Universitat Oberta de Catalunya

uoc.edu

Elaboración de un plan de aplicación de tecnologías SASE y Zero Trust

Jordi Guillem Ferrer Bozzano
Máster Universitario en Ciberseguridad y Privacidad
Seguridad empresarial

Iñaki Moreno Fernández
Víctor García Font

10 de enero de 2023


Esta obra está sujeta a una licencia de Reconocimiento-NoComercial-CompartirIgual 3.0 España de Creative Commons

Este trabajo de fin de máster está dedicado a:

A mi mujer y mis dos hijas quienes por su inagotable paciencia y amor han hecho posible que pueda ir logrando mis metas, gracias a las tres por acompañarme en todos los momentos importantes de mi vida.

A mis padres y mis hermanos por todo su cariño, apoyo y confianza que gracias a sus consejos y palabras me han hecho ser una mejor persona.

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Elaboración de un plan de aplicación de tecnologías SASE y Zero Trust*
Nombre del autor:	*Jordi Guillem Ferrer Bozzano*
Nombre del consultor/a:	*Iñaki Moreno Fernández*
Nombre del PRA:	*Víctor García Font*
Fecha de entrega (mm/aaaa):	*01/2023*
Titulación o programa:	*Máster Universitario en Ciberseguridad y Privacidad*
Área del Trabajo Final:	*Seguridad empresarial*
Idioma del trabajo:	*Castellano*
Palabras clave	*Zero Trust* *SASE* Seguridad en el perímetro

Resumen del Trabajo

La finalidad de este trabajo es estudiar las ventajas que ofrece la adopción de un marco de arquitectura SASE en el mundo empresarial e implementar una prueba de valor en una organización. Para ello, se estudian los componentes principales como el Next Generation *Secure Web Gateway* (NG SWG), *Zero Trust Network Access* (ZTNA), *Cloud Access Security Broker* (CASB), *Firewall as a Service* (FWaaS), *Data protection* y otros conceptos interesantes.

Seguidamente, se realiza un estudio de los proveedores en el mercado que ofrecen soluciones SASE y se selecciona uno de ellos. Mediante el análisis de diversos casos de uso se analiza e implementa en una organización una solución de navegación web segura en la nube (NG SWG) y una solución de confianza cero para el acceso a recursos internos (ZTNA). Adicionalmente, se implementa un control de las acciones que se realizan en el acceso a aplicaciones SaaS (CASB) y se implementa un caso de prevención de pérdida de datos sensibles (DLP). Todos estas soluciones ubicadas y diseñadas en la nube con una gestión centralizada de las políticas de seguridad desde un único punto.

La transformación en la seguridad es necesaria para que las organizaciones puedan conseguir sus objetivos estratégicos y para ello es importante adoptar una arquitectura de seguridad convergente en la nube como es SASE.

Abstract

The purpose of this paper is to study the benefits of adopting a SASE architecture framework in the enterprise world and to implement a proof of value in an organization. To do this, the main components such as Next Generation Secure Web Gateway (NG SWG), Zero Trust Network Access (ZTNA), Cloud Access Security Broker (CASB), Firewall as a Service (FWaaS), Data protection and other interesting concepts are studied.

Next, a survey of the vendors in the market offering SASE solutions is carried out and one of them is selected. Through the analysis of several use cases, a secure web browsing solution in the cloud (NG SWG) and a zero trust solution for access to internal resources (ZTNA) are analyzed and implemented in an organization. Additionally, a control of the actions performed on access to SaaS applications (CASB) and a case of prevention of loss of sensitive data (DLP) is implemented. All these solutions are located and designed in the cloud with centralized management of security policies from a single point.

Security transformation is necessary for organizations to achieve their strategic objectives and for this it is important to adopt a converged security architecture in the cloud such as SASE.

Índice

Índice de ilustraciones

1. Introducción

1.1. Contexto y justificación del Trabajo

La **transformación digital** hacia la nube se está transformando rápidamente, acelerada sobre todo por la pandemia mundial del COVID-19 vivida en los últimos años, y con más frecuencia trabajamos con aplicaciones e infraestructura en la nube con el objetivo de aprovechar las ventajas organizativas de eficiencia, velocidad y agilidad empresarial.

Los datos y servicios de las organizaciones están migrando a la nube y ello implica que estos activos ya no residan en sus centros de datos *on premises*[1] sino que viajen a un entorno de nube o multi nube. Este nuevo paradigma de trabajo rompe las barreras tradicionales y obliga a que los departamentos de seguridad de las organizaciones afronten retos cada vez más difíciles y que deban replantearse su seguridad. Un claro ejemplo es el auge del teletrabajo que permite el acceso del personal a recursos internos desde Internet.

Podemos decir claramente que la **transformación de la seguridad** es necesaria para poder lograr y mantener el éxito en los diferentes proyectos de transformación digital y juntas deben de ir alineadas, el hecho que la transformación digital vaya de la mano con la transformación de la seguridad da la oportunidad de que ambas formen parte de la estrategia empresarial desde un inicio.

Uno de los retos importantes en esta transformación es que la seguridad sea más **inteligente** protegiendo al personal en una organización independientemente donde se encuentre para posteriormente poder aplicar controles de accesos que validen la autenticación y otros factores en la conexión. Otro reto importante es **proteger y seguir a los datos** independientemente de donde residan o viajen con el objetivo de proteger el acceso y proteger el uso de estos.

Es importante mencionar que toda esta transformación no es posible sin una **experiencia de persona** positiva, el rendimiento de trabajo del personal empleado o externo no debe de verse afectada por la seguridad. El objetivo es que la persona trabaje cómodamente sin complejidades y aportándole protección y tranquilidad en materia de ciberseguridad en su trabajo diario.

Los sistemas de seguridad del pasado no han nacido ni están diseñados para la nube con lo que para poder enfrentarnos a estos retos nos centraremos en una solución de seguridad diseñada para la nube llamada **Secure Access Service Edge** (SASE).

SASE es un marco para poder implementar una infraestructura de seguridad convergente basada en la nube con el objetivo de proteger a los datos, aplicaciones, servicios y datos. Es un nuevo paradigma de seguridad donde se

[1] Un centro de datos on premises significa en las instalaciones del cliente.

desvanece el perímetro físico y se desacoplan o desdibujan los perímetros de seguridad tradicionales. Cabe destacar que los centros de datos dejan de ser el foco principal en las infraestructuras de seguridad y se convierten en un destino más en la arquitectura SASE.

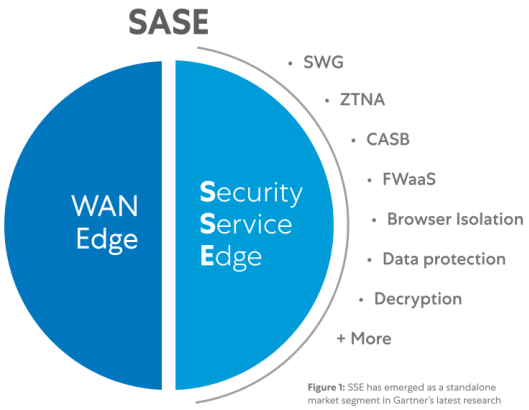


Ilustración 1: Elementos SASE
de https://www.zscaler.es/resources/security-terms-glossary/what-is-security-service-edge

Este trabajo tiene como objetivo estudiar los diferentes componentes que forman una arquitectura SASE definiendo cada uno de los conceptos como son el *Secure Web Gateway* (SWG), *Zero Trust Network Access* (ZTNA), *Cloud Access Security Browser* (CASB), *Firewall as a Service* (FWaaS), *Data protection* y más conceptos interesantes. Para poder poner en práctica los conocimientos adquiridos se va a realizar una prueba de valor (PoV) la cual va a enseñar como se implanta una arquitectura SASE en una organización.

1.2. Objetivos del Trabajo

Los objetivos de este trabajo son:

- Implementar una solución de navegación web segura en la nube para las personas de una organización independientemente del lugar de donde se encuentren.

- Implementar una solución de acceso de confianza cero evaluando la identidad y el contexto de la conexión a los recursos internos de una organización para las personas que trabajan remotamente.

- Identificar la extracción no aprobada de datos sensibles y confidenciales de una organización realizada entre o hacia instancias de aplicaciones en la nube.

- Gestionar y controlar de una manera centralizada en una sola consola los componentes de seguridad en la nube que forman parte de la arquitectura *SASE*.

1.3. Impacto en sostenibilidad, ético-social y de diversidad

Los impactos de las tres dimensiones de la competencia de compromiso ético y global (CCEG)[2] en una implantación de una solución SASE son importantes para ser sostenibles, éticos, defensores de los derechos humanos y responsables sociales.

En la dimensión de **sostenibilidad** se obtiene un impacto positivo basado en la reducción del consumo energético del dentro de datos local *on premise* debido a que una solución SASE permite la reducción de hardware empleado para la seguridad perimetral de la organización. Aunque este consumo energético se traspasa a la nube, la reutilización de recursos energéticos para cientos o miles de clientes y la selección de un proveedor que cumpla con los estándares de centro de datos ecológicos (Certificación LEED) es un claro beneficio medioambiental y de sostenibilidad.

En la dimensión de **comportamiento ético y responsabilidad social,** no se obtiene ningún impacto negativo o positivo, aunque el cambio de paradigma de seguridad basado en la nube con una solución SASE pueda ocasionar un cambio organizativo y posible cambios de personal y empresas proveedoras, es fruto del avance digital y tecnológico. Por otro lado, no se ve un comportamiento poco ético por parte de las personas que usan la solución ni las personas que lo ofrecen.

En la dimensión de **diversidad, género y derechos humanos** se obtiene un impacto negativo basado en la poca presencialidad de *Points of presence* (PoPs)[3], esto ocurre en algunos países dentro de los continentes como África, Asia y América del Sur provocando que las organizaciones que residen en estos países no puedan disponer de una experiencia de persona tan positiva como la que tienen otros donde hay más presencialidad de PoPs.

1.4. Enfoque y método seguido

Este proyecto está enfocado para las organizaciones que necesitan transformar su seguridad adaptando un marco SASE rompiendo las barreras perimetrales tradicionales con el objetivo de proteger a sus empleados y activos y poder así adaptarse rápidamente a los cambios tecnológicos y digitales. Se puede diferenciar una fase de investigación, una fase de análisis y una fase de implementación:

En la **fase de investigación** se estudian y definen los conceptos que forman parte de una solución SASE, qué proveedores se adecuan al proyecto y cuales permiten realizar una prueba de concepto PoC y prueba de valor PoV.

[2] CCEG significa actuar de manera honesta, ética, sostenible, socialmente responsable y respetuosa con los derechos humanos y la diversidad, tanto en la práctica académica como en la profesional, y diseñar soluciones para mejorar estas prácticas.

[3] *Points of presence* (PoP) es un lugar físico donde un proveedor de servicios tiene equipamiento.

En la **fase de análisis** se estudia la empresa ficticia donde se va a implantar las soluciones SASE, se analiza la situación actual (As is), la situación futura (To be) como también los requerimientos y objetivos a cumplir.
En la **fase de implementación** se lanzan diferentes pruebas de concepto PoC que permiten evaluar las soluciones de seguridad SASE y probarlas en un entorno semi real con el objetivo de preparar unos casos de uso que sirvan para lanzar una prueba de valor PoV. La diferencia entre una prueba de concepto PoC y prueba de valor PoV es que en la PoC se prueba que las soluciones de seguridad propuestas funcionan mientras que en la PoV se prueba si estas sirven realmente para la empresa u organización.

La metodología utilizada para la realización de este proyecto es en cascada o *waterfall* la cual tiene un diseño secuencial y cada fase no empieza hasta que la anterior no ha finalizado. Se establecen puntos de control cada quince días con el director de proyecto para hacer un seguimiento del trabajo.

La estrategia llevada a cabo para poder conseguir los objetivos del proyecto se considera adecuada porque la investigación, análisis y pruebas realizadas en este proyecto van alineadas con la implantación de una solución SASE en una empresa real, este hecho ha facilitado poder realizar una PoC y PoV con diferentes soluciones y poder elegir la adecuada.

1.5. Planificación del Trabajo

Id	Tarea	Inicio	Fin	Duración
1	**Planificación**			
1.1	Definir el contexto y justificación	28/09/2022	05/10/2022	5
1.2	Definir los objetivos	28/09/2022	05/10/2022	2
1.3	Definir el impacto en sostenibilidad, ético-social y diversidad	28/09/2022	05/10/2022	2
1.4	Definir la metodología utilizada	06/10/2022	10/10/2022	2
1.5	Elaborar el cronograma de hitos y tareas	06/10/2022	10/10/2022	4
1.6	Definir los contenidos del proyecto	06/10/2022	10/10/2022	2
1.7	**Entrega del plan de trabajo**	**11/10/2022**	**11/10/2022**	**Hito**
2	**Investigación**			
2.1	Estudio del marco SASE	12/10/2022	16/10/2022	5
2.2	Estudio del componente Secure Web Gateway (SWG)	17/10/2022	23/10/2022	4
2.3	Estudio del componente Zero Trust Network Access (ZTNA)	17/10/2022	23/10/2022	4
2.4	Estudio del componente Firewall as a Service (FWaaS)	24/10/2022	30/10/2022	4
2.5	Estudio del componente Data Loss Prevention (DLP)	24/10/2022	30/10/2022	4
2.6	Estudio del componente Cloud Access Security Broker (CASB)	24/10/2022	30/10/2022	4
2.7	Estudio de diferentes casos de uso	31/10/2022	06/11/2022	3
2.8	Estudio de mercado	17/10/2022	30/10/2022	5
2.9	Valorar la viabilidad económica	31/10/2022	07/11/2022	3
2.10	**Entrega de la fase de investigación**	**08/11/2022**	**08/11/2022**	**Hito**
3	**Análisis**			
3.1	Elaborar el diagrama actual (AS IS) de una organización	09/11/2022	13/11/2022	5
3.2	Elaborar el diagrama futuro (TO BE) de una organización	14/11/2022	20/11/2022	5
3.3	Establecer potenciales casos de uso	14/11/2022	27/11/2022	4
3.4	Elaborar la lista de segmentación de aplicaciones necesarias	14/11/2022	27/11/2022	4
3.5	Diseñar las políticas de seguridad	28/11/2022	04/12/2022	4
3.6	**Entregar la fase de análisis y diseño**	**06/12/2022**	**06/12/2022**	**Hito**
4	**Implantación y pruebas**			
4.1	Preparación y planificación de la prueba de valor PoV	06/12/2022	07/12/2022	1
4.2	Alta del *tenant*	09/12/2022	10/12/2022	1
4.4	Desplegar infraestructura necesaria en los centros de datos para ZTNA	06/12/2022	13/12/2022	4
4.5	Configurar reglas de acceso necesarias en cortafuegos	13/12/2022	14/12/2022	2
4.6	Configurar el provisionado y autenticación con AzureAD	12/12/2022	14/12/2022	2
4.7	Realizar pruebas de acceso con usuarios de dominio a la consola	15/12/2022	17/12/2022	1
4.8	Instalar y desplegar el agente a usuarios de prueba	12/12/2022	18/12/2022	3
4.10	Crear los segmentos de aplicaciones necesarios	19/12/2022	21/12/2022	2
4.11	Crear las políticas de navegación	22/12/2022	24/12/2022	2
4.12	Crear las políticas de acceso ZTNA a los recursos internos	25/12/2022	27/12/2022	2
4.13	Crear las políticas de protección de datos (CASB y DLP)	28/12/2022	30/12/2022	2
4.14	Realizar las pruebas a partir de los casos de uso definidos	31/12/2022	09/01/2023	10
4.15	Conclusiones	06/01/2023	09/01/2023	1
4.16	**Entrega de la memoria del proyecto**	**10/01/2023**	**10/01/2023**	**Hito**

Ilustración 2: Planificación del trabajo (Lista de tareas)

1.6. Cronograma del trabajo

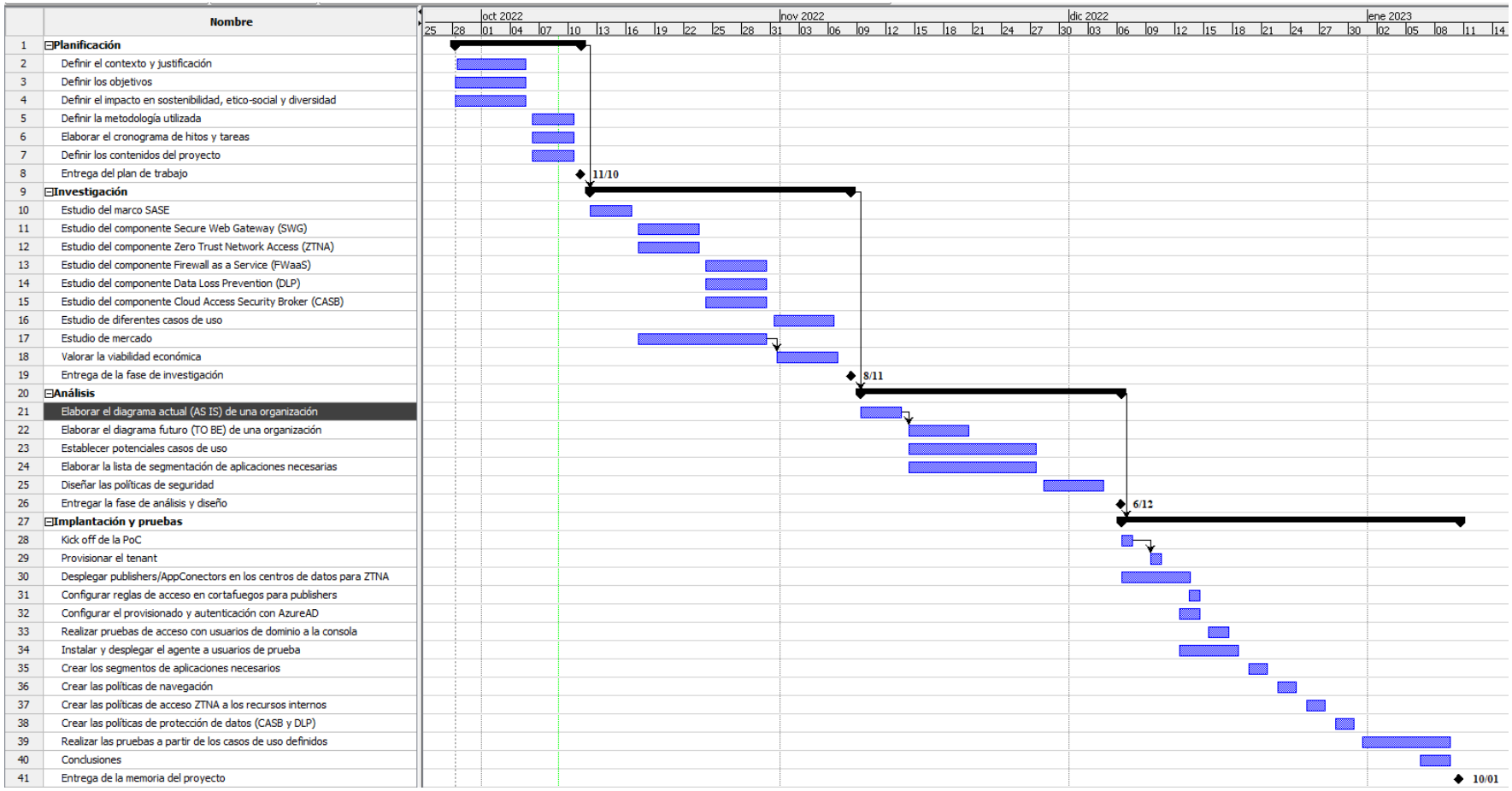


Ilustración 3: Cronograma del trabajo (Diagrama de Gantt)

1.7. Estado del arte

Para poder realizar este trabajo se busca información en Internet con el fin de poder recopilar información sobre proveedores de seguridad en la nube que permitan desplegar una arquitectura SASE en un entorno empresarial. La información obtenida se obtiene principalmente de algunos de los proveedores líderes en estas soluciones de seguridad en la nube como son Netskope y Zscaler, el prestigio de estos proveedores se contrasta con la empresa investigadora sobre tecnologías de información Gartner[4]:

Ilustración 4: https://www.netskope.com/

Ilustración 5: https://www.zscaler.es/

Aunque las diferentes fases de este trabajo se realizan en una empresa ficticia llamada Zanomme, S.A, realmente se van implementando en una empresa real, este hecho hace posible tener la oportunidad de conocer mejor el producto a manos de los comerciales e ingenieros preventa. Se convocan reuniones con cada uno de los proveedores y en estas sesiones se obtiene numerosa información, la cual se intenta explicar de la mejor manera en este trabajo.

Durante el desarrollo de este trabajo todas las informaciones como investigaciones consultadas están indicadas como cita en cada una de las secciones de investigación, análisis, implementación y anexos como también en la sección de referencias.

Con base a los análisis e investigaciones obtenidos en la fase de investigación y análisis, se selecciona al proveedor Netskope para desarrollar la sección de implementación debido a la facilidad que aporta este proveedor para la realización de las pruebas de concepto y pruebas de valor.

[4] https://www.gartner.es/

2. Fase de investigación

2.1. La transformación en la seguridad

Trasladémonos unos años al pasado y veamos cómo ha ido cambiando el paradigma de la tecnología y sistemas de almacenamiento hasta ahora. Durante los años 90 las organizaciones almacenaban sus datos, aplicaciones y servicios privados dentro de sus centros de datos *on premise* los cuales estaban protegidos y controlados por una seguridad en el perímetro centralizada llamado *Firewall* o cortafuegos.

Esto provocaba que el perímetro de seguridad y los sistemas tecnológicos se tuvieran que dimensionar y acondicionar frecuentemente debido a las necesidades de negocio de las organizaciones que cada vez eran más ambiciosas y necesarias, lo que suponía un alto coste de inversión y una respuesta lenta en ejecución.

Posteriormente, con la aparición del *Cloud Computing* o computación en la nube las organizaciones empezaron a alquilar espacio de almacenamiento y sistemas flexibles de cómputo fuera de sus instalaciones con el objetivo de ofrecer mejor servicio, mayor flexibilidad y mejor eficiencia en los futuros cambios tecnológicos con un menor coste en inversión inicial. Este nuevo paradigma tecnológico ofrecía una diferencia competitiva a las organizaciones debido a las cambiantes necesidades de negocio y este hecho provocó una gran inversión tecnológica en la nube en todo el mundo.

Muchas organizaciones empezaron a utilizar el *Cloud Computing* fruto de las ventajas que les ofrecía lo que facilitó la extensión de las redes de comunicaciones desde sus diferentes centros de datos a un entorno multi nube. Los departamentos de seguridad de las organizaciones tuvieron que afrontar nuevos retos para transformar sus sistemas de seguridad legadas con el objetivo de poder continuar garantizando la seguridad en este nuevo escenario.

Llegados a este punto se puede deducir que el cambio de paradigma tecnológico causado por el *Cloud Computing* tiene que ir alineado con un cambio de paradigma de la seguridad. Los sistemas de seguridad del pasado no han nacido ni han sido diseñados para la nube, solo han sido modelados para este uso con lo que es de vital importancia trasladar la seguridad del perímetro a la nube con el objetivo de afrontar los nuevos retos del futuro en materia de ciberseguridad.

2.2. ¿Qué es SASE?

Security Access Service Edge (SASE) es un marco estratégico que puede adoptar una empresa u organización con el objetivo de diseñar una arquitectura de seguridad y redes convergente en la nube. La principal finalidad de SASE es trasladar toda esta arquitectura del perímetro del centro de datos a la nube con el objetivo de proteger a las identidades, aplicaciones y los datos en el borde o *edge* mediante una gestión centralizada desde un solo punto. Este hecho posibilita depender en menor medida del hardware dedicado a productos de

seguridad en los centros de datos *on premise* con la ventaja de poder eliminar el perímetro central de seguridad y así reducir su dependencia.

Los empleados se conectan al servicio SASE en la nube para poder navegar en Internet y trabajar con sus datos privados ubicados en las oficinas o en diferentes aplicaciones en la nube de una manera segura, simple y con una buena experiencia de persona. Cabe destacar que los empleados tienen estas ventajas de protección y seguridad desde la red interna o cualquier otra ubicación donde se conecten.

Este nuevo paradigma de seguridad permite un control de acceso más detallado y rico en parámetros de conexión que las soluciones convencionales de seguridad ya que en estas soluciones legadas solo se permite o se deniega la conexión a los recursos en función de si las credenciales de la identidad del empleado son correctas. Ahora, con muchas de las aplicaciones ubicadas en la nube el hecho de aceptar o denegar la conexión a un recurso ya no es suficiente y se requiere algo más que nos informe de parámetros como el *qué*, *quién* y *por qué* intentan acceder. Estos parámetros condicionantes reciben el nombre de *contexto* de conexión.

Como se ha mencionado anteriormente SASE es un marco o guía de referencia con lo que no se considera un servicio, pero sí un conjunto de ellos, entre los pilares que forman SASE encontramos los siguientes:

CASB *Cloud Access Service Broker*, implementa políticas de seguridad con el objetivo de poder acceder a los recursos de la nube de una manera segura.

DLP *Data Loss Prevention*, protege en tránsito y en reposo los datos de una organización con el objetivo de evitar la exfiltración de estos.

NG SWG *Next Generation Secure Web Gateway*, protege la navegación a Internet y el acceso a aplicaciones en la nube.

RBI Remote Browser Isolation, aísla el contenido de un sitio web en un contenedor remoto para poder proteger el navegador del dispositivo que lo utiliza.

ZTNA *Zero Trust Network Access*, permite acceder a aplicaciones privadas con el mínimo privilegio y con una postura de seguridad sin necesidad que el empleado se encuentre en la red interna.

ATP *Advanced Threat Protection,* protege de las amenazas de la red como el *malware*, las amenazas de día cero *zero days*[5], campañas de *phishing* o los ataques dirigidos entre otros.

[5] *zero days*: Ataque de día cero es un ataque contra una aplicación o sistema que explota vulnerabilidades desconocidas hasta el momento con el objetivo de ejecutar código malicioso.

FWaaS *Firewall as a Service,* permite la protección de intrusiones por cualquier protocolo y puerto que no sean los de web a los equipos cliente de los empleados.

SD-WAN *Software-Defined WAN*[6], permite la interconexión de sedes y filiales a través de la WAN de una manera segura sin tener que utilizar costosas infraestructuras de red como las MPLS[7].

SSE *Security Service Edge*, unifica e integra todos los anteriores servicios con el objetivo de sumar sinergias y poder ofrecer más ventajas de seguridad a las organizaciones.

Recordemos que todos los servicios anteriormente mencionados protegen a un empleado de una organización independientemente de donde se encuentre acompañándole y ofreciéndole seguridad siempre en el borde o *edge*. En siguientes secciones se explica en más detalle todos estos servicios, las funcionalidades que ofrecen y las ventajas que se obtienen de ellos.

2.3. La necesidad de inspeccionar el tráfico

Los datos en tránsito que circulan por las redes deben de ir cifrados con el objetivo de conseguir confidencialidad en las comunicaciones, es decir que el tráfico que circula por un canal sea incomprensible para un tercero que intercepte la comunicación. Este cifrado de datos en tránsito se realiza en su defecto con el protocolo *Transport Layer Security* o TLS en versiones anteriores llamado *Secure Socket Layers* o SSL.

Aunque el dato circule por un canal cifrado no quiere decir que ese dato que viaja sea seguro. Por ejemplo, es posible descargarnos un fichero por un canal debidamente cifrado desde un sitio web que parece legítimo, pero realmente al descargarlo lo que obtenemos no ese fichero realmente sino contenido malicioso o *malware*. Con esto, la ciberdelincuencia despliega el *malware* a través de canales cifrados para poder evadir la seguridad de las organizaciones. De un estudio de **Zscaler ThreadLabz**[8] podemos destacar los siguientes datos:

- El ataque a través de canales cifrados aumentó un **314%** del año 2020 al 2021.
- Los atacantes despliegan el *malware* con prácticamente el **70%** de las aplicaciones web cifradas.

Con este ejemplo aparece un reto ¿Cómo protegemos a un empleado de las amenazas cifradas? La respuesta es: **inspeccionar el tráfico cifrado desde cualquier lugar en la nube**.

[6] WAN es la sigla de Wide Area Network ("Red de Área Amplia"). Es una red que se extiende en una gran franja de territorio.

[7] MPLS es un protocolo que permite la comunicación entre redes internas de diferentes sedes de una organización.

[8] https://info.zscaler.com/resources-whitepaper-threatlabz-the-state-of-encrypted-attacks

Aunque muchas organizaciones disponen de sistemas de seguridad tradicionales que permiten inspeccionar el tráfico cifrado en sus centros de datos y sedes, no disponen de los sistemas de seguridad adecuados que permitan inspeccionar el tráfico cifrado en la nube con garantías de rendimiento y eficiencia. El motivo es que el tráfico necesita ser descifrado, analizado y cifrado nuevamente para ser entregado al personal haciendo que sea un trabajo muy intenso, lo que requiere una gran inversión de hardware tradicional y coste de mantenimiento para tal propósito. Las soluciones SASE ofrecen la posibilidad de poder inspeccionar el tráfico cifrado en la nube con un gran rendimiento y eficacia desde cualquier lugar. La inspección del tráfico es esencial para que una solución SASE pueda cumplir sus objetivos.

Cabe destacar que existe un proceso en TLS llamado fijación de certificado o ***certificate pinning*** que tiene como objetivo evitar que un atacante actúe como intermediario en la comunicación entre un cliente y un servidor mitigando el riesgo de ataque de hombre en el medio o *man in the middle*. El *certificate pinning* restringe qué certificados son considerados válidos para un sitio web. Ciertas aplicaciones, sobre todo en los dispositivos móviles, incluyen en su código un certificado específico para establecer la comunicación con el servidor evitando que un intermediario malicioso o una inspección legítima como un proxy web pueda inspeccionar el tráfico. En estos casos cualquier solución de seguridad que realice inspección del tráfico deberá de hacer *bypass* de la aplicación y no se podrá hacer inspección de ese tráfico.

La inspección de tráfico cifrado SSL/TLS en la GDPR

Las regulaciones de privacidad de datos Europea (GDPR) o la del Reino Unido (NIS) se implementaron con el objetivo de proteger los datos personales y preservar el acceso libre a Internet, para ello es necesario inspeccionar el tráfico cifrado con el objetivo de descartar amenazas ocultas que pongan en riesgo los datos personales de las personas.

El hecho de poder inspeccionar el tráfico cifrado SSL/TLS hace pensar que los datos dejen de ser privados y esto es una preocupación para los departamentos legales de las organizaciones ya que interpretan que no pueden inspeccionar el tráfico por las normativas de protección de datos, pero realmente estas normativas requieren inspeccionarlos para protegerlos. Por ejemplo, el **artículo 5 de la GDPR (Principles relating to processing of personal data)[9]** establece:

> *"Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality"*

[9] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679#d1e1807-1-1

Además, el **artículo 32 (Security of Processing)**[10] de la misma regulación establece una obligación de que las organizaciones protejan los datos personales implementando medidas de seguridad:

> *"… the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk…"*

Como se ha comentado anteriormente, el tráfico cifrado aumenta cada año y las amenazas se encuentran ocultas en este tipo de tráfico, sin inspección de tráfico no es posible distinguir si el tráfico se considera legítimo o ilegítimo con lo que las organizaciones no podrán cumplir los artículos de privacidad y seguridad de las regulaciones de privacidad de datos como GDPR o NIS.

2.4. *Cloud Access Security Broker* (CASB)

Los datos de las organizaciones almacenados en la nube se acceden a través de Internet con tráfico web por lo que es necesario tener controles adecuados para protegerlos, una solución que ayuda a las organizaciones a conseguir este propósito es el *Cloud Access Security Broker* CASB. CASB es un intermediario entre los consumidores y los proveedores de servicio en la nube y su objetivo es proteger el acceso y almacenamiento de los datos a través de políticas de seguridad. Para que una solución CASB haga su función de una manera eficiente debe de cumplir con estas cuatro áreas básicas:

La visibilidad, es necesario tener el control de las aplicaciones administradas y no administradas en la nube. Las aplicaciones administradas son aquellas que el departamento de IT tiene el conocimiento que se están utilizando, en cambio las no administradas o Shadow IT[11] son aquellas que el departamento de IT desconoce el uso que se hace de estas. Por ejemplo, si Microsoft® OneDrive es la aplicación oficial para almacenamiento de ficheros en una organización correspondería a una aplicación administrada mientras que una aplicación utilizada por diferentes empleados para transferir ficheros como WeTransfer sería una aplicación no administrada o *Shadow IT*.

[10] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679#d1e3383-1-1

[11] Shadow IT son implementaciones de aplicaciones que conectan a servicios en la nube sin el consentimiento ni control del departamento de IT.

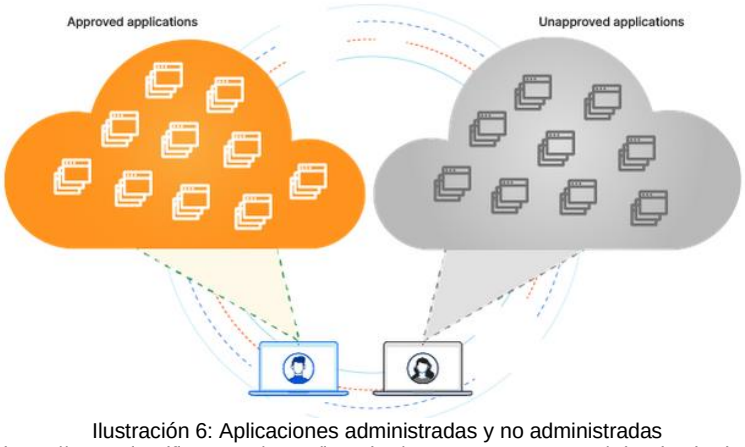


Ilustración 6: Aplicaciones administradas y no administradas
de https://www.cloudflare.com/es-es/learning/access-management/what-is-shadow-it/

Es posible que en determinadas ocasiones se necesite trabajar con aplicaciones administradas o no administradas, por esa razón es necesario tener visibilidad y poder diferenciar de una manera granular las acciones que se realizan con el objetivo de poder establecer políticas y restringir o aceptar dependiendo de la acción.

La normativa, el cumplimiento de requisitos normativos es importante para las organizaciones, la dispersión de la información en la nube es tan amplia que es necesario tener controles de seguridad que permitan cumplir normativas como HIPAA o RGPD.

La seguridad de los datos, es importante detectar y, en determinados casos, impedir la exposición de datos sensibles que se realizan de una organización a diferentes aplicaciones en la nube, para este propósito CASB ayuda a proteger los datos a través de la prevención de pérdida de datos DLP.

La protección de amenazas, CASB ayuda a las organizaciones a que el personal empleado no suba ni descargue aplicaciones maliciosas con lo que es importante que se pueda analizar el contenido en tiempo real para reducir el riesgo de infección.

Un CASB puede proteger los datos en línea o en tránsito como también los datos fuera de línea o en reposo. La protección en tránsito se refiere a la inspección de los datos en tiempo real, por ejemplo, cuando una persona almacena u obtiene contenido desde una aplicación web en la nube mientras que protección en reposo es la que aplica mediante integraciones con API para poder analizar el contenido fuera de línea en plataformas de almacenamiento en la nube.

2.5. *Data Loss Prevention* (DLP)

La información es un recurso muy valioso y las organizaciones necesitan protegerla de la mejor manera debido a que la exposición no autorizada de los datos sensibles y confidenciales puede llegar a ser perjudicial para el negocio dañando la marca y provocando pérdidas económicas. Los tipos de datos sensibles y confidenciales pueden llegar a ser patentes, procesos, planes, entre

otros datos de la organización como *Personally Identifiable Information* PII de clientes o empleados.

Data Loss Prevention DLP es una solución que ayuda a combatir la fuga de información originada desde dentro de una organización enviada hacia a un recurso como puede ser una Shadow IT, una aplicación administrada en la nube, un almacenamiento extraíble o mediante el correo electrónico. La fuga de información también recibe el nombre de exfiltración de la información.

Algunos tipos de organizaciones como pueden ser las de sector sanitario y financiero están obligadas por ley a proteger sus datos sensibles. Algunos reglamentos conocidos son los siguientes:

Ilustración 7: HIPAA

Ilustración 8: PCI DSS

Ilustración 9: RGPD

RGPD[12], Reglamento general de protección de datos de la Unión Europea.
HIPAA, Ley de transferencia y responsabilidad de seguros de salud de EE. UU.
PCI DSS, Estándar de seguridad para la industria de las tarjetas de crédito.

Las soluciones de DLP hacen posible su trabajo **identificando la información** a través de etiquetas relacionadas con diferentes reglamentos e **identificando la fuga de datos** a través de procesos automáticos con inteligencia artificial en datos en reposo o en tránsito.

2.6. *Next Generation Secure Web Gateway* (NG SWG)

La transformación digital de las empresas ha hecho que el uso de aplicaciones y servicios en la nube haya aumentado rápidamente, según datos de **Netskope ThreatLabs**[13] el 79% del personal de las organizaciones almacena, comparte, sube y descarga datos en la nube y desde inicios del año 2022 este uso se ha incrementado en un 35%. Este hecho hace que las amenazas y riesgos de la red causados por la ciberdelincuencia también aumenten y sea necesario disponer de soluciones que protejan de una manera ágil y eficiente ante estas amenazas.

Podemos definir a *Next Generation Secure Web Gateway* (NG SWG) como una solución nativa en la nube que protege a las organizaciones de las amenazas y riesgos de los datos en el tráfico web de aplicaciones e instancias en la nube. Es la evolución de la solución tradicional *Secure Web Gateway* SWG la cual protegía solamente de las amenazas de la web sin tener en cuenta las aplicaciones de las organizaciones o servicios en la nube.

[12]https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_es.htm
[13] https://resources.netskope.com/cloud-reports/cloud-and-threat-report-cloud-data-sprawl

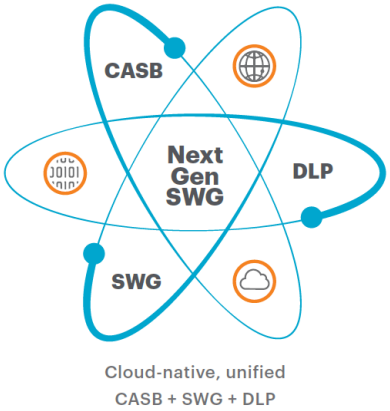


Ilustración 10: Next Generation Secure Web Gateway NG SWG
de https://www.netskope.com/lp/sase-adoption-guide/

Las funcionalidades que nos ofrece NG SWG es la de poder adaptar políticas de seguridad adecuadas a los accesos web o accesos a aplicaciones en la nube que realiza el personal de las empresas independientemente de donde se conecten. Estas políticas de seguridad se adaptan a través de otras soluciones que forman la arquitectura SASE como Data Loss Prevention **DLP** o *Cloud Access Service Broker* **CASB** las cuales permiten ampliar sus capacidades. Con NG SWG incluso se acepta o deniega el acceso a datos en relación de la confianza que se dispone de una aplicación, sensibilidad de datos o incluso del riesgo que tiene la identidad de la persona que intenta acceder en un momento determinado.

2.7. *Remote Browser Isolation* (RBI)

Remote Browser Isolation **RBI** es una solución de seguridad que permite proteger a las personas de la navegación que realizan en los sitios web. RBI aísla en un contenedor en la nube los componentes de riesgo que se cargan de un sitio web y se los muestra a la persona de una manera segura mediante píxeles en el navegador de su dispositivo. La finalidad del RBI es complementar la protección que nos brinda NG SWG reduciendo los riesgos en la navegación y protegiendo a las personas de las amenazas existentes en los sitios web.

RBI es un componente que se encuentra dentro de una solución de NG SWG aportando una protección avanzada. Si un sitio web es seguro NG SWG permite el acceso, si es malicioso lo bloquea en cambio si el sitio web tiene un riesgo o no está clasificado es donde entra la solución RBI para aislarlo y ejecutarlo remotamente mostrando a la persona un contenido seguro y sin riesgos en su navegador.

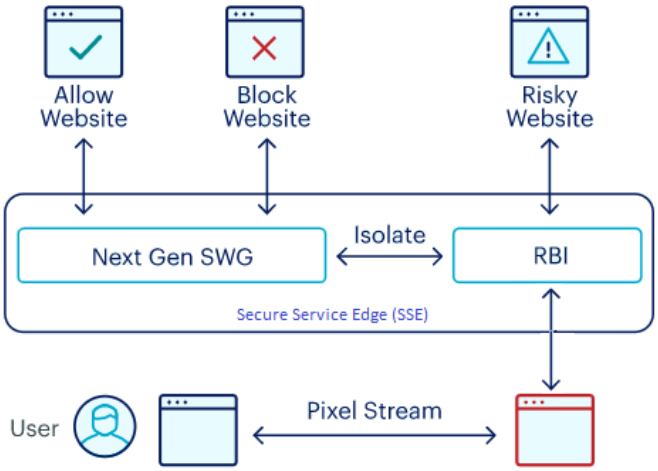


Ilustración 11: Remote Browser Isolation (RBI)
https://www.netskope.com/es/products/remote-browser-isolation

Existen diferentes formas en como RBI representa las páginas web en un navegador de un dispositivo, una de ellas es la **representación mediante pixeles**, es la más segura ya que el navegador no ejecuta ningún contenido de la web, RBI lo aísla y luego lo representa mediante pixeles al navegador del usuario. Otra forma es la **representación basada en DOM**, menos segura que la representación mediante pixeles porque en este caso RBI aísla solamente los elementos con más riesgos en los sitios web como scripts y los representa en pixeles en el navegador del dispositivo, en cambio hojas de estilo e imágenes se cargan directamente en el navegador. La tercera representación es la **representación de medios**, es la menos segura de las anteriores, RBI aísla los componentes DOM con más riesgo, esta representación es utilizada para la visualización de contenido multimedia la cual necesita muy buena experiencia de persona.

2.8. *Firewall as a Service* (FWaaS)

Anteriormente hemos citado las soluciones de NG SWG y CASB que protegen de las amenazas y riesgos existentes en el tráfico web y servicios en la nube, aunque estas soluciones protegen cualquier tráfico web independientemente del puerto de comunicaciones utilizado no protegen del tráfico de salida originado desde un equipo cliente que trabaje por los protocolos TCP[14], UDP[15] o ICMP[16].

Firewall as a Service (FwaaS) es una solución en la nube que protege el tráfico de salida que se origina desde cualquier protocolo que no sea el de web desde los equipos cliente de una organización independientemente de donde se conecten. Por ejemplo, la solución FWaaS permite proteger el tráfico DNS que

[14] TCP *Transmision Control Protocol*, protocolo de la capa de transporte que crea conexiones dentro de una red que garantiza que los paquetes enviados se entreguen sin errores y con orden.
[15] UDP User Datagram Protocol, protocolo de la capa de transporte que no crea conexión inicialmente sino que el datagrama se envía directamente, utilizado para tráfico en tiempo real.
[16] ICMP Control Message Protocol, protocolo de la capa de red, no es principalmente utilizado para intercambiar información entre redes sino es utilizado con fines de diagnóstico.

viaja por el protocolo UDP con el objetivo de bloquear túneles o bloquear conexiones de salida a servicios comunes que no sean necesarios para un cliente como puede ser el tráfico de salida para *Remote Desktop Protocol* RDP, *File Transfer Protocol* FTP, *Secure SHell* SSH entre otros. Es importante tener en cuenta que FWaaS es una solución en la nube para la protección del tráfico *egress* o de salida de los equipos clientes con lo que no analiza el tráfico *ingress* o, de entrada.

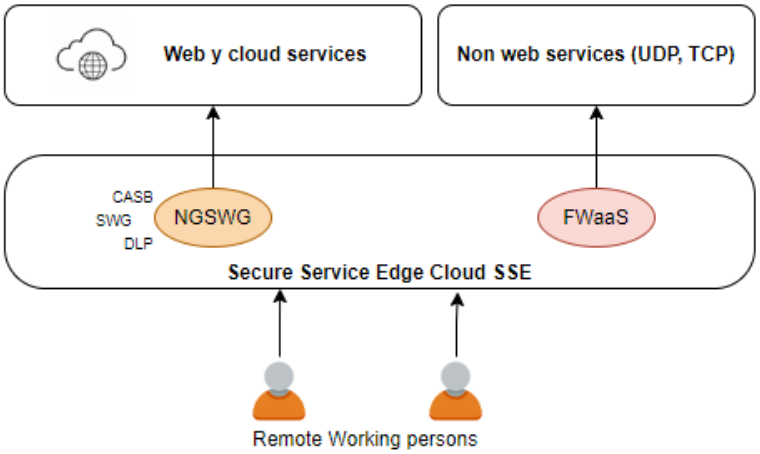


Ilustración 12: Firewall as a Service in SSE

La solución FWaaS aporta una gestión centralizada de las políticas de seguridad en la nube con un alto rendimiento e integrado con *Secure Service Edge* SSE, lo cual permite formar parte de una arquitectura SASE.

2.9. *Zero Trust Network Access* (ZTNA)

El principio de *Zero Trust* es permitir o denegar el acceso a una aplicación a través de un puntaje de confianza que adquiere una persona autenticada mediante una constante supervisión de la postura de seguridad y con un privilegio mínimo de acceso.

Para entenderlo mejor, cuando una persona o identidad necesita acceder a una aplicación protegida por *Zero Trust* primero debe autenticarse y luego cumplir una serie de condiciones que le permitirán ganarse su confianza con el objetivo de acceder o no al recurso (inicialmente no se confía en nadie ni en nada). *Zero Trust* constantemente supervisa estas condiciones o **posturas de seguridad** permitiendo que la confianza sea adaptable al entorno y conexión en cada momento. Con esta definición podemos ver que ya no solo se acepta o deniega el acceso a un recurso con el mero hecho de solo autenticarse, sino que evalúa diferentes parámetros constantemente para que sea la confianza de la identidad quien autorice o deniegue el acceso.

Las posturas de seguridad también reciben el nombre de **contexto de conexión**. Algunos ejemplos de posturas de seguridad son la identidad, la ubicación

geográfica, la fecha y hora, si se dispone de protección de *malware*, si se está bajo un dominio específico, el riesgo asociado a la identidad o *User Confidence Index* **CCI**, aplicación o servicio que se solicita, etc...

Además, *Zero Trust* limita el acceso al recurso con un mínimo privilegio permitiendo que una persona tenga el acceso justo y necesario sin tener que dar acceso a otros recursos. *Zero Trust Network Access* ZTNA evita que el equipo de una persona resida dentro de la red interna de la organización con lo que evita la enumeración de servicios y reduce el riesgo de ser víctimas de la táctica de movimiento lateral[17] usada por la ciberdelincuencia para el robo de información empresarial.

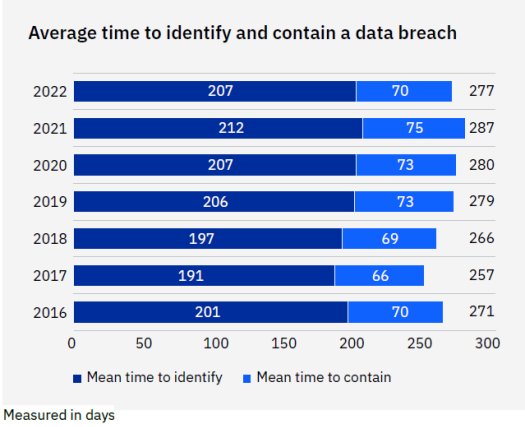


Ilustración 13: Cost of a data breach 2022. (n.d.).

Las brechas de seguridad provocadas por estos ataques derivan en cuantiosas pérdidas de dinero. En un estudio de IBM[18] del año 2022 se demuestra que las organizaciones consumen 277 días para identificar que tienen una brecha de seguridad. Otra ventaja que aporta ZTNA es la de reducir la superficie de ataque de las organizaciones en Internet debido a la reducción de concentradores de *Virtual Private Network* VPN[19] la razón es que ZTNA sustituirá sin duda a esta tecnología por los motivos de seguridad anteriormente citados.

2.10. *Advanced Threat Protection* (ATP)

Las soluciones mencionadas anteriormente como NG SWG y ZTNA deben de estar protegidas contra las amenazas existentes en la web y en la nube, por esta razón es importante disponer de una solución de protección avanzada de amenazas. El objetivo del ATP es proteger los datos y a las personas contra los ataques como el *malware*, ataques de día cero (*zero days)*, campañas de phishing, puertas traseras (*backdoors)*, movimientos laterales, *ransomware, Advanced Persistent Threat (*APT*)* entre otros que se realizan en las diferentes

[17] https://attack.mitre.org/tactics/TA0008/
[18] Cost of a data breach 2022. (n.d.). IBM. Retrieved October 25, 2022, from https://www.ibm.com/reports/data-breach
[19] Virtual Private Network es una tecnología que permite una extensión de una red de área local sobre una red pública

fases de la *Cyber Security Kill Chain* utilizado por la ciberdelincuencia con el propósito de completar un ataque con éxito.

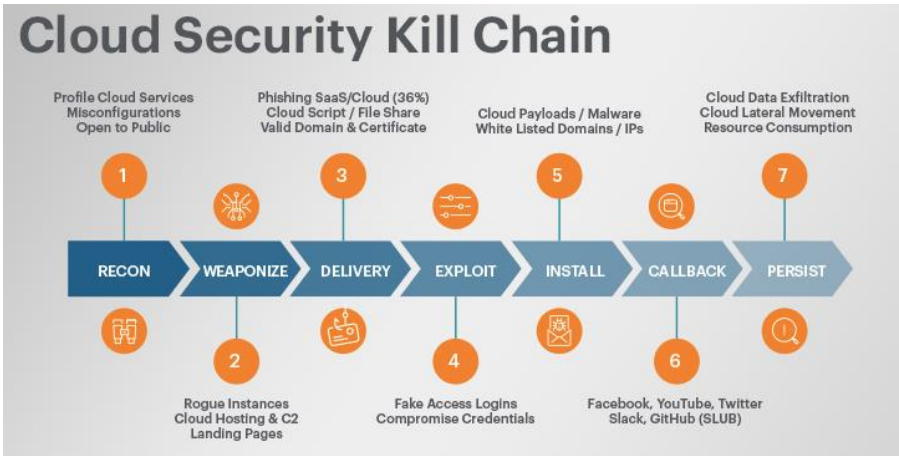


Ilustración 14: Fases de la Cyber Security kill Chain
https://www.netskope.com/es/security-defined/cyber-security-kill-chain

ATP es una solución de protección proactiva que actúa antes de causar la pérdida de datos y perjudicar a las organizaciones con el objetivo de poder dar una respuesta rápida ante incidentes de seguridad, para ello ATP utiliza diferentes técnicas como el *sandboxing*[20], intercambio de indicadores de compromisos IoC[21], análisis del tráfico de red, detección de anomalías, heurística, análisis de comportamiento para detectar las amenazas.

Como se ha comentado anteriormente las soluciones de NG SWG y ZTNA deben de estar protegidas con ATP ante amenazas, pero es muy recomendable disponer de protección en el equipo final con *Endpoint Protection Platform* EPP y *Endpoint Dectection and Response* EDR en los equipos para poder ofrecer una segunda capa de protección a los equipos corporativos. La diferencia entre EPP y EDR es que el primero tiene el objetivo de prevenir ataques que se realizan en un equipo mediante los módulos de *antimalware*, IPS, filtrado web, DLP, Firewall entre otros, mientras que EDR tiene el objetivo de identificar ataques y alertar en tiempo real de los ataques que se están produciendo con ayuda de indicadores de compromiso IoC.

2.11. *Software-Defined WAN* (SD-WAN)

La solución *Software-Defined Wide Area Network* SD-WAN proporciona una arquitectura WAN virtual inteligente que permite gestionar y administrar mediante *software* y de una manera centralizada la infraestructura WAN de las sucursales en una organización. El objetivo de la SD-WAN es poder conectar a través de la WAN los usuarios a las aplicaciones y servicios de una manera segura. Las SD-WAN permiten integrar cualquier tecnología de transporte como MPLS, 5G o

[20] Sanboxing: Mecanismo de seguridad que tiene el objetivo de aislar programas y procesos del equipo de la persona con el objetivo de analizar su comportamiento y detectar amenazas de red.
[21] IoC : Es cualquier información relevante que describe cualquier incidente de seguridad, por ejemplo el hash de un fichero o una dirección IP.

FTTH entre otras con el fin de poder aprovechar de una manera más eficiente, segura y simple el ancho de banda.

El modelo que utiliza SD-WAN a diferencia de las WAN tradicionales es que cada sucursal conectada, independientemente de donde esté ubicada, pueda encaminar de la manera más eficiente el tráfico de red optimizando los saltos de conexión de una manera inteligente. Un modelo SD-WAN evita la centralización de infraestructura de red en los centros de datos haciendo posible que cada sucursal conectada sea independiente en la manera que los usuarios conectan con las aplicaciones de una manera segura, eficiente y gestionada de una manera centralizada desde un solo punto en la nube.

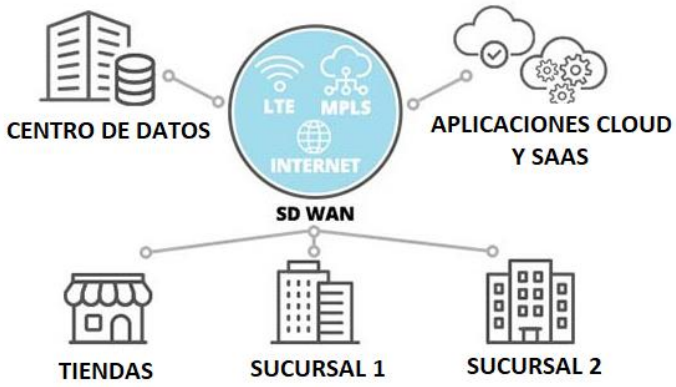


Ilustración 15: Diagrama alto nivel SD-WAN
www.securewirelessworks.com

La idea es que cada sucursal, centro de datos o tienda de una organización solamente disponga de un acceso WAN para poder conectarse al servicio SD-WAN en la nube y empezar a dar servicio al personal empleado simplificando la infraestructura de red, administración y reduciendo altos costes asociados a redes dedicadas como las MPLS.

Con SD-WAN es posible combinar la optimización de la WAN, el enrutamiento y FWaaS mediante el *Service Secure Edge* SSE con el objetivo de trasladar a la nube la gestión de seguridad y la administración. La transformación de la tecnología WAN como lo es SD-WAN debe de ir acompañado de una transformación de seguridad adecuada para poder administrar de una manera eficiente las políticas de seguridad necesarias.

2.12. *Secure Service Edge* (SSE)

Todas las soluciones de red y seguridad vistas hasta ahora son fundamentales para conseguir una arquitectura SASE en una organización, pero falta algo que las haga entenderse y coordinarse entre ellas para conseguir una solución convergente e integral de seguridad en la nube. *Secure Service Edge* SSE es el componente que identifica, integra y ejecuta todas estas soluciones bajo un único punto de administración y gestión para dotar a los departamentos de seguridad

de las organizaciones una seguridad más eficaz. SSE es como un cerebro que gobierna los componentes de seguridad en una manera conjunta.

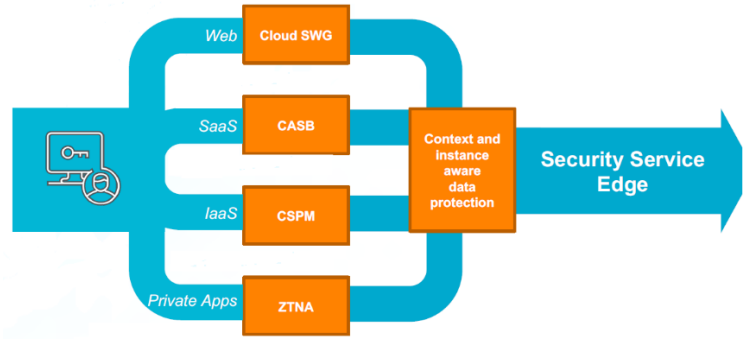


Ilustración 16: Secure Service Edge SSE, combinación e integración
https://www.netskope.com/es/products/security-service-edge

La implementación por separado de las soluciones de seguridad en la nube como SWG, CASB, DLP o ZTNA aportan valor a las organizaciones, pero el hecho de tenerlas separadas hace que tengan que utilizar diferentes agentes dificultando su integración y coordinación. Para sacar un máximo partido de estas soluciones en la nube es necesario combinarlas e integrarlas con SSE.

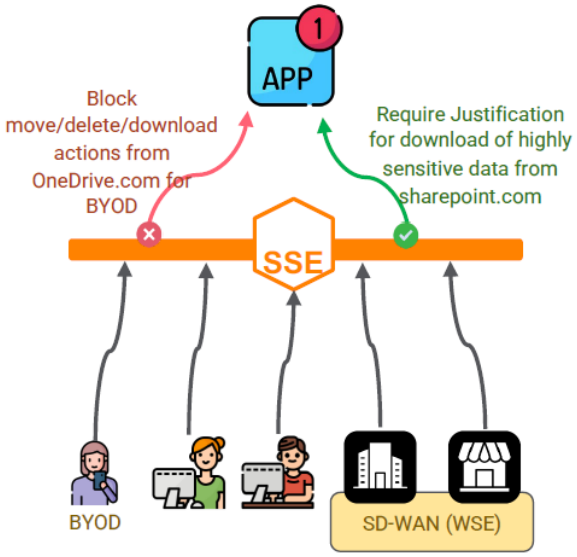


Ilustración 17: Secure Service Edge SSE, protección desde cualquier lugar
https://www.netskope.com/es/products/security-service-edge

Un SSE implementado correctamente hace posible un trabajo en paralelo de todos los componentes funcionando al unísono en tiempo real.

2.13. Las ventajas de SASE

Las organizaciones que han decidido invertir en una solución SASE para transformar su seguridad con el objetivo de llevar a cabo su transformación digital adquieren las siguientes ventajas:

- **Evita el modelo perimetral** apostando por el modelo de borde o *edge* donde cualquier dispositivo está protegido independientemente de donde se conecte evitando así la centralización de tráfico en un solo punto.

- **Aumenta el rendimiento de acceso a los recursos en Internet** con la ayuda de una red global de *Point Of Presence* PoP garantizando una baja latencia y alta disponibilidad.

- **Aplica un acceso de mínimo privilegio** proporcionando un acceso seguro y contextual a las aplicaciones en la nube mediante *Zero Trust Network Access* ZTNA.

- **Permite el acceso desde cualquier lugar** a recursos internos o en la nube sin necesidad de levantar túneles ni circuitos de transporte complejos.

- **Reduce la complejidad** de administración y de operación de los departamentos de seguridad como son la gestión simple y centralizada de las políticas de seguridad y la facilidad en escalar funcionalidades de una manera rápida.

- **Ahorra costes** en la inversión de infraestructura *on premise* y permite la compra de las soluciones de seguridad en un modelo de pago por subscripción.

- **Protege de las amenazas y reduce los riesgos** de la navegación en Internet y el acceso a los recursos internos protegiendo contra el *malware*, *ransomware* o el *phishing*.

- **Protege los datos** que viajan de dentro de la organización a cualquier destino como nubes públicas o instancias personales del personal previniendo fugas de información sensible.

2.14. Crecimiento y pronóstico de SASE en el mercado

SASE ha tenido un crecimiento significativo en años anteriores y el pronóstico de aquí unos años es muy positivo, los intereses de los clientes finales sobre SASE crecieron un **89%** en el año 2021 comparándolas con el 2020 y crecieron un **15%** más en el año 2022 en comparación con el 2021 (*Market Guide for Single-Vendor SASE*[22] de Gartner).

[22] https://www.gartner.com/document/4019183?ref=solrAll&refval=345029393

Esto quiere decir que, desde que se acuñó el concepto SASE en 2019, el interés que se ha depositado en esta arquitectura se ha disparado, impulsado principalmente por la necesidad de cambio tecnológico de las organizaciones.

Ilustración 18: Predicciones Gartner sobre SASE

Se estima que para el año 2023 el 20% de las empresas habrán adoptado soluciones NG SWG, CASB, ZTNA y FWaaS y que para el 2024 tendrán estrategias claras para desplegar una arquitectura SASE (*The Future of Network Security Is in the Cloud*[23] de Gartner).

La predicción para el año 2025 es que el 80% de las empresas hayan adoptado una estrategia para unificar la web, los servicios en la nube y el acceso a aplicaciones privadas utilizando una arquitectura SASE.

La tendencia de crecimiento es clara y se espera que durante los próximos cuatro años el mercado SASE crecerá a una *Compound Annual Growth Rate* CAGR del 32%, alcanzando casi $15 mil millones para 2025.

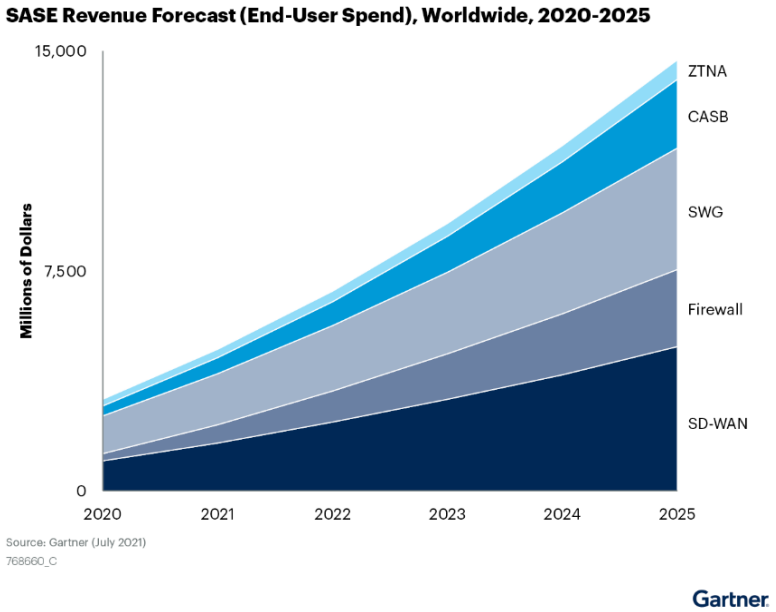


Ilustración 19: Crecimiento anual de SASE hasta 2025

2.15. Estudio de mercado

El crecimiento que ha tenido SASE en estos últimos años y los buenos pronósticos de los años venideros han hecho que proveedores hayan agregado su propia solución SASE en la nube en su cartera de servicios y productos. Los proveedores actuales que ofertan una arquitectura SASE en la nube han tenido que crear y evolucionar ciertas capacidades para poder ofrecer este servicio, por

[23] https://www.gartner.com/document/3956841?ref=solrAll&refval=345035181

ejemplo, proveedores que estaban especializados en la protección del dato han tenido que agregar una pila SD-WAN o de *proxy* web para crear SASE mientras que los líderes en tecnología en redes como SD-WAN han tenido que agregar una pila de seguridad basada en la protección del dato en la nube para ofrecer su servicio. Cabe destacar que ningún proveedor es líder en todas las capacidades que tiene la arquitectura SASE.

Es posible adoptar SASE con una oferta de un único proveedor, mediante una selección de dos proveedores o un SASE administrado:

Adopción SASE con un único proveedor, tiene la ventaja de facilitar la integración de los componentes de seguridad y gestión desde un solo punto debido a que son nativos del propio proveedor, aunque tiene la desventaja que en alguna capacidad SASE, como puede ser las redes SD-WAN o la protección del dato, el proveedor único no sea líder en alguna de ellas.

Adopción SASE selección de dos proveedores, tiene la ventaja de poder seleccionar un proveedor líder en redes SD-WAN y otro proveedor líder en seguridad en la nube y protección del dato, con esta sinergia es posible disponer de todas las capacidades SASE líderes en el mercado, pero tiene el inconveniente de que hay que estudiar detenidamente la integración entre las soluciones de los dos proveedores.

Adopción SASE administrado, es posible de poder adoptar SASE a un proveedor gestionado el cual se encarga de utilizar una adopción SASE de un único proveedor o dos proveedores. Esta adopción sería como una subcontratación del servicio SASE.

Ya sea una adopción SASE de un único proveedor, dos proveedores o gestionado es importante que una oferta de un proveedor SASE tenga las siguientes características:

- Todos los servicios deben de estar totalmente integrados, no puede haber módulos acoplados débilmente.

- Un modelo de datos unificado para para poder almacenar la información de registros y eventos de las soluciones de seguridad.

- Un único punto de administración para reducir la utilización de múltiples consolas.

- Facturación bajo demanda dependiendo del consumo, por ejemplo basado en identidad.

- *Point Of Presence* PoP distribuidos en todo el globo para que las políticas de seguridad estén lo más cerca posible de los equipos del personal y las sedes.

Para poder evaluar un proveedor SASE es importante preparar y ejecutar un piloto funcional con diferentes usuarios y ubicaciones de la manera más real

posible. Un proveedor debe de facilitar la realización de estos pilotos para que la organización pueda garantizar que el producto cumple con las necesidades y requisitos establecidos.

En la ilustración siguiente se pueden ver los proveedores líderes para servicios SD-WAN y servicios *Secure Service Edge* SSE:

SD-WAN

Ilustración 20: Cuadrante mágico Gartner para SD-WAN (2022)

***Secure Service Edge* (SSE)**

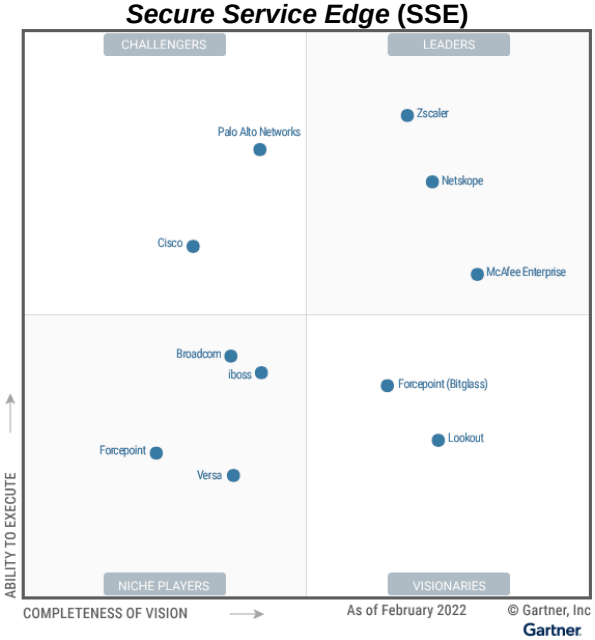


Ilustración 21: Cuadrante mágico de Gartner para SSE (2022)

En la siguiente tabla se muestran diferentes proveedores con la información del país de origen y el nombre de su producto SASE:

Proveedor	**Ciudad y país**	**Nombre oferta SASE**
Cato Networks	Tel Aviv (Israel)	Cato SASE Cloud
Cisco	San Jose, California (U.S.)	Cisco Umbrella
Citrix	Fort Lauderdale, Florida (U.S.)	Citrix Secure Internet Access / Citrix SD-WAN
Forcepoint	Austin, Texas (U.S.)	Forcepoint ONE with FlexEdge Secure SD-WAN
Fortinet	Sunnyvale, California (U.S.)	FortiSASE
Netskope (Infiot)	Santa Clara, California (U.S.)	Netskope SASE
Palo Alto Networks	San Jose, California (U.S.)	Prisma SASE
Versa Networks	Santa Clara, California (U.S.)	Versa SASE
Vmware/Broadcom	Palo Alto, California (U.S.)	VMware SASE
Zscaler	San Jose, California (U.S.)	Zscaler SASE
McAfee Enterprise	Santa Clara, California (U.S.)	McAfee MVISION UCE
Cloudflare	San Francisco, California (U.S.)	Cloudflare One

Ilustración 22: Tabla de proveedores SASE (2022)

2.16. Evaluación y selección del proveedor

El proceso de evaluación y selección de un proveedor es una fase muy importante para poder saber cual se adapta mejor a la empresa y el proyecto. La correcta selección de un proveedor ayudará a que una empresa u organización pueda cumplir sus objetivos y metas de una manera eficiente y con garantías. En este proyecto evaluaremos a los proveedores del mercado SASE basándonos en los siguientes criterios:

Perfil general del proveedor, es el primer paso de evaluación de los proveedores SASE y se analiza el prestigio, las referencias, trayectoria en la industria, cumplimiento normativo, tamaño, ubicación de la sede central.

***Service Level Agreement* (SLA)**, un *Service Level Agreement* (SLA) es un contrato que explica el nivel de servicio que un cliente espera de un proveedor con el objetivo de poder asegurar el cumplimiento del contrato, para poder explicar o describir este nivel de servicio se utilizan diferentes indicadores. El acuerdo de nivel de servicio es importante para poder conocer la calidad del servicio y las garantías que nos pueden ofrecer los proveedores SASE con el objetivo de prevenir y mitigar riesgos en el servicio.

Estabilidad financiera, es importante estudiar la situación financiera de los proveedores SASE para saber si son solventes y que puedan permanecer en el negocio a largo plazo con el objetivo de poder negociar un contrato con garantías.

Precio, aunque el precio no es un factor determinante en la selección del proveedor SASE sí que es de interés para la organización para poder ajustarse a su presupuesto anual.

Infraestructura tecnológica global, en un proyecto de implantación de una arquitectura SASE es importante poder analizar la infraestructura tecnológica global de los proveedores debido a que la calidad del servicio y la experiencia del usuario se verán reflejados por este factor. Recordemos que SASE es una arquitectura de soluciones de seguridad convergente en la nube donde las personas deben de poder acceder a sus recursos públicos o privados de una manera segura independientemente de donde se conecten, de esta manera es necesario que los proveedores dispongan del mayor número de puntos de presencia o *Point Of Presence* (PoP) en todo el planeta con el objetivo de dar a las personas una experiencia positiva.

Responsabilidad social, todas las empresas u organizaciones deberían de estar motivadas por ser socialmente responsables, es un factor importante que los proveedores SASE dispongan de planes de responsabilidad social como el cuidado del medio ambiente y la sostenibilidad, bienestar de los empleados, donaciones benéficas para la ayuda en salud o catástrofes entre otras.

Rapidez y flexibilidad, las necesidades del negocio y la transformación digital obliga a que la carga de proyectos sea elevada con lo que es un factor relevante que los proveedores proporcionen soluciones rápidas y flexibles que permitan al

cliente poder realizar pruebas de concepto y poder evaluar el producto sin mucha burocracia y con el menor tiempo posible.

De la tabla de proveedores (**Ilustración 19**) y a partir de los criterios definidos anteriormente, **Netskope** y **Zscaler** han sido seleccionados como posibles proveedores del servicio SASE en este proyecto. No entra dentro del alcance de este proyecto presentar un documento de solicitud de propuesta o *Request For Proposal* (RFP) pero sí que se realizará una comparativa más detallada o *benchmark* de estos dos proveedores.

2.17. Comparativa proveedores Netskope y Zscaler

2.17.1. Perfil General y situación financiera

	Netskope	Zscaler
Ubicación de la sede	Santa Clara, California (U.S.)	San Jose, California (U.S.)
Fecha de fundación	2012	2007
Número de clientes	+1500	+6700
Número empleados	+1500	+4900
Valor de empresa	$USD 7.500M	$USD 16.800M
Crecimiento en 2021	$USD 300M	$USD 673M
Premios y Galardones[24] [25]	Gartner Líder SSE & CASB CRN Forbes Cloud CyberDefense Magazine Battery InfoSec Awards Best Places to Work Fortress Cybersecurity Awards Cybersecurity Excelence Awards ISC Awards	Gartner Líder SSE & SWG CRN Forrester CyberDefense Magazine Deloitte Fortune CEO World

Ilustración 23: Tabla comparativa Netskope vs Zscaler (Perfil General y financiera)

La situación financiera de ambos proveedores es muy buena con crecimientos muy positivos en este último año. Se puede observar que Zscaler es más veterana que Netskope y con una solvencia y ganancias en el último año también mayores. Ambos proveedores disponen de un buen prestigio galardonados y premiados en diferentes organizaciones.

2.17.2. Infraestructura global

	Netskope	Zscaler
Centros de datos	+55 regiones 15 en expansión	+50 regiones +15 en expansión
Equipo de investigación	Netskope Threat Research Labs	Zscarler ThreatLabz
Nombre de nube privada	NewEdge	-

[24] https://www.netskope.com/es/company/affiliations-and-awards
[25] https://www.zscaler.es/company/faqs

Soluciones SASE	NG SWG ZTNA CASB DLP CSPM, SSPM RBI CFW (Cloud Firewall) Sandbox Soporte TLS 1.3	ZIA (Zscaler Internet Access) ZPA (Zscaler Private Access) CASB DLP CSPM, SSPM RBI FWaaS Deception Sandbox Soporte TLS 1.3
Rendimiento de red	>100Tbps	200.000 millones de transacciones al día

Ilustración 24: Tabla comparativa Netskope vs Zscaler (Infraestructura global)

Se muestra el mapa de los puntos de presencia o *Point Of Presence* PoP de la red de **NewEdge** de Netskope:

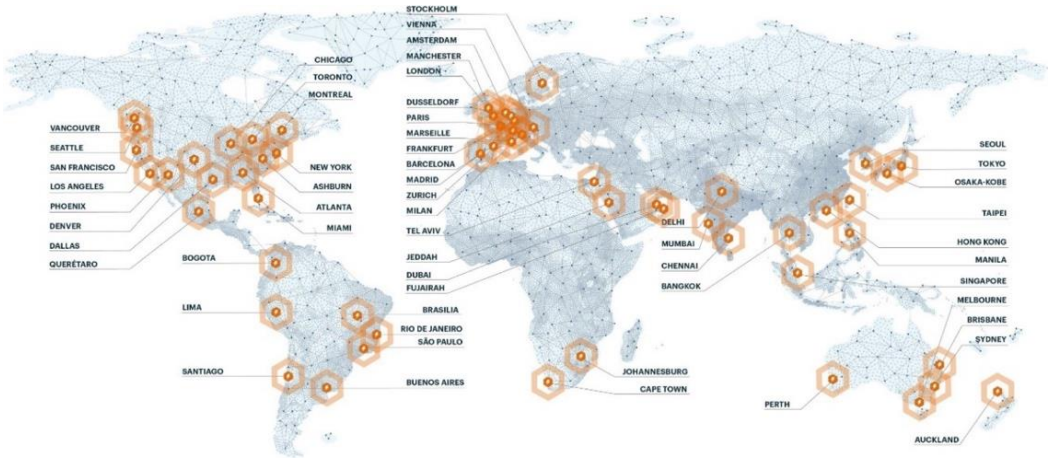


Ilustración 25: Red de puntos de presencia de Netskope (NewEdge)
https://www.netskope.com/platform/newedge

Es posible obtener visibilidad en tiempo real del estado de *Netskope Security Cloud Service* y la infraestructura de **NewEdge** mediante la siguiente referencia[26]

El mapa de los puntos de presencia o *Point Of Presence* PoP de la red de Zscaler es la siguiente:

[26] https://trust.netskope.com/

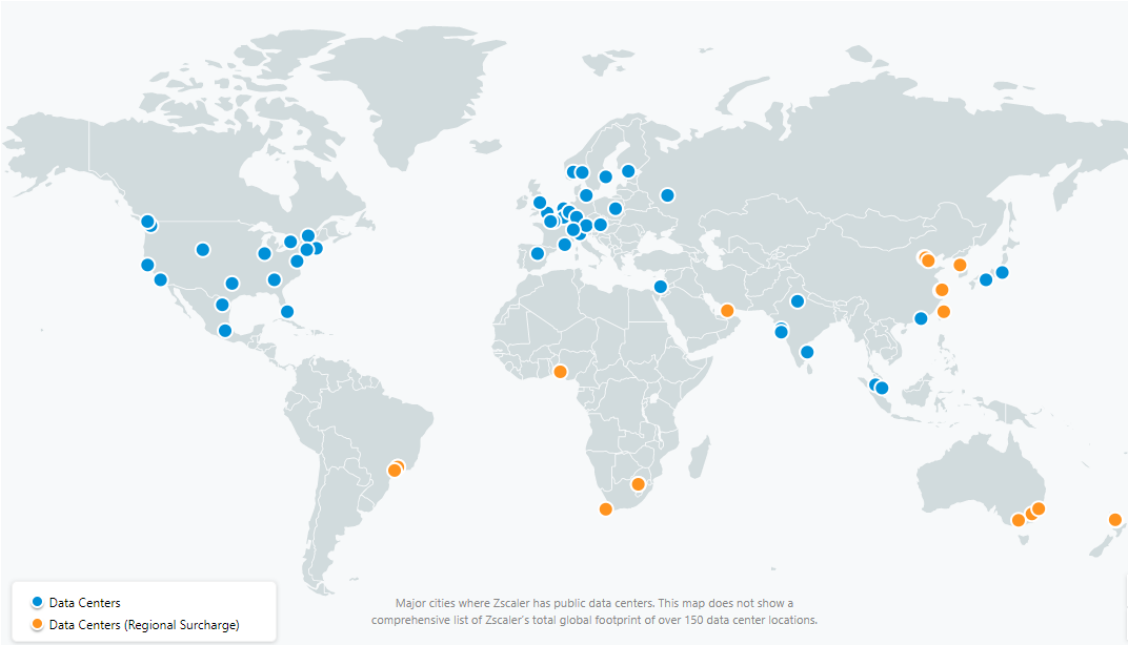


Ilustración 26: Red de puntos de presencia Zscaler
https://trust.zscaler.com/zscaler.net/data-center-map

Al igual que Netskope, Zscaler permite obtener visibilidad en tiempo real del estado de sus servicios en *Cloud* y la infraestructura de su red mediante la siguiente referencia[27]

Ambos proveedores disponen de una red de puntos de presencia extendida en todo el mundo siendo Netskope la que dispone de más centros de datos sobre todo la zona de América Latina y el Este asiático.

2.17.3. Service Level Agreement (SLA) y servicios de soporte

Netskope y Zscaler utilizan indicadores de nivel de servicio como **disponibilidad**, **latencia** o **protección de *malware*** en las diferentes soluciones de seguridad que ofrecen. En el caso de incumplimiento de algunos de estos indicadores están obligados a indemnizar al cliente mediante créditos, los cuales están detallados en sus contratos. El tipo de soporte que prestan van de un soporte básico a otros más avanzados los cuales ofrecen alcances y tiempos de respuestas diferentes ante una incidencia o consulta de un cliente.

Ambos proveedores utilizan los mismos indicadores en sus acuerdos, pero Zscaler lo hace de una manera más granular segmentando por sus diferentes servicios mientras que Netskope no es tan granular y se centra en tres categorías de servicio. Todo el detalle de estos indicadores y servicios de soporte se pueden consultar desde sus correspondientes páginas web Zscaler[28] y Netskope[29].

[27] https://trust.zscaler.com/zscaler.net
[28] https://www.zscaler.com/legal/sla-support
[29] https://www.netskope.com/es/support-terms

2.17.4. Licenciamiento de productos por capacidades

Netskope y Zscaler ofrecen sus productos por paquetes que corresponden con las diferentes soluciones que forman una arquitectura SASE completa. Estos paquetes se ofrecen al cliente por niveles, los cuales tienen diferentes capacidades de funcionalidad agrupados en *bundles* lo que implica un precio diferente por licencia. En las imágenes siguientes se muestran los productos y bundles de los proveedores de Netskope y Zscaler:

Productos y bundles Netskope

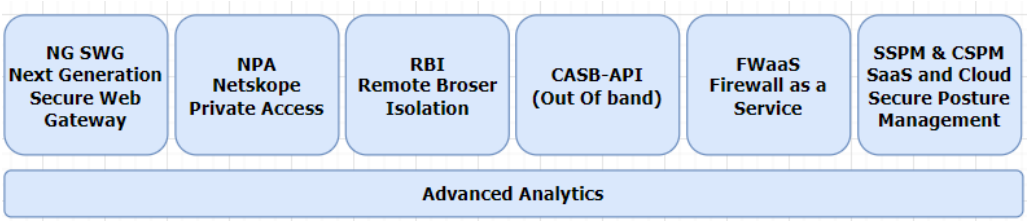


Ilustración 27: Productos de Netskope

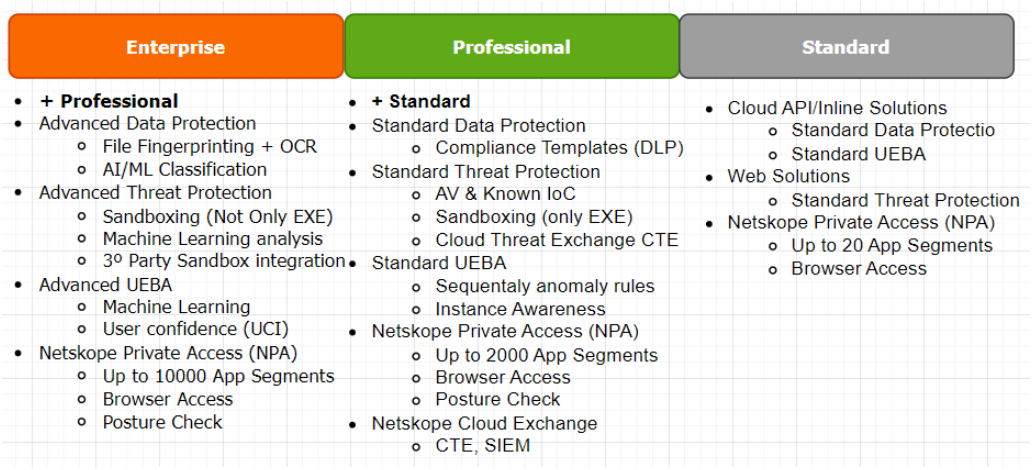


Ilustración 28: Bundles de Netskope

Productos y bundles Zscaler

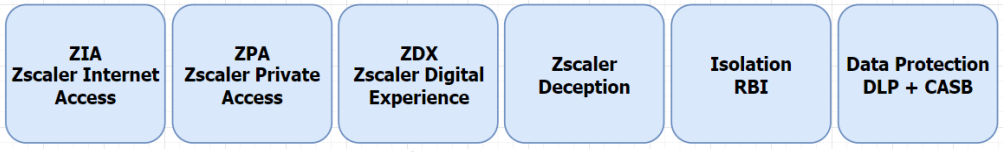


Ilustración 29: Productos de Zscaler

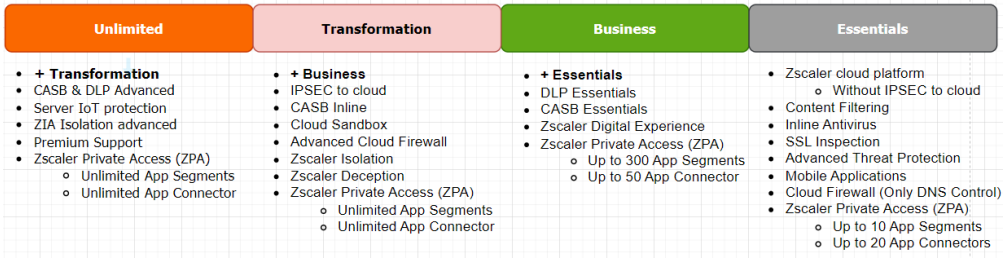


Ilustración 30: Bundles de Zscaler

2.17.5. Otros datos comparativos de interés

Segmentos de aplicación

Las aplicaciones internas que son accesibles por ZTNA se les llama segmentos de aplicación y pueden estar formados por URLs, IPs, puertos de comunicaciones los cuales forman el acceso a una aplicación concreta. Netskope ofrece más segmentos de aplicación que Zscaler. Comparando los *bundles* Professional y Business, Netskope ofrece 2000 frente a 300 de Zscaler.

ZTNA en la red interna

La solución ZTNA permite al personal de una organización acceder a las aplicaciones internas de una manera segura, con el mínimo privilegio y de una manera contextualizada, para ello es necesario colocar unas sondas en la red para que estas conecten con el PoP del proveedor SSE más cercano y se puedan establecer políticas de acceso centralizadas en la nube.

Cuando el personal de una organización trabaja remotamente ambos proveedores utilizan ZTNA de una manera similar, pero cuando el personal se ubica en la misma red donde se encuentra la aplicación interna es ineficiente salir a Internet para volver a entrar, para solucionarlo Zscaler ofrece una solución llamada *Private Service Edge* **PSE** la cual permite trasladar la seguridad ZTNA a la red interna cuando el personal trabaja desde dentro de la red corporativa. Por el momento, Netskope no ofrece esta solución y ofrece el *On Premises Detection* sin poder utilizar las ventajas de seguridad del ZTNA en la red interna.

FWaaS *Firewall as a Service*

Recordemos que *Firewall as a Service* FWaaS es una solución de seguridad en la nube que protege el tráfico de salida que se origina desde cualquier protocolo que no sea el de web. Ambos proveedores ofrecen FWaaS capa 4 y capa 7 pero en Netskope no está incluido con NG SWG, en cambio, Zscaler integra un *Basic Firewall* dentro de su solución de navegación *Zscaler Internet Access* ZIA.

Ingesta de eventos de seguridad a SIEM

La posibilidad de poder almacenar los eventos de seguridad que generan las soluciones SASE a un *Security Information and Event Management* SIEM es posible con ambas soluciones. Netskope proporciona la solución *Netskope Cloud Exchange* **CE** que está formada por una máquina virtual VM desplegada *on premises* la cual recoge los eventos de las soluciones de seguridad de Netskope y los envía al SIEM. Zscaler ofrece una solución parecida a la de Netskope, en cambio la mejora con la solución Cloud NSS que evita disponer de una VM *on premises* enviando los eventos directamente desde la nube de Zscaler al SIEM.

2.17.6. Madurez de las soluciones de seguridad

Zscaler lleva más años en el mercado que Netskope, aunque Netskope lídera las soluciones CASB, Zscaler destaca en las demás tecnologías como NG SWG y ZTNA. En la siguiente imagen se puede observar la madurez de las soluciones de seguridad de cada uno de los proveedores:

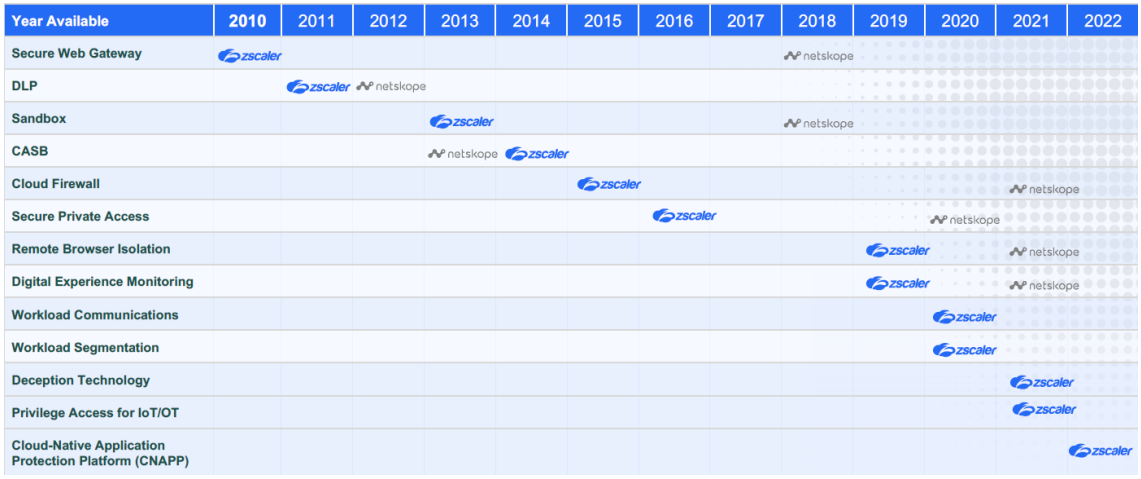


Ilustración 31: Madurez de las soluciones de seguridad (Netskope y Zscaler)

Ambos proveedores son competidores y ambos son muy buenas soluciones para poder ofrecer una arquitectura SASE.

2.18. La figura del *Partner*

Un *Partner* tecnológico es una figura importante en los proyectos tecnológicos porque acompaña y asesora en los procesos de transformación digital a las empresas. Los *Partners* permiten a las organizaciones delegar la operativa o la gestión de su infraestructura de IT con el objetivo que estas se puedan centrar en su actividad empresarial.

Los proveedores de soluciones SASE les interesa que su producto se implemente y se mantenga con éxito para dar una experiencia positiva a sus clientes, por ese motivo ellos mismos pueden ofrecen los contactos de sus Partners de confianza para garantizar una implementación exitosa en la *organización*.

2.19. Estudio económico de SASE

El estudio económico es una de las fases más importantes antes de comenzar cualquier proyecto porque permite conocer si su puesta en marcha será factible o no. Después de haber analizado las necesidades y el alcance de un proyecto de implementación de una arquitectura SASE hay que tener en cuenta los siguientes costes económicos:

Coste económico de licencias por usuario, el coste de la mayor parte de soluciones de seguridad que forman SASE se computa por identidad o persona con lo que es importante analizar las necesidades de la organización para poder

hacer un recuento lo más real posible con el objetivo de ajustar el presupuesto. Por ejemplo, si el personal empleado de una empresa hace uso de navegación por Internet y uso de aplicaciones en la nube, pero no necesitan acceder a recursos internos remotamente entonces necesitarán licenciamiento de la solución *Next Generation Secure Web Gateway* NG SWG pero no la de *Zero Trust Network Access* ZTNA.

Los proveedores pueden ofertar sus productos de seguridad por separado o por agrupación de productos o *bundles*, dependiendo de la necesidad y presupuesto de la empresa le puede interesar adquirir uno u otro. El coste orientativo de estos *bundles* son los siguientes[30]:

Bundle	**Coste**
ZIA + ZPA - Essentials / Standard	$42 / identity (1Year)
ZIA + ZPA - Business / Professional	$80 / identity (1Year)
ZIA + ZPA - Transformation / Enterprise	$130 / identity (1Year)

Ilustración 32: Coste orientativo *bundles*

En el caso de las soluciones de NG SWG y ZTNA por separado, el precio orientativo por son los siguientes:

Producto	**Coste**
ZIA / SWG – Essentials / Standard	$30 / identity (1Year)
ZIA / SWG – Business / Professional	$38 / identity (1Year)
ZIA / SWG – Transformation / Enterprise	$55 / identity (1Year)
ZPA / NPA – Essentials / Standard	$30 / identity (1Year)
ZPA / NPA – Business / Professional	$58 / identity (1Year)
ZPA / NPA – Transformation / Enterprise	$65 / identity (1Year)

Ilustración 33: Coste orientativo SWG y ZTNA por separado

Coste económico de soporte del producto, el soporte del producto consiste en disponer de un acceso telefónico o online al servicio técnico del proveedor para poder realizar consultas. Con el servicio de soporte se le da la oportunidad al cliente de poder acceder al conocimiento *knowledgebase* del producto o tener contacto con ingenieros de soporte para poder abrir casos o incidencias. Existen diferentes niveles de soporte los cuales indican que tipo de servicio se va a prestar, por ejemplo, la disponibilidad horaria del soporte (24x7 o 8x5) o el tiempo de respuesta de las consultas. El coste económico asociado al servicio de soporte suele venir implícito en el precio de las licencias por usuario y el cliente tiene la posibilidad de poder elegir el nivel que desee.

Coste económico de la implantación del proyecto, la planificación, gestión y operativas del proyecto son tareas necesarias que se pueden asignar a personal externo, personal interno o a *Partners* tecnológicos y es necesario tener en cuenta estos costes económicos asociados los cuales van ligados a la gestión interna y el tipo de organización que la empresa utilice.

[30] En este proyecto no se mostrarán los costes reales de licencia de los productos de los diferentes proveedores por razones de confidencialidad, pero sí un coste aproximado.

3. Fase de análisis

3.1. La empresa Zanomme, S.A

La empresa Zanomme, S.A es una empresa ficticia nacida en el año 1946 en Cataluña dedicada al mercado de perfumes y cosméticos, el gran éxito de sus productos internacionalizó la empresa con la apertura de tiendas en países de Europa y América y seguidamente en Asia y Oceanía. Zanomme, S.A dispone de filiales en México, España, Polonia, Rusia, China y Australia.

Zanomme, S.A tiene 400 tiendas repartidas en todo el mundo y un total de 2300 trabajadores, en la tabla inferior se puede ver el número total del personal empleado repartidos en cada una de sus localizaciones:

Código	País	Empleados	Descripción
BOHQ	España	820	Sede Central
BOCL	España	210	Centro logístico
BOLA	España	55	Laboratorios
BOMX	México	60	Sucursal México
BOPL	Polonia	50	Sucursal Polonia
BORU	Rusia	40	Sucursal Rusia
BOCH	China	25	Sucursal China
BOAU	Australia	40	Sucursal Australia
BOSH	-	1000	Tiendas en todo el mundo

Ilustración 34: Tabla del personal de Zanomme, S.A

Debido a la organización y modelo de negocio de años anteriores Zanomme, S.A es una empresa que tiene una inmadurez tecnológica importante y esto dificulta a sus objetivos estratégicos de transformación digital que quieren impulsar sus nuevos dirigentes. Debido a los ataques cibernéticos que han sufrido varias empresas en todo el mundo, Zanomme, S.A ha apostado por la creación de un departamento de ciberseguridad el cual es responsable de transformar la seguridad de la empresa con el objetivo de reducir los riesgos tecnológicos.

El departamento de ciberseguridad aboga con adquirir soluciones de seguridad y redes convergentes en la nube para poder implementar una arquitectura SASE con el objetivo de ir alineados con los objetivos estratégicos de la empresa. Seguidamente se muestra el estado actual de infraestructura y comunicaciones de la empresa (AS IS), los desafíos e impactos y el estado futuro (TOBE).

3.2. Estado actual (AS IS)

En el proyecto de implantación de una arquitectura SASE es importante conocer el estado actual de la infraestructura y comunicaciones con el objetivo de poder identificar de una manera más sencilla los desafíos e impactos en seguridad. La empresa Zanomme, S.A tiene el siguiente diagrama de red:

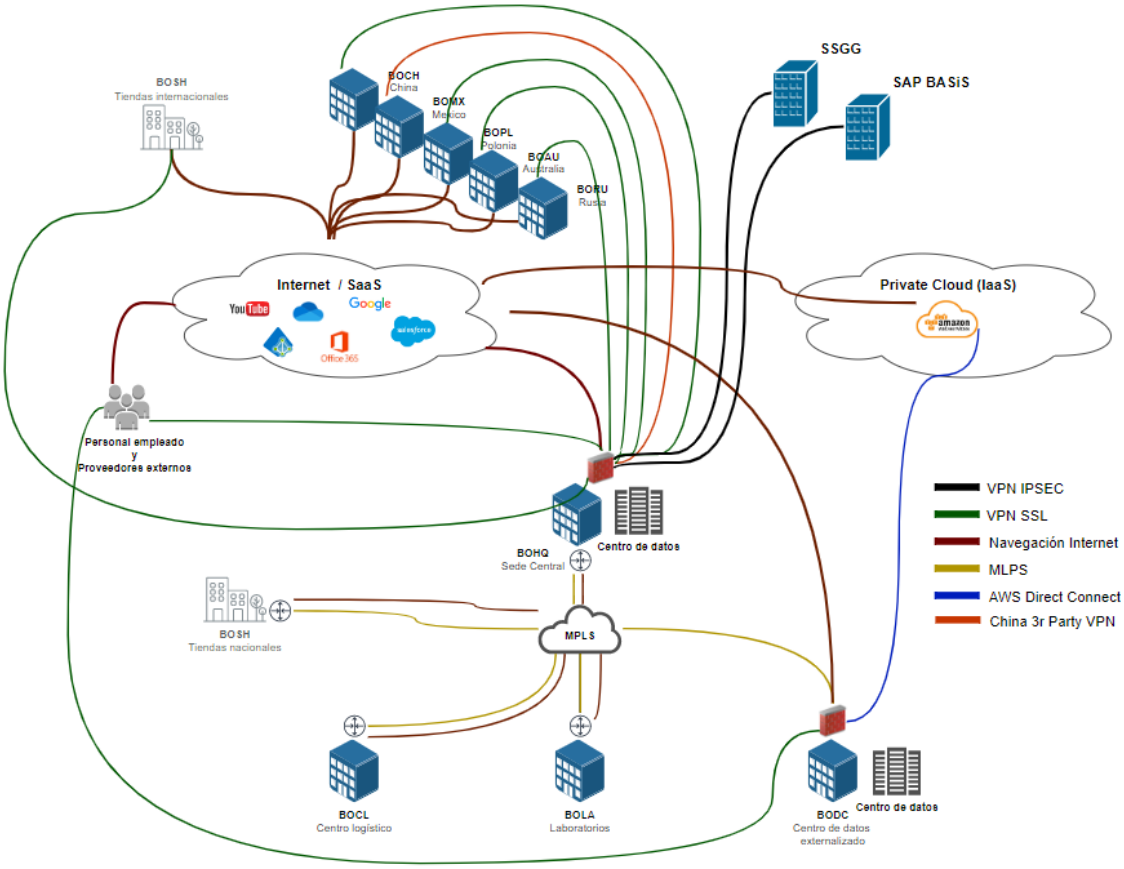


Ilustración 35: Diagrama de red de Zanomme, S.A (Situación actual)

En la leyenda de la imagen anterior se diferencian en diferentes colores las comunicaciones que participan en Zanomme, S.A, las comunicaciones de navegación a Internet, VPN SSL, VPN IPSEC, VPN de terceros para China, MPLS y AWS Direct Connect. Seguidamente, se muestra una tabla con los puntos más destacados del diagrama de la situación actual y una breve explicación.

Centros de datos (CPD)	**Instancias IaaS**
▪ CPD en sede central (BOHQ) ▪ CPD externalizado (BODC) **CPDs con granja de máquinas virtuales, storage, servicios y electrónica de red.*	▪ Amazon Web Services (AWS) **Servicio de consumo SaaS data warehouse (RedShift) y VMs de cómputo EC2.*
Cortafuegos Perimetrales (FW)	**Servicios VPN SSL**
▪ Cortafuegos en BOHQ ▪ Cortafuegos en BODC **Control de navegación por categorización y listas negras, control de aplicaciones, VPN SSL, VPN IPSEC, Enrutamiento redes internas, publicación a Internet de servicios.*	▪ VPN SSL en BOHQ ▪ VPN SSL en BODC ▪ VPN SSL para China (BOCH) **Terminadores VPN SSL corporativo en Central y en CPD externalizado, el terminador VPN SSL de China es de un software de terceros para evadir la seguridad del Firewall de China.*

Servicios VPN IPSEC	Servicios SaaS
▪ Túnel IPSEC con SSGG ▪ Túnel IPSEC con SAP Basis **Terminador de conexiones VPN IPSEC para poder establecer una conexión tunelizada y segura con los proveedores de servicios.*	▪ Microsoft Office365 ▪ Microsoft OneDrive ▪ Azure Identity Manager ▪ Salesforce CRM
Sucursales internacionales	**Sucursales nacionales**
▪ BOCH (China) ▪ BOMX (México ▪ BOPL (Polonia) ▪ BORU (Rusia) ▪ BOAU (Australia) ▪ Tiendas internacionales	▪ BOLA (Laboratorios) ▪ BOCL (Centro logístico) ▪ Tiendas Nacionales

Ilustración 36: Tabla informativa de infraestructura en Zanomme, S.A (Situación actual)

Para poder entender mejor la situación actual se hace un resumen de los flujos de comunicación y tecnología empleada:

1) El personal empleado ubicado en cualquiera de las sucursales nacionales como también las tiendas nacionales se conectan a Internet a través del cortafuegos de BOHQ centralizando el tráfico haciendo *backhauling*.

2) El personal empleado utiliza el servicio VPN SSL para conectar a recursos internos ubicados en los centros de datos e IaaS cuando están teletrabajando. La configuración de la VPN SSL es mediante *split tunneling* con lo que el acceso a Internet se dirige hacia el enrutador ISP donde está conectada la persona.

3) Las tiendas internacionales utilizan el servicio VPN SSL con el objetivo de poder alcanzar los recursos internos asociados al Punto de venta (POS). La configuración de la VPN SSL es mediante *split tunneling* con lo que el acceso a Internet se dirige hacia el enrutador ISP de la tienda.

4) Los servicios de VPN SSL que utilizan las tiendas internacionales, el personal empleado y los colaboradores autentican directamente con el Active Directory (AD) *on premises*.

5) El personal empleado de la sucursal China (BOCH) utiliza un servicio de VPN SSL de terceros debido a las restricciones del Firewall de China.

6) Las sucursales nacionales se interconectan con la tecnología MPLS para poder acceder a los recursos internos de los centros de datos.

7) Las tiendas nacionales utilizan la tecnología FlexWan integrado con la MPLS para poder alcanzar los recursos internos asociados al punto de venta (PoS).

8) La inspección del tráfico SSL no se realiza en ningún supuesto.

9) La prevención de pérdida de datos o fugas de información DLP no se realiza en ningún supuesto.

10) El *cloud* privado en Amazon Web Services AWS se utilizará para poder migrar servicios a la nube, actualmente se utiliza para el servicio de *Data Warehouse* RedShift.

11) El proveedor de servicios gestionados y el proveedor de SAP Basis disponen de una conexión tunelizada con IPSEC al cortafuegos de la sede central (BOHQ) para minimizar el uso de la VPN SSL.

12) Todos los equipos de la empresa están protegidos por la solución de *Endpoint Protection Platform* EPP + *Endpoint Detection Response* EDR para poder ofrecer una respuesta rápida ante los riesgos y amenazas.

3.3. Desafíos e impactos

Ahora que conocemos la infraestructura y comunicaciones de la empresa Zanomme, S.A se listan las situaciones que la empresa debería superar y mejorar **"desafíos"** como también las consecuencias que se ocasionarían en estas situaciones **"impactos"**. A continuación, se enumeran estos desafíos e impactos en el ámbito de la navegación en Internet y el acceso a aplicaciones en la nube (SaaS), en el acceso a los recursos internos a través de *Virtual Private Network* (VPN) y en el de la gestión de las políticas de seguridad.

3.3.1. Navegación en Internet y en aplicaciones SaaS

DESAFÍOS	IMPACTOS
Tráfico de navegación a Internet centralizado El tráfico a Internet de las sucursales y tiendas se centraliza en la sede central haciendo *backhauling*.	**Riesgo de infectarse con *malware*** Según un estudio de Zscaler ThreadLabz[31] El 70% del *malware* viaja cifrado con lo que la empresa no está protegida de esta amenaza.
Protección contra *malware* limitada No se inspecciona el tráfico SSL en la navegación a Internet y SaaS y no se dispone de Sandbox.	**Riesgo de fuga de información sensible** Exfiltración de datos como información de datos financieros como tarjetas de crédito, o información de identificación personal PII como el DNI.
Ninguna visibilidad de la navegación en Internet en el teletrabajo No hay visibilidad ni trazabilidad del tráfico a Internet de los empleado y colaboradores cuando están teletrabajando.	**Mínima evolución de la seguridad** La transformación de seguridad no está alineada con la transformación digital de la compañía.

[31] https://info.zscaler.com/resources-whitepaper-threatlabz-the-state-of-encrypted-attacks

Exposición de información sensible No hay monitorización ni control de la información confidencial que el personal empleado sube a plataformas de almacenamiento en la nube o mediante mensajería.	**Empeoramiento de la experiencia de usuario** La centralización incrementa la sobrecarga de los equipos de seguridad y hace que las latencias sean mayores.
Arquitectura no alineada con transformación en la nube La tecnología tradicional utilizada no está diseñada para el trabajo en la nube.	**Incremento de costes de red** La centralización del tráfico en un punto central hace que el crecimiento y escalabilidad sean más complejos.

Ilustración 37: Tabla desafíos e impactos de Zanomme, S.A. (Navegación Internet y SaaS)

3.3.2. Acceso recursos internos a través de VPN

DESAFÍOS	IMPACTOS
Problemas de acceso del personal de países con restricciones No es posible que países como China puedan utilizar la VPN Corporativa debido a las restricciones de conexión del Firewall Chino.	**Riesgo de movimientos laterales en la red** Un usuario dentro de la red puede moverse lateralmente entre recursos.
El personal conectado remotamente por VPN se sitúa dentro de la red El usuario tiene acceso a la red interna cuando establece la conexión por VPN a la empresa.	**Enumeración de servicios en la red** Un usuario con acceso a la red le permite escanear recursos y servicios internos debido a que tiene visibilidad de la red interna.
No hay contexto de la conexión del personal empleado No se realiza un control de acceso condicional de los equipos e identidades que se conectan remotamente a la empresa como, por ejemplo, denegar la conexión a un recurso en caso de que el dispositivo no tenga un antivirus o que el equipo no esté en el dominio interno.	**Riesgo de ataques DDoS** La necesidad de tener el servicio VPN a Internet aumenta la superficie de ataque aumentando el riesgo.
Activos de red expuestos a Internet Las conexiones VPN dependen de terminadores VPN que están expuestos a Internet.	**Riesgo de pérdida de rendimiento** En caso de sobrecarga en los equipos podrían generar micro cortes y latencias altas en el acceso a recursos.
Experiencia de usuario (UX) pobre El usuario necesita levantar la conexión VPN cada vez que arranca su equipo.	**Riesgo de introducción de *Malware*** Aumenta la probabilidad de infección de *malware* debido al no validar los equipos que se conectan por VPN a la red interna.
Alta carga de trabajo en los equipos de seguridad Las conexiones VPN sobrecargan los equipos de seguridad tradicionales debido a la centralización de estas conexiones.	**Riesgo de ataques de fuerza bruta en el Active Directory (AD) *on premise*.** Dada la dificultad de implantación de los sistemas de VPN con SSO en la nube se requiere autenticación con el AD lo que implica exposición del AD *on premises* a los terminadores VPN SSL.

Dificultad en la implantación del *Single Sign On* SSO en la nube. Los equipos que dan los servicios de VPN SSL autentican a través del Active Directory on premise debido a que no disponen de integración con SSO en la nube.	

Ilustración 38: Tabla desafíos e impactos de Zanomme, S.A. (Acceso VPN)

3.3.3. Gestión de políticas de seguridad

DESAFÍOS	IMPACTOS
Descentralización de las políticas de seguridad. Políticas de seguridad repartidas debido a diferentes equipos de seguridad independientes.	**Poca eficiencia del departamento de TI al aplicar medidas de seguridad.** El hecho de tener equipos de seguridad independientes hace que se multiplique el trabajo al gestionar políticas de seguridad.
Falta de coordinación entre las diferentes soluciones de seguridad. Cada sistema de seguridad actúa de una manera independiente sin una coordinación ni integración entre ellos.	**Mayor probabilidad de error humano** Al tener que gestionar políticas en los diferentes sistemas de seguridad por separado hace que aumente la probabilidad de error humano.
Complejidad en la ingesta de eventos de seguridad en el SIEM. Cada equipo de seguridad debe de hacer la ingesta sus eventos de seguridad por separado en el SIEM[32].	**Mayor coste económico y administrativo en la ingesta de eventos al SIEM.** La ingesta de eventos de seguridad de los sistemas de seguridad por separado incrementa la complejidad de correlación de eventos y aumento de caudal en el SIEM.
	Dificultad en medir los indicadores de gestión (KPI). Al disponer de múltiples portales de administración y de gestión, los KPIs de cada uno de ellos pueden dar datos generales incompletos.

Ilustración 39: Tabla desafíos e impacto de Zanomme, S.A (Gestión políticas)

3.4. Objetivos y requerimientos

En este punto vamos a especificar los requisitos o requerimientos que son necesarios para poder conseguir los Objetivos del Trabajo.

1) **Implementar una solución de navegación web segura en la nube para las personas empleadas de Zanomme, S.A independientemente del lugar de donde se encuentren.**

   Para conseguir este objetivo es necesario poner foco a la protección contra el *malware* y protección de la información en la navegación en Internet y en

[32] SIEM. *Security Information and Event Management*. Es un sistema que centraliza los eventos de seguridad con el objetivo de analizarlos y dar algun tipo de notificación.

el acceso a las aplicaciones en la nube (SaaS) y mantener esta misma seguridad a todas las identidades del personal de Zanomme, S.A. independientemente si navegan desde su casa, la oficina o cualquier otra ubicación. Seguidamente, se enumeran los requerimientos que Zanomme, S.A fijará para poder alcanzar este objetivo.

- Utilizar una arquitectura proxy de navegación en la nube con la solución de *Next Generation Secure Web Gateway* **NG SWG**.

- No utilizar la centralización de tráfico de navegación en ningún equipo perimetral de la empresa evitando así el *backhauling* y propiciar el *edge security*.

- Realizar inspección SSL/TLS de toda la navegación que no esté en términos de cumplimiento legal o de *compliance*.

- Disponer de *Advanced Threat Protection* **ATP**, detección de *malware* y también protección de amenazas desconocidas con soluciones Sandbox.

- Dejar de utilizar el concepto de túnel dividido o *split tunneling* con el objetivo de que todo el tráfico de navegación viaje cifrado hacia NG SWG.

- Utilizar un *Endpoint Protection Platform* **EPP** + *Endpoint Detection Response* **EDR** en todos los equipos corporativos. Aunque las soluciones de arquitecturas SASE ya disponen de esta protección en la navegación es recomendable que cada equipo corporativo tenga una solución EPP+EDR para tener doble capa de protección contra el *malware*.

- Integrar los *Indicators of Compromise* IoC[33] con la solución EDR actual de Zanomme, S.A. con el objetivo proteger de una manera más eficiente los accesos.

2) Implementar una solución de acceso de confianza cero evaluando la identidad y el contexto de la conexión a los recursos internos de Zanomme, S.A para el personal interno y externo que trabajan remotamente.

Asegurar y garantizar con una buena experiencia el acceso a los recursos internos independientemente desde donde se conecten las personas es un objetivo primordial para Zanomme, S.A. Una de las premisas para conseguirlo es sustituir las conexiones *Virtual Private Network* VPN de la compañía por una solución *Zero Trust Network Access* ZTNA en la nube. Una de las ventajas en seguridad que aportaría ZTNA contra las VPN sería la de evitar situar los equipos en la red interna con el objetivo de eliminar el riesgo de movimientos laterales en la red y enumeración de servicios. Seguidamente, se enumeran los requerimientos que Zanomme, S.A fijará para poder alcanzar este objetivo.

[33] IoC : Es cualquier información relevante que describe cualquier incidente de seguridad, por ejemplo el hash de un fichero o una dirección IP.

- Disponer de una arquitectura de Zero Trust Network Access ZTNA en la nube.

- El cliente de ZTNA en los equipos debe de ser el mismo que se utiliza para la navegación por NG SWG.

- El personal empleado interno y proveedores con equipo corporativo deben de poder acceder a los recursos internos siempre y cuando se cumpla el contexto de conexión o postura de seguridad del equipo, la cual debe de cumplir lo siguiente:

  - ✓ Protegido por el antivirus corporativo.
  - ✓ Estar en el dominio interno.
  - ✓ Cifrado de disco con el producto BitLocker

  En el caso de los equipos no corporativos que usen proveedores o colaboradores solo necesitarán estar protegidos por un antivirus.

- El acceso a ZTNA será transparente por el personal y no será necesario hacer ninguna acción para iniciar ni cerrar el acceso.

- Eliminar los terminadores VPN SSL de la empresa y así reducir la carga del cortafuegos perimetral como también la superficie de exposición en Internet.

- Mejorar la experiencia del personal con la reducción de latencias en las comunicaciones.

- Reducir la complejidad de puesta en marcha de las tiendas a nivel de comunicaciones como también reducir la gestión administrativa asociado a las comunicaciones.

- Dotar a la sucursal China BOCH de la misma solución ZTNA para el acceso a recursos internos para dejar de utilizar soluciones de VPN SSL de terceros.

3) Identificar la extracción no aprobada de datos sensibles y confidenciales de una organización realizada entre o hacia instancias de aplicaciones en la nube.

La información es un activo muy importante para las empresas por esa razón Zanomme, S.A necesita proteger los datos y tener el control de que operaciones se hacen con estos. Se enumeran los requerimientos que Zanomme, S.A fijará para poder alcanzar este objetivo.

- Utilizar Cloud Access Security Broker **CASB** para controlar las acciones que se realizan en las aplicaciones Shadow IT.

- Utilizar *Data Loss Prevention* **DLP** para evitar la fuga de información confidencial de la empresa como también datos de identificación personal (PII) de los clientes y empleados.

- El cliente utilizado para los equipos debe de ser el mismo que para las soluciones NG SWG y ZTNA.

4) Gestionar y controlar de una manera centralizada en una sola consola los componentes de seguridad en la nube que forman parte de la arquitectura SASE.

La plataforma de seguridad en la nube debe de permitir una visibilidad de los datos de navegación y accesos en tiempo real, una gestión eficiente de las políticas de seguridad y la administración de todas las soluciones mediante una única consola. Con *Secure Service Edge* **SSE** todas las soluciones que forman la arquitectura SASE convergen e integran para poder dar una mejor respuesta a las amenazas de la red. Se enumeran los requerimientos que Zanomme, S.A fijará para poder alcanzar este objetivo.

- Administrar la plataforma de seguridad en la nube desde una única consola.

- Gestionar de una manera simple y centralizada las políticas de seguridad con el objetivo de facilitar la tarea de administración al personal de seguridad.

- Disponer de indicadores de desempeño o *Key Performance Indicators* **KPI**[34] con el objetivo de resumir la eficacia de las acciones que realizan las soluciones de seguridad utilizadas.

- Ingestar los eventos de seguridad deseados a un SIEM con la finalidad de poder crear casos de uso para notificar y alertar de incidentes de seguridad.

3.5. Estado futuro (TO BE)

En el siguiente diagrama de red se puede observar el cambio de comunicaciones que se consigue con los objetivos y requerimientos definidos anteriormente:

[34] KPI: *Key Performance Indicator* o Indicador de desempeño se utiliza para cuantificar el grado de cumplimiento de los objetivos con el propósito de reflejar el estado actual de estos.

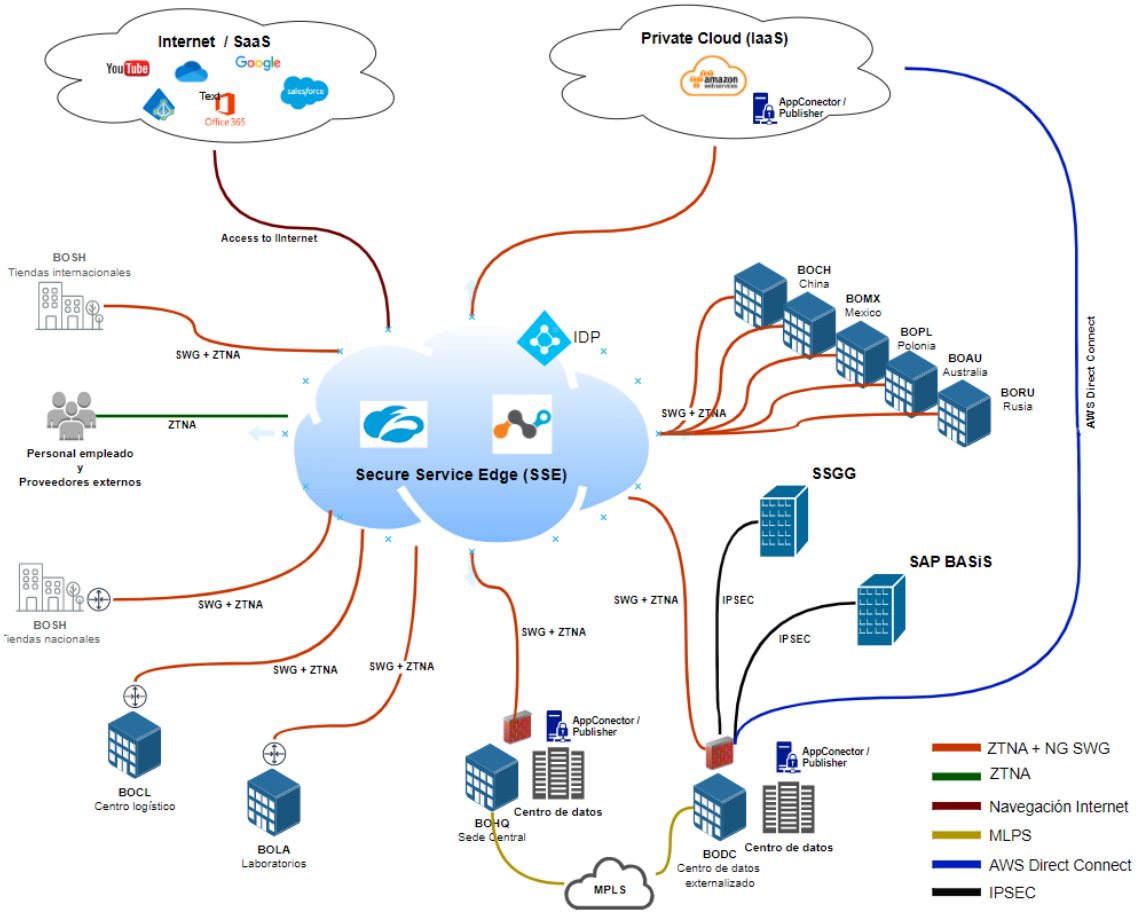


Ilustración 40: Diagrama de red de Zanomme, S.A (Situación futura)

Se observa que la navegación en Internet y a aplicaciones en la nube de todas las sucursales, tiendas y personal empleado como el acceso a recursos internos de la compañía se centralizan en el *Secure Service Edge* SSE mediante las soluciones de seguridad de NG SWG y ZTNA. El centro de datos de BOHQ deja de centralizar las comunicaciones y deja de ser un punto crítico en la compañía.

Se elimina la necesidad de centralizar el tráfico de la navegación mediante el cortafuegos de BOHQ evitando el *backhauling* y reduciendo la necesidad de este cortafuegos para la navegación de múltiples sucursales. Con esto se minimiza el uso de la MPLS y la carga del cortafuegos.

Se elimina la necesidad de hacer *split-tunneling* en la navegación en Internet de sucursales, personal empleado y tiendas internacionales. El tráfico de navegación viaja cifrado hacia *Secure Service Edge* SSE en la nube independientemente donde el personal empleado o colaboradores externos se conecten.

Se elimina la necesidad de autenticar con el Active Directory *on premises* desde las soluciones tradicionales de VPN delegando la autenticación al *Azure Identity Management* también en la nube.

Se reduce la complejidad de la gestión y administración de las políticas de seguridad de la infraestructura debido a que las soluciones se centralizan en la nube con *Secure Service Edge* SSE, mediante una única consola se consigue

gestionar la seguridad de las soluciones de seguridad NG SWG y ZTNA. Seguidamente, se muestra una tabla con los componentes añadidos en el diagrama:

<table>
<tr><th>Azure Identity Management</th><th>AppConnector / Publisher</th></tr>
<tr><td>IDP (Identity Provider)
*Las soluciones de seguridad de NG SWG y ZTNA delegaran la autenticación de las identidades con el IDP de Azure. Evita usar la autenticación directamente del Active Directory on premises. Permite el múltiple factor de autenticación MFA para una mayor seguridad.</td><td>Desplegado en BOHQ
Desplegado en BODC
Desplegado en AWS
*Corresponden a máquinas virtuales VM desplegadas en cada uno de los centros de datos donde es necesario acceder por ZTNA. Los Appconnectors/Publishers no están publicados a Internet solo conectan del centro de datos a la nube SSE con el objetivo de poder dar acceso a los recursos internos mediante ZTNA.</td></tr>
<tr><th colspan="2">Secure Service Edge (SSE)
Netskope o Zscaler</th></tr>
<tr><td colspan="2">Secure Service Edge (SSE)
*El Secure Service Edge SSE es el cerebro e integrador de las soluciones de seguridad SASE, en nuestro caso de las soluciones NG SWG y ZTNA. En este caso se ponen de ejemplos los dos proveedores elegidos Netskope y Zscaler.</td></tr>
</table>

Ilustración 41: Tabla informativa de infraestructura en Zanomme, S.A (Situación futura)

3.6. Resumen situación actual vs situación futura

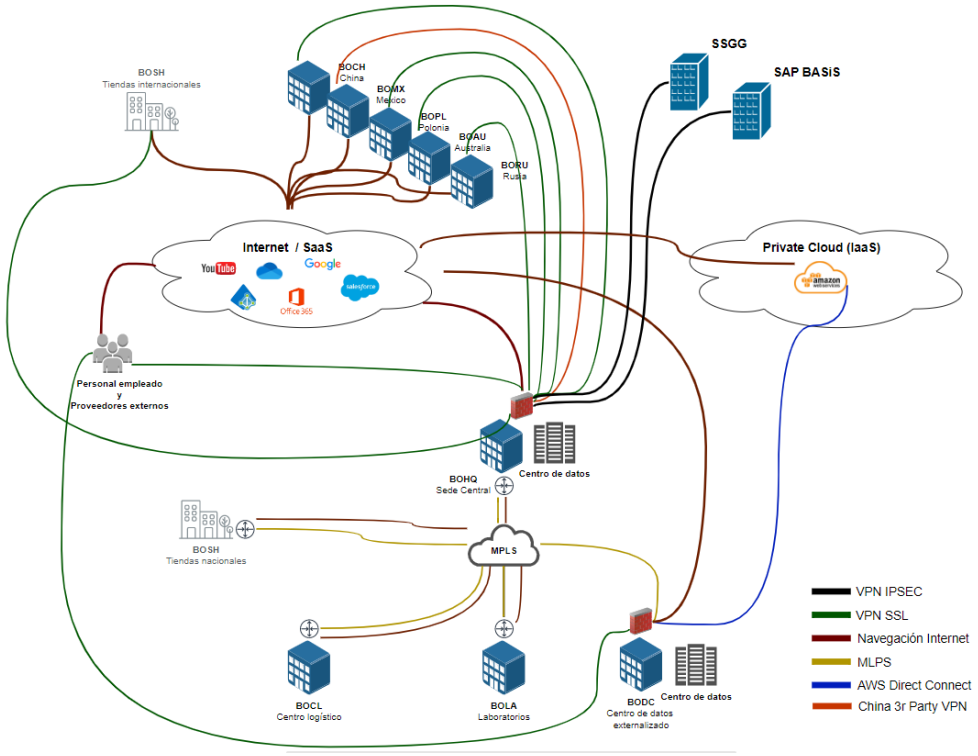
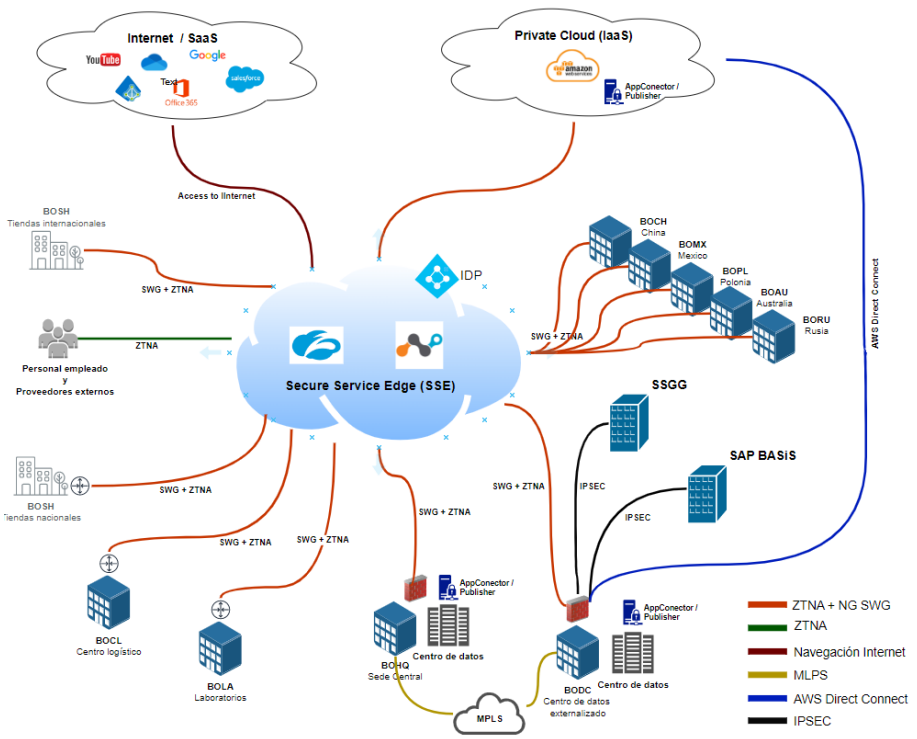
Situación actual (As Is)	Situación futura (To Be)
	
• **Problemas de seguridad en la navegación** a Internet y a aplicaciones en nube (*split-tunnel*). • **Descontrol de accesos** en la red con VPN, se sitúa al equipo de la persona en la red interna. • **Concentradores de VPN SSL expuestos.** • **Centralización de tráfico en cortafuegos *backhauling*** el cual incrementa costes de red. • **Arquitectura no alineada con la transformación *cloud* de la compañía.**	• **Solución de seguridad SaaS unificada** con un *tenant* único. • **Política de acceso y seguridad común**, independientemente del tipo de usuario, localización y dispositivo. • **Visibilidad y monitorización** del tráfico en la navegación y hacia aplicaciones internas. • **Mejora de la experiencia de usuario**. • **El usuario no se sitúa en la red interna** al acceder a aplicaciones internas, eliminando el movimiento lateral y enumeración de servicios en la red.

Ilustración 42: Resumen situación actual vs situación futura

3.7. Análisis de las aplicaciones internas utilizadas

Para poder implementar la solución *Zero Trust Network Access* ZTNA con el objetivo de dar acceso a aplicaciones internas al personal empleado en Zanomme, S.A es necesario hacer un análisis de las aplicaciones con el fin de crear las políticas de acceso, seguidamente se muestra una tabla con las aplicaciones y servicios que se deberían dar de alta en las políticas de ZTNA:

Aplicación interna	Descripción
Active Directory DNS	Acceso a la resolución de nombres del DNS interno.
Active Directory DC	Acceso a los controladores de dominio on premise para la actualización de directivas y Kerberos.
wsus	Windows Update Services para el provisionamiento de actualizaciones de Windows.
cifs	Acceso a los recursos compartidos on premise.
sap gui	Acceso al ERP SAP mediante su aplicación.
ecommerce backend	Servicio PaaS para la administración del ecommerce.
pim	Product Information Management para la gestión de la información de productos.
ssh management	Acceso SSH para administrar servidores.
rdp management	Acceso de escritorio remoto para administrar servidores.
legal app	Acceso a la aplicación de expedientes del departamento de Legal.
salesforce CRM	Servicio SaaS para la gestión de cliente de la compañía.
office365	Servicio SaaS para el uso de las herramientas colaborativas y correo electrónico (Teams, Outlook, Sharepoint, OneDrive).

Ilustración 43: Tabla de aplicaciones internas utilizadas en Zanomme, S.A

Cabe destacar que en algunas de estas aplicaciones internas se necesita el acceso a entornos alternativos de preproducción, calidad y desarrollo. Los servicios de SaaS y PaaS están protegidos mediante lista blanca de IPs públicas, el acceso a estos servicios se realizará mediante ZTNA obteniendo la IP de la sede mediante su correspondiente AppConector o Publisher.

3.8. Proveedor SASE elegido

Zscaler tiene un producto de *proxy* web NG SWG más avanzado y maduro que Netskope debido a que nació con esta tecnología y aporta una gran experiencia mientras que Netskope es líder en la protección de las aplicaciones SaaS en la nube con CASB.

Ilustración 44: Logo de Netskope

Ambos proveedores son líderes en las soluciones de *Secure Service Edge* SSE y ambas empresas son muy aptas para poder implementar SASE en cualquier empresa, pero por la facilidad y flexibilidad de poder desplegar una prueba de valor POV se elige **Netskope** para realizar la fase de implementación de este proyecto.

4. Fase de Implementación

En esta fase de implementación se realiza una prueba de valor PoV para poder evaluar las soluciones de seguridad SASE adquiridas con el objetivo de hacer frente a los requerimientos definidos en la fase de análisis de este proyecto y demostrar así que las soluciones de seguridad en la nube propuestas ayudan en la estrategia de transformación digital de Zanomme, S.A.

Las soluciones de seguridad en la nube a evaluar en esta PoV serán *Next Generation Secure Web Gateway* **NGSWG**, Zero Trust Network Access **ZTNA**, *Cloud Access Security Broker* **CASB** y *Data* Loss Prevention **DLP** con el proveedor Netskope.

En paralelo al lanzamiento de esta PoV se realizan PoCs de cada una de las soluciones de seguridad para garantizar que funcionan correctamente y cumplen su objetivo. La PoV consiste en diferentes fases resumidas a continuación:

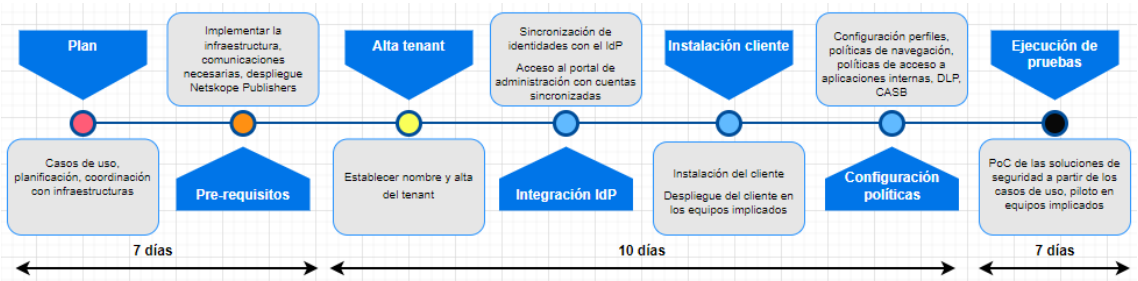


Ilustración 45: Fases de la prueba de valor PoV

Plan, es la primera fase y consiste en la preparación y planificación de la PoV, en esta etapa se definen los diferentes casos de uso y la coordinación con los diferentes departamentos implicados.

Provisión del *tenant*, se establece un nombre de *tenant* para que el proveedor Netskope lo de de alta en la nube con el objetivo de poder empezar a configurarlo y usarlo.

Pre-Requisitos, en esta fase se prepara la infraestructura y las comunicaciones necesarias para poder desplegar las máquinas virtuales de Netskope, como los Publisher, el Netskope Cloud Exchange CE y los clientes.

Integración con IdP, es la fase donde se sincronizan las identidades de la organización con el *Identity Provider* **idP** y el acceso al portal de administración con el fin de poder establecer las políticas de seguridad y de acceso.

Instalación del cliente, esta fase consiste en evaluar y probar los métodos de instalación del cliente de Netskope con el objetivo de poder desplegarlo por toda la compañía de una manera ágil.

Configuración de políticas de seguridad, se prepara los perfiles de inspección del tráfico, se dan de alta los segmentos de aplicación, las políticas de

navegación, reglas DLP, CASB, acceso a aplicaciones internas entre otras configuraciones alineados con los casos de uso definidos en el plan.

Ejecución de pruebas, finalmente se prueban los diferentes casos de uso en un equipo controlado con el objetivo de hacer una prueba de concepto PoC de cada solución de seguridad y finalmente probarlos en un conjunto de equipos para demostrar que la arquitectura y herramientas propuestas dan valor para la compañía.

4.1. Plan

Antes de empezar a realizar cualquier prueba es necesario trazar un plan para saber qué pruebas realizar, medir tiempos de cada una de las fases e involucrar a los departamentos implicados, para ello se describen los casos de uso y la planificación de la PoV.

4.1.1. Planificación de la PoV

Id	Tarea	Inicio	Fin	Duración
4.1	**Plan**			
4.1.1	Planificación de la PoV	**06/12/2022**	07/12/2022	2
4.1.2	Definir casos de uso	08/12/2022	09/12/2022	2
4.1.3	Coordinación con departamentos implicados	12/12/2022	13/12/2022	2
4.2	**Provisión del tenant**			
4.2.1	Establecer el nombre del tenant	14/12/2022	15/12/2022	2
4.2.2	Creación del tenant	16/12/2022	16/12/2022	1
4.3	**Pre-requisitos**			
4.3.1	Analizar y ejecutar los requerimientos de comunicaciones	19/12/2022	19/12/2022	1
4.3.2	Preparar los Netskope Publisher	19/12/2022	21/12/2022	3
4.3.3	Preparar el Netskope Cloud Exchange (CE)	19/12/2022	21/12/2022	3
4.4	**Integración del idP (Azure AD)**			
4.4.1	Creación de grupos de administración y provisión	21/12/2022	22/12/2022	2
4.4.2	Provisión de usuarios SCIM	23/12/2022	26/12/2022	2
4.4.3	Configuración de la autenticación SAML	23/12/2022	26/12/2022	2
4.4.4	Configuración de Netskope administration console	23/12/2022	26/12/2022	2
4.5	**Instalación del cliente de Netskope**			
4.5.6	Instalación manual	26/12/2022	27/12/2022	2
4.5.7	Instalación por el MDM de WorkSpaceOne de Vmware	26/12/2022	28/12/2022	3
4.5.8	Instalación por directivas de grupo (GPO)	26/12/2022	28/12/2022	3
4.6	**Configuración de políticas de seguridad**			
4.6.1	Steering configuration	29/12/2022	30/12/2022	2
4.6.2	Inspección SSL/TLS	29/12/2022	30/12/2022	2
4.6.3	Configuración del cliente	29/12/2022	30/12/2022	2
4.6.4	Segmentos de aplicación	29/12/2022	02/01/2023	3
4.6.5	Politicas de seguridad SWG	30/12/2022	02/01/2023	2
4.6.6	Políticas de seguridad ZTNA	02/01/2023	03/01/2023	2
4.6.7	Reglas y políticas de Data Loss Prevention (DLP)	02/01/2023	04/01/2023	2
4.6.8	Políticas de CASB	02/01/2023	04/01/2023	2
4.7	**Ejecución de pruebas**			
4.7.1	Pruebas controladas con un equipo (PoCs)	04/01/2023	07/02/2023	3
4.7.2	Piloto con diferentes equipos de diferentes areas funcionales	07/01/2023	**10/01/2023**	3

Ilustración 46: Tabla de planificación de la prueba de valor (PoV)

4.1.2. Casos de uso

Objetivo	Caso de uso	Prueba de caso
NG SWG - Mejora de la seguridad en la navegación web.	**1.1.** Aplicación de políticas de seguridad consistentes y granulares a través de la sincronización de identidades de la compañía.	**1.1.1.** Validar Integración de Netskope con Azure AD. **1.1.2.** Comprobar el provisionado de identidades en Netskope a través del idP. **1.1.3.** Comprobar la autenticación con MFA de las identidades en Netskope.
	1.2. Filtrado en la navegación web	**1.2.1.** Aplicar políticas de filtrado de direcciones web (whitelist y blacklist) a personas o grupos, tipos de dispositivo. **1.2.2.** Aplicar políticas de filtrado de direcciones web a través de sus categorías (New created domains, no categorizados, etc) a personas o grupos, tipos de dispositivo.
	1.3. Protección contra las amenazas	**1.3.1.** Aplicar políticas de protección y bloqueo de *malware*.
	1.4. Inspección del tráfico SSL/TLS y *steering configuration*	**1.4.1.** Crear excepciones en la inspección SSL/TLS a aplicaciones con certificado fijado o Certificate Pinned. **1.4.2.** Aplicar reglas de steering configuration para evitar que el tráfico de determinadas aplicaciones pase por la nube de Netskope.
	1.5. Control de acceso de las aplicaciones en la nube	**1.5.1.** Aplicar controles de subida y descarga de datos a aplicaciones de Microsoft o Gmail de cuentas que no sean corporativas (CASB). **1.5.2.** Aplicar controles de descarga y subida de datos a páginas catalogadas como web storage (CASB).
NG SWG - Protección de los datos sensibles y confidenciales	**2.1.** Prevenir las fugas de información.	**2.1.1.** Bloquear o advertir al usuario en caso de que envíe información clasificada como confidencial o secreta. **2.1.2.** Notificar a los administradores en caso del envío de datos sensibles o confidenciales.
	2.2. Garantizar el cumplimiento regulatorio	**2.2.1.** Bloquear o advertir a las personas en caso de que se envíen datos con información de PII (Cumplimiento GDPR). **2.2.2.** Notificar a los administradores en estos casos.

ZTNA - Acceso seguro con un mínimo privilegio y contextualizado a aplicaciones internas	**3.1.** Sustituir el uso de la VPN a las personas que necesiten conectarse a aplicaciones internas.	**3.1.1.** Comprobar la instalación del cliente de Netskope mediante GPO de dominio. **3.1.2.** Comprobar la instalación del cliente de Netskope mediante Vmware WorkSpaceOne (MDM). **3.1.3.** Valorar la experiencia de usuario al no necesitar conectar o desconectar la conexión a la compañía.
	3.2. Proporcionar microsegmentación de los recursos a través de la identidad de la persona y contexto de conexión.	**3.2.1.** Comprobar el acceso granular a las aplicaciones internas para las personas y grupos estrictamente necesarios (servidores de ficheros, controladores de dominio, …). **3.2.2.** Comprobar que las directivas de grupo del dominio y scripts de inicio se aplican correctamente. **3.2.3.** Comprobar que los equipos con acceso con ZTNA no se sitúan en la red corporativa con el objetivo de evitar la enumeración de servicios en la red interna. **3.2.4.** Comprobar la pérdida de acceso de ZTNA a los equipos que en un determinado momento no cumpla con la postura de seguridad establecida.
SSE - Administración centralizada y eficiente de las políticas de seguridad y visibilidad total de las soluciones de seguridad empleadas.	**4.1.** Visibilidad total de los eventos de las soluciones de seguridad en la nube de Netskope.	**4.1.1.** Comprobar en envío de eventos completos e integrados con las diferentes soluciones de seguridad al SIEM corporativo. **4.1.2.** Visualizar los eventos en tiempo real de la navegación y acceso a recursos de las personas y equipos conectados. **4.1.3.** Comprobar la facilidad de administración desde una única consola.

Ilustración 47: Tabla de casos de uso de la prueba de valor (PoV)

4.2. Provisión del tenant de Netskope

La plataforma de administración de Netskope es una aplicación web SaaS centralizada desde la cual es posible gestionar y administrar todas las soluciones de seguridad desde una única consola, el acceso a esta plataforma se realiza a través de una dirección web única para cada compañía la cual tiene el siguiente formato:

https://**<nombre-tenant>**.**<ubicacion>**.goskope.com

Donde **nombre-tenant** y **ubicación** es un nombre que lo establece el cliente y suele tener el nombre de la compañía y su localización. Para poder disponer de este acceso es necesario contactar con el preventa o comercial de Netskope para que ayude a provisionar el *tenant*. En el caso de Zanomme, S.A el nombre del tenant es el siguiente:

https://zanomme.eu.goskope.com

Una vez el *tenant* esté provisionado será posible acceder a la plataforma centralizada de administración a través de la dirección web definida para el *tenant* y unas credenciales creadas por el preventa o comercial de Netskope. El aspecto que tiene la consola de administración es la siguiente:

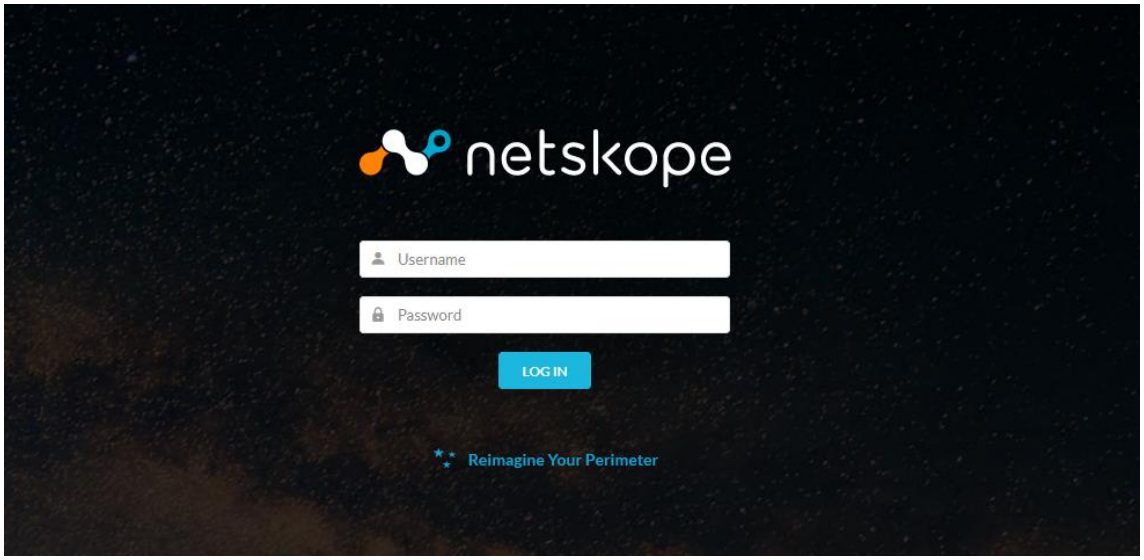


Ilustración 48: Acceso a la consola de administración de Netskope

4.2.1. Consola de administración

La consola de administración de Netskope está formada por una columna de opciones y un *dashboard* central y tiene el siguiente aspecto:

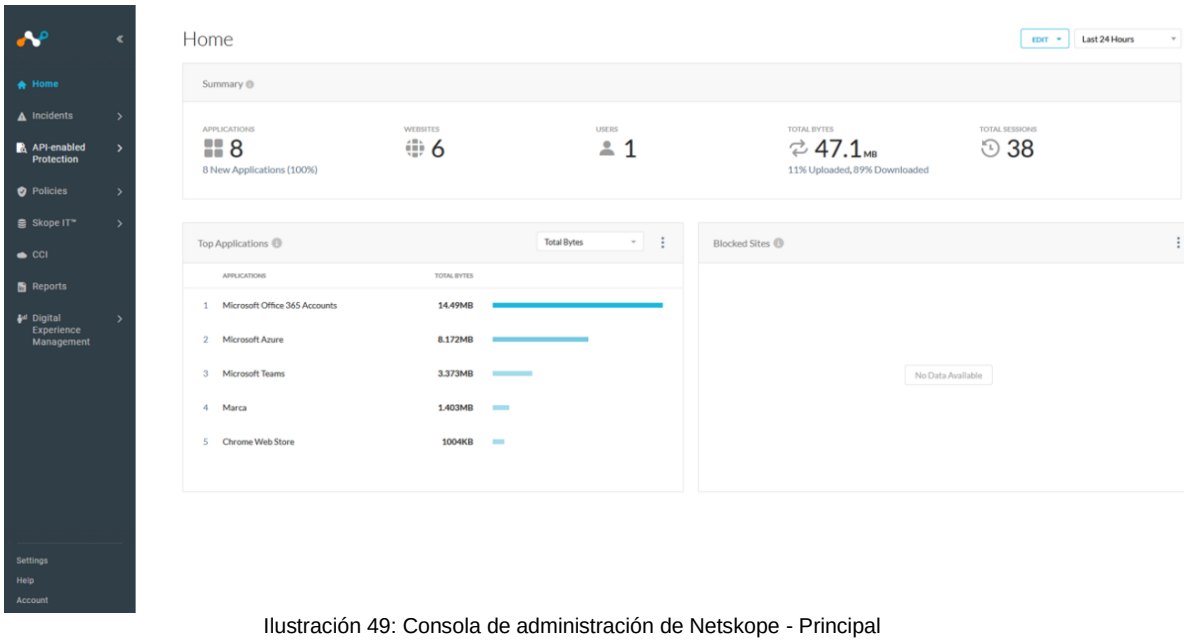


Ilustración 49: Consola de administración de Netskope - Principal

Como se puede ver en la anterior imagen se puede diferenciar diferentes secciones en la columna de la izquierda:

Home, corresponde con la sección principal donde se muestra el resumen por fecha de aplicaciones y sitios web accedidos, resumen de alertas de DLP y *malware* entre otra información.

Incidents, en esta sección se muestran con más detalle los eventos relacionados con incidentes de DLP, *malware*, sitios maliciosos y comportamiento que han realizado las personas que tienen el cliente de Netskope.

API-enabled Protection, se utiliza para la protección fuera de banda de aplicaciones en la nube. La inspección del contenido no es en tránsito si no que es en la aplicación directamente. Netskope inspecciona el tráfico con una conexión directa a la aplicación en la nube mediante sus correspondientes APIs y mediante el protocolo OAuth[35].

Policies, se muestran las políticas de seguridad configuradas para las diferentes soluciones de seguridad, como son las políticas de inspección de SSL/TLS, las reglas de navegación NG SWG, reglas de acceso a aplicaciones internas ZTNA, perfiles de DLP, Web, instancias de aplicaciones, entre otras opciones.

Skope IT, en esta sección se pueden encontrar todas las aplicaciones y sitios web accedidos por las personas de la compañía como también los eventos de aplicación, red y alertas.

CCI, corresponde con el acrónimo de *Cloud Confidence* Index[36] y es la sección que muestra el índice de confianza de más de 54.000 aplicaciones en la nube.

[35] OAuth: https://oauth.net/2/

[36] https://docs.netskope.com/en/cloud-confidence-index.html

Este índice se obtiene de la evaluación de más de 48 criterios. En esta sección se puede consultar el nivel de confianza de una aplicación en la nube.

Reports, corresponde al *reporting* del portal de administración, en esta sección es posible crear *reports* personalizados a partir de una librería. Estos *reports* se pueden lanzar *ad hoc* o programarlos para que se vayan ejecutando periódicamente.

Digital Experience Management, se puede ver el resumen de actividad en tiempo real del *tenant* con el objetivo de poder tener métricas para garantizar la seguridad sin comprometer el rendimiento, así como el estado de los servicios de Netskope, rendimiento de los Netskope Publisher o incluso latencias en cada uno de los PoPs, etc.

Settings, esta sección es utilizada para poder definir la configuración del tenant como el *Single Sign On* (SSO) con el idP, definición de segmentos de aplicación, obtener los Audit logs, alta de los Netskope Publisher entre otras muchas más opciones de configuración. La sección de Settings tiene el siguiente aspecto:

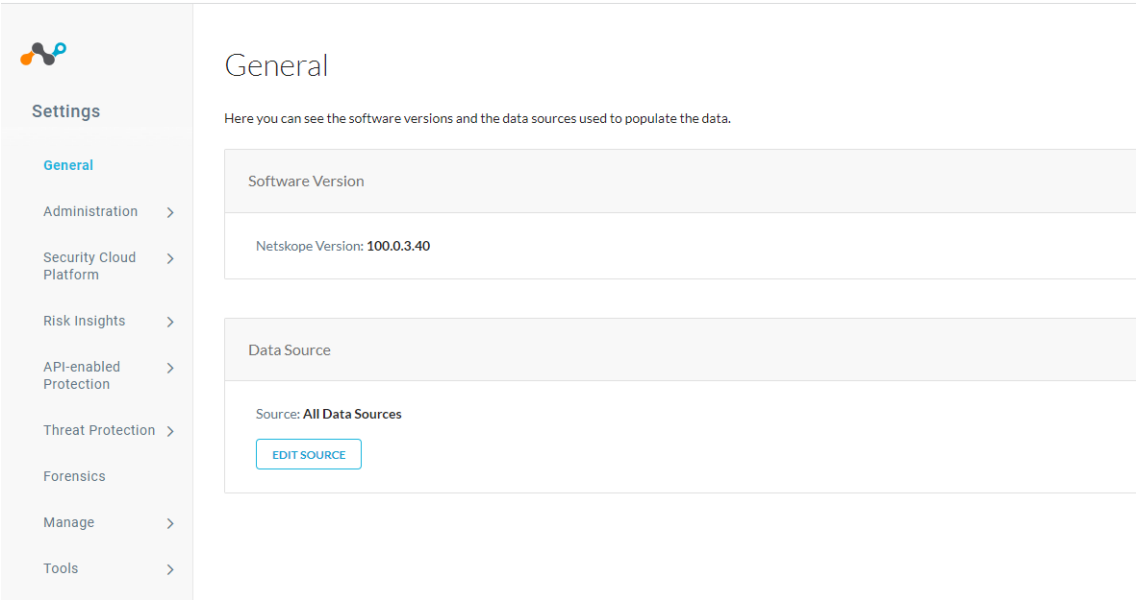


Ilustración 50: Consola de administración de Netskope - Settings

4.3. Preparación de los componentes

Es importante cumplir con una serie de necesidades y requerimientos antes de poder empezar a la configuración de políticas de seguridad y realizar pruebas de concepto. Los requerimientos de comunicaciones, la preparación de los Netskope Publisher y el Netskope Cloud Exchange son algunos de ellos.

4.3.1. Netskope Publisher

Los Publisher son máquinas virtuales VM desplegadas en los centros de datos *on premises* de una organización o en entornos IaaS como Amazon Web Services, Google Cloud o Azure. El objetivo de los Publisher es habilitar la conexión privada de aplicaciones internas desde el correspondiente centro de datos hacia la nube de Netskope habilitando su acceso mediante políticas de seguridad y la red de *Zero Trust Network Access* ZTNA.

Ilustración 51: Netskope para acceso privado - Publishers
vía https://docs.netskope.com/en/netskope-private-access.html

Los clientes de Netskope instalados en los equipos del personal empleado de las organizaciones acceden a las aplicaciones internas a través de la nube de Netskope y las localiza a través de los Publishers instalados en los respectivos centros de datos. Los Publisher no necesitan estar publicados a Internet debido a que son ellos mismos que conectan con la nube de Netskope sin necesidad de exponer ningún servicio a Internet.

Los requerimientos y capacidades de cada Publisher es la siguiente:

Requerimientos para cada VM/Publisher	
CPU	2 vCPUs
Memoria	4GB RAM
HDD	8 GB
Requerimientos de comunicaciones	
Entrada	SSH: Puerto 22/tcp (solamente para gestión de uso interno)
Salida	DNS: Puerto 53/udp (consultas dns) HTTPS: Puerto 443/tcp a los siguientes hostnames: https://gateway.npa.goskope.com https://stitcher.npa.goskope.com *.docker.com *.docker.io *.ubuntu.com https://ns-<TENANTID>.<POPNAME>.npa.goskope.com

	*Es necesario que los Publisher tengan acceso las IPs y puertos de las aplicaciones internas para que se pueda acceder desde ZTNA.
Capacidades por cada Publisher	
Límites cantidad	Hasta 100 en total / Hasta 16 en un cluster.
Rendimiento	500Mbps/Publisher de *Throughput*
Conexiones concurrentes	32.000 conexiones concurrentes (TCP o UDP).

Ilustración 52: Tabla de requerimientos y capacidades para Publisher
vía https://docs.netskope.com/en/deploy-a-publisher.html

El despliegue de los Publisher se puede realizar a través de un OVA en Vmware ESX, una AMI en Amazon Web Services, un VHDX en HyperV o directamente en Google Cloud Platform o Azure como se detalla en la sección Deploy Publisher[37] de la página oficial de Netskope. La imagen de OVA, AMI o VHDX se pueden descargar desde la consola de administración de Netskope. Para poder desplegar correctamente el Publisher es necesario desplegarlo en la red interna y registrarlo en la consola de administración de Netskope. Se muestra el detalle del proceso de despliegue y registro en los anexos de este trabajo Despliegue y registro de un Publisher en Vmware ESXi

Cabe destacar que para poder disponer de alta disponibilidad y contingencia es recomendable desplegar como mínimo dos Publisher en cada centro de datos y dependiendo de las necesidades será necesario desplegar una cantidad superior.

4.3.2. Netskope Cloud Exchange (CE)

Cloud Exchange de Netskope (CE) es una solución de software desplegada como una máquina virtual en el centro de datos de la organización. El objetivo de Netskope CE es facilitar herramientas de integración con otros productos de seguridad de la organización a partir de cuatro módulos con diferentes funcionalidades los cuales disponen de más de 60 integraciones.

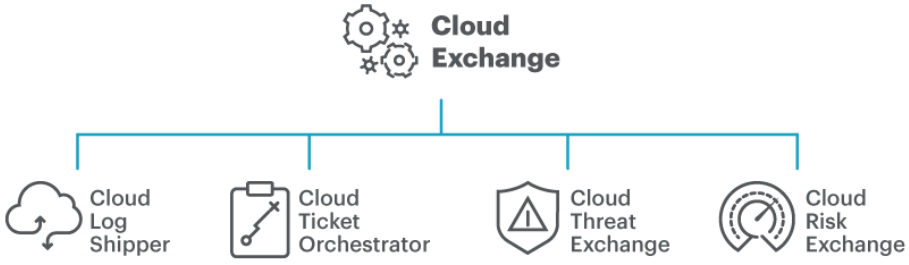


Ilustración 53: Módulos de Netskope Cloud Exchange
https://www.netskope.com/products/cloud-exchange

[37] https://docs.netskope.com/en/deploy-a-publisher.html

Los cuatro módulos se describen a continuación:

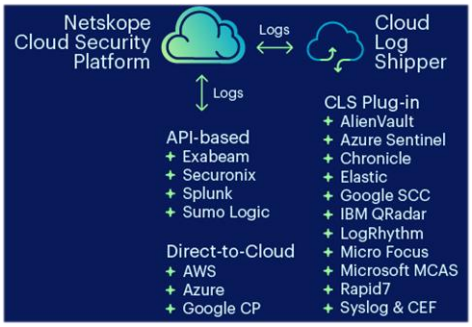


Ilustración 54: Netskope Cloud Log Shipper

Cloud Log Shipper (CLS), módulo utilizado para poder exportar los eventos de seguridad del tenant de Netskope al correspondiente SIEM de la organización o a otros servicios. Es posible integrar productos de terceros como Exabeam, Securonix, Splunk o Sumo Logic, IBM Qradar, Rapid7, Elastic, AlienVault entre otros.

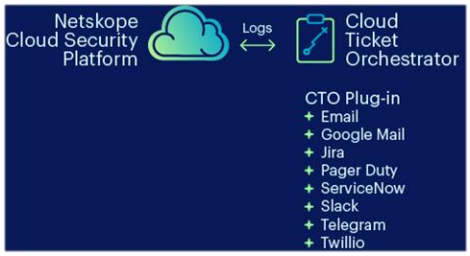


Ilustración 55: Netskope Clout Tikcet Orchestrator

Cloud Ticket Orchestrator (CTO), módulo utilizado para crear y gestionar tickets y notificaciones en herramientas colaborativas como Jira Cloud, ServiceNow o Slack entre otros productos.

Ilustración 56: Netskope Cloud Threat Exchange

Cloud Threat Exchange (CTE), módulo utilizado para poder integrar la información de amenazas como los indicadores de compromiso IoC (IPs, hashes de ficheros, URLs) alimentados desde un producto de seguridad de terceros. El objetivo es poder alimentar el motor de reglas de Netskope con los IoC obtenidos del producto de seguridad de la organización.

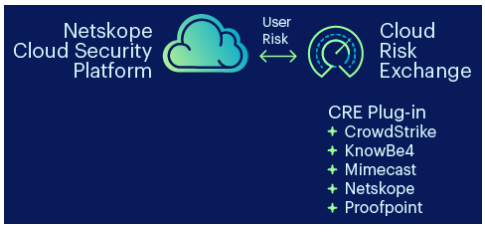


Ilustración 57: Netskope Cloud Risk Exchange

Cloud Risk Exchange (CRE), módulo utilizado para intercambiar y normalizar las clasificaciones de riesgo entre soluciones de seguridad como CrowdStrike o Proofpoint entre otras soluciones con el objetivo de mejorar la monitorización de riesgos tecnológicos.

La utilización de las integraciones de estos cuatro módulos se incluye dentro de las licencias adquiridas por la organización y es posible activarlos por separado según las necesidades. La máquina virtual de Netskope CE debe de cumplir los siguientes requerimientos:

Requerimientos para Netskope Cloud Exchange (CE)	
CPU	4 vCPUs
Memoria	4GB RAM
HDD	40 GB
Sistema operativo	Ubuntu 20.04 LTS CentOS 8 Red Hat Enterprise Linux 7.9 and 8.0
Requerimientos de comunicaciones	
Entrada	SSH: Puerto 22/tcp (solamente para gestión de uso interno)
Salida	DNS: Puerto 53/udp (consultas dns) HTTPS: Puerto 443/tcp a los siguientes hostnames: • https://github.com • https://*.goskope.com • https://hub.docker.com • https://auth.docker.io • https://registry-1.docker.io • https://index.docker.io/ • https://dseasb33srnrn.cloudfront.net/ • https://production.cloudflare.docker.com/ • *.googleapis.com *Es necesario disponer de acceso a los repositorios del sistema operativo con el objetivo de poder actualizarlo como también el acceso a los diferentes APIs de productos de seguridad de terceros que se necesite integrar.

Para poder desplegar la máquina virtual empleada para Netskope CE es necesario instalarle un sistema operativo, no se importa desde OVA o AMI como lo hace el Publisher. Aunque los pasos necesarios se muestran en la sección de integraciones de Netskope Cloud Exchange[38] se muestra el detalle del proceso de despliegue y registro en los anexos de este trabajo Despliegue de Netskope CE en Redhat 9. En este trabajo se activa el módulo de **Cloud Log Shipper** con el objetivo de enviar los eventos de seguridad del tenant de Netskope al SIEM corporativo IBM QRADAR.

4.3.3. Netskope Client

El cliente de Netskope es una aplicación que permite a los dispositivos del personal utilizar las diferentes soluciones que forman el ecosistema de seguridad de la nube de Netskope como es el *Next Generation Secure Web Gateway* (NG SWG), *Cloud Access Security Broker* (CASB), *Cloud Firewall* (CFW), *Endpoint Data Loss Prevention* (DLP) y *Zero Trust Network Access* (ZTNA). La aplicación es compatible con los siguientes sistemas operativo y plataformas:

[38] https://docs.netskope.com/en/netskope-cloud-exchange.html

Sistema operativo	Versiones
Microsoft Windows Desktop	7, 8.1, 10, 11
Microsoft Windows Server	2016, 2019, 2022
Linux	Ubuntu 18.04 and 20.04 LTS
MacOS	Sierra, High Sierra, Mojave, Catalina, Big Sur, Monterey, Ventura
Android	9, 10, 11, 12, 13
ChromeOS	Chrome Browser 84
iOS	12, 13, 14, 15.1

Ilustración 58: Tabla de compatibilidad (Netskope Client)

El cliente de Netskope es un agente ligero que descarga las configuraciones y políticas de seguridad que el administrador gestiona desde la consola de administración de Netskope, las configuraciones de los clientes se configuran concretamente en **Settings** > **Security Cloud Platform** > **Devices > Client Configuration.** En esta sección es posible configurar el comportamiento del cliente de Netskope en los dispositivos del personal.

Traffic Steering

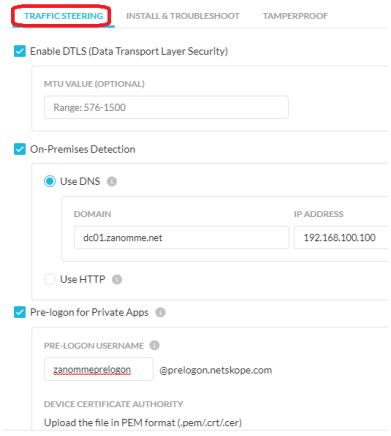


Ilustración 59: Client (Traffic Steering)

En la pestaña de ***Traffic Steering*** es posible configurar opciones como las siguientes:

Enable DTLS**,** reemplaza el túnel TLS (TCP) por un túnel DTLS (UDP) para mejorar el rendimiento de la comunicación.

On-Premises Detection, permite saber si el dispositivo se encuentra en la red local de la organización a partir de comprobación DNS o HTTP.

Pre-Logon for Private Apps, permite autenticar el cliente de Netskope antes de que la persona inicie sesión con el objetivo de poder aplicar scripts de inicio del dominio o GPOs.

Install & Troubleshoot

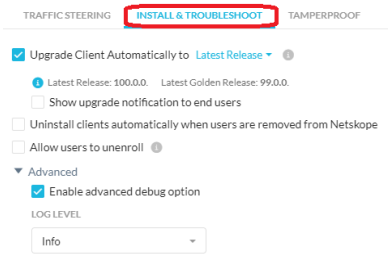


Ilustración 60: Client (Install & Troubleshoot)

En la pestaña de **Install & Troubleshoot** es posible configurar el comportamiento de las actualizaciones de los propios clientes como también el registro o log que los clientes podrán registrar.

Tamperproof

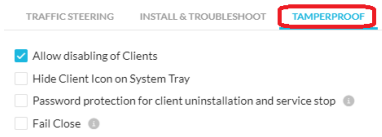


Ilustración 61: Client (Tamperproof)

En la pestaña de ***Tamperprof*** se pueden destacar las siguientes opciones de configuración:

Allow disabling of Clients, permite a las personas poder desactivar el cliente de Netskope.

Password protection, permite proteger la desactivación del agente en dispositivos Windows o Mac a través de una contraseña.

Fail Close, permite el bloqueo de todo el tráfico en caso de que la identidad no se pueda autenticar o si el dispositivo no está provisionado en la nube de Netskope.

El cliente de Netskope para Windows se puede desplegar de una manera manual o a través de GPOs de dominio o a través de productos de *Mobile Device Management* (MDM) o *System Center Configuration Management* (SCCM). El ejecutable consiste en un paquete MSI. Un detalle completo de las opciones de la instalación del cliente de Netskope se puede encontrar en la sección Netskope Client Deployment Option[39] de la página oficial de Netskope. Se muestra el detalle del proceso de instalación del cliente en el anexo Despliegue del cliente de Netskope en Windows donde se puede ver el detalle de la instalación manual del paquete MSI como el despliegue a través de GPOs de dominio.

4.4. Integración del *Identity Provider* (idP)

Además del acceso adaptativo y el análisis de la confianza recurrente en la conexión, la identidad es un factor esencial a la hora de ofrecer un acceso seguro a los recursos. Netskope facilita el provisionado de usuarios[40] y autenticación *Single Sign On* (SSO) a través de diferentes *Identity providers* (idP) como Azure AD u Okta.

Netskope trabaja con el estándar de *System for Cross-Domain Identity Management* (SCIM) con el objetivo de poder abastecer y desabastecer usuarios y grupos de una manera sencilla y eficiente mediante una API estandarizada. Para la autenticación de las identidades con SSO, Netskope utiliza el estándar SAML con el objetivo de integrar el inicio de sesión con o sin *Multi Factor Autentication* (MFA).

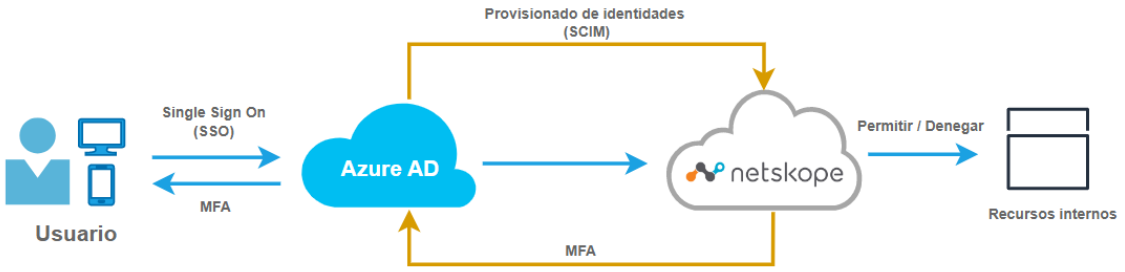


Ilustración 62: Provisionado y autenticación SSO (Netskope y Azure AD)

[39] https://docs.netskope.com/en/netskope-client-for-windows.html
[40] https://docs.netskope.com/en/scim-based-user-provisioning.html

En este proyecto se integra el provisionado de identidades, autenticación SSO de los clientes y acceso a la consola de administración Netskope con Azure AD, se muestra el detalle del proceso de integración de provisionado y autenticación en el anexo Provisión y autenticación de identidades con Azure AD en este documento se puede ver el detalle de la configuración de la parte de Netskope como de la parte de Azure AD. Los grupos empleados para el provisionamiento y administración son GS_AZUREAD_NETSKOPE y GS_AZUREAD_NETSKOPE_ADMINS respectivamente.

En la consola de administración de Netskope en **Settings** > **Security Cloud Platform Groups** > **Groups** se puede ver los grupos provisionados para el uso con el cliente de Netskope:

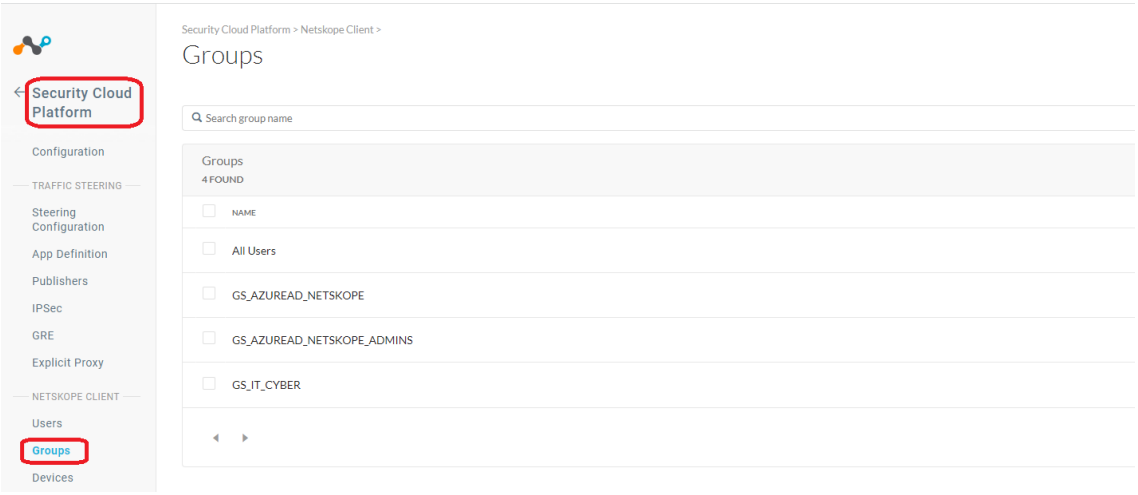


Ilustración 63: Ventana de grupos provisionados en Netskope

Mientras que en **Settings** > **Security Cloud Platform Groups** > **Users** se pueden visualizar los grupos provisionados y locales para también el uso del cliente de Netskope:

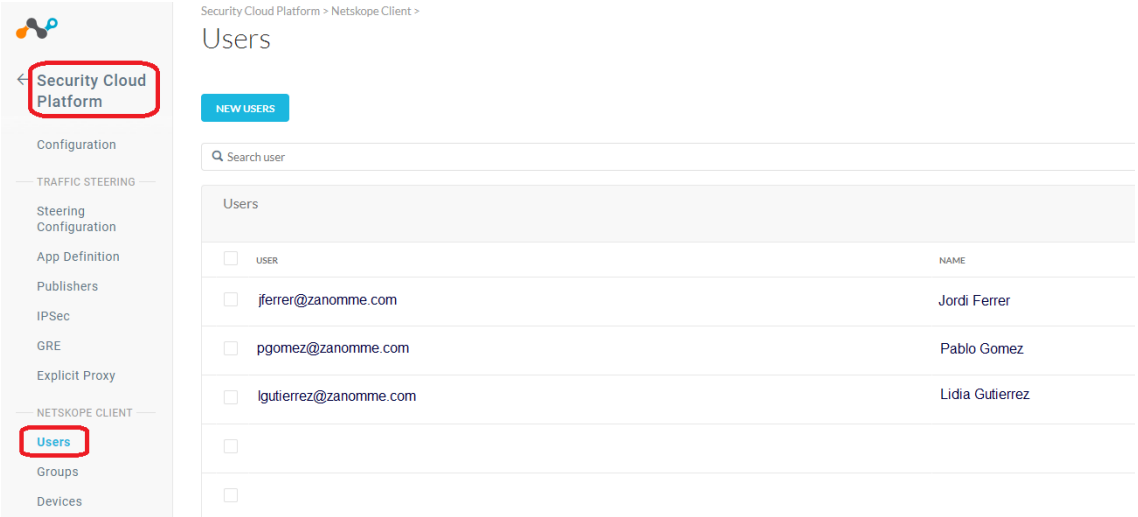


Ilustración 64: Ventana de usuarios provisionados en Netskope

La frecuencia de tiempo en el provisionamiento de identidades entre Netskope y Azure AD es de 40 minutos, es decir en el caso que en Azure AD haya algún cambio de identidades tardará 40 minutos en el peor de los casos en aparecer listado el usuario o grupo en la consola de administración de Netskope.

4.5. Configuración de dirección del tráfico (*steering*)

steering configuration es la configuración que determina qué tráfico se dirige a la nube de Netskope para poder ser inspeccionado y analizado, podemos diferenciar en tres tipos de tráfico, las aplicaciones cloud, los protocolos HTTP y HTTPS (Cualquier puerto) o todo el tráfico. Para dirigir todo el tráfico es necesario la licencia de Cloud Firewall (FWaaS). El *steering configuration* aplica solo a los equipos que utilizan la aplicación de Netskope Client.

Es posible crear una configuración básica a través de la consola de administración de Netskope, **Settings** > **Security Cloud Platform** > **Steering Configuration** > **New Configuration** y crearlo como se muestra en la imagen:

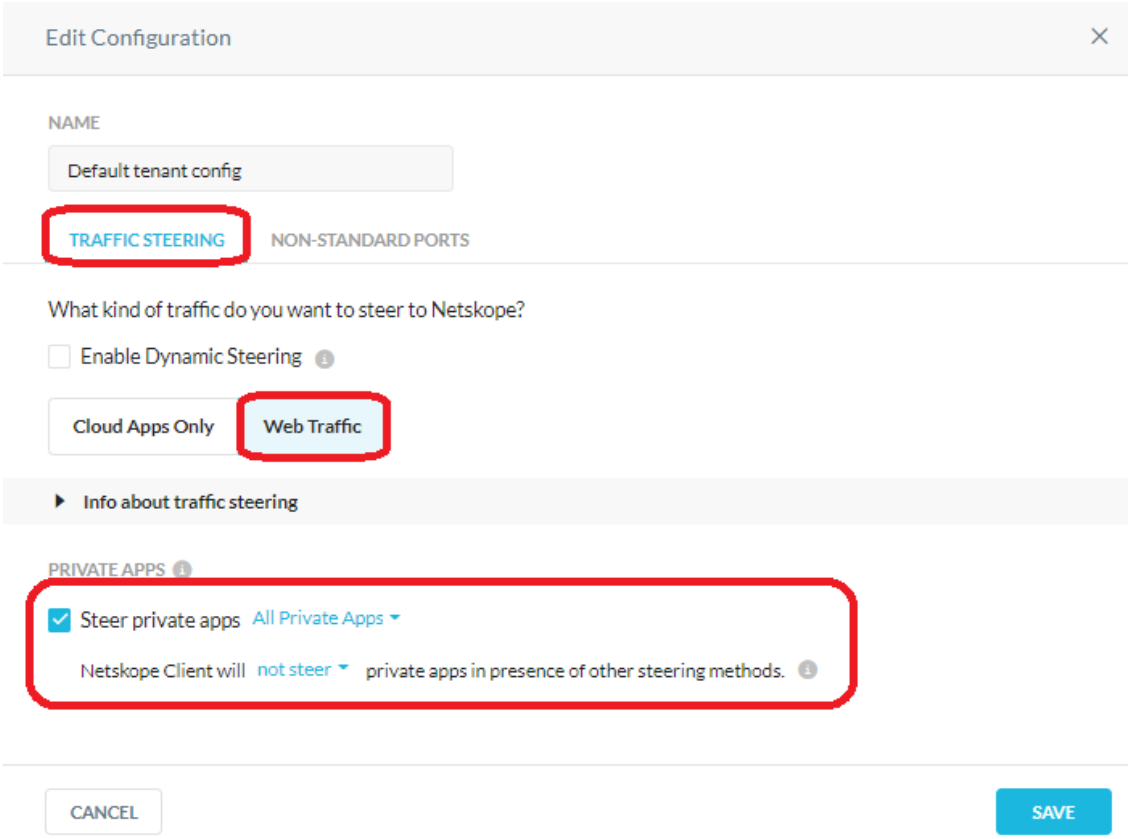


Ilustración 65: Steering configuration en Netskope

En la configuración es posible añadir excepciones para evitar que determinado tráfico no se diriga a Netskope, un caso de uso podría ser aplicaciones de movil que utilizan el Certificado fijado o *pinned* y es necesario bypasearlas para consguir que funcionen correctamente. En la imagen siguiente es posible ver ciertas excepciones:

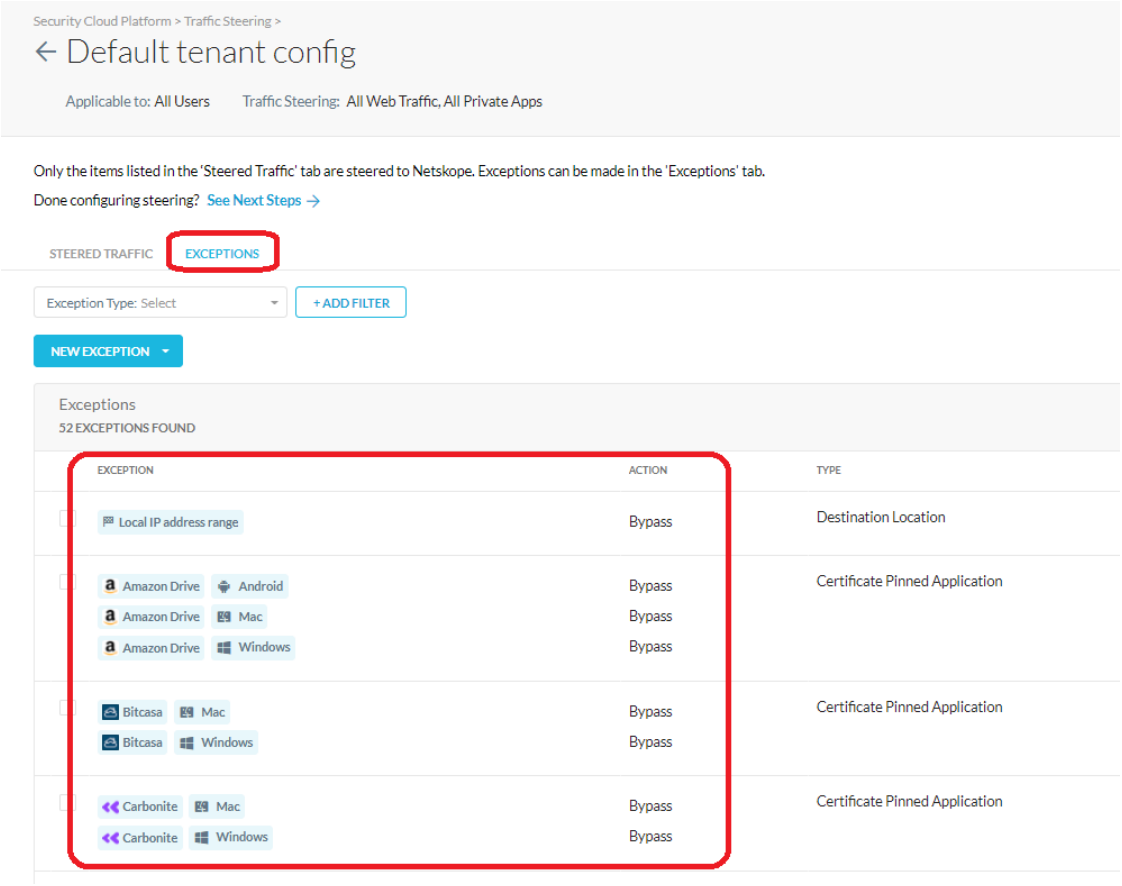


Ilustración 66: Excepciones steering configuration en Netskope

Las configuraciones se pueden aplicar por usuario o grupo y es posible crear diferentes que solo permitan utilizar aplicaciones internas o ZTNA u otras que solamente utilicen navegación. Por ejemplo, a los proveedores externos no interesa inspeccionar su navegación, pero sí que puedan acceder a aplicaciones internas de la organización por ZTNA, en cambio al personal corporativo interesa disponer de los dos tráficos.

4.6. Creación de regla de inspección de tráfico SSL/TLS

Es posible hacer excepciones de inspección de tráfico SSL/TLS por posibles preocupaciones de complimiento en la organización, por ejemplo, que la organización no necesite que se inspeccione de las páginas financieras, de salud o gubernamentales. Se puede crear estas excepciones desde la consola de administración de Netskope, **Policies** > **SSL Decryption** > **Add Policy** como se muestra en la siguiente imagen:

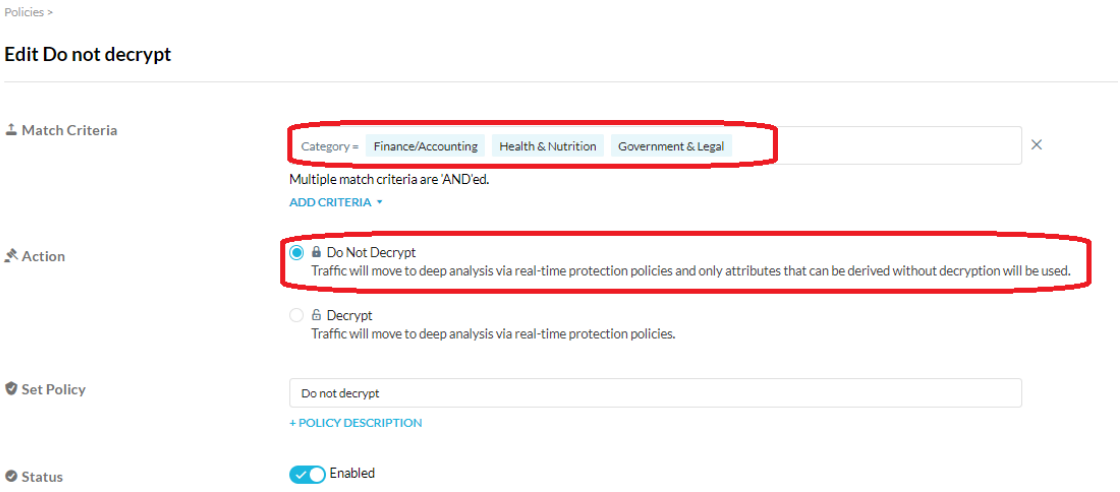


Ilustración 67: Inpección TLS/SSL en Netskope

4.7. Creación de Listas de URL para web

La creación de listas URL son útiles para poder construir categorías mas completas, es posible hacer a través de **Policies** > **Web** > **URL Lists** > **New URL List**. Como se muestra en la siguiente imagen:

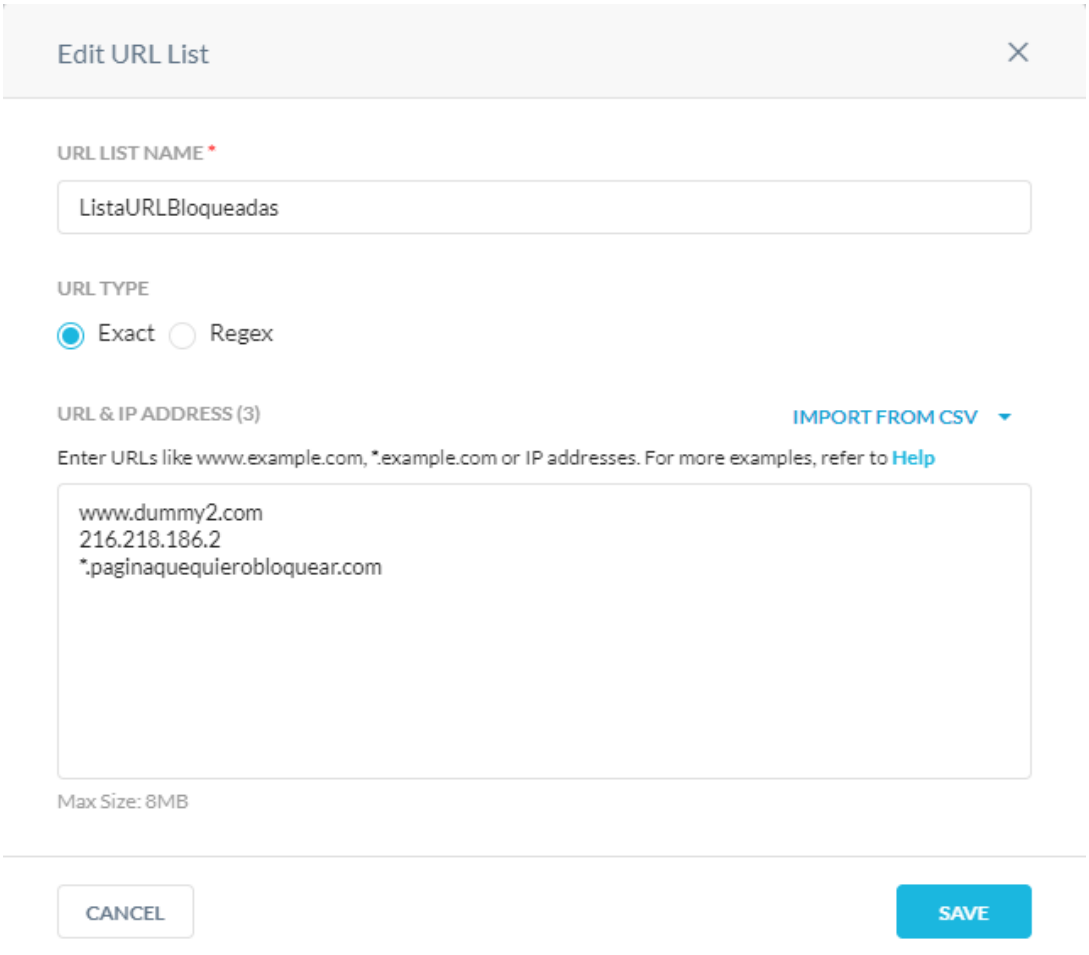


Ilustración 68: Creación de listas URL en Netskope

4.8. Creación de categorías web

Las categorías web pueden ser utilizadas en las reglas de navegación para poder hacer bloqueos de páginas categorizadas en la organización como de riesgo. Para ello, se accede a **Policies** > **Web** > **Custom Categories** > **New Custom Category**:

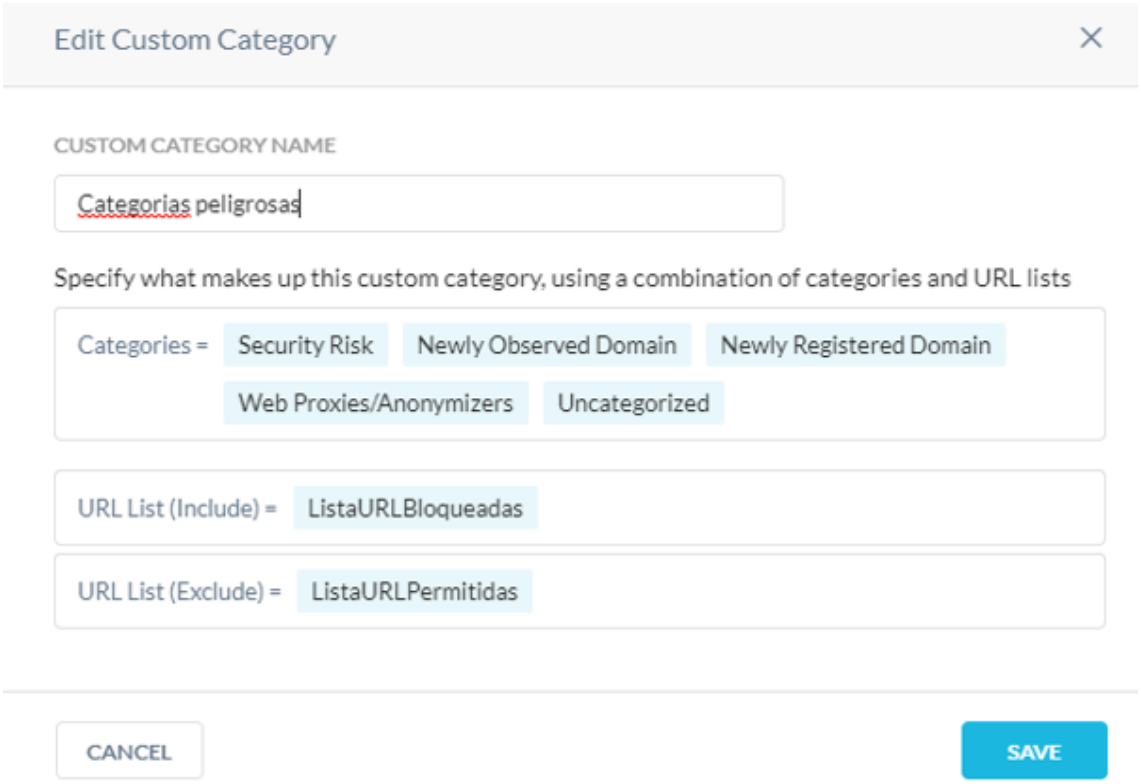


Ilustración 69: Creación de categorias web en Netskope

Como se puede ver se hace uso de la lista URL creada en la sección anterior con el objetivo de crear una categoría más completa y funcional.

4.9. Creación de plantillas de notificación

Las plantillas de notificación son utilizadas para poder mostrar e informar al usuario posibles bloqueos o advertencias que ocurran durante su navegación o acceso a un recurso interno. Por ejemplo, es posible mostrar una ventana informativa cuando un usuario intenta enviar contenido de un fichero catalogado como información sensible o también cuando el usuario intenta acceder a una página de riesgo entre otras muchas opciones.

Es posible crear múltiples plantillas con un logo personalizado, configurar los mensajes con un idioma determinado, parametrizar las acciones que puede hacer el usuario entre otras posibilidades. La configuración de una plantilla de usuario se realiza desde la consola de administración de Netskope, **Policies** > **Templates** > **User Notification** > **Add Template**

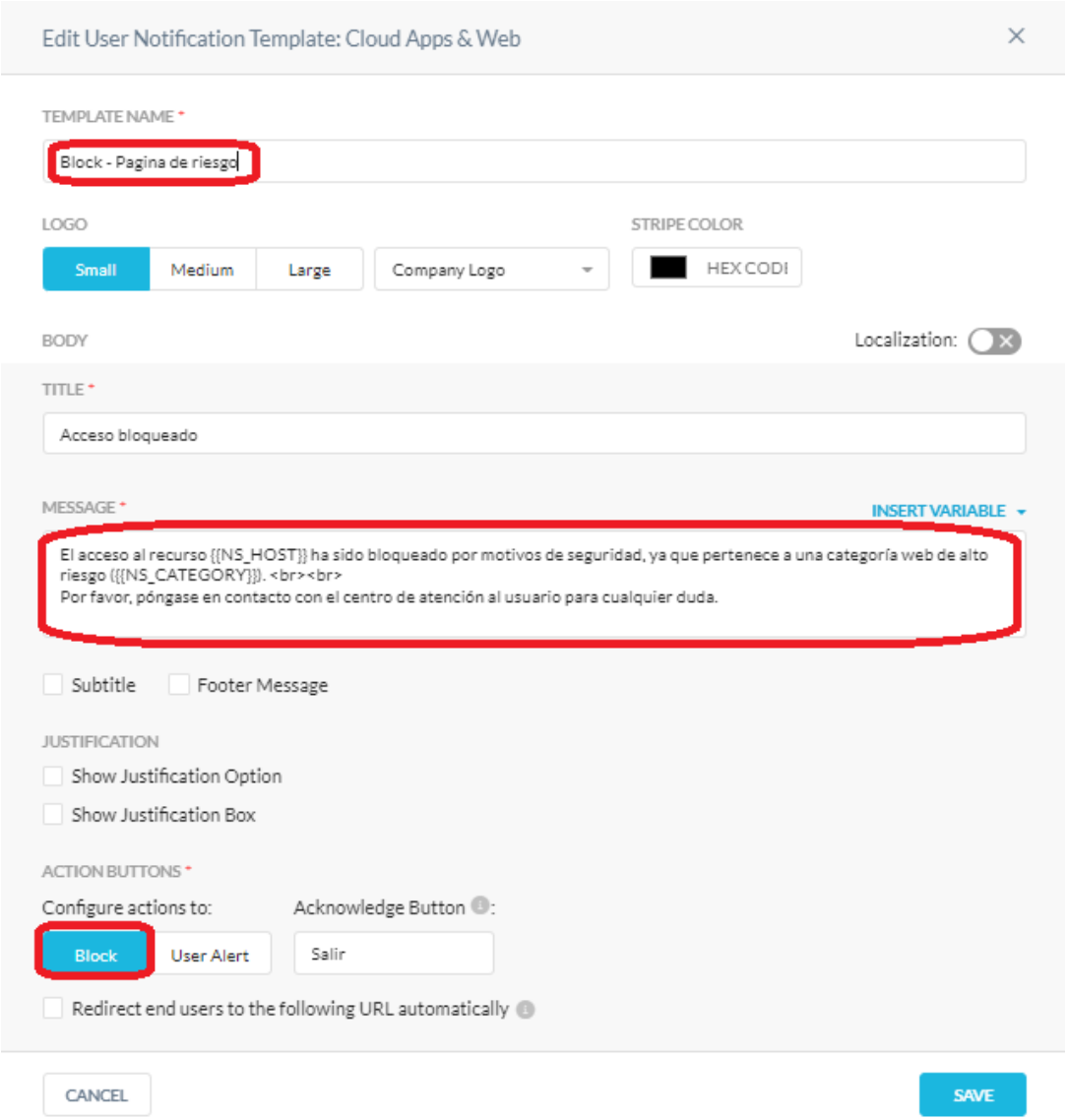


Ilustración 70: Creación de plantilla de notificación en Netskope

En la plantilla de la imagen anterior se puede ver que muestre un mensaje de bloqueo de recurso con la acción como *block* y con un botón de *acknowledge* **Salir.** Cabe destacar que dentro del mensaje se pueden añadir diferentes variables asociadas con el objetivo de dar un mensaje más informativo al usuario.

4.10. Creación de una regla de navegación web (NG SWG)

Las reglas de protección de navegación web permiten aceptar o denegar las acciones de navegación de los usuarios mediante un refuerzo granular basado en categorías, usuarios, grupos, aplicaciones, DLP entre otros. La creación de una regla de navegación se realiza desde la consola de administración de Netskope, **Policies** > **Real-time Protection** > **New Policy** > **Web Access:**

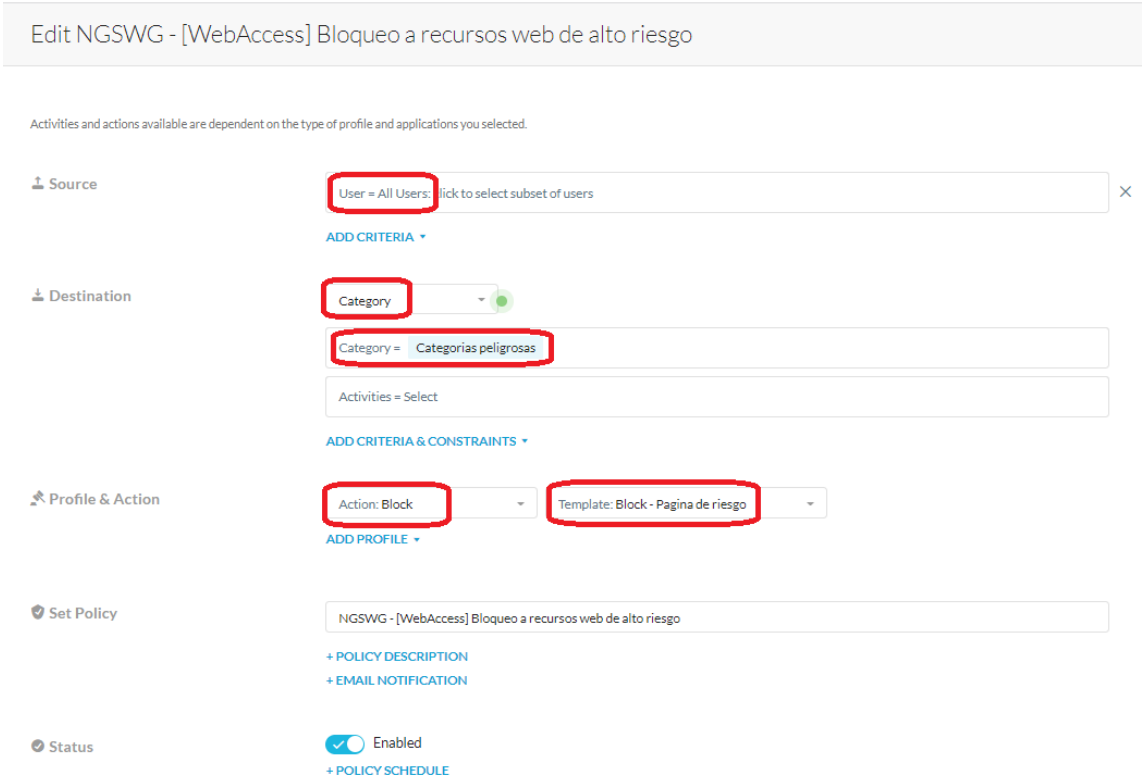


Ilustración 71: Creación de regla de navegación web en Netskope

La imagen superior muestra como una regla de navegación bloquea la navegación a todos los usuarios **All users** a través de la categoría de **Categorías peligrosas** mostrando la notificación de la plantilla **Block – Página de riesgo**. Es importante mencionar que la política por defecto en las reglas de navegación web es por defecto *accept*.

4.11. Creación de una regla DLP y CASB

La creación de una regla DLP y CASB es posible hacerla desde la misma sección que las reglas de navegación y tienen el objetivo bloquear o denegar las acciones determinadas que realizan las personas cuando acceden a una aplicación en la nube (CASB) y también bloquear o denegar en envió de información sensible fuera de la organización o determinadas aplicaciones en la nube (DLP).

Para crear una regla de este tipo es necesario dirigirse a la consola de administración de Netskope, **Policies** > **Real-time Protection** > **New Policy** > **Cloud App Access:**

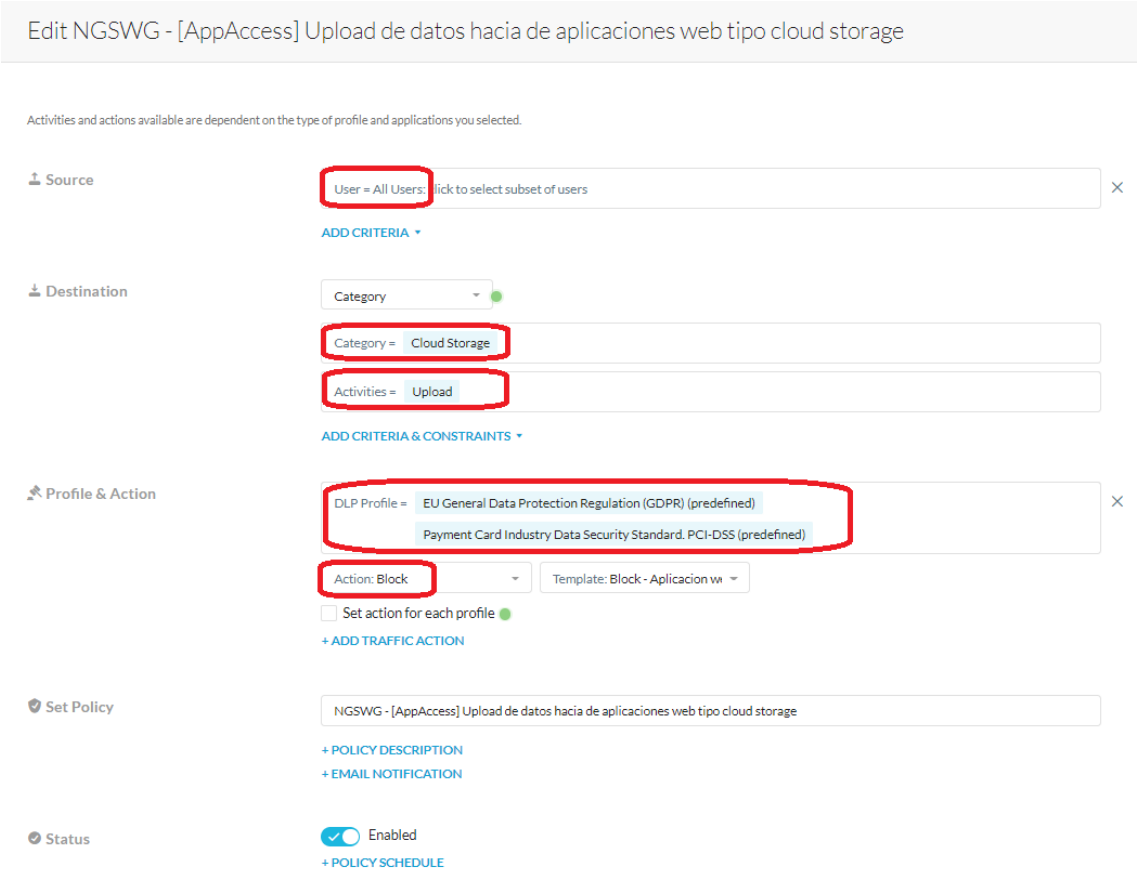


Ilustración 72: Creación de una regla DLP y CASB en Netskope

En la regla de acceso a aplicación anterior se muestra el bloqueo a todos los usuarios **All users** cuando la acción sea la de subir información **Upload** en las aplicaciones web categorizadas como **Cloud Storage** y cuando se le aplica un **DLP Profile** predefinido de GDPR o PCI-DSS. En el caso que una persona haga esta acción se le muestra una notificación definida en la plantilla **Block-Aplicación storage**.

4.12. Definición de segmentos de aplicación para ZTNA

Para empezar a crear reglas de acceso a aplicaciones internas que haga uso del Zero Trust Network Access (ZTNA) es necesario definir las aplicaciones llamadas segmentos de aplicación. Los segmentos de aplicación son definiciones de URL, IP, puerto y DNS que se aplica a una aplicación interna o conjunto de estas. Es decir, es un objeto que posteriormente se debe de aplicar a una política de acceso para bloquear o permitir el tráfico a determinados usuarios y posturas de seguridad. Para ello es necesario dirigirse a la consola de administración de Netskope, **Settings** > **Security Cloud Platform** > **Traffic steering** > **App Definition** > **Private Apps** > **New Private App:**

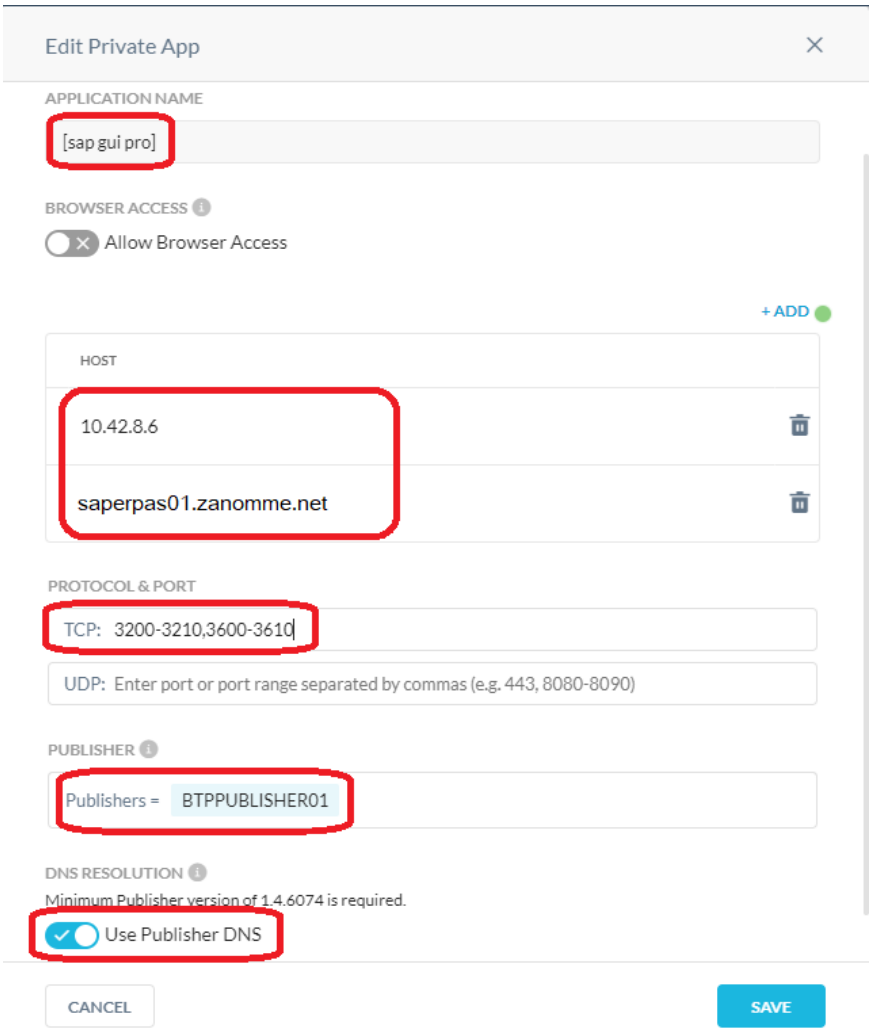


Ilustración 73: Definición de un segmento de aplicación en Netskope

En la imagen anterior se muestra cómo se crea un segmento de aplicación para el acceso a SAP GUI. El nombre de este segmento de aplicación tiene el nombre **sap gui pro** con un nombre DNS **saperpas01.zanomme.net** resolviendo a la dirección IP **10.42.8.6** a través del rango de puertos TCP **3200-3210 y 3600-3621.** Esta aplicación es accesible a través del Publisher de **BTPUBLISHER01** y utiliza la resolución DNS del mismo Publisher **Use Publisher DNS** para resolver el nombre de host.

La opción **Allow Browser Access** es utilizada para aplicaciones que trabajen por puertos Web y para personas que no puedan tener el Netskope Client instalado, en este caso el usuario iniciará sesión con su identidad sincronizada en un portal donde se podrá acceder a la aplicación directamente por navegador.

4.13. Clasificación de dispositivo

La clasificación de dispositivo permite restringir el acceso a determinados recursos internos solamente a equipos corporativos, para ello necesita hacer una serie de comprobaciones que si el equipo la cumple se cataloga como **Managed** o por el contrario en **Unmanaged**. Las posibles comprobaciones pueden ser las siguientes:

- Cifrado de disco.
- Determinado proceso en ejecución.
- Determinado valor en una rama de registro.
- Existencia de fichero en el sistema.
- Miembro del dominio corporativo.
- Disposición de certificado.

La condición de cumplimiento de estas comprobaciones puede seguir la operación lógica AND o OR, es decir que se cumplan todas las seleccionadas o alguna de ellas, esto permite dar a la conexión una postura de seguridad que se comprueba recurrentemente durante la sesión al recurso interno, en el caso de no cumplir la postura de seguridad la conexión se cierra aunque el usuario esté correctamente identificado y autenticado.

Para la creación de una regla de clasificación de dispositivo es necesario acceder a la consola de administración de Netskope, **Settings** > **Manage** > **Device Classification** > **New Device Classification**:

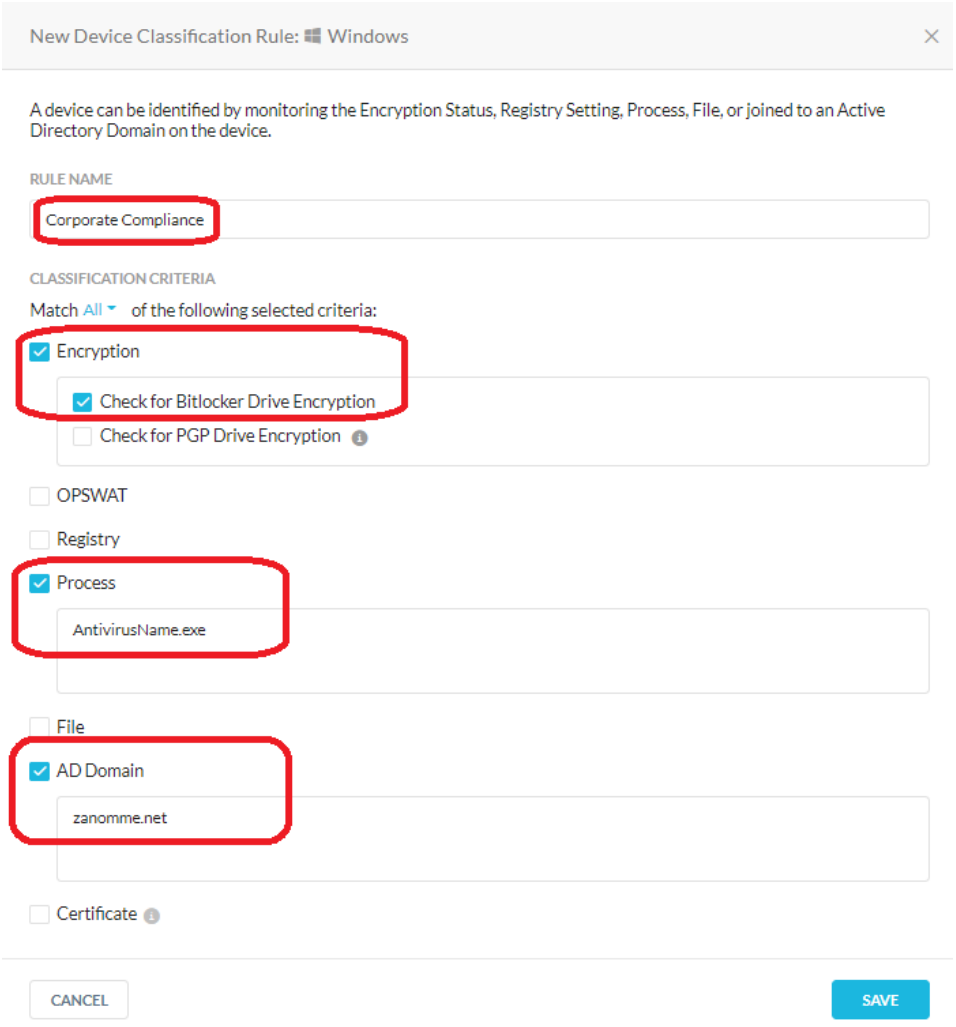


Ilustración 74: Clasificación de dispositivo en Netskope

En la imagen superior se observa que se crea una regla de clasificación de dispositivo que comprueba que se cumplan todos los siguientes criterios: Disco

cifrado y proceso ejecutando llamado AntivirusName.exe y unido al dominio zanomme.net.

4.14. Creación de regla de acceso a aplicaciones internas (ZTNA)

Para crear una regla de acceso a una aplicación interna es necesario dirigirse a la consola de administración de Netskope, **Policies** > **Real-time Protection** > **New Policy** > **Private App Access**:

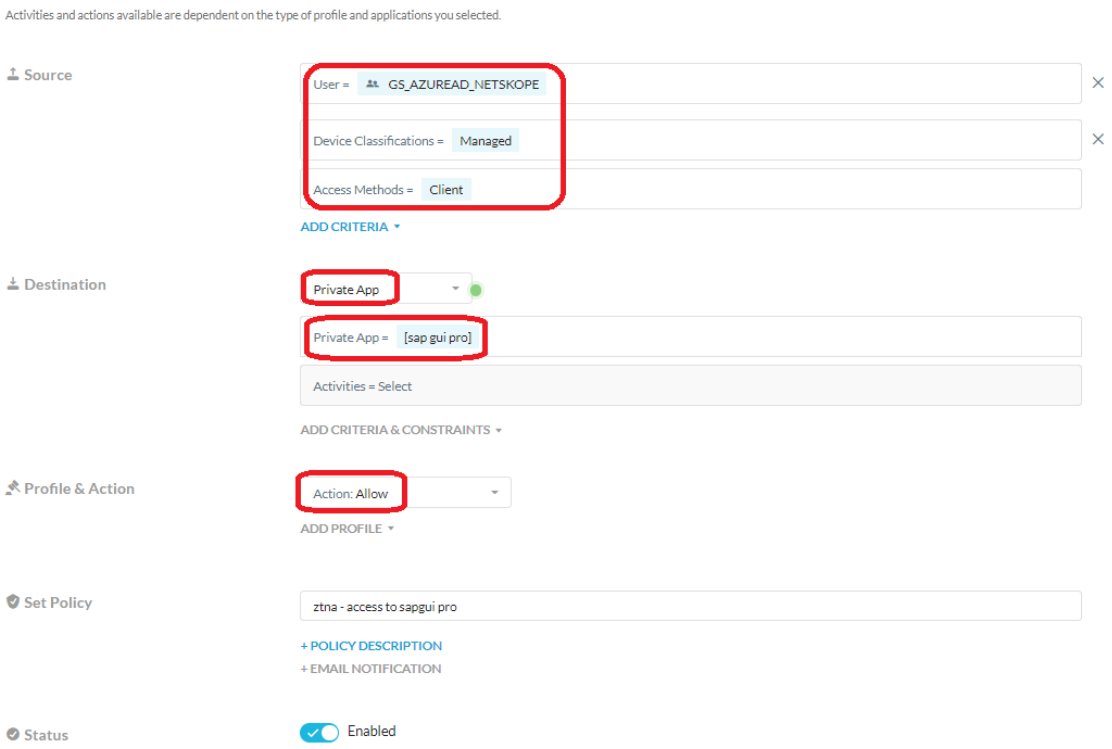


Ilustración 75: Creación de regla de acceso ZTNA en Netskope

En la regla anterior se permite el acceso **Allow** a la aplicación privada definida con nombre **sap gui pro** cuando se accede por el cliente de Netskope **Client**, el equipo es clasificado como **Managed** y el usuario se encuentra dentro del grupo **GS_AZUREAD_NETSKOPE**.

4.15. Ejecución de PoCs y pilotos

Una prueba de concepto PoC tiene el objetivo de probar un concepto o funcionalidad y poder validar su rendimiento mientras que un piloto es un ensayo real en la operativa de un departamento o área funcional.

Antes de hacer un piloto involucrando a personal empleado es necesario hacer pruebas de concepto PoC de las diferentes soluciones de seguridad de Netskope con el objetivo de entender técnicamente el producto y tratar de afectar lo menos

posible en el trabajo del personal de la compañía. Para tratar de hacer estas pruebas iniciales se seleccionan los tipos de dispositivos que los empleados utilizan para su trabajo diario.

Nombre dispositivo	Tipo de dispositivo	Sistema operativo
WINLP01	Portátil	Windows 10 y 11
MACLP01	Portátil	MacOS 11 y 12
ANDSMA01	Smartphone	Android 12 y 13
IOSSMA01	Smartphone	iOS 14, 15 y 16

Ilustración 76: Tabla de dispositivos de prueba para PoC

Con estos dispositivos de prueba se realizan las pruebas pertinentes para poder empaparse de la tecnología y así reducir el riesgo de errores en la implantación de los pilotos. Los responsables en la ejecución de las PoCs son los departamentos de ciberseguridad e infraestructuras. Las PoCs realizadas son las siguientes:

- Instalación manual, GPO y MDM del cliente de Netskope.
- Evaluar el funcionamiento de las diferentes políticas de seguridad de navegación (NGSWG) y aplicaciones internas (ZTNA).
- Comprobar que la aplicación de venta en tienda (POS) funcionan correctamente desde las tablets.
- Evaluar el tiempo de actualización a la hora de hacer cambios en las políticas de seguridad o cambios en los segmentos de aplicación.
- Comprobar el correcto funcionamiento de las aplicaciones corporativas y aplicaciones de seguridad instalados en los dispositivos.
- Comprobar las políticas a prueba de manipulaciones (*tamper proof*) del cliente de Netskope.
- Comprobar el funcionamiento de la característica del cliente de *Fail Close*.
- Comprobar el funcionamiento de la característica de cliente de *On Premises Detection*.
- Evaluar las latencias de comunicación comparándolo con la VPN tradicional.
- Comprobar el funcionamiento del Browser Access para acceder a aplicaciones internas web a través de un navegador sin cliente de Netskope.

- Comprobar la actualización de políticas GPO del dominio.

- Comprobar la desinstalación del cliente de Netskope.

Una vez finalizadas las pruebas bajo el entorno controlado es el momento de involucrar a las áreas funcionales necesarias con el objetivo de lanzar un piloto a determinados usuarios clave o *key users*. El propósito de los pilotos es poder comprobar la productividad de las soluciones y recibir una validación de negocio, para ello es necesario coordinarse con cada uno de los responsables de los departamentos y establecer las operativas críticas del negocio. En la siguiente tabla se listan las funciones a probar más importantes para la compañía separadas por departamento:

Departamento	**Funciones** ***Accesos desde dentro de la red como externamente (teleworking)**
Todos	• Utilización de las herramientas colaborativas de la empresa (Teams, Outlook, OneDrive, …). • Acceso al ERP SAP y al ERP *Legacy*. • Acceso a la herramienta de *ticketing* JIRA. • Navegación en Internet. • Evaluar la experiencia de la persona para cada uno de los *Key Users*.
Tiendas	• Escaneo de etiquetas de los productos para obtener su información. • Gestión de clientes desde la aplicación de punto de venta. • Venta de productos desde la aplicación de punto de venta. • Impresión de *tickets*.
Gerentes	• Acceso a las aplicaciones estratégicas de la compañía como el *Business Inteligence* (BI). • Acceso a la validación de facturas. • Conexión desde cualquier lugar a las personas con sus dispositivos corporativos.
Finanzas Compras Personas Legal Comercial	• Acceso al servidor de ficheros on premises. • Conexión desde cualquier lugar a las personas con sus dispositivos corporativos.
Diseño Fotografía Marketing	• Acceso rápido y eficiente a los repositorios de imágenes y fotografía. • Utilizar las diferentes suites de diseño de la compañía. • Acceso a las redes sociales y a su gestión con Hootsuite.

Talleres Logística	• Acceso a la aplicación de elaboración propia en los talleres. • Realizar Picking y el Packing en la logística. • Acceder a los servicios necesarios de los transportistas. • Realizar inventarios. • Realizar el almacenaje de productos.
IT / Ciber	• Acceso al servidor de ficheros on premises. • Acceso de administración y gestión a los servidores y equipos. • Acceso a la aplicación de gestión de identidades. • Conexión desde cualquier lugar a las personas con sus dispositivos corporativos.

Ilustración 77: Tabla de funciones por departamento para la realización de pilotos

Una vez realizados los pilotos en cada uno de los departamentos o áreas funcionales es hora de fijar una fecha para hacer el despliegue gradual de la herramienta.

5. Conclusiones y trabajo futuro

En este último punto se describen las conclusiones obtenidas después de la realización de este trabajo, como también un análisis del seguimiento de la planificación y metodología utilizados, una reflexión de los objetivos alcanzados y una evaluación de los impactos ético-sociales, sostenibles y de diversidad. Además, se incluye el trabajo futuro que podría llegar a realizarse después de este proyecto.

5.1. Conclusiones

Este trabajo demuestra que la transformación digital de las organizaciones debe de ir acompañada de una **transformación en la seguridad** con el objetivo de poder hacer frente a los nuevos retos que nos depara el futuro. Se menciona que las soluciones tradicionales de seguridad como, por ejemplo, firewalls perimetrales centralizados sirven para determinados casos, pero no están diseñados para proteger las aplicaciones en la nube debido a que los datos ya no se encuentran en un centro de datos sino difuminados la nube.

Se ha querido definir el marco **Secure A*ccess Service Edge*** (SASE) el cual nos permite transformar la seguridad para poder hacer frente a los retos de diarios, así mismo, al ser una solución en la nube da la posibilidad de poder escalar y adaptar nuestras necesidades bajo demanda. SASE nos permite proteger las identidades, las aplicaciones y los datos de una organización independientemente de donde se encuentren las personas que lo utilizan permitiendo que la seguridad las acompañe en todo momento.

Desde el año 2019 la adopción de soluciones SASE ha ido creciendo significativamente cada año, acelerado sobre durante la pandemia del COVID, y la tendencia es seguir creciendo durante los cinco años siguientes.

A lo que se refiere al control de las soluciones de seguridad, para una eficiente administración y gestión de las soluciones de seguridad es importante poder disponer de un centro de mando único donde poder aplicar políticas de seguridad y obtener indicadores del estado de la seguridad. El ecosistema de seguridad es amplio por lo que es fundamental adoptar una integración de todos sus componentes ***Secure Service Edge*** (SSE) con el objetivo de ofrecer una seguridad integral.

5.2. Seguimiento de la planificación establecida

Se puede decir que en general se ha cumplido y seguido la planificación del proyecto y se han abordado los principales temas que se querían investigar, analizar e implementar. Cabe destacar que a medida que se iba avanzando en el desarrollo del proyecto se iban actualizando ciertas secciones debido a nuevos conceptos aprendidos.

Aunque este proyecto está desarrollado para una empresa ficticia llamada Zanomme, S.A realmente se está implementando para una organización real,

este hecho ha dado la posibilidad de estar en contacto con los ingenieros y comerciales del producto y agilizar el análisis e implementación de PoC necesarias para cumplir con la planificación establecida.

La metodología seguida ha sido el modelo en cascada y se confirma que ha sido la adecuada, como he comentado anteriormente, a medida que iba desarrollando el proyecto y profundizando en algunos conceptos se volvía a revisar todas las secciones y actualizando su contenido en el proyecto.

5.3. Evaluación de los objetivos planteados

De los objetivos definidos en el proyecto, se han citan a continuación los comentarios:

- **Implementar una solución de navegación web segura en la nube para las personas empleadas de una organización independientemente del lugar de donde se encuentren.**

  Con Netskope se ha podido implementar una solución de navegación segura a través del módulo de *Next Generation Secure Gateway* (NG SWG). No se ha mostrado la creación de todas las reglas necesarias para la navegación debido a que la longitud del proyecto excedería de su límite, pero se ha mostrado la creación de una regla asociada a las URL de alto riesgo.

- **Implementar una solución de acceso de confianza cero evaluando la identidad y el contexto de la conexión a los recursos internos de una organización para el personal interno y externo que trabajan remotamente.**

  Con Netskope se ha podido crear un segmento de aplicación y asociarle una regla de acceso *Zero Trust Network Access* (ZTNA) a las personas que utilicen un dispositivo *Managed* de la organización. Con el segmento de aplicación se define el recurso acotado y la postura de seguridad o contexto es que el dispositivo cumpla con unos criterios de seguridad que se defina en *Managed*.

- **Identificar la extracción no aprobada de datos sensibles y confidenciales de una organización realizada entre o hacia instancias de aplicaciones en la nube.**

  Con Netskope se ha podido definir una regla en las políticas de seguridad que detecta las posibles filtraciones de datos que contengan contenido GPR o PCI DSS hacia aplicaciones de almacenamiento en la nube. Aunque es solo una regla no está en el alcance de este proyecto crear todas las necesarias para la organización.

- **Gestionar y controlar de una manera centralizada en una sola consola los componentes de seguridad en la nube que forman parte de la arquitectura *SASE*.**

Con la consola de administración única de Netskope se ha podido implementar todas las pruebas y gestionar todas las políticas de seguridad desde un solo lugar, así mismo esta consola de gestión única permite disponer de todas la métricas y datos a tiempo real del tráfico que fluye en el *tenant*.

Se hubiera querido profundizar en estos mismos objetivos con la solución del otro proveedor Zscaler (citado en este proyecto, como competidor de Netskope) pero no ha sido posible debido a las dificultades burocráticas que se han tenido para poder dar luz verde a la PoV del producto.

5.4. Evaluación de impactos en ético-sociales, sostenibilidad y diversidad

De los impactos previstos en la sección Impacto en sostenibilidad, ético-social y de diversidad se puede decir que se está mitigado el impacto sobre la dimensión de **sostenibilidad** asociado al **ahorro energético** debido a que este proyecto traslada a la nube los servicios de navegación segura y acceso remoto sustituyendo hardware dedicado para tal efecto, con esto se reduce consumo energético de la organización y el planeta. En las demás dimensiones correspondientes a la **ético-social** y de **diversidad** no se han evaluado cambios en los impactos definidos.

5.5. Trabajos futuros

Se han detectado algunos trabajos futuros no implementados en el proyecto actual que se consideran necesarios para poder conseguir una arquitectura SASE más completa y así construir una seguridad integral, se listan a continuación:

- Implementar una solución SDWAN en las filiales nacionales e internacionales con el objetivo que recursos internos ubicados en diferentes centros de datos de la organización puedan realizar conexiones a las diferentes sedes. Con la solución de ZTNA como agente la conexión que se permite es de cliente a recurso (outbound) y no permite actualmente una conexión a la inversa.

- Desplegar una solución de *Firewall as a Service* (FWaaS) con el objetivo de poder gestionar de una manera centralizada en la nube las conexiones de los dispositivos a puertos de comunicación que no sean solo los correspondiente a webs.

- Conseguir que dentro de la red local se traslade las funcionalidades de seguridad del ZTNA que hay en la nube con el objetivo de que si una persona necesita acceder a un recurso interno estando ya en la red interna sea posible hacerlo mediante la microsegmentación y Zero Trust. Este punto es importante para homogeneizar el funcionamiento de las redes. Aunque Zscaler dispone actualmente de esta herramienta llamada *Private Service Edge* (PSE), Netskope la está desarrollando y está previsto que en el primer trimestre del año 2023 esté desarrollada para utilizarla.

- Exportar los eventos de seguridad de la consola de administración de Netskope al SIEM corporativo directamente *cloud to cloud* sin tener que depender del recurso software ubicado *on premises* llamado Netskope Cloud Exchange (CE).

- Supervisar y monitorizar la postura de seguridad de la nube en el IaaS y SaaS a través de *Cloud Security Posture Management* (CSPM) y *SaaS Security Posture Management* (SSPM) con el objetivo de detectar amenazas de seguridad y poder dar respuesta a ellas.

6. Glosario

A

Active Directory · 36, 38, 43, 44, 46
ATP: Advanced Threat Protection · 9, 18, 19, 40
Azure Identity Management · 43, 44

B

backdoors · 18
backhauling · 36, 37, 40, 43, 45
BitLocker · 41

C

CAGR: Compound Annual Growth Rate · 23
CASB: Cloud Access Service Broker · iv, v, 2, 5, 9, 12, 13, 15, 16, 21, 23, 27, 28, 32, 41, 46, 47, 48, 49, 57, 66, 67, 80
CCI: Cloud Confidence Index · 18, 52
certificate pinning · 11
Cloud Computing · 8
CLS: Cloud Log Shipper · 56
CRE: Cloud Risk Exchange · 56
CSPM: Cloud Security Posture Management · 28, 77
CTO: Cloud Ticket Orchestrator · 56
***Cyber Security Kill Chai**n* · 19

D

dashboard · 51
DDoS: Sistributed Denial of Service · 38
DLP: Data Loss Prevention · iv, v, 5, 9, 13, 14, 15, 19, 21, 28, 37, 42, 47, 48, 52, 57, 65, 66, 67, 80

E

edge · 2, 8, 10, 21, 22, 40, 80
edge security · 40
EDR: Endpoint Dectection and Response · 19, 37, 40
EPP: Endpoint Protection Platform · 19, 37, 40

F

Firewall · iv, v, 2, 5, 8, 10, 16, 17, 19, 28, 31, 35, 36, 38, 57, 61, 76
FWaaS: Firewall as a Service · iv, v, 2, 5, 10, 16, 17, 20, 23, 28, 31, 61, 76

G

Gartner · 7, 22, 23, 25, 27
GDPR: **General Data Protection Regulation** · 11, 12, 49, 67

H

HIPAA: Health Insurance Portability and Accountability Act · 13, 14

I

IaaS: Infrastructure as a Service · 35, 36, 54, 77
ICMP · 16
IDP: Identity Provider · 44
IoC: Indicator of Compromise · 19, 40, 56
IPS: Intrusion Prevention System · 19

K

KPI: Key Performance Indicators · 39, 42

L

LEED: Leadership in Energy & Environmental Design · 3

M

malware · 9, 10, 18, 22, 29, 37, 38, 39, 40, 49, 52
man in the middle · 11

N

Netskope Cloud Exchange · 31, 47, 48, 53, 55, 57, 77, 81
Netskope ThreatLabs · 14
NewEdge · 27, 28
NG SWG: Next Generation Secure Web Gateway · iv, v, 9, 14, 15, 18, 19, 28, 31, 32, 33, 40, 41, 42, 43, 44, 46, 49, 52, 57, 65, 75
NIS: Network & Information Systems · 11, 12

O

On Premises Detection · 31, 71

7. Bibliografía

7.1. Libros de referencia

- Riley & Clark. (2022). *Security Service Edge (SSE) Para Dummies®, edición especial de Netskope* [PDF]. https://resources.netskope.com/ebooks/security-service-edge-sse-for-dummies

- Adoption Guide: Secure Access Service Edge (SASE). (s. f.). En *Is your security Arquitecture SASE-ready?* https://www.netskope.com/lp/sase-adoption-guide/

7.2. Trabajos de referencia

- Salom Martín. (2019, 4 junio). *Ventajas e implementación de un sistema IDS/SIEM en el ámbito familiar*. https://openaccess.uoc.edu/bitstream/10609/95087/6/joansaTFM0619memoria.pdf

- Pérez Peló, S. (2018, junio). Búsqueda de puntos débiles en redes de comunicaciones mediante algoritmos metaheurísticos. https://openaccess.uoc.edu/bitstream/10609/81971/6/sperez0TFM0618memoria.pdf

7.3. Páginas web de referencia

- *What is a CASB*. (s. f.). https://www.cloudflare.com/es-es/learning/access-management/what-is-a-casb/

- Netskope. (2022, 22 septiembre). *What is DLP? Data Loss Prevention*. https://www.netskope.com/es/security-defined/what-is-data-loss-prevention-dlp

- Brainard, J. (2022, 5 julio). *SD-WAN and Security Service Edge (SSE): Building Blocks for SASE*. Netskope. https://www.netskope.com/es/blog/sd-wan-and-security-service-edge-sse-building-blocks-for-sase

- Encryption, Privacy & Data Protection: A Balancing Act: The Business, Privacy, and Security Mandates for Comprehensive SSL/TLS Inspection. (2019). En Zscaler, *Securing the data: SSL/TLS decryption in a GDPRgoverned environment*. https://www.zscaler.com/resources/white-papers/encryption-privacy-data-protection.pdf

- colaboradores de Wikipedia. (s. f.). *Wikipedia, la enciclopedia libre*. https://es.wikipedia.org/wiki/Wikipedia:Portada

8. Anexos

Los anexos incluidos en este trabajo están incluidos como ficheros en formato PDF, a continuación, se listan los anexos con una breve explicación y nombre del fichero.

Despliegue y registro de un Publisher en VMware ESXi

El objetivo de este anexo es mostrar con capturas de pantalla el despliegue y registro del Publisher de Netskope en un entorno de Vmware:
(**Anexo1. Despliegue y registro de un Publisher en VMware ESXi.pdf**).

Despliegue de Netskope CE en Redhat 9

El objetivo de este anexo es enseñar el despliegue del componente Netskope Cloud Exchange en el sistema operativo de Redhat 9
(**Anexo2. Despliegue de Netskope CE en Redhat 9.pdf**).

Despliegue del cliente de Netskope en Windows

El propósito de este anexo es mostrar la instalación del cliente de Netskope en el sistema operativo de Windows 10
(**Anexo3. Despliegue del cliente de Netskope en Windows.pdf**).

Provisión y autenticación de identidades con Azure AD

Este anexo enseña la provisión de identidades desde el Identity Provider Azure AD al tenant de Netskope
(**Anexo4. Provisión y autenticación de identidades con Azure AD.pdf**).