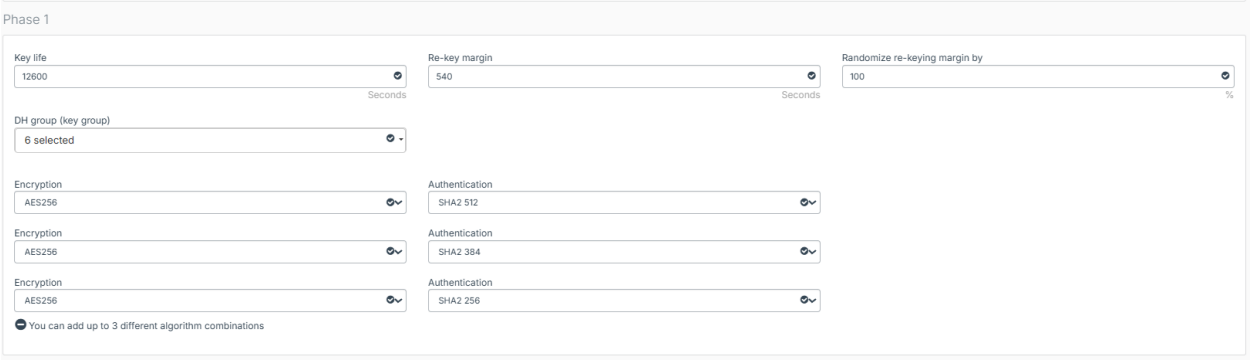


Figura 16: Configuración Phase 1 VPN, elaboración propia.

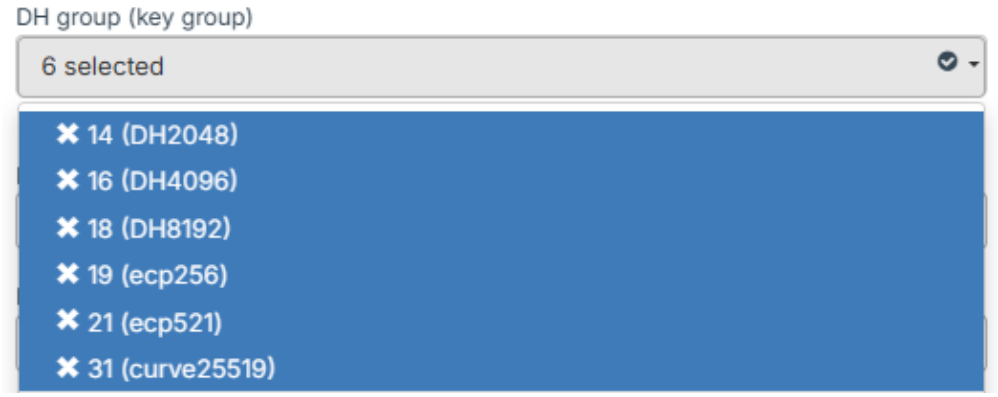


Figura 17: Configuración DH GROUP, elaboración propia.

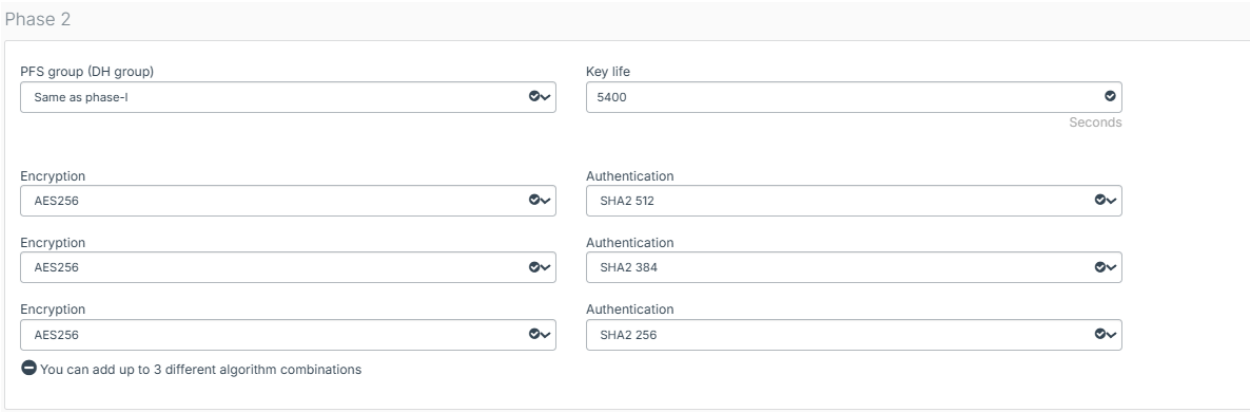


Figura 18: Configuración DH GROUP, elaboración propia.

Una vez definidas estas configuraciones en el Sophos Firewall (SFOS) y replicadas de forma equivalente en el dispositivo del peer ubicado en la sucursal, se establece correctamente la negociación del túnel IPsec entre ambos extremos, permitiendo la creación del canal seguro de comunicación.

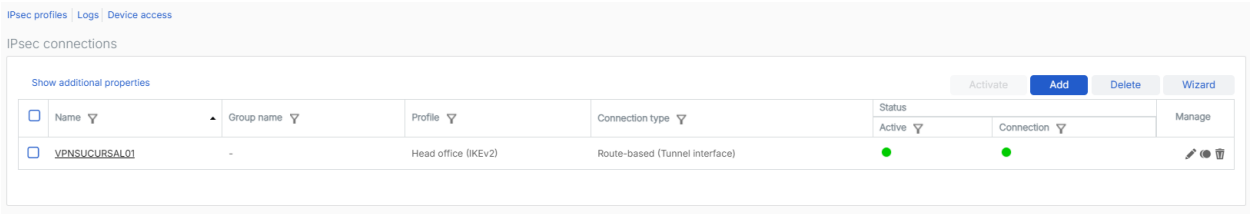


Figura 19: IPsec SINCRONIZACIÓN, elaboración propia.

Posteriormente, al tratarse de una VPN de tipo route-based, se procede a la configuración de una interfaz de túnel XFRM, a la cual se le asigna una dirección IP lógica de túnel 10.102.102.1/30 y en el peer 10.102.102.2/30. Esta interfaz actúa como punto de tránsito para el tráfico entre las redes de la casa matriz y la sucursal.

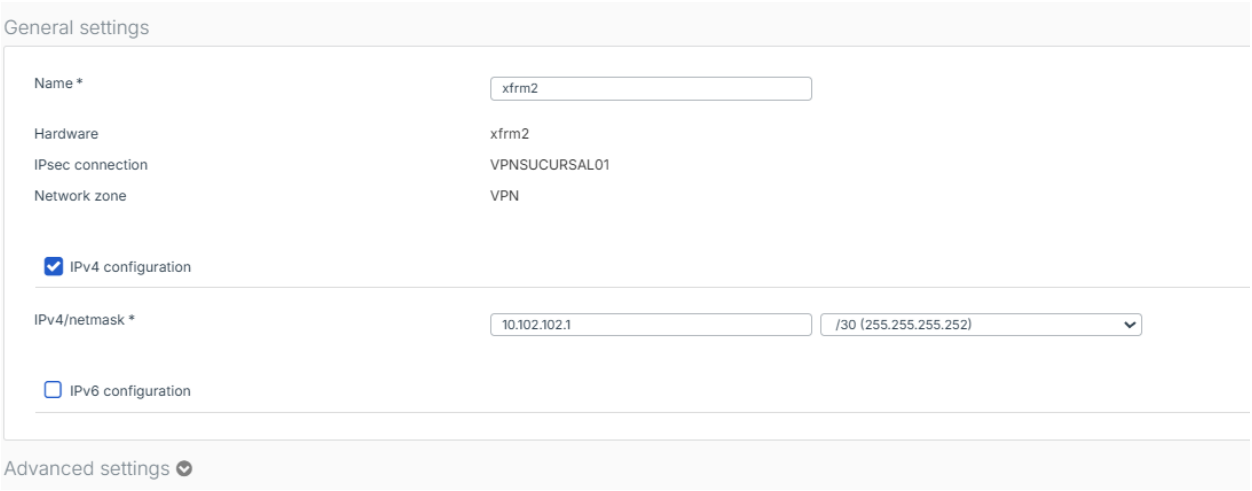


Figura 20: Interfaz XFRM, elaboración propia.

Finalmente, se implementan las rutas estáticas correspondientes, de manera que el tráfico destinado a las redes remotas sea dirigido hacia la interfaz del túnel IPsec, permitiendo la comunicación bidireccional entre los segmentos de red de la matriz y la sucursal. No obstante, aunque el túnel permite el alcance entre las redes internas, el tráfico continúa estando controlado por las políticas de firewall. En la fase inicial se permite el reconocimiento entre redes para validar la conectividad del túnel, y posteriormente se aplican reglas de firewall específicas con el objetivo de restringir y controlar el acceso entre los distintos segmentos según los requerimientos de seguridad definidos.

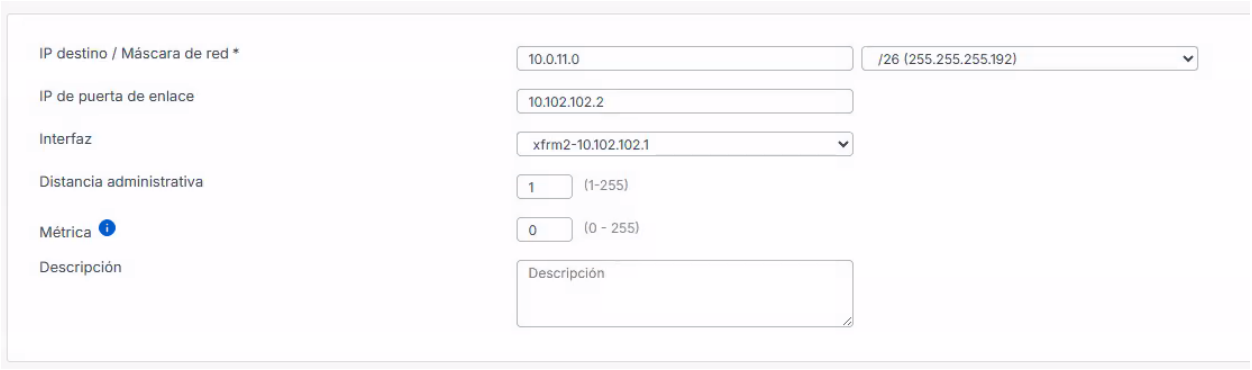


Figura 21: Interfaz XFRM, elaboración propia.

6.3.4. Integración de identidad de usuarios mediante Active Directory

Se integró el Sophos Firewall con Active Directory (AD) para fortalecer el control y la visibilidad en la red, permitiendo asociar el tráfico a cuentas reales de usuarios autenticados en el dominio, en lugar de solo direcciones IP. Para ello, se habilitó Client Authentication en la zona Servidores y se configuró el servidor Active Directory en Authentication. Esta integración también permite consumir grupos de seguridad de AD, facilitando controles alineados con la estructura organizacional.

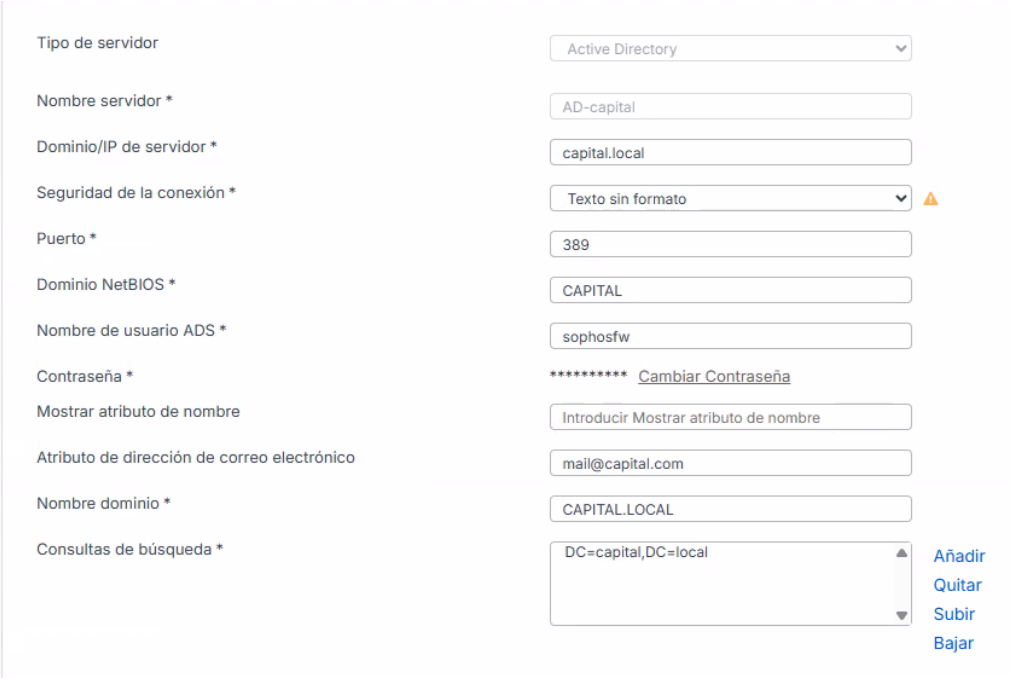


Figura 22: Server AD Integration, elaboración propia.

6.3.5. Definición de reglas de Firewall

Una vez definida la estrategia de segmentación, se procedió a la creación inicial de las reglas de firewall necesarias para controlar el flujo de tráfico entre las distintas zonas de la red. Estas políticas se implementan siguiendo el modelo de segmentación previamente definido, permitiendo administrar de forma ordenada el acceso entre usuarios, servicios internos, zonas expuestas y redes remotas.

- Política de navegación web y control de aplicaciones para usuarios internos

Esta política permite habilitar la navegación hacia Internet para los usuarios de la red interna. Para ello se implementan mecanismos de control de aplicaciones y filtrado web, los cuales permiten regular el acceso a distintos servicios y categorías de contenido en Internet conforme a las políticas de seguridad de la organización.

Adicionalmente, el tráfico web es procesado mediante el motor de proxy del Sophos Firewall, lo que permite realizar inspección completa del tráfico (full web scanning). A través de este mecanismo el firewall puede aplicar controles avanzados como filtrado de contenido, análisis de amenazas, inspección de tráfico HTTP/HTTPS y aplicación de políticas de seguridad sobre las conexiones generadas por los usuarios hacia Internet.

- Configuración de autenticación y habilitación de STAS en Sophos Firewall

Una vez realizada la integración inicial con el servicio de directorio, se procedió con la importación de los grupos de usuarios desde Active Directory. Para ello se accedió al menú Authentication →Servers → Import, donde se definió como base de búsqueda el Base DN DC=capital,DC=local. A partir de esta consulta se importaron los grupos de usuarios necesarios desde el directorio activo, quedando posteriormente disponibles dentro del firewall en el apartado Authentication → Groups, permitiendo su utilización dentro de los controles de acceso y políticas de seguridad.



Figura 23: Groups AD, elaboración propia.

Posteriormente se realizó la configuración de los servicios de autenticación del firewall. Para ello se accedió al menú Authentication → Services, donde se configuró el servidor

Active Directory previamente integrado como el primer método de autenticación del firewall, garantizando que las consultas de identidad y grupos de usuarios se realicen contra el directorio corporativo.

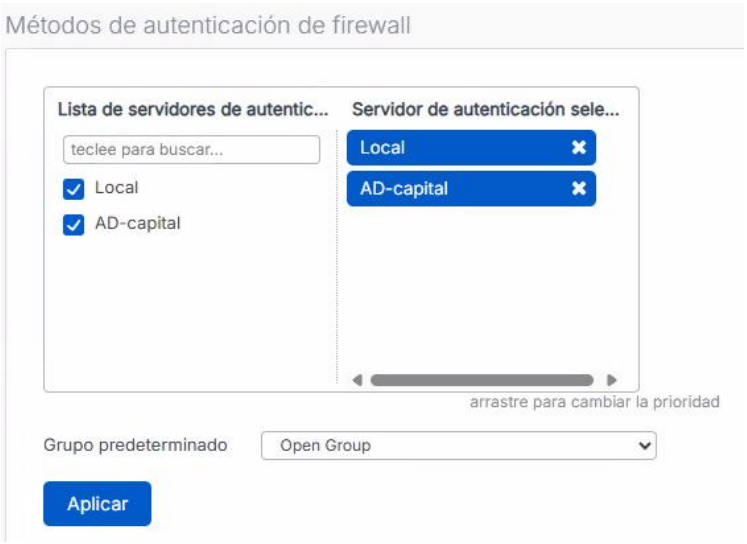


Figura 24: Métodos de Autenticación, elaboración propia.

Una vez completada la configuración de autenticación, se habilitó Sophos Transparent Authentication Suite (STAS) desde el menú Authentication → STAS, activando la opción Enable Sophos Transparent Authentication Suite y luego Activate STAS. Esto permite que el firewall identifique automáticamente a los usuarios del dominio que generan tráfico en la red.

Luego se ajustaron parámetros para evitar interrupciones durante la identificación: se configuró el Identity probe timeout en 3 segundos, se deshabilitó Restrict client traffic during identity probe y se mantuvo deshabilitada Enable user inactivity detection. Estos ajustes permiten que el firewall procese el tráfico mientras realiza las consultas de identidad.

Finalmente, se registró el servidor STAS Collector en Authentication → STAS → Add Collector, agregando la dirección IP 10.0.20.5 (servidor donde está instalado STAS). Una vez registrado, el firewall se comunica con el Collector para recibir la información de usuarios autenticados y asociar esa identidad al tráfico generado en la red.

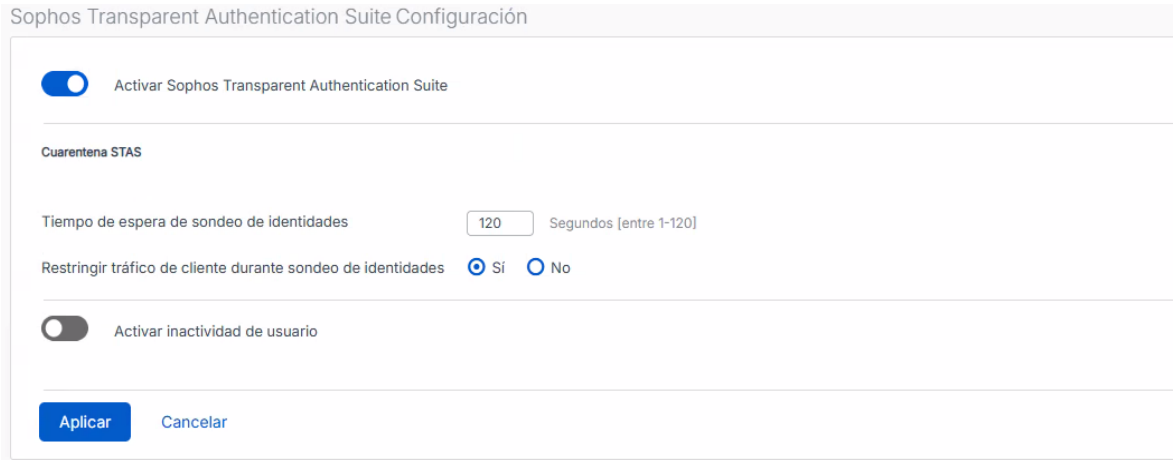


Figura 25: STAS Cuarentena, elaboración propia

Se instaló Sophos Transparent Authentication Suite (STAS) directamente en el controlador de dominio (10.0.20.5), descargando el instalador desde Authentication → Client Downloads del firewall. La suite incluye STA Agent (detecta eventos de inicio de sesión) y STA Collector (envía la información al firewall). En el STA Agent se configuró el dominio: NetBIOS como CAPITAL y FQDN como capital.local. En el STA Collector se verificó el puerto de escucha.

Se habilitó la política de auditoría Audit Kerberos Authentication Service vía GPO para generar el evento 4768, y se permitió WMI mediante regla de firewall entrante para consultar usuarios activos en estaciones. También se habilitaron los puertos necesarios: TCP 5566, UDP 6677, UDP 50001 y UDP 6060.Finalmente, se registró el Collector en el firewall (Authentication → STAS → Add Collector) con IP 10.0.20.5, y se verificó el correcto funcionamiento mostrando usuarios autenticados asociados a sus IP en Live Users del firewall.

- Configuración de políticas de navegación a Internet basadas en grupos de Active Directory

Una vez integrado Active Directory y verificada la detección de usuarios mediante STAS, se configuraron reglas de firewall para la navegación a Internet utilizando

grupos de usuarios importados desde AD: IT, Contabilidad, RRHH, Ventas, Operaciones y Gerencia.

Se crearon políticas de navegación que permiten aplicar filtrado web, control de aplicaciones e inspección mediante el motor proxy del firewall, aplicando políticas diferenciadas según el perfil de usuario. El firewall identifica al usuario autenticado vía STAS, lo asocia a su grupo de AD y aplica la política correspondiente.

Bajo el principio de mínimo privilegio, se permite únicamente el acceso a servicios estrictamente necesarios para cada área, reduciendo la superficie de exposición ante amenazas externas. Los perfiles de Web Filter y App Control se definen según la Tabla 2-3 de Web Filtering y App Control.

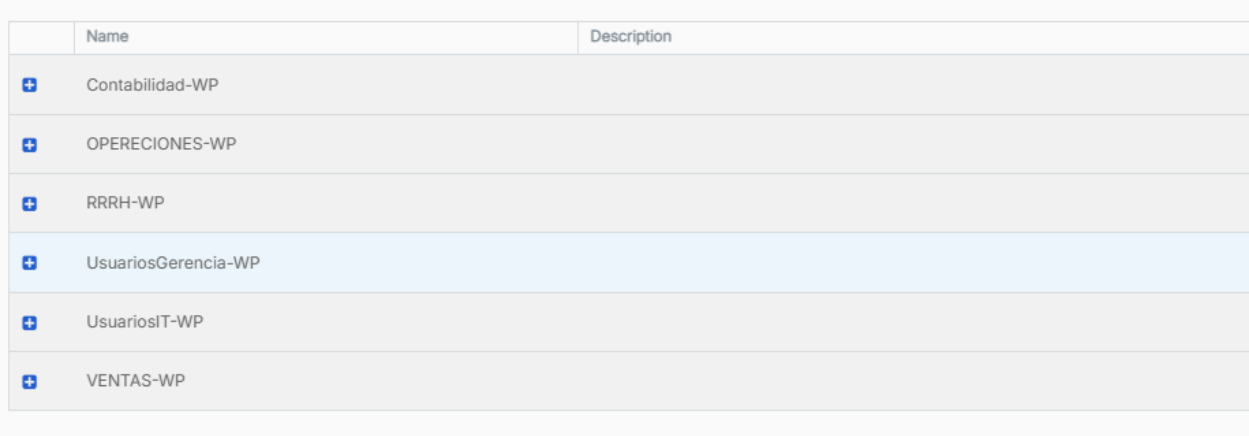


Figura 26: Perfiles Web, elaboración propia.

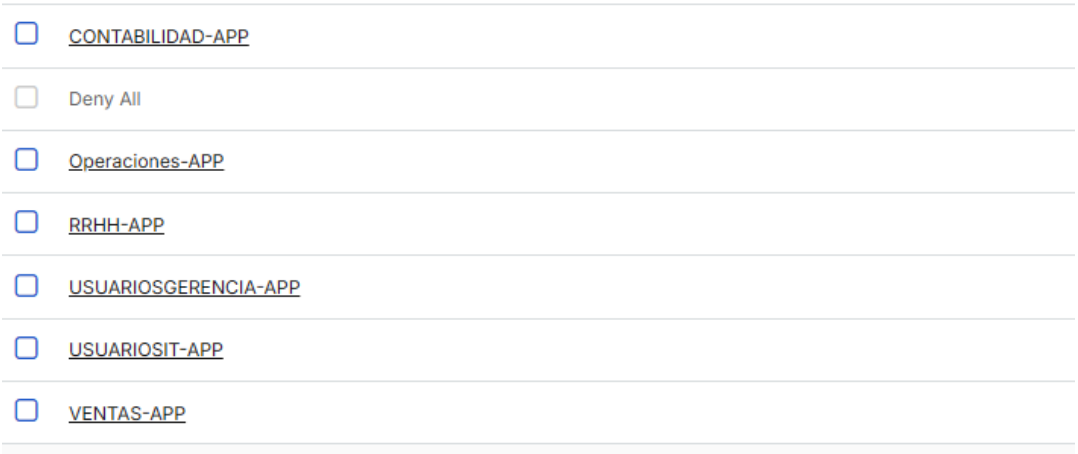


Figura 27: Perfiles App, elaboración propia.

Se tomó un perfil como referencia para explicar su configuración. Para el Application Control se accedió a Applications → Application Filter, creando un perfil por grupo de usuarios con política de bloqueo por defecto: solo se permiten las aplicaciones definidas explícitamente, restringiendo automáticamente el resto. Se utilizó la funcionalidad Smart Filter para agrupar aplicaciones por categoría, habilitando únicamente servicios necesarios como actualizaciones del sistema o herramientas operativas. El perfil se asocia luego a la regla de firewall correspondiente, permitiendo inspeccionar el tráfico y controlar con precisión las aplicaciones usadas en la red, reduciendo la exposición a riesgos (Ver figura 28).

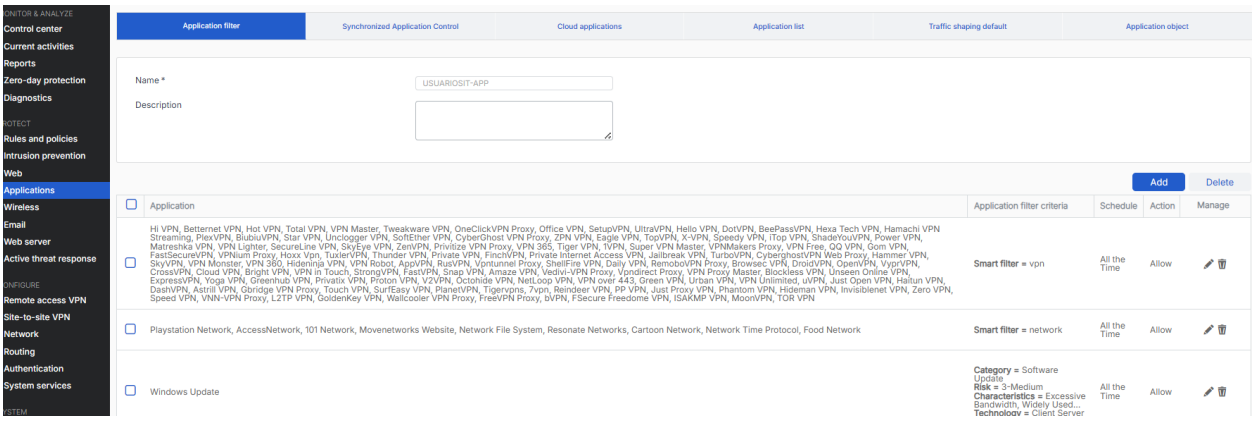


Figura 28:Perfiles App – Usuarios IT, elaboración propia.

De forma similar al control de aplicaciones, se configuró el perfil de Web Filtering en Web - Policies, creando el perfil UsuariosIT-WP. Se utilizaron categorías de contenido para habilitar únicamente las relacionadas con actividades laborales: Business Cloud Apps, Business Networking, General Business, Information Technology, News y Reference. El resto de categorías se mantienen con la acción por defecto.

Adicionalmente, se activaron controles de seguridad como Enforce SafeSearch con filtros de imágenes, y restricción de contenido en YouTube en nivel Moderate para limitar contenido inapropiado.

Este perfil se asocia a la regla de firewall correspondiente, permitiendo evaluar el tráfico web según las categorías y restricciones definidas (Ver figura 29).

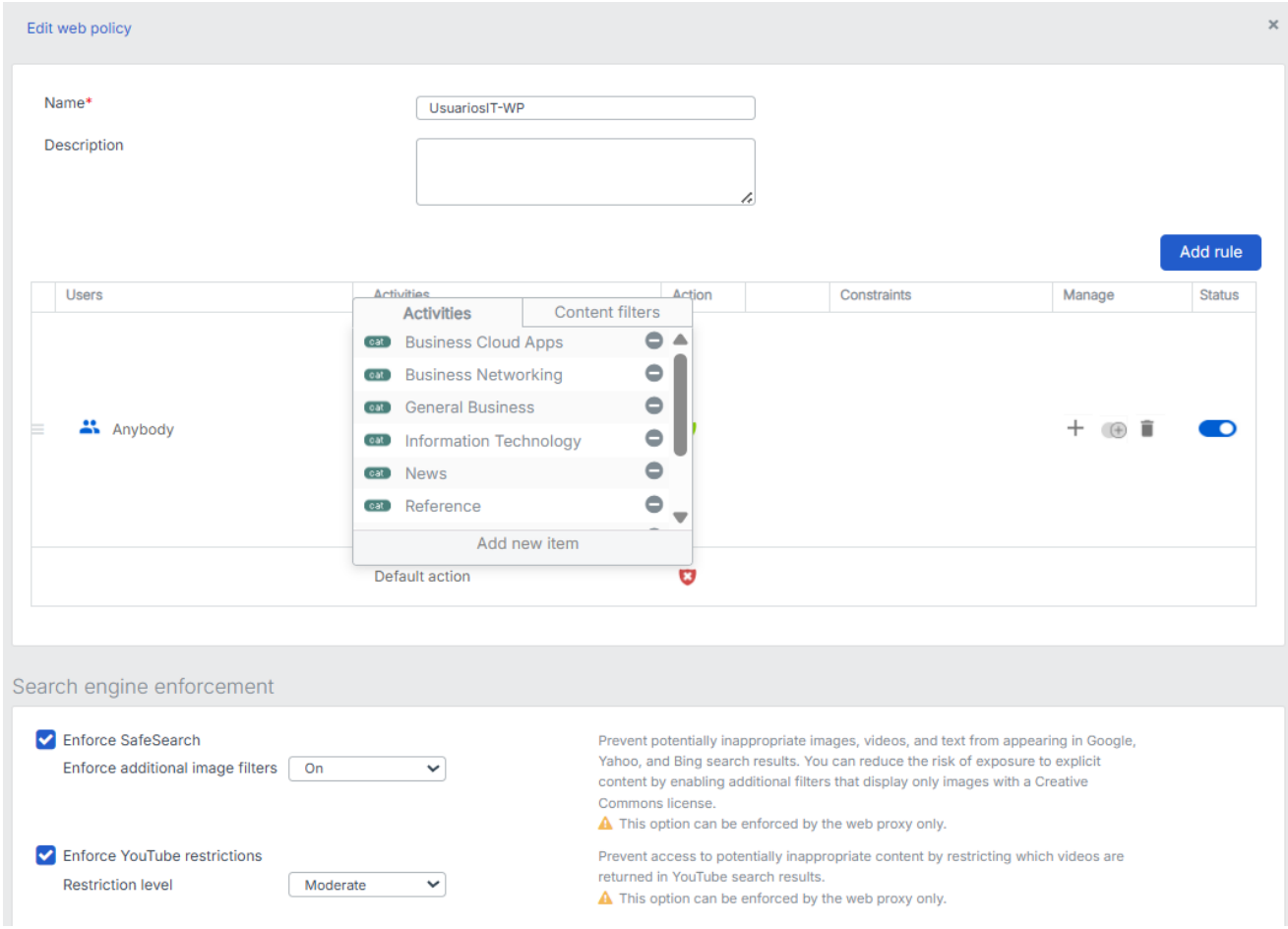


Figura 29: Perfiles WEB – Usuarios IT, elaboración propia.

Una vez definidos los perfiles de Web Filtering y Application Control, se crearon reglas de firewall individuales para cada grupo de Active Directory. En cada regla se definió como origen las zonas LAN y MPLS, como destino Internet, permitiendo únicamente tráfico HTTPS. El criterio principal es la identidad del usuario obtenida mediante STAS.

Debido a que el control se basa en usuario, un mismo usuario puede autenticarse desde distintos segmentos de red; el firewall lo identifica por su sesión y aplica la política correspondiente a su grupo. Por esta razón se permite como origen el tráfico

desde cualquier red interna, independientemente del segmento, reforzando el control mediante autenticación y reconocimiento de identidad (Ver figura 30).

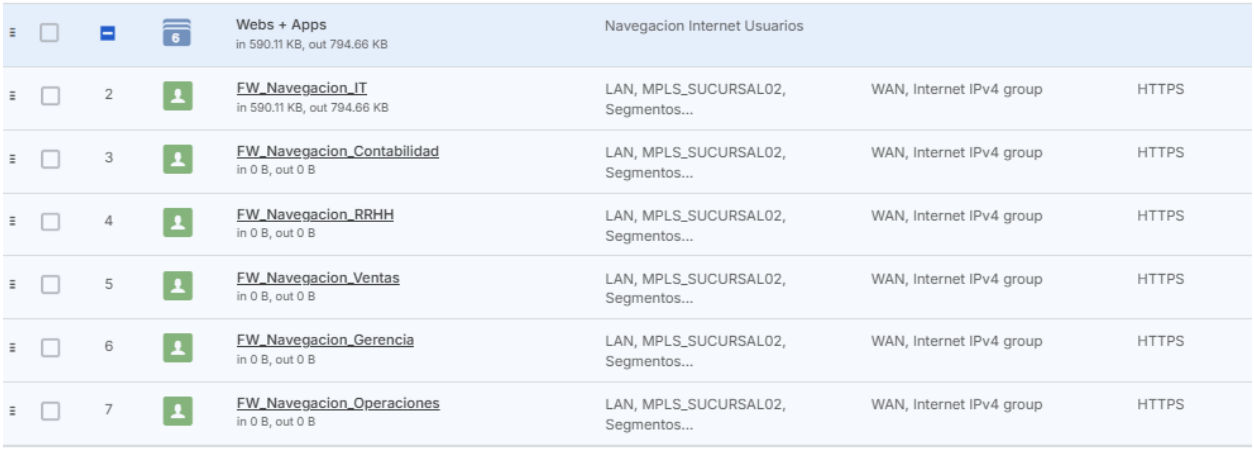


Figura 30: Perfiles WEB – Usuarios IT, elaboración propia.

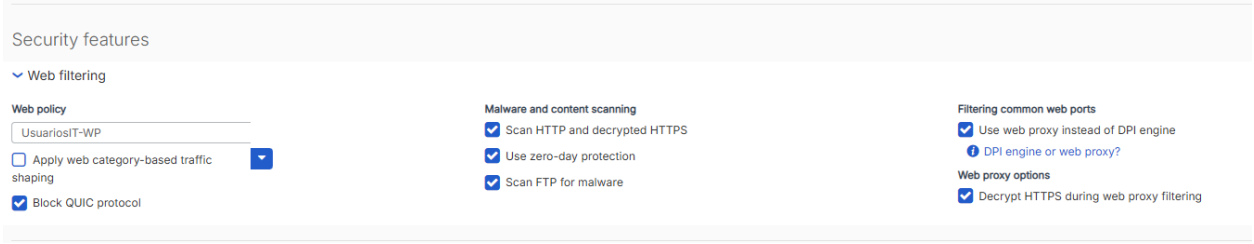


Figura 31: Perfiles WEB Proxy, elaboración propia.

En las reglas de firewall para navegación a Internet se habilitaron mecanismos de seguridad de forma uniforme para todos los grupos de usuarios. Se asoció el perfil de Web Filtering (UsuariosIT-WP), se activó Apply web category-based traffic shaping para control de tráfico por categorías, y se bloqueó el protocolo QUIC para evitar evasión de inspección.

En Malware and content scanning se habilitaron: Scan HTTP and decrypted HTTPS, Use zero-day protection y Scan FTP for malware.

En Filtering common web ports se configuró el uso del motor proxy (Use web proxy instead of DPI engine) y se habilitó Decrypt HTTPS during web proxy filtering para inspeccionar tráfico cifrado.

Adicionalmente, se habilitó el IPS (Intrusion Prevention System) en estas políticas para analizar tráfico en busca de patrones maliciosos. De esta manera, las políticas de navegación incorporan múltiples capas de seguridad (Ver figuras 31 y 32).

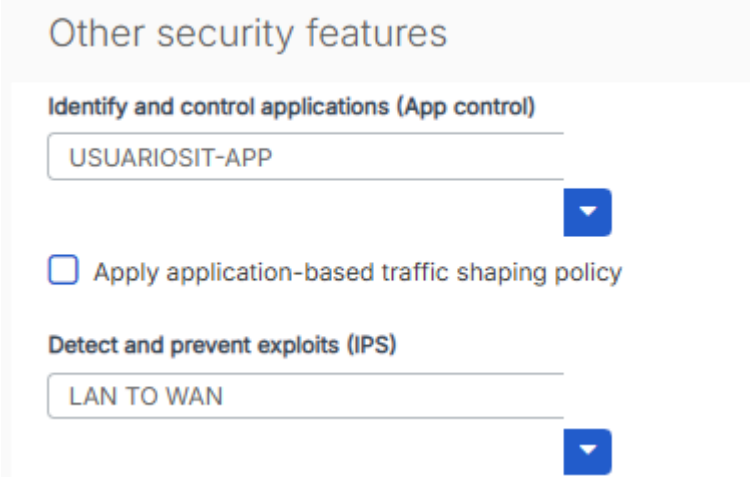


Figura 32: Perfiles IPS, elaboración propia.

- Configuración de reglas para comunicación interna entre usuarios y servidores

En este apartado se definen las reglas de firewall para la comunicación interna entre segmentos de usuarios y la red de servidores, basadas en la arquitectura detallada en la sección 6.2.4.

Se configuraron políticas que permiten acceso desde segmentos internos hacia el servidor de infraestructura (10.0.20.5) con funciones de AD y DNS, habilitando únicamente los puertos necesarios para autenticación y resolución de nombres.

Adicionalmente, se definieron reglas para comunicarse con los servidores web en la DMZ, restringiendo el acceso solo al puerto TCP 443 (HTTPS). También se habilitó el acceso administrativo RDP (TCP 3389) exclusivamente desde el segmento de Usuarios IT para administración controlada.

Estas configuraciones aplican el principio de mínimo privilegio, permitiendo solo los flujos necesarios para el funcionamiento de la infraestructura descrita en la sección 6.2.4, mientras que el resto del tráfico intersegmento permanece restringido por defecto.



		Internet - Servidores in 0 B, out 0 B			
	9	Internet_AD in 0 B, out 0 B	Servidores, host-srv-ad	WAN, DNS-SERVER	DNS
		SITE-TO-SITE-SUCURSAL01 in 4.51 MB, out 8.02 MB			
	10	FWR_INBOUND_SUCURSAL01_AD in 4.51 MB, out 8.02 MB	VPN, RED_SUCURSAL01-USUARIOS	Servidores, host-srv-ad	AD-PORT-AUTH
	11	FW_IT_TO_SUCURSAL01 in 0 B, out 1.05 KB	LAN, MPLS_SUCURSAL02, Segmentos...	VPN, RED_SUCURSAL01-USUARIOS	Any service
		INTERNAL - SERVIDORES in 5.01 MB, out 5.13 MB	trafico lan a servidores		
	12	FW_Internal - AD in 0 B, out 0 B	LAN, VLAN-RRHH , VLAN-VENTAS , ...	Servidores, host-srv-ad	AD-PORT-AUTH
	13	FW-Sucursal02-AD in 299.79 KB, out 374.56 KB	MPLS_SUCURSAL02, RED_SUCURSAL02...	Servidores, host-srv-ad	AD-PORT-AUTH
	14	FW-DMZ-AUTH-AD in 4.72 MB, out 4.76 MB	DMZ, NET_Servidores_DMZ	Servidores, host-srv-ad	AD-PORT-AUTH
		Traffic VPN in 449.92 MB, out 463.28 MB			
	15	VPN_INTERNO in 449.92 MB, out 463.28 MB	VPN, Any host, soporteit	Any zone, Any host	Any service
	16	Traffic to AD in 12.11 MB, out 16.23 MB	LAN, Servidores, Any host	LAN, Servidores, Any host	Any service

Figura 33: FW-Rules, elaboración propia.

- Implementación del Web Application Firewall (WAF)

Con el objetivo de proteger las aplicaciones web publicadas, se implementa el módulo Web Application Firewall (WAF) del Sophos Firewall, el cual opera bajo un modelo de reverse proxy, actuando como intermediario entre los clientes externos y los servidores web internos. Todo el tráfico entrante es procesado por el firewall antes de ser

reenviado al servidor interno, permitiendo aplicar controles de seguridad avanzados a nivel de aplicación HTTP.

Para habilitar esta protección se crea una regla llamada WAF-WEB dentro del grupo de reglas WAF. Esta regla define el punto de acceso público hacia el servicio web y los servidores internos que alojan la aplicación. Dentro del apartado Hosted Server se define la dirección del firewall que recibirá las conexiones externas.

Parámetro	Configuración
Rule name	WAF-WEB
Hosted address	PortB
Listening port	80
HTTPS	Deshabilitado
Redirect HTTP	No configurado
Domains	No especificado

Tabla 4: Firewall WAF parte 1, elaboración propia.

La interfaz PortB del firewall funciona como punto de publicación del servicio web, permitiendo que los clientes externos puedan establecer conexión hacia la aplicación alojada internamente. Posteriormente se especifican los servidores internos protegidos por el WAF, seleccionando el servidor SERVER-WEB, que aloja la aplicación web dentro de la red interna y representa el destino final del tráfico una vez inspeccionado y validado por el firewall. En cuanto al control de acceso al servicio web, el firewall permite definir restricciones para controlar qué clientes pueden conectarse al servicio publicado. En esta implementación, con fines de pruebas dentro del entorno de laboratorio, se permitió el acceso desde cualquier red IPv4.

Parámetro	Configuración
Allowed client networks	Any IPv4
Blocked client networks	Ninguno
Blocked countries	Ninguno
Authentication	None

Tabla 5: Firewall WAF parte 2, elaboración propia.

Esta configuración permite evaluar el comportamiento del WAF frente a diferentes tipos de tráfico sin restricciones iniciales.

Política de protección WAF

Para proteger la aplicación web se crea una política de seguridad denominada WAF_RULE_LOGIN, la cual define los mecanismos de inspección y filtrado que se aplicarán al tráfico HTTP.

Configuración general de la política

Parámetro	Configuración
Mode	Reject
Cookie signing	Habilitado
Static URL hardening	Deshabilitado
Form hardening	Habilitado

Tabla 6: Firewall WAF parte 3, elaboración propia.

El modo Reject permite que el firewall bloquee inmediatamente cualquier solicitud que coincida con patrones de ataque definidos dentro de la política.

Las funciones de Cookie Signing y Form Hardening proporcionan protección adicional contra manipulación de sesiones y parámetros de formularios.

Protección y controles de seguridad del WAF

La política WAF implementada incorpora múltiples mecanismos de protección. Incluye análisis antivirus del tráfico HTTP en modo Dual Scan (dos motores de detección, bloqueo de contenido no escaneable, límite de 2 MB). Se habilitan controles específicos para detectar SQL Injection, XSS, ataques a nivel de aplicación, escáneres, control de protocolo y prevención de fuga de datos.

Se activa el Common Threat Filter (nivel Level 2) para bloquear solicitudes asociadas a firmas conocidas de ataques web. También se habilita el bloqueo de clientes con mala reputación y se establece un límite de tamaño de solicitud de 10 MB para prevenir abusos.

Finalmente, la regla WAF se integra con el IPS mediante la política WAN to DMZ, analizando el tráfico a nivel de red para detectar exploits antes de que alcancen el servidor web. De esta forma, el firewall implementa un modelo de defensa en profundidad que combina múltiples capas de seguridad para proteger las aplicaciones web publicadas.

6.4. Procedimiento para el dimensionamiento del Firewall

Para la selección del modelo de firewall dentro del escenario Enterprise propuesto, se consideran los lineamientos de dimensionamiento establecidos por el fabricante. Para ello se toma como referencia la herramienta oficial Sophos Firewall Sizing Calculator, la cual permite estimar el modelo de firewall más adecuado —ya sea appliance físico de la serie XGS o un Virtual Appliance en función de las características operativas del entorno. El dimensionamiento del firewall se realiza a partir de variables relacionadas con el comportamiento del tráfico de red y los servicios de seguridad que serán habilitados. Entre los principales parámetros evaluados se encuentran el ancho de banda WAN total, el consumo promedio del enlace, el crecimiento proyectado del

tráfico a tres años, así como los picos de demanda esperados. Adicionalmente, la herramienta permite incorporar factores como el número de usuarios, túneles VPN concurrentes y la activación de módulos de seguridad como IPS, Web Protection, Anti-Malware y descifrado SSL/TLS, los cuales impactan directamente en el rendimiento del firewall.

En el contexto del presente estudio no se cuenta con un histórico de consumo de ancho de banda ni con un número definido de usuarios finales que permita realizar un cálculo preciso de dimensionamiento. No obstante, se deja documentado el procedimiento y la herramienta utilizada por el fabricante para este tipo de análisis, con el fin de establecer la metodología que debería aplicarse en un escenario de implementación real.

- Ancho de banda WAN total, correspondiente a la capacidad del enlace hacia Internet.
- Consumo promedio de ancho de banda, que representa el uso habitual del enlace bajo condiciones normales de operación.
- Crecimiento proyectado del tráfico WAN a tres años, utilizado para evaluar la escalabilidad del equipo seleccionado.
- Crecimiento estimado en picos de tráfico, que contempla incrementos temporales en la demanda del servicio.
- Crecimiento promedio del tráfico, empleado para estimar la evolución progresiva del consumo de ancho de banda.

Adicionalmente, la herramienta permite considerar funcionalidades de seguridad que impactan directamente en el rendimiento del firewall, tales como Intrusion Prevention System (IPS), Web Protection, Anti-Malware, Application Control y descifrado SSL/TLS, así como el número de túneles VPN concurrentes y usuarios autenticados. A partir de estos parámetros, el sistema calcula el throughput requerido y recomienda el modelo de firewall más adecuado dentro de la serie Sophos XGS, permitiendo

seleccionar un equipo que garantice capacidad suficiente para operar en el escenario propuesto. (Sophos, n.d.)

6.5. Análisis de Viabilidad Económica mediante el Modelo ROSI

6.5.1. Aplicación del modelo ROSI con datos reales

Con base en la metodología establecida en la sección 5.6, se procedió a aplicar el análisis costo–beneficio utilizando una cotización de referencia para la solución Sophos Firewall XGS 2100. Los valores utilizados en el análisis corresponden a precios reales de mercado; sin embargo, la fuente específica que generó la cotización no se menciona en el presente documento con el fin de evitar la divulgación de información comercial sensible. En este contexto, el modelo XGS 2100 se selecciona como referencia para ejemplificar la aplicación de la metodología de evaluación financiera, permitiendo ilustrar el análisis de retorno de inversión de una solución de firewall de nueva generación dentro de un entorno empresarial.

A continuación, se presentan los resultados del análisis financiero:

- Inversión en Hardware y Licenciamiento (Periodo 36 meses)

Descripción	Cantidad	Precio (C$)
Sophos XGS 2100: 8 GE + 2 SFP, SSD, Base License (FW, VPN, Wireless)	1	C$ 91,741.50
Licencia Xstream Protection (36 meses)	1	C$ 292,873.50
Licencia Webserver Protection (36 meses)	1	C$ 44,011.50
Subtotal Equipamiento		**C$ 428,626.50**

Tabla 7: Inversión en Hardware y Licenciamiento (Periodo 36 meses), adaptada de (Grupo Intelector, 2026).

- Costos de Servicios Profesionales

Descripción	Cantidad	Precio (C$)
Costos de importación y aseguramiento de carga	1	C$ 14,979.45
Instalación y configuración por ingenieros certificados	1	C$ 42,862.65
Soporte técnico 7×24 por 12 meses	1	C$ 64,294.16
Subtotal Servicios		**C$ 122,136.26**

Tabla 8: Costos de servicios profesionales, adaptado de (Grupo Intelector, 2026).

- Consolidado de Inversión Total

Concepto	Monto (C$)	Monto (USD)
Subtotal Equipamiento	C$ 428,626.50	$ 11,703.34
Subtotal Servicios	C$ 122,136.26	$ 3,334.84
Subtotal antes de impuestos	**C$ 550,762.76**	**$ 15,038.18**
IVA (15%)	C$ 82,614.41	$ 2,255.73
INVERSIÓN TOTAL	**C$ 633,377.17**	**$ 17,293.91**

Tabla 9: Consolidado de inversión total, adaptado de (Grupo Intelector, 2026).

Tipo de cambio referencial: C$ 36.6243 por USD (Banco Central de Nicaragua, 2026).

6.5.2. Costo anualizado de la solución

Para efectos del cálculo ROSI, es necesario anualizar la inversión considerando el periodo de licenciamiento de 36 meses:

$$Costo_{anual} = \frac{Costo_{total}}{3\ años} = \frac{633{,}377.17}{3} = C\$\ 211{,}125.72\ anuales$$

Este valor (C$ 211,125.72) representa el Costo de la Solución de Seguridad que se utilizará en la fórmula ROSI.

6.5.3. Estimación de pérdidas anuales esperadas (ALE)

- Identificación de escenarios de riesgo relevantes

Basado en el análisis de la infraestructura Enterprise de CAPITAL, S.A. con estadísticas de incidentes reportados en IBM Cost of a Data Breach Report (2025) y

Verizon DBIR (2025), ajustados al contexto Enterprise nicaragüense. y en reportes de la industria, se identifican cuatro escenarios de incidente con mayor probabilidad de impacto económico:

Escenario	Descripción	Activos afectados	Impacto
E1: Ransomware	Cifrado de datos críticos mediante malware avanzado	Servidores AD, DNS, bases de datos	Indisponibilidad operativa, costos de recuperación
E2: Filtración de Datos	Exfiltración de información sensible de clientes	Portal web DMZ, bases de datos	Multas regulatorias, daño reputacional
E3: Ataque a Aplicación Web	Explotación de vulnerabilidades en portal público	Servidores web en DMZ	Interrupción de servicios, pérdida de confianza
E4: Movimiento Lateral	Propagación interna tras compromiso inicial	VLANs internas, servidores críticos	Escalada del incidente, mayor tiempo de recuperación

Tabla 10: Identificación de escenarios de riesgos relevantes, adaptado de (Verizon DBIR, 2025).

- Cálculo de SLE por escenario

Se estiman los impactos económicos considerando: costos de respuesta técnica, horas de inactividad, recuperación de datos, y sanciones potenciales. Los valores se expresan en USD para facilitar comparación con estándares internacionales.

Escenario	Componentes del impacto	SLE estimado (USD)	SLE estimado (C$)
E1: Ransomware	- 48 h de indisponibilidad operativa - Recuperación de backups - Horas técnicas de respuesta - Pérdida de productividad (150 usuarios)	$42,000	C$ 1,538,220.6
E2: Filtración de Datos	- Notificación a clientes afectados - Asesoría legal y cumplimiento - Campaña de comunicación de crisis - Multas potenciales (estimado bajo)	$28,000	C$ 1,025,480.4
E3: Ataque a Aplicación Web	- Tiempo de inactividad del portal - Reparación de vulnerabilidades - Pérdida de transacciones estimadas	$15,000	C$ 549,364.5
E4: Movimiento Lateral	- Investigación forense interna	$12,000	C$ 439,491.6

Escenario	Componentes del impacto	SLE estimado (USD)	SLE estimado (C$)
	- Reconfiguración de políticas - Capacitación de refuerzo al personal		

Tabla 11: Cálculo de SLE por escenario, adaptado de (IBM Cost of a Data Breach Report ,2025).

- Frecuencia anual de ocurrencia (ARO) estimada

La probabilidad de ocurrencia se estima considerando:

- Exposición actual de la infraestructura (servicios web públicos, tráfico cifrado sin inspección)
- Estadísticas sectoriales para instituciones financieras de tamaño similar
- Ausencia de controles NGFW en el perímetro actual

Escenario	Justificación de la frecuencia	ARO estimado
E1: Ransomware	Sector financiero es objetivo prioritario; 1 de cada 4 PYME sufre intento anual (Verizon DBIR 2025)	0.25 (1 cada 4 años)
E2: Filtración de Datos	Portal web expuesto sin WAF; vulnerabilidades comunes en aplicaciones web	0.20 (1 cada 5 años)
E3: Ataque a Aplicación Web	Servicios HTTPS públicos; ausencia de inspección de capa 7	0.33 (1 cada 3 años)
E4: Movimiento Lateral	Segmentación lógica sin control granular; tráfico inter-VLAN sin inspección	0.50 (1 cada 2 años)

Tabla 12: Estimación de annual rate of occurrence (ARO), adaptado de (IBM Cost of a Data Breach Report ,2025).

- Cálculo de ALE Base (Sin Controles NGFW)

$$ALE = SLE \times ARO$$

Escenario	SLE (C$)	ARO	ALE (C$)
E1: Ransomware	C$ 1,538,220.6	0.25	C$ 384,555.15
E2: Filtración de Datos	C$ 1,025,480.4	0.20	C$ 205,096.08
E3: Ataque a Aplicación Web	C$ 549,364.5	0.33	C$ 181,290.28
E4: Movimiento Lateral	C$ 439,491.6	0.50	C$ 219,745.8
ALE Total base			**C$ 990,687.31**

Tabla 13: Pérdida anual esperada - escenario actual (Sin NGFW), adaptado de (IBM Cost of a Data Breach Report ,2025).

En el escenario actual, sin la implementación de Sophos Firewall, la organización enfrenta una pérdida anual esperada estimada de C$ 990,687.31 (USD $27,049.99) derivada de incidentes de seguridad probables.

6.5.4. Estimación de reducción de riesgo con Sophos Firewall

- Eficacia esperada de los controles NGFW

Cada funcionalidad de Sophos Firewall contribuye a mitigar escenarios específicos. Se estima la eficacia de mitigación basándose en capacidades técnicas documentadas y estudios de efectividad de NGFW:

Escenario	Controles aplicables NGFW	Eficacia estimada de mitigación
E1: Ransomware	- IPS con firmas actualizadas - Sandbox en la nube (Sophos Labs Intelix) - Control de aplicaciones y tráfico cifrado - Security Heartbeat con endpoints	75%
E2: Filtración de Datos	- DLP básico en políticas de salida - Registro y auditoría de tráfico - Inspección SSL/TLS para detectar exfiltración - Políticas basadas en identidad	60%
E3: Ataque a Aplicación Web	- Web Application Firewall (WAF) - Protección contra SQLi, XSS, CSRF - Rate limiting y hardening de URLs - Terminación SSL con inspección	80%
E4: Movimiento Lateral	- Segmentación por zonas y políticas inter-VLAN - Principio de mínimo privilegio aplicado - Registro detallado de tráfico este-oeste	70%

Escenario	Controles aplicables NGFW	Eficacia estimada de mitigación
	- Detección de anomalías en flujos internos	

Tabla 14: Eficacia de mitigación por escenario, adaptado de (Han,2024).

Estimación basada en documentación técnica de Sophos Firewall y estudios de efectividad de NGFW (Han, 2024).

- Cálculo de ALE reducida (con NGFW implementado)

$$ALE_{reducida} = ALE_{base} \times \left(1 - Eficacia_{mitigación}\right)$$

Escenario	ALE base (C$)	Eficacia mitigación	ALE reducida (C$)	Reducción lograda (C$)
E1: Ransomware	C$ 384,555.15	75%	C$ 96,138.79	C$ 288,416.36
E2: Filtración de Datos	C$ 205,096.08	60%	C$ 82,038.43	C$ 123,057.65
E3: Ataque a Aplicación Web	C$ 181,290.28	80%	C$ 36,285.06	C$ 145,005.22
E4: Movimiento Lateral	C$ 219,745.8	70%	C$ 65,923.74	C$ 153,822.06
ALE Total Reducida	**C$ 990,687.31**		**C$ 280,386.02**	**C$ 710,301.29**

Tabla 15: Pérdida anual esperada - escenario con Sophos Firewall, elaboración propia.

Con la implementación de Sophos Firewall, la pérdida anual esperada se reduce de C$ 990,687.31 a C$ 280,386.02, lo que representa un beneficio anual por mitigación de C$ 710,301.29 (USD $19,394.26).

6.5.5. Cálculo final del ROSI

- Aplicación de la Fórmula ROSI

Variable	Valor (C$)	Valor (USD)
Beneficio de Seguridad (Reducción ALE)	C$ 710,301.29	$ 19,394.26
Costo Anual de la Solución	C$ 211,126	$ 5,737

Tabla 16: Aplicación de la fórmula ROSI, elaboración propia.

$$ROSI = \frac{(710{,}301.29 - 211{,}126)}{211{,}126} \times 100 = \frac{499{,}175.29}{211{,}126} \times 100 = 236.43\%$$

- Interpretación del resultado

Un ROSI del 236.43% indica que:

- Por cada córdoba invertido en la solución de seguridad, la organización obtiene un retorno de C$ 2.36 en pérdidas evitadas.
- El beneficio económico de la mitigación de riesgos supera en más del doble el costo anual de la solución.
- La inversión se considera económicamente viable y estratégicamente justificable bajo los supuestos conservadores aplicados.

- Análisis de sensibilidad

Para evaluar la robustez del resultado, se presenta un escenario pesimista con reducciones en la eficacia de mitigación:

Escenario	Eficacia promedio	Beneficio anual (C$)	ROSI resultante	Viabilidad
Base (conservador)	71.25%	710,301.29	236.43%	Altamente viable
Pesimista	50%	497,720	135.75%	Viable
Muy pesimista	35%	348,404	65.02%	Marginalmente viable

Tabla 17: Análisis de sensibilidad del ROSI, elaboración propia.

Conclusión del análisis de sensibilidad: Incluso bajo supuestos conservadores que reducen a la mitad la eficacia esperada de los controles, el ROSI permanece positivo (135.75%), lo que refuerza la solidez de la recomendación de inversión.

6.5.6. Consideraciones cualitativas y beneficios intangibles

Además del análisis cuantitativo, la implementación de Sophos Firewall genera beneficios estratégicos no monetizables directamente, pero críticos para la organización:

Cumplimiento Normativo: Facilita la adherencia a estándares de seguridad financiera y protección de datos personales, reduciendo riesgo regulatorio futuro.

Confianza de clientes: La protección robusta del portal web fortalece la reputación institucional y la confianza de los usuarios en los servicios digitales.

Continuidad operativa: La reducción de probabilidad de incidentes graves contribuye a la estabilidad del negocio y la capacidad de servir a clientes sin interrupciones.

Visibilidad y gobernanza: El registro centralizado y los reportes del firewall permiten una toma de decisiones informada y una auditoría eficiente de la postura de seguridad.

Escalabilidad técnica: La arquitectura Xstream y el licenciamiento por usuarios ilimitados permiten crecer sin costos marginales significativos por nuevo usuario.

VII. CONCLUSIONES

A partir del desarrollo del presente estudio fue posible analizar la integración del Sophos Firewall como solución de firewall de nueva generación dentro de una arquitectura de red Enterprise escalable, considerando aspectos técnicos, funcionales y económicos asociados a su implementación.

En primer lugar, se logró identificar los elementos técnicos de la red y los requerimientos necesarios para la integración de la solución de seguridad, considerando factores como la segmentación de red, la arquitectura jerárquica de core, distribución y acceso, así como los riesgos derivados de la exposición de servicios hacia redes externas. Este análisis permitió establecer las condiciones necesarias para la incorporación del Sophos Firewall como gateway principal de seguridad.

Asimismo, se desarrolló la formulación de políticas de seguridad en Sophos Firewall orientadas a la protección perimetral de servicios web y al control de acceso basado en VLAN y perfiles de usuario. Mediante la implementación de reglas de firewall, políticas WAF, inspección de tráfico y mecanismos de prevención de intrusiones, se establecieron controles que permiten restringir el acceso a recursos críticos y proteger aplicaciones publicadas frente a amenazas comunes dirigidas a la capa de aplicación.

De igual forma, se realizó el análisis de la efectividad funcional del Sophos Firewall dentro de un escenario Enterprise definido como caso de estudio, utilizando un entorno emulado desarrollado en la plataforma PNETLab. Este laboratorio permitió validar el comportamiento del firewall en un entorno controlado, demostrando la capacidad de la solución para gestionar el tráfico entre distintas zonas de seguridad, aplicar políticas de inspección profunda de paquetes y proteger los servicios expuestos mediante mecanismos de seguridad multicapa.

Finalmente, se llevó a cabo un análisis costo–beneficio basado en el modelo ROSI (Return on Security Investment), con el objetivo de evaluar la viabilidad económica de

la implementación de Sophos Firewall dentro de una infraestructura empresarial. Los resultados obtenidos evidencian que la adopción de una solución de firewall de nueva generación no solo contribuye a fortalecer la postura de seguridad de la organización, sino que también puede representar un retorno positivo de la inversión al reducir los riesgos asociados a incidentes de seguridad y a la posible exposición de información crítica.

En consecuencia, los resultados del estudio permiten concluir que la integración de Sophos Firewall dentro de una arquitectura Enterprise segmentada constituye una alternativa viable tanto desde el punto de vista técnico como económico, proporcionando mecanismos avanzados de protección, control del tráfico y capacidad de adaptación a entornos de red en crecimiento.

VIII. RECOMENDACIONES

La adopción de soluciones de firewall de nueva generación puede fortalecerse mediante la integración de plataformas de gestión y correlación de eventos de seguridad (SIEM), lo cual permite centralizar los registros generados por el firewall y otros sistemas de seguridad. Esta centralización mejora la visibilidad de la infraestructura tecnológica, facilita la detección temprana de incidentes y fortalece los procesos de monitoreo y análisis de eventos dentro de la red.

Asimismo, resulta conveniente considerar la integración con soluciones de detección y respuesta ante amenazas, como MDR (Managed Detection and Response) o XDR (Extended Detection and Response). Estas plataformas permiten correlacionar información proveniente de múltiples fuentes de seguridad, tales como endpoints, servidores, dispositivos de red y servicios en la nube, proporcionando una visión más completa del estado de seguridad de la infraestructura y facilitando la respuesta ante posibles incidentes.

De igual manera, la incorporación de fuentes externas de inteligencia de amenazas (Threat Intelligence) provenientes de terceros permite enriquecer los mecanismos de detección del firewall mediante información actualizada sobre direcciones IP maliciosas, dominios comprometidos y patrones de ataque emergentes. Esto contribuye a fortalecer los controles de seguridad y mejorar la capacidad de prevención ante amenazas conocidas.

Finalmente, resulta pertinente evaluar la implementación de arquitecturas de alta disponibilidad (High Availability) para los dispositivos de firewall, con el fin de garantizar la continuidad operativa de los servicios de red ante posibles fallas de hardware o interrupciones del equipo principal. La utilización de configuraciones redundantes permite mantener la disponibilidad de los servicios críticos y reducir el impacto de incidentes que puedan afectar la infraestructura de seguridad.

IX. BIBLIOGRAFÍA

Abarca, S., & Luna , J. A. (2015). Solución de autenticación para redes WLAN mediante protocolo RADIUS y dispositivos AP unifi en la empresa ABC. León. Obtenido de http://riul.unanleon.edu.ni:8080/jspui/bitstream/123456789/4968/1/230516.pdf

Abarca, S., & Luna, J. A. (2015). Solución de autenticación para redes WLAN mediante protocolo RADIUS y dispositivos AP unifi en la empresa ABC. León.

Aguaza, O. (2012). Análisis Coste-Beneficio. Obtenido de https://portaldelainvestigacion.uma.es/documentos/663137d638b3d85bb144f19c

Aguilar, J. M. (2012). Desarrollo de una interfaz de configuración para la herramienta TC e implementación del protocolo RADIUS en la red inalámbrica de la UNAN-RUCFA. León, Nicaragua. Obtenido de http://riul.unanleon.edu.ni:8080/jspui/handle/123456789/6019

CEIM. (2024). Informe sobre ciberseguridad y su impacto en las empresas. Obtenido de https://ceim.es/documento/publication-document-1736782515.pdf

checkpoint. (2025). checkpoint. Obtenido de https://www.checkpoint.com/es/cyber-hub/threat-prevention/what-is-malware/

Cisco, S. (2018). Cisco Collaboration System 12.x Solution Reference Network Designs – Network Infrastructure. Obtenido de Cisco: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab12/collab12/netstruc.html

Cloud Google. (s.f.). TLS inspection overview. Obtenido de Google Cloud firewall Docs: https://cloud.google.com/firewall/docs/about-tls-inspection

cloudflare.com. (s.f.). Obtenido de ¿Qué es un enrutador?: https://www.cloudflare.com/es-la/learning/network-layer/what-is-a-router/

Cruz, D. A., Cardoza, C. J., & Espinoza, K. S. (2023). Diseño de una Red Privada Virtual Dinamica Multipunto (DMVPN) para renovar la tecnología WAN de la empresa Megabyte S.A. Managua, Nicaragua.

DBIR, V. (2025). 2025 Data Breach Investigations Report.

Espin, D. O. (2022). Diseño e implementación de un firewall de nueva generación usando herramientas de código abierto para el instituto superior tecnológico libertad. Quito-Ecuador. Obtenido de http://dspace.ups.edu.ec/handle/123456789/23007

Forouzan, B. A. (2007). Data communications and networking. New York: MacGraw-Hill.

FORTINET. (s.f.). What is cibersecurity? Recuperado el Octubre 20, 2025, de https://www.fortinet.com/resources/cyberglossary/what-is-cybersecurity?

Fuentes, J. F., & Guido, R. J. (2018). Implementación de la tecnología MPLS en el emulador GNS3 con propositos academicos. Managua. Obtenido de https://ribuni.uni.edu.ni/2313/1/93027.pdf

Halley, J., Prajapati, D., Leza, A., & & Saini, V. (2025). Zero Trust in Resilient Cloud and Network Architectures. Cisco Press. Obtenido de https://ptgmedia.pearsoncmg.com/images/9780138204600/samplepages/9780138204600_Sample.pdf

Han, J. (2024, 07 4). Sophos Named a 2024 Gartner® Peer Insights™ Customers' Choice for Network Firewalls and Endpoint Protection Platforms. Obtenido de https://www.sophos.com/en-us/blog/sophos-named-a-2024-gartner-peer-insights-customers-choice-for-network-firewalls-and-endpoint-protection-platforms

HUAWEI. (2024, ENERO 17). HUAWEI. Obtenido de https://forum.huawei.com/enterprise/intl/es/thread/introducci%C3%B3n-tecnolog%C3%ADa-de-transferencia-de-datos-mpls/747756033549418496?blogId=747756033549418496

IBM. (2025). Cost of a Data Breach Report 2025. Obtenido de https://www.ibm.com/reports/data-breach

introducción a los firewalls. (2025). Obtenido de Cisco.com: https://www.cisco.com/site/us/en/learn/topics/security/what-is-a-firewall.html

IR teams. (s.f.). Deep Packet Inspection (DPI): How it works and why it's important. Obtenido de https://www.ir.com/guides/deep-packet-inspection

Kurose , J. F., & Ross, K. W. (2017). Redes de computadoras. Un enfoque descendente. Madrid: Pearson.

López, J. B. (2012, 11 30). Estudio de viabilidad sobre la inversión en seguridad informática para las PYMES. Obtenido de http://bdigital.dgse.uaa.mx:8080/xmlui/handle/11317/2672

McCarthy, C. (2023). Network Segmentation and Zero Trust: A Practical Guide. Pearson. Obtenido de https://ptgmedia.pearsoncmg.com/images/9780138204600/samplepages/9780138204600_Sample.pdf

McCormack, C. (2022, Marzo 24). Xstream Fastpath in SFOS v19. Obtenido de Sophos: https://www.sophos.com/en-us/blog/xstream-fastpath-in-sfos-v19

Microsoft. (s.f.). Filtrado de contenido web. Obtenido de Microsoft Learn: https://learn.microsoft.com/es-es/defender-endpoint/web-content-filtering

Nicaragua, B. C. (2026). BCN publica tipo de cambio oficial del año 2026. Obtenidode https://www.bcn.gob.ni/node/10376

NIST. (2020, 12 10). Security and Privacy Controls for Information Systems and Organizations. Obtenido de https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

Obando, M. A., Gonzalez, M. A., & Tardencilla, O. O. (2023). Diseño de una red SD-WAN para la interconexión de las sucursales de la empresa EDISA. Managua.

Oppenheimer, P. (2010). Top-Down Network Design. Indianapolis, IN: Cisco Press. Obtenido de https://faculty.kfupm.edu.sa/COE/marwan/richfiles/Cisco.Press.Top-Down.Network.Design.3rd.Edition.Aug.2010.pdf

Penaloza Seijas, D. S. (2018, Junio 28). CISCO Community. Obtenido de https://community.cisco.com/t5/documentos-routing-y-switching/introducci%C3%B3n-a-mpls/ta-p/3407436

Sophos Firewall. (2024). Sophos Firewall Features and the atack kill chain.

Sophos Firewall. (2024, Enero). Sophos Firewall Web Protection Overview. Obtenido de Sophos.com

Sophos Firewall. (2025). Getting Started with Firewall and NAT Rules on Sophos Firewall. Obtenido de Sophos.com

Sophos Firewall. (2025). What is Sophos Firewall.

What are network switches. (2025, October 16). Obtenido de www.hpe.com: https://www.hpe.com/emea_middle_east/en/what-is/network-switch.html

What Is Multiprotocol Label Switching. (2025). Obtenido de www.paloaltonetworks.com: https://www.paloaltonetworks.com/cyberpedia/mpls-what-is-multiprotocol-label-switching

Wirton, C. G. (2021, 06). Ciberseguridad en el Sector Financiero. Obtenido de ¿Cómo transformar una amenaza en una oportunidad?: https://repositorio.comillas.edu/xmlui/bitstream/handle/11531/46570/TFG-Garcia%20Wirton%2C%20Carlota.pdf

X. ANEXOS

Anexo A: Cotización y dimensionamiento de Sophos NGFW

No. ITEM	DESCRIPCIÓN	CANTIDAD	PRECIO UNITARIO	TOTAL
1	Adquisicion de 01 equipo SOPHOS XGS 2100, que incluye: 8 GE + 2 SFP ports, 1 expansion bay for optional Flexi Port module, SSD + Base License (incl. FW, VPN & Wireless) for unlimited users + power cable	1	C$ 91,741.50	C$ 91,741.50
2	Licenciamiento Xstream Protection for 36 MONTHS	1	C$ 292,873.50	C$ 292,873.50
3	Licenciamiento Webserver Protection for 36 MONTHS	1	C$ 44,011.50	C$ 44,011.50
	Sub-Total			**C$ 428,626.50**

Tabla 18: Compra de equipos requeridos para la red, adaptado de (Grupo Intelector, 2026).

SERVICIOS				
1	Costos de Importación y aseguramiento de la carga	1	C$ 14,979.45	C$ 14,979.45
2	Instalación y Configuración con Ingenieros Certificados	1	C$ 42,862.65	C$ 42,862.65

SERVICIOS				
3	Soporte 7x24 con Ingenieros de Certificados en la solución ofertada por un año.	1	C$ 64,294.16	C$ 64,294.16
	Sub Total			**C$ 122,136.26**
	SUB TOTAL			**C$ 550,762.76**
	IVA (15%)			**C$ 82,614.41**
	TOTAL INVERSION			**C$ 633,377.17**

Tabla 19: Cotización, adaptado de (Grupo Intelector, 2026).

Anexo B: Topología de red del escenario Enterprise

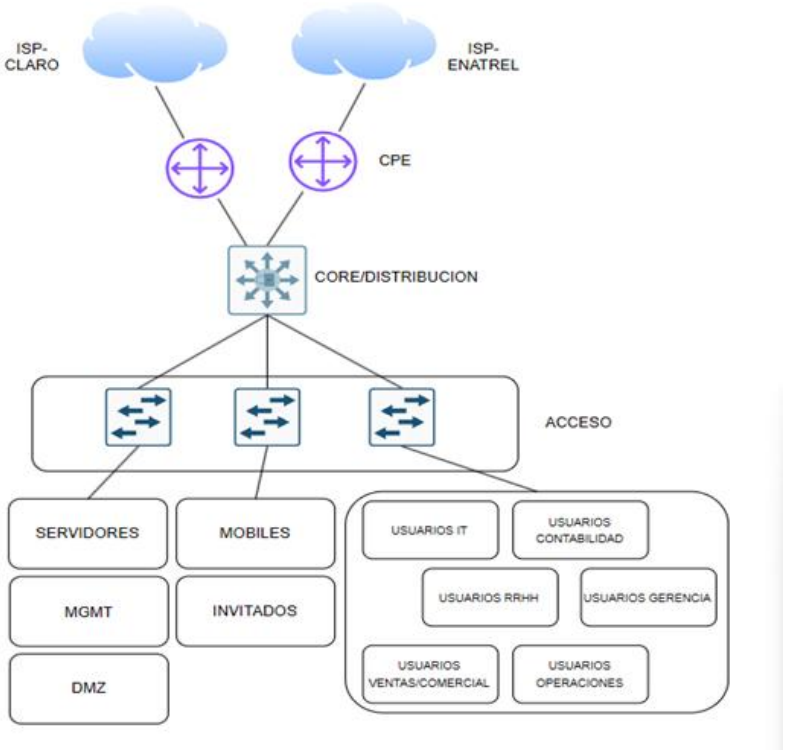


Figura 34: Diagrama de Red Casa Matriz, elaboración propia.

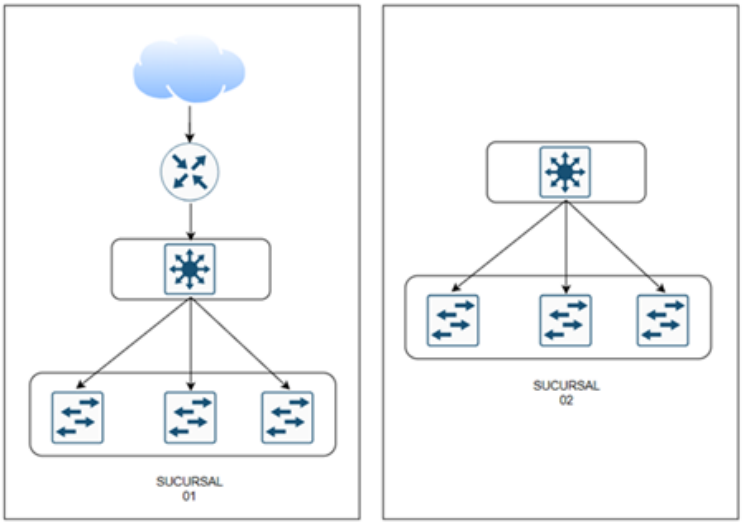


Figura 35: Diagrama de red sucursales, elaboración propia.

Anexo C: Segmentación lógica de la red

Sitio	VLAN	Segmento	Red (CIDR)	Gateway Core	Hosts útiles	Definidos (usuarios/equipos)
Casa Matriz	50	Usuarios – IT	10.0.10.0/28	10.0.10.1	14	3
Casa Matriz	60	Usuarios – Contabilidad	10.0.10.16/28	10.0.10.17	14	3
Casa Matriz	70	Usuarios – RRHH	10.0.10.32/28	10.0.10.33	14	3
Casa Matriz	80	Usuarios – Ventas / Comercial	10.0.10.48/28	10.0.10.49	14	3
Casa Matriz	90	Usuarios – Operaciones /	10.0.10.64/28	10.0.10.65	14	3

Sitio	VLAN	Segmento	Red (CIDR)	Gateway Core	Hosts útiles	Definidos (usuarios/equipos)
		Administración				
Casa Matriz	100	Usuarios – Gerencia / Dirección	10.0.10.80/28	10.0.10.81	14	2
Casa Matriz	110	MOBILES	10.0.10.128/26	10.0.10.129	62	15
Casa Matriz	120	WiFi Invitados (Aparte)	10.0.30.0/26	10.0.30.1	62	20
Casa Matriz	20	Servidores (Aparte)	10.0.20.0/27	10.0.20.1	30	12
Casa Matriz	30	DMZ (Aparte)	10.0.21.0/28	10.0.21.1	14	6
Casa Matriz	40	Gestión MGMT (Aparte)	10.0.22.0/28	10.0.22.1	14	8
Sucursal 1	210	Usuarios	10.0.11.0/26	10.0.11.1	62	12
Sucursal 1	220	Camaras	10.0.11.64/28	10.0.11.65	14	6
Sucursal 2	310	Usuarios	10.0.11.128/26	10.0.11.129	62	12
Sucursal 2	320	Camaras	10.0.11.192/28	10.0.11.193	14	6

Tabla 20: Tabla VLSM, elaboración propia

GRUPOS	Autenticación AD	Proxy Web	Política Base
Usuarios IT	Obligatoria	Sí	Deny by default
Contabilidad	Obligatoria	Sí	Deny by default
RRHH	Obligatoria	Sí	Deny by default
Gerencia	Obligatoria	Sí	Deny by default
Ventas	Obligatoria	Sí	Deny by default
Operaciones	Obligatoria	Sí	Deny by default

Tabla 21: Matriz general de control de navegación, elaboración propia.

Perfiles	Perfil: Contabilidad		Perfil: Usuarios IT		Perfil: RRHH	
Nº	Categoría web	Aplicación	Categoría web	Aplicación	Categoría web	Aplicación
1	Finance	Microsoft Outlook	Information Technology	Remote Desktop	Government	Microsoft Outlook
2	Banking	ERP financiero	Software Updates	Secure Shell (SSH)	Job Search & Career	RRHH SaaS
3	Accounting	Microsoft Teams	Software Development	Microsoft Teams	Human Resources	Microsoft Teams
4	Business & Economy	Web Conferencing corporativo	IT Help & Support	Microsoft Outlook	Business & Economy	Secure File Transfer

Perfiles	Perfil: Contabilidad		Perfil: Usuarios IT		Perfil: RRHH	
5	Email	VPN corporativo	Business & Economy	Windows Update	Email	Cloud Storage corporativo
6	Government	Secure File Transfer	Reference & Research	WSUS	Cloud Services	PDF Reader
7	Cloud Services	Cloud Accounting Apps	News & Media	Git	Productivity Tools	Web Conferencing
8	Productivity Tools	PDF Reader	Cloud Services	VPN corporativo	Health & Safety	VPN corporativo
9	Tax & Legal	Time Sync Tools	Email	Network Monitoring Tools	Reference & Research	Time Sync Tools
10	Reference & Research	Aplicaciones SaaS financieras	Productivity Tools	IT Support Tools	News & Media	Document Management Tools

Tabla 22: Matriz general de control de navegación, elaboración propia.

Perfiles	Perfil: Operaciones		Perfil: Ventas	
Nº	**Categoría web**	**Aplicación**	**Categoría web**	**Aplicación**
1	Business & Economy	Microsoft Teams	Sales & Marketing	CRM oficial

Perfiles	Perfil: Operaciones		Perfil: Ventas	
2	Operations Tools	Productivity Suite	CRM Tools	Microsoft Teams
3	Cloud Services	Operational Tools	Business & Economy	Microsoft Outlook
4	Productivity Tools	Enterprise Messaging	Cloud Services	Sales Tools
5	Email	VPN corporativo	Email	Web Conferencing
6	Government	Secure Remote Clients	Productivity Tools	VPN corporativo
7	Manufacturing	Monitoring Services	Advertising	Cloud Analytics
8	Reference & Research	Time Sync Tools	Collaboration Tools	Sales Enablement
9	Collaboration Tools	Secure File Transfer	News & Media	Secure File Transfer
10	News & Media	Network Management Tools	Reference & Research	Time Sync Tools

Tabla 23: Matriz general de control de navegación, elaboración propia.

Anexo D: Repositorio de imágenes PnetLab.

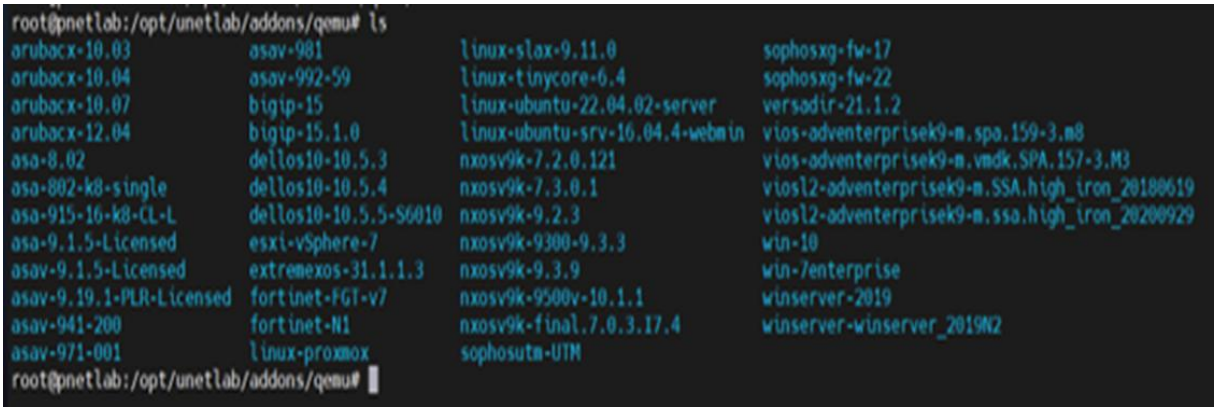


Figura 36: Repositorio de Imágenes en Pnetlab, elaboración propia.

Anexo E: Configuración de políticas en Sophos Firewall

VPN IPsec MATRIZ -SUCURSAL01			
Categoría	**Parámetro**	**Casa Matriz (Sophos Firewall)**	**Sucursal01 (Peer)**
General	Nombre de la VPN	VPNSUCURSAL01	VPNMATRIZ
	Tipo de conexión	Route-based (Tunnel interface)	Route-based (Tunnel interface)
	Versión IP	Dual (IPv4 / IPv6)	Dual (IPv4 / IPv6)
	Gateway type	Initiate the connection	Respond Only Connection
	Activación automática	Sí	N/A

VPN IPsec MATRIZ -SUCURSAL01			
Categoría	**Parámetro**	**Casa Matriz (Sophos Firewall)**	**Sucursal01 (Peer)**
Autenticación	Método de autenticación	Preshared Key (Rjz#lk1V^Byf%71@XU5S)	Preshared Key (Rjz#lk1V^Byf%71@XU5S)
	Perfil IPsec	Head office (IKEv2)	Head office (IKEv2)
Local Gateway	Interfaz	PortD – 10.0.137.121	10.0.137.42
	Local ID type	IP address	IP address
	Local ID	10.0.137.121	10.0.137.42
Remote Gateway	Gateway address	10.0.137.42	10.0.137.121
	Remote ID type	IP address	IP address
	Remote ID	10.0.137.42	10.0.137.121

Tabla 24: Matriz de configuración VPN IPsec entre sucursal 1 y casa matriz, elaboración propia.

VPN IPsec MATRIZ -SUCURSAL01			
Categoría	**Parámetro**	**Casa Matriz (Sophos Firewall)**	**Sucursal01 (Peer)**
Phase 1 (IKE)	Key exchange	IKEv2	IKEv2
	Authentication mode	Main mode	Main mode
	Key lifetime	12600 s	12600 s
	DH Groups	14, 16, 18, 19, 21, 31	14, 16, 18, 19, 21, 31
	Encryption	AES-256	AES-256

VPN IPsec MATRIZ -SUCURSAL01			
Categoría	**Parámetro**	**Casa Matriz (Sophos Firewall)**	**Sucursal01 (Peer)**
	Authentication	SHA2-512 / SHA2-384 / SHA2-256	SHA2-512 / SHA2-384 / SHA2-256
Phase 2 (IPsec)	PFS group	Same as Phase-1	Same as Phase-1
	Key lifetime	5400 s	5400 s
	Encryption	AES-256	AES-256
	Authentication	SHA2-512 / SHA2-384 / SHA2-256	SHA2-512 / SHA2-384 / SHA2-256

Tabla 25: Matriz de configuración VPN IPsec entre sucursal 1 y casa matriz, elaboración propia.

Anexo F: Registros de Eventos y Resultados de Pruebas de Seguridad del Sophos Firewall

Application filter	2026-03-12 02:22:21	Denied	usuarioventa@capital.local	10.0.11.131	142.251.211.238	Infrastructure	Secure Socket Layer Protocol
Application filter	2026-03-12 02:22:21	Denied	usuarioventa@capital.local	10.0.11.131	142.251.211.238	Infrastructure	Secure Socket Layer Protocol
Application filter	2026-03-12 02:22:21	Denied	usuarioventa@capital.local	10.0.11.131	142.251.211.238	Infrastructure	Secure Socket Layer Protocol
Application filter	2026-03-12 02:22:21	Denied	usuarioventa@capital.local	10.0.11.131	142.251.211.238	Infrastructure	Secure Socket Layer Protocol
Application filter	2026-03-12 02:21:03	Denied	usuarioventa@capital.local	10.0.11.131	142.251.211.238	Infrastructure	Secure Socket Layer Protocol

Figura 37: Logs Bloqueos Application Control, elaboración propia.

Web filter	2026-03-12 02:20:46	Allowed	12	10.0.11.131	142.251.211.238	usuarioventa@capital.local	Search Engines	17	VENTAS-WP	https://clients2.google.com/	
Web filter	2026-03-12 02:20:46	Allowed	12	10.0.11.131	142.251.211.238	usuarioventa@capital.local	Search Engines	17	VENTAS-WP	https://clients2.google.com/	
Web filter	2026-03-12 02:20:46	Denied	12	10.0.11.131	216.239.32.116	usuarioventa@capital.local	Information Technology	17	VENTAS-WP	https://beacons5.gvt2.com/domainr	
Web filter	2026-03-12 02:20:46	Allowed	12	10.0.11.131	142.251.211.238	usuarioventa@capital.local	Search Engines	17	VENTAS-WP	https://clients2.google.com/	
Web filter	2026-03-12 02:20:46	Denied	12	10.0.11.131	142.251.35.99	usuarioventa@capital.local	Information Technology	17	VENTAS-WP	https://beacons3.gvt2.com/domainr	
Web filter	2026-03-12 02:20:45	Denied	12	10.0.11.131	216.239.32.116	usuarioventa@capital.local	Information Technology	17	VENTAS-WP	https://beacons5.gvt2.com/domainr	

Figura 38: Logs Bloqueos Web Filter, elaboración propia.

Web server rotection	2026-03-12 01:18:06	185.16.39.146	/	WAF Anomaly	Inbound Anomaly Score Exceeded (Total Score: 5)	403	68	344	17071
Web server rotection	2026-03-12 01:14:37	193.24.211.224	/.git/config	WAF Anomaly	Inbound Anomaly Score Exceeded (Total Score: 10)	403	109	344	17071
Web server rotection	2026-03-12 01:11:45	185.16.39.146	/	WAF Anomaly	Inbound Anomaly Score Exceeded (Total Score: 5)	403	68	344	17071
Web server rotection	2026-03-12 01:05:39	185.16.39.146	/	WAF Anomaly	Inbound Anomaly Score Exceeded (Total Score: 5)	403	68	344	17071
Web server rotection	2026-03-12 01:02:01	45.156.129.189	/	-	-	200	191	836	17071

Figura 39: Logs Bloqueos WAF, elaboración propia.

Authentication	2026-03-12 02:22:37	Firewall Authentication	Successful	sophosfw@capital.local	10.0.20.1	CTA	N/A	User sophosfw@capita
Authentication	2026-03-12 02:22:24	Firewall Authentication	Successful	usuarioventa@capital.local	10.0.11.131	CTA	N/A	User usuarioventa@cap
Authentication	2026-03-12 02:13:47	Firewall Authentication	Successful	sophosfw@capital.local	10.0.20.1	CTA	AD	User sophosfw@capita
Authentication	2026-03-12 02:13:46	Firewall Authentication	Successful	usuarioventa@capital.local	10.0.11.131	CTA	AD	User usuarioventa@cap 10.0.11.131
Authentication	2026-03-12 02:12:27	Firewall Authentication	Successful	sophosfw@capital.local	10.0.20.1	CTA	N/A	User sophosfw@capita
Authentication	2026-03-12 02:12:13	Firewall Authentication	Successful	usuarioventa@capital.local	10.0.11.131	CTA	N/A	User usuarioventa@cap
Authentication	2026-03-12 02:03:30	Firewall Authentication	Successful	sophosfw@capital.local	10.0.20.1	CTA	AD	User sophosfw@capita

Figura 40: Logs STAS, elaboración propia.

VPN	2026-03-11 21:04:27	SSL VPN	Terminated	soporteit	SSL VPN User 'soporteit' disconnected
VPN	2026-03-11 21:02:44	SSL VPN	Established	soporteit	SSL VPN User 'soporteit' connected
Authentication	2026-03-11 21:02:42	SSL VPN Authentication	Successful	soporteit	User soporteit authenticated successfully to login to SSLVPN through Local authentication mechanism
VPN	2026-03-11 20:38:56	SSL VPN	Terminated	soporteit	SSL VPN User 'soporteit' disconnected
VPN	2026-03-11 19:23:05	SSL VPN	Established	soporteit	SSL VPN User 'soporteit' connected

Figura 41: Logs VPN SSL, elaboración propia.

10.0.11.11 Add filter Timer filter

	Time	Log comp	Log subtype	Username	Firewall rule	Firewall rule name	NAT rule	NAT rule name	In interface	Out interface	Src IP	Dst IP	Src port	Dst port	Protocol	Rule type	Live PCAP
Firewall	2026-03-12 02:31:33	Firewall Rule	Allowed		3	FWR_INBOUND_SUCU...	0		xfrm2	PortC.20	10.0.11.11	10.0.20.5	53283	389	UDP	1	Open PCAP
Firewall	2026-03-12 02:31:30	Firewall Rule	Allowed		3	FWR_INBOUND_SUCU...	0		xfrm2	PortC.20	10.0.11.11	10.0.20.5	53282	53	UDP	1	Open PCAP
Firewall	2026-03-12 02:28:26	Firewall Rule	Allowed		3	FWR_INBOUND_SUCU...	0		xfrm2	PortC.20	10.0.11.11	10.0.20.5	61862	445	TCP	1	Open PCAP
Firewall	2026-03-12 02:18:54	Firewall Rule	Allowed		3	FWR_INBOUND_SUCU...	0		xfrm2	PortC.20	10.0.11.11	10.0.20.5	50209	53	UDP	1	Open PCAP
Firewall	2026-03-12 02:18:49	Firewall Rule	Allowed		3	FWR_INBOUND_SUCU...	0		xfrm2	PortC.20	10.0.11.11	10.0.20.5	50210	389	UDP	1	Open PCAP
Firewall	2026-03-12 02:18:06	Firewall Rule	Allowed		3	FWR_INBOUND_SUCU...	0		xfrm2	PortC.20	10.0.11.11	10.0.20.5	62829	53	UDP	1	Open PCAP
Firewall	2026-03-12 02:13:24	Firewall Rule	Allowed		3	FWR_INBOUND_SUCU...	0		xfrm2	PortC.20	10.0.11.11	10.0.20.5	61858	445	TCP	1	Open PCAP
Firewall	2026-03-12 02:06:07	Firewall Rule	Allowed		3	FWR_INBOUND_SUCU...	0		xfrm2	PortC.20	10.0.11.11	10.0.20.5	61360	389	UDP	1	Open PCAP
Firewall	2026-03-12 02:06:03	Firewall Rule	Allowed		3	FWR_INBOUND_SUCU...	0		xfrm2	PortC.20	10.0.11.11	10.0.20.5	61359	53	UDP	1	Open PCAP
Firewall	2026-03-12 01:58:32	Firewall Rule	Allowed		3	FWR_INBOUND_SUCU...	0		xfrm2	PortC.20	10.0.11.11	10.0.20.5	55278	53	UDP	1	Open PCAP
Firewall	2026-03-12 01:58:30	Firewall Rule	Allowed		3	FWR_INBOUND_SUCU...	0		xfrm2	PortC.20	10.0.11.11	10.0.20.5	61854	445	TCP	1	Open PCAP
Firewall	2026-03-12 01:53:24	Firewall Rule	Allowed		3	FWR_INBOUND_SUCU...	0		xfrm2	PortC.20	10.0.11.11	10.0.20.5	52202	53	UDP	1	Open PCAP

Figura 42: Logs VPN IPsec (Comunicación Sucursal01 a AD), elaboración propia.