Configuración de Netskope Cloud Security Platform para una entidad bancaria

Edison Sthy Valbuena Moreno

Asesor

Ivan Camilo Nieto Sanchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas Tecnología e Ingeniería ECBTI

Ingeniería de Telecomunicaciones

2026

Resumen

El informe presenta el proceso de implementación de la plataforma de seguridad en la nube Netskope en un banco, con el objetivo de centralizar y fortalecer su arquitectura de ciberseguridad. La solución, basada en Netskope Client y las capacidades de CASB y SSE, permite aplicar políticas de seguridad en tiempo real, proteger datos y mitigar amenazas al acceder a aplicaciones web, servicios SaaS y recursos privados desde cualquier ubicación. El proyecto contempla cinco fases técnicas que incluyen la instalación masiva del cliente, su integración con Active Directory, la configuración de políticas, la definición de reglas de Prevención de Pérdida de Datos (DLP) y el ajuste de parámetros esenciales como la inspección SSL.

La institución adquirió licencias SASE Professional y SSE, que incorporan funcionalidades avanzadas como filtrado web por categorías, protección de datos, detección de amenazas y capacidades de ZTNA bajo el principio de “nunca confiar, siempre verificar”. Asimismo, la implementación del Netskope Cloud Firewall amplía la protección hacia tráfico no web, ofreciendo control granular, inspección de protocolos, integración con políticas de DLP y administración centralizada. El trabajo colaborativo con el equipo de ingeniería permitió diseñar una arquitectura sólida y un plan de despliegue seguro del agente, garantizando un proceso alineado con los estándares corporativos y orientado a optimizar la postura de seguridad del banco.

***Palabras clave*:** Netskope, ciberseguridad, SSE, ZTNA, DLP

Abstract

The report presents the implementation process of the Netskope cloud security platform at a bank, with the goal of centralizing and strengthening its cybersecurity architecture. The solution, based on the Netskope Client and the capabilities of CASB and SSE, allows for the application of real-time security policies, data protection, and threat mitigation when accessing web applications, SaaS services, and private resources from any location. The project comprises five technical phases, including the mass installation of the client, its integration with Active Directory, policy configuration, the definition of Data Loss Prevention (DLP) rules, and the adjustment of essential parameters such as SSL inspection.

The institution acquired SASE Professional and SSE licenses, which incorporate advanced functionalities such as categorical web filtering, data protection, threat detection, and Zero-Trust Non-Accident (ZTNA) capabilities under the "never trust, always verify" principle. Furthermore, the implementation of the Netskope Cloud Firewall extends protection to non-web traffic, offering granular control, protocol inspection, integration with DLP policies, and centralized management. Collaborative work with the engineering team enabled the design of a robust architecture and a secure deployment plan for the agent, ensuring a process aligned with corporate standards and focused on optimizing the bank's security posture.

***Keywords*:** Netskope, cybersecurity, SSE, ZTNA, DLP.

Tabla de Contenido

Introducción 12

Planteamiento del Problema 16

Justificación 17

Objetivos 19

Objetivo General 19

Objetivos Específicos 19

Desarrollo del Proyecto 21

Fase I: Planeación y Diseño 21

Licenciamiento 26

Integración de Netskope con el Directorio Activo 33

Fase II: Configuraciones del Tenant y Políticas de Real Time 38

Despliegue del Cliente 40

Cuentas de Usuarios Locales 42

Client Configuration 46

Steering Configuration 50

Politicas de Protección en Tiempo Real 56

Fase III: Configuraciones Web y DLP 75

Fase IV: API Data Protection y Cloud Firewall 102

API Data Protection 102

Cloud Firewall 111

Excepciones de Red 120

Fase V: Monitoreo de Políticas y Tráfico Web 129

Categorías de Netskope 134

Reportes en Netskope 137

Conclusiones 141

Recomendaciones 143

Referencias Bibliográficas 147

Lista de Figuras

Figura 1 *Diagrama funcional de la integración* 24

Figura 2 *Diagrama de flujo Cisco Umbrela y Netskope* 25

Figura 3 *Diagrama de funcionamiento NGSWG* 27

Figura 4 *Diagrama de funcionamiento Cloud Firewall* 28

Figura 5 *Diagrama de funcionamiento EndPoint DLP* 29

Figura 6 *Diagrama de funcionamiento CASB-API* 30

Figura 7 *Matriz de navegación web* 31

Figura 8 *Protección de datos recomendada por Kriptos* 32

Figura 9 *Interfaz de heraamientas de Directpry tools* 34

Figura 10 *Integración de AD con Netskope* 35

Figura 11 *Integración SCIM para Postman* 36

Figura 12 *Sincronización de usuarios mediante Postman API* 37

Figura 13 *Grupos sincronizados* 38

Figura 14 *Plantilla de despliegue para Netskope Client* 40

Figura 15 *Métricas de seguridad configuradas en el cliente* 41

Figura 16 *Cantidad de usuarios instalados* 42

Figura 17 *Roles predefinidos en Netskope* 43

Figura 18 *Interfaz de creación de roles* 44

Figura 19 *Cuentas de usuario locales configuradas en el tenant de Netskope* 45

Figura 20 *Dominios de cuentas administradoras* 46

Figura 21 *Ventana de configuración de cliente* 47

Figura 22 *Métricas de seguridad configuradas en el cliente* 48

Figura 23 *Métricas de actualización configuradas en el cliente* 49

Figura 24 *Métricas de túnel configuradas en el cliente* 50

Figura 25 *Steering Configuration* 51

Figura 26 *Ejemplo detección de tráfico* 52

Figura 27 *Ejemplo de Steering Configuration* 53

Figura 28 *Agregar puertos no standard* 54

Figura 29 *Configuración de errores SSL* 55

Figura 30 *Listado de políticas Web Real time Protection* 58

Figura 31 *Mejores prácticas organización de políticas* 62

Figura 32 *Grupos de políticas* 63

Figura 33 *Creación de grupos de políticas* 64

Figura 34 *Política de Malware Scan* 65

Figura 35 *Política Utility DNS* 66

Figura 36 *Política Utility ITAR* 67

Figura 37 *Política Utility Online Ads* 68

Figura 38 *Política de Lista Blanca* 69

Figura 39 *Política con categorías prohibidas por la organización* 70

Figura 40 *Política de Dominios maliciosos* 70

Figura 41 *Política bloqueo descargas* 71

Figura 42 *Política de CASB Google Meet* 72

Figura 43 *Política de tráfico Web para Nicaragua* 73

Figura 44 *URL List configurada* 75

Figura 45 *Categorías personalizadas* 76

Figura 46 *Categoría personalizada para Panamá* 78

Figura 47 *Política con categoría personalizada* 79

Figura 48 *Perfiles de DLP predefinidos* 80

Figura 49 *Perfiles DLP Custom* 81

Figura 50 *Política de Etiquetas* 82

Figura 51 *Regex para los procedimientos* 83

Figura 52 *Validación de palabras* 85

Figura 53 *Elaboración de regla DLP* 86

Figura 54 *Expresión lógica perfil de DLP* 87

Figura 55 *Ejemplo severidad de las reglas* 88

Figura 56 *Perfil de archivos txt para Nicaragua* 89

Figura 57 *Política con perfiles de DLP personalizados* 90

Figura 58 *App Instance creadas* 91

Figura 59 *Política DLP con uso de una App Instance* 92

Figura 60 *Perfiles de Constraint creados* 93

Figura 61 *Creación de perfil de malware* 94

Figura 62 *Motores de detección* 95

Figura 63 *Política 1.2 BlockList Hashes* 95

Figura 64 *Ejemplo de política con CCL* 96

Figura 65 *Aplicaciones Permitidas por etiqueta* 97

Figura 66 *Política programada con rango de tiempo* 98

Figura 67 *Perfil de política programada* 99

Figura 68 *Plantillas configuradas* 100

Figura 69 *Template de Acceso Restringido* 101

Figura 70 *Banner de Aplicación Bloqueada* 102

Figura 71 *CASB API de Netskope* 103

Figura 72 *Ejemplo de Incidente DLP* 104

Figura 73 *Listado de Políticas API Data* 106

Figura 74 *Perfiles de dominio* 107

Figura 75 *Política API-DLP para Google Drive y Google Gmail* 108

Figura 76 *Perfil de Cuarentena configurado* 109

Figura 77 *Escaneo de malware para datos en reposo* 110

Figura 78 *Integraciones API configuradas en la organización* 111

Figura 79 *Acción por defecto tráfico No web* 113

Figura 80 *Ejemplo de aplicación para Teams* 115

Figura 81 *Política de tipo Firewall* 116

Figura 82 *Lista de Firewall* 117

Figura 83 *Azure permitido en todo el tráfico* 118

Figura 84 *Creación de lista blanca para Firewall* 119

Figura 85 *Política de lista blanca tipo Firewall* 119

Figura 86 *Bloque de aplicaciones por Firewall* 120

Figura 87 *Listado de excepciones para Steering Configuration Honduras* 122

Figura 88 *Excepciones de Netskope* 123

Figura 89 *Visualización de tráfico desde el Firewall perimetral* 124

Figura 90 *Lista de Network Location configuradas* 126

Figura 91 *Excepción para aplicación* 127

Figura 92 *Políticas de DND y Decrypt configuradas* 128

Figura 93 *Panel de monitoreo* 130

Figura 94 *Skope IT trafico web* 132

Figura 95 *Detalles de la conexión web* 133

Figura 96 *Reporte de alertas de seguridad* 139

Figura 97 *Informes predeterminados* 140

Figura 98 *Configuración de actualizaciones recomendada* 145

Lista de Tablas

Tabla 1 *Cronograma de actividades fase 1* 22

Tabla 2 *Categorías de Netskope* 135

Introducción

El presente informe detalla el proceso de implementación de la plataforma de seguridad en la nube de Netskope, una solución integral que ofrece a los usuarios del banco (empleados, contratistas y administradores) un acceso rápido y seguro a sus aplicaciones web, ya sea que estén trabajando en la oficina o de forma remota, ya que actualmente utilizan varias soluciones para administrar los accesos seguros y con Netskope se puede centralizar la arquitectura de ciberseguridad. La plataforma de seguridad en la nube se basa en el componente Netskope Client, que forma parte de la solución CASB (Cloud Access Security Broker). Esta solución permite a las empresas implementar políticas de seguridad y cumplimiento en los dispositivos de los usuarios que acceden a aplicaciones en la nube y servicios SaaS. También incluye Netskope Intelligent SSE, se basa en Netskope Security Cloud y brinda visibilidad incomparable y protección de datos y amenazas en tiempo real al acceder a servicios en la nube, sitios web y aplicaciones privadas desde cualquier lugar y en cualquier dispositivo.

En el proceso de implementación de la plataforma para el banco, se planean llevar a cabo sesiones remotas que abarcaran una serie de pasos técnicos esenciales divididos en cinco fases y que forman parte de la pasantía. Estos incluyen la instalación y despliegue del cliente de Netskope, su integración con el directorio activo AD de la compañía, la configuración detallada de políticas en tiempo real, el establecimiento de reglas de Prevención de Pérdida de Datos (DLP) y otros ajustes necesarios para excepciones y la capacidad de desencriptar paquetes. Durante estas sesiones, se planean adaptar meticulosamente los ajustes de configuración de acuerdo con los requisitos específicos de la compañía, siendo la detección de tráfico SSL un aspecto fundamental por la naturaleza de los certificados privados y públicos que se manejan en los bancos afines. La implementación masiva del cliente se puede lograr mediante la distribución

de un script y un instalador general de tipo msi, ambos se pueden distribuir de forma masiva a través del software que emplea la compañía para desplegar agentes o por medio de una política de GPO, esta instalación se debe realizar en modo silencio, con el propósito de proteger al usuario final brindando un proceso de instalación transparente. En términos de licenciamiento, la empresa de banca adquirió la categoría Netskope Security Service Edge (SASE) Professional, que brindó un conjunto de funcionalidades para la prevención de malware, detección de amenazas avanzadas, filtrado de sitios web basado en categorías, protección de datos y administración de aplicaciones y servicios en la nube, aplicables a cualquier usuario, ubicación o dispositivo. Uno de los aspectos destacados de la plataforma es su proxy en línea de paso único, cuya capacidad para descifrar el tráfico web y en la nube, incluyendo instancias y actividades, resulta excepcional.

Esto permite realizar configuraciones de manera controlada, evitando cualquier interrupción en los servicios. Durante la fase de diseño se optó por utilizar plantillas de navegación web y listas de navegación permitidas y bloqueadas para configurar políticas por categorías personalizadas, teniendo en cuenta la nueva clasificación de sitios web, que incluye un total de 132 categorías predefinidas. Dado que Netskope se va integrar en una red con múltiples soluciones de seguridad, es indispensable realizar una configuración adicional de aplicaciones y dominios en estado de bypass para garantizar el funcionamiento óptimo de todos los componentes de la red corporativa. Además, se adquirió el licenciamiento Netskope Security Service Edge SSE, para asegurar un nivel completo de protección y funcionalidad: Next Gen Secure Web Gateway Professional y Endpoint DLP Advanced. Cada una de estas licencias ofrece características y capacidades específicas para proteger las aplicaciones web y los servicios SaaS utilizados por la organización. La selección cuidadosa de las licencias adecuadas

garantizará un nivel completo de protección y funcionalidad en la plataforma, lo que permitirá a los usuarios acceder de manera rápida y segura a sus aplicaciones web desde cualquier ubicación. En este contexto, es crucial resaltar la incorporación del concepto de Acceso a la Red de Confianza Cero (Zero Trust Network Access, ZTNA) como un pilar fundamental de la plataforma Netskope, presente en todos sus componentes. Esta filosofía de seguridad parte del principio de "nunca confiar, siempre verificar", lo que implica una validación continua del usuario, dispositivo, aplicación y contexto antes de permitir cualquier tipo de acceso. Esta aproximación refuerza la seguridad perimetral moderna, especialmente en entornos distribuidos, híbridos o completamente en la nube.

Dentro de este marco, la implementación de Netskope Cloud Firewall (CFW) ha sido clave para fortalecer significativamente la postura de seguridad de la organización. A diferencia de los firewalls tradicionales, que operan en entornos físicos o limitados a la red corporativa, Netskope Cloud Firewall ofrece una solución completamente as-a-service, escalable y geodistribuida, proporcionando una administración centralizada, visibilidad unificada del tráfico y políticas coherentes para todos los usuarios, independientemente de su ubicación. El Cloud Firewall de Netskope amplía las capacidades tradicionales al brindar control exhaustivo sobre el tráfico no web (non-HTTP/HTTPS), un componente históricamente descuidado en muchas soluciones de seguridad en la nube. Esto incluye protocolos como TCP, UDP, ICMP, y permite aplicar políticas de seguridad con un alto grado de granularidad a conexiones salientes hacia Internet, que no pasan por los canales típicos de navegación web. Entre sus funcionalidades destacadas se encuentran: Control basado en la quinteta de red (dirección IP y puerto de origen, dirección IP y puerto de destino, y protocolo), lo que permite establecer políticas muy precisas. Identificación de usuarios y grupos mediante integración con directorios corporativos,

permitiendo aplicar reglas contextuales y alineadas al rol del usuario. Filtrado por nombres de dominio totalmente cualificados (FQDN) y uso de comodines, lo que permite manejar dinámicamente destinos no conocidos por IP. Inspección a nivel de aplicación para protocolos específicos, como FTP, mediante gateway de aplicación, asegurando que se inspeccionen los comandos y contenidos dentro del protocolo, no solo las conexiones. Integración nativa con políticas de DLP, amenazas avanzadas y análisis de comportamiento, lo que garantiza que incluso en tráfico no web se puedan detectar exfiltraciones, malware o actividad anómala.

Con base en el análisis previo y tras realizar diversas sesiones de trabajo colaborativo con el equipo de ingeniería del banco, se diseñó una arquitectura robusta y se estableció un plan de acción detallado. Este plan permitirá iniciar la configuración de la plataforma y desplegar, de forma segura y controlada, el agente Netskope Client. En las secciones que siguen, se profundizará en cada etapa del proceso, describiendo metodologías, criterios de seguridad y mecanismos de monitoreo aplicados para garantizar un despliegue eficaz y conforme a los estándares institucionales.

Planteamiento del Problema

Actualmente, el banco enfrenta una arquitectura de ciberseguridad fragmentada, en la que coexisten múltiples herramientas independientes para la gestión de accesos, la protección de datos, el filtrado de tráfico y la administración de aplicaciones en la nube. Esta dispersión de soluciones genera dificultades significativas en la visibilidad del tráfico, en la correlación de eventos y en la aplicación consistente de políticas de seguridad. Como consecuencia, los equipos técnicos deben invertir tiempo considerable en tareas operativas, mientras que la organización queda expuesta a posibles brechas debido a configuraciones desalineadas o a la falta de controles unificados. A esta problemática se suma la creciente adopción de servicios en la nube y de esquemas híbridos de trabajo, donde empleados y contratistas acceden a aplicaciones corporativas desde diversas ubicaciones y dispositivos.

Este entorno distribuido exige controles avanzados y dinámicos que garanticen la protección de los datos sensibles, especialmente en el sector bancario, donde el cumplimiento normativo y la detección temprana de amenazas son elementos críticos. Sin embargo, la infraestructura actual del banco carece de una solución centralizada que permita inspeccionar el tráfico web y no web, aplicar políticas de protección en tiempo real y gestionar adecuadamente el riesgo asociado al acceso remoto. Por lo anterior, es evidente que el banco requiere consolidar su arquitectura de seguridad bajo una plataforma moderna, escalable y orientada a modelos Zero Trust, que permita estandarizar políticas, fortalecer el monitoreo y asegurar un acceso confiable a los recursos corporativos. La necesidad de garantizar una protección consistente y efectiva en un entorno tecnológico cada vez más complejo constituye el problema central que este proyecto busca abordar.

Justificación

La modernización de la infraestructura tecnológica y la consolidación de los mecanismos de ciberseguridad se han convertido en prioridades estratégicas para las organizaciones financieras, especialmente ante el crecimiento de servicios en la nube, el trabajo remoto y la expansión del perímetro digital. En este contexto, el banco enfrenta el reto de gestionar múltiples soluciones de seguridad para controlar los accesos, proteger los datos sensibles y garantizar la continuidad operativa. Esta dispersión tecnológica no solo aumenta la complejidad administrativa, sino que puede generar brechas de seguridad y dificultades en la visibilidad del tráfico generando riesgos potenciales para la organización.

La implementación de la plataforma de seguridad en la nube de Netskope surge como una respuesta integral a estas necesidades, permitiendo centralizar, simplificar y fortalecer los controles de seguridad a través de una arquitectura unificada. Netskope ofrece una visibilidad completa del tráfico, protección de datos en tiempo real, capacidad avanzada de detección de amenazas y mecanismos de control aplicables desde cualquier ubicación y dispositivo. Su enfoque Zero Trust Network Access (ZTNA) y la integración con servicios como Cloud Firewall y CASB permiten reforzar la postura de seguridad adoptando prácticas modernas que superan los límites de los esquemas tradicionales basados en perímetros fijos.

Asimismo, la compañía adquirió licenciamientos avanzados que incluyen funciones de prevención de pérdida de datos, filtrado web, análisis de comportamiento, administración segura de aplicaciones SaaS y protección frente a tráfico no web. Esta inversión evidencia la necesidad institucional de contar con una plataforma robusta que responda a los riesgos actuales, que se ajuste a las regulaciones del sector financiero y que soporte la escalabilidad y evolución futura de los servicios digitales del banco. El proyecto también se justifica por su contribución a la

eficiencia operativa. La instalación masiva del Netskope Client, su integración con el directorio activo y la configuración de políticas centralizadas permiten reducir tiempos de gestión, minimizar errores y asegurar una experiencia de usuario transparente. La capacidad de descifrar tráfico SSL, junto con las políticas DLP y de navegación personalizadas, permitirá mantener altos estándares de seguridad sin afectar la productividad. Además, el despliegue meticuloso en fases, acompañado de sesiones remotas de trabajo técnico y validación con el equipo de ingeniería del banco, garantiza que la transición hacia este nuevo modelo de seguridad sea controlada, segura y alineada con las necesidades específicas de la organización. Esto resulta indispensable considerando la naturaleza crítica del sector financiero y la sensibilidad de sus datos e infraestructuras.

Objetivos

Objetivo General

Implementar la plataforma Netskope Security Cloud, habilitando sus capacidades avanzadas para supervisión y control de acceso a aplicaciones y servicios en entornos híbridos, garantizando acceso productivo a los colaboradores y reforzando la protección de los activos digitales de la organización de forma eficiente.

Objetivos Específicos

Definir políticas precisas que regulen el acceso a aplicaciones y servicios en la nube por parte del personal, balanceando productividad y seguridad mediante reglas detalladas para categorías web, usuarios, aplicaciones y escenarios, y asegurando un entorno operacional eficaz y protegido.

Proteger el tráfico de datos en todos los canales tecnológicos mediante controles técnicos y marcos regulatorios aplicables, alineados con ISO 27001, NIST SP 80053, GDPR y normativas internas

Proteger la información sensible en los dispositivos corporativos mediante una solución de Prevención de Pérdida de Datos en Endpoints que permita un monitoreo continuo de datos, evitando accesos no autorizados y garantizando el cumplimiento de las políticas de seguridad de la organización.

Monitorear en tiempo real la actividad de los colaboradores en aplicaciones y servicios en la nube mediante un sistema que genere automáticamente informes a través del módulo Advanced Analytics, destacando tendencias, posibles amenazas y actividades sospechosas facilitando una respuesta oportuna ante incidentes de seguridad.

Fortalecer la postura de seguridad de la organización mediante la implementación de Netskope Cloud Firewall como componente clave de una arquitectura basada en Confianza Cero (ZTNA), brindando visibilidad centralizada y protección avanzada del tráfico no web, garantizando un acceso seguro, eficiente y contextualizado a Internet para usuarios distribuidos y aplicaciones corporativas.

Desarrollo del Proyecto

Fase I: Planeación y Diseño

Para fortalecer su postura de seguridad, la compañía ha decidido implementar la plataforma Netskope Security Cloud, una solución avanzada que le permitirá no solo reducir el riesgo de fugas de información, sino también optimizar el rendimiento de sus aplicaciones corporativas. Netskope proporciona un control exhaustivo sobre el tráfico de aplicaciones en la nube SaaS y, en general, sobre todo el tráfico web, así como sobre el uso de aplicaciones en la nube y la protección de datos mediante una plataforma integrada y gestionada desde una única consola. Adicionalmente, con la incorporación de Netskope Cloud Firewall, la organización amplía su capacidad de protección más allá del tráfico web tradicional, obteniendo visibilidad y control granular sobre el tráfico no web (como protocolos TCP, UDP e ICMP), lo cual resulta esencial para detectar y mitigar riesgos asociados a servicios, aplicaciones y transferencias de datos que no utilizan HTTP/HTTPS. Esta funcionalidad permite aplicar políticas de seguridad a nivel de red de forma centralizada, garantizando un enfoque coherente y moderno dentro de la arquitectura de Confianza Cero.

La infraestructura de la compañía administra usuarios y grupos a través de un Directorio Activo local, permitiendo una organización eficiente de colaboradores en distintos grupos de seguridad y acceso. En el pasado, el Banco empleaba una combinación de servicios, como un proxy independiente, una VPN tradicional y una solución DLP (Data Loss Prevention) separada, lo que presentaba desafíos significativos de administración y limitaba la visibilidad centralizada de sus controles de seguridad. Ahora, con la implementación de Netskope, el Banco unifica todas estas capacidades en una sola herramienta, facilitando la gestión, supervisión y control de los accesos internos y de la navegación. Además, se ha adquirido un paquete de licencias Netskope,

integradas en el plan de trabajo y cronograma de implementación. Este plan, diseñado para una ejecución efectiva y en fases, está disponible en la

Tabla 1.

Tabla 1

Cronograma de actividades fase 1

#	ACTIVIDAD	AVANCE	RESPONSABLE
	FASE 1: PLANEACIÓN Y DISEÑO		
1.1	Verificar el estado actual de las licencias dentro del Tenant de Netskope. Confirmar funcionalidades disponibles y requeridas para la implementación.	0%	Implementador
1.2	Verificar acceso administrativo al Tenant de Netskope. Crear cuentas necesarias para la configuración y gestión del servicio.	0%	Implementador/Cliente
1.3	Envio del listado de perfiles de filtrado web y grupo de usuarios que puedan acceder. Completar formulario NGSWG.	0%	Cliente
1.4	Levantar información de la infraestructura de seguridad en la nube existente. Determinar el estado de la	0%	Implementador

	plataforma antes de iniciar configuraciones.		
1.5	Validación configuraciones Actuales de Cisco Umbrella (Proxy actual), con el objetivo de replicar las configuraciones base.	0%	Implementador/Cliente
1.6	Creación de cuentas de administración del tenant para el cliente. Asignar permisos adecuados según roles y responsabilidades.	0%	Implementador/Cliente
1.7	Integración Tenant con los directorios activos locales AD del cliente (sincronización de usuarios y grupos).	0%	Cliente

Nota. Se hace incluyen las actividades de la primera fase de implementación para consultar el cronograma del proyecto diríjase al siguiente enlace: Cronograma Netskope SWG-DLP.xlsx.

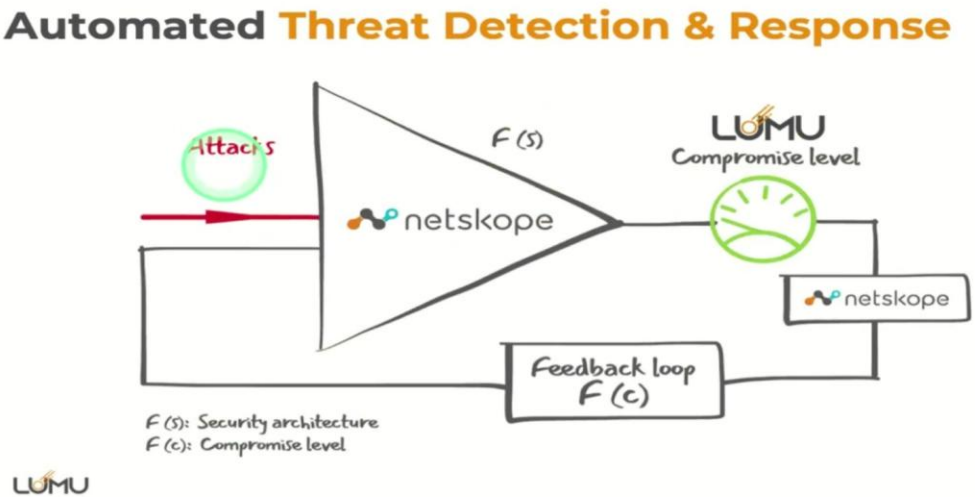
Fuente: Autoría propia.

Por otro lado, el banco cuenta con LUMU, una plataforma que ofrece soluciones para la gestión de incidentes cibernéticos y la visibilidad de amenazas, utilizando inteligencia artificial para identificar, analizar y responder a riesgos en tiempo real. Por esta razón, resulta fundamental integrar Netskope con LUMU en las próximas fases, con el fin de fortalecer la postura de seguridad y asegurar que ambas soluciones operen de forma conjunta. Una integración exitosa de LUMU con Netskope permite el envío automatizado de indicadores de compromiso (IoC) a la consola de administración de Netskope, lo que garantiza una visibilidad

proactiva a partir de reglas y perfiles previamente configurados, mediante listas de recepción definidas. Se procede a mostrar el diagrama de funcionamiento de esta integración. Ver Figura 1.

Figura 1

Diagrama funcional de la integración



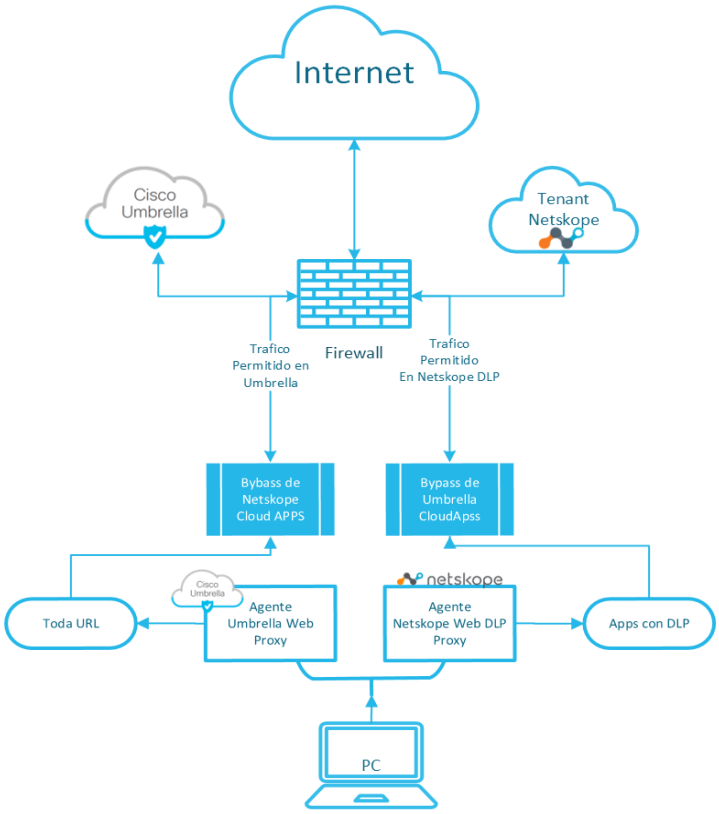
Nota. El diagrama ilustra el flujo de detección y respuesta automática ante amenazas, integrando Netskope y Lumu para evaluar el nivel de compromiso de seguridad. Tomado de Lumu Technologies (s. f.).

Anteriormente, la función de filtrado web era administrada mediante Cisco Umbrella, lo que implicaba una sobrecarga operativa considerable y restringía la agilidad en la actualización de políticas de acceso. Con la adopción de Netskope, esta capacidad se ha trasladado a una arquitectura más dinámica y contextual, lo que mejora significativamente la postura de seguridad frente a amenazas emergentes y permite una adaptación proactiva a nuevos vectores de ataque. En paralelo, la organización optó por reemplazar íntegramente su solución de Prevención de Pérdida de Datos (DLP) existente, migrando hacia la solución unificada de DLP de Netskope. Esta nueva implementación habilita capacidades avanzadas de inspección, correlación y control de datos sensibles en entornos críticos como servicios en la nube, aplicaciones SaaS, correo

electrónico, aplicaciones privadas y dispositivos endpoint, fortaleciendo de manera integral la estrategia de protección de la información. Considerando una base de usuarios superior a los 9.000 colaboradores, fue necesario diseñar un modelo de interoperabilidad y flujo de datos que garantice la coexistencia eficiente entre la solución heredada (Cisco Umbrella) y la nueva plataforma de seguridad convergente Netskope OneCloud. A continuación, se presenta un diagrama de arquitectura que ilustra este diseño transitorio.

Figura 2

Diagrama de flujo Cisco Umbrela y Netskope



Nota. El diagrama representa el flujo del tráfico web entre Cisco Umbrella y Netskope, mostrando la interacción entre el firewall, los agentes de proxy y las aplicaciones con y sin políticas de prevención de pérdida de datos (DLP).

El diagrama de la Figura 2 muestra la arquitectura transitoria diseñada para permitir la interoperabilidad entre Cisco Umbrella y Netskope durante el proceso de migración del servicio de filtrado web. Actualmente, todo el tráfico generado desde los endpoints es redirigido inicialmente a través de los agentes locales de proxy: Umbrella Web Proxy Agent y Netskope Web DLP Proxy Agent, según el tipo de URL y la aplicación accedida. Las solicitudes dirigidas a aplicaciones con políticas activas de prevención de pérdida de datos (DLP) son inspeccionadas por el agente de Netskope, mientras que el resto del tráfico es procesado por el agente de Umbrella. Posteriormente, las políticas de bypass definidas en ambos extremos, Netskope Cloud Apps y Umbrella CloudApps, determinan qué tráfico es autorizado y redirigido hacia sus respectivos servicios en la nube. Finalmente, el firewall organiza el enrutamiento del tráfico hacia Internet en función de las reglas predefinidas para cada plataforma. Esta configuración híbrida garantiza continuidad operativa, visibilidad de seguridad y control granular mientras se completa la transición definitiva hacia Netskope como solución unificada de seguridad web y DLP.

Licenciamiento

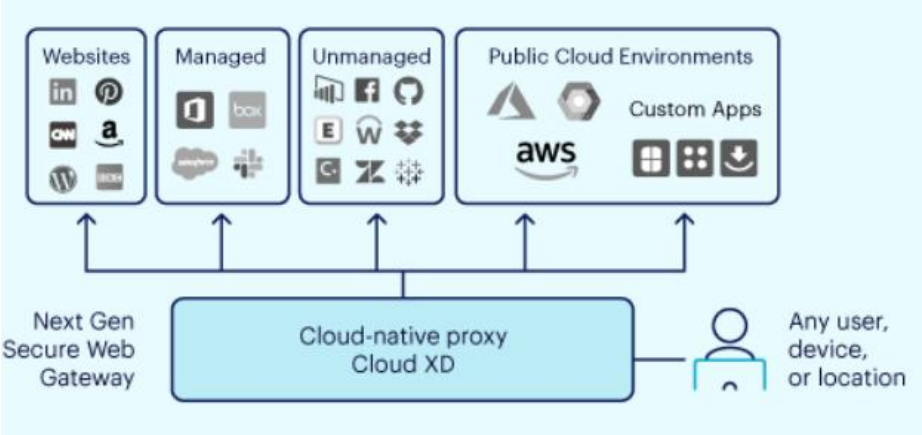
Adquirir licencias de Netskope es esencial para garantizar la seguridad y la protección de los datos y aplicaciones en un entorno de nube en constante evolución. Para llevar a cabo un proceso eficiente y atendiendo las recomendaciones del fabricante la compañía adquirió el siguiente licenciamiento para el despliegue de la solución de seguridad en nube:

Nex Generation Secure Web Gateway Professional cantidad 8724. Se utiliza para proporcionar una solución de seguridad web avanzada que ayuda a proteger a las organizaciones contra las amenazas web y los ataques cibernéticos. Esta solución se basa en una puerta de enlace de seguridad web, que actúa como un filtro entre los usuarios de la red y los sitios web

que visitan, es decir, se comporta como proxy que blinda el tráfico de las aplicaciones web. Algunas de sus características son: filtrado de contenido, detección de amenazas avanzadas, protección contra ataques de phishing, el monitoreo y análisis de la actividad de red. En la actualidad, las empresas en línea utilizan un promedio de 2415 aplicaciones en la nube con 89% de sus usuarios activos en la nube1. Más del 98% de estas aplicaciones son no administradas, Netskope Next Gen SWG decodifica en línea miles de aplicaciones cloud. Las amenazas habilitadas para la nube abarcan todas las etapas de la cadena de eliminación y representan el 68% de las descargas de malware en 2021, principalmente desde la nube aplicaciones de almacenamiento. Vease la Figura 3.

Figura 3

Diagrama de funcionamiento NGSWG

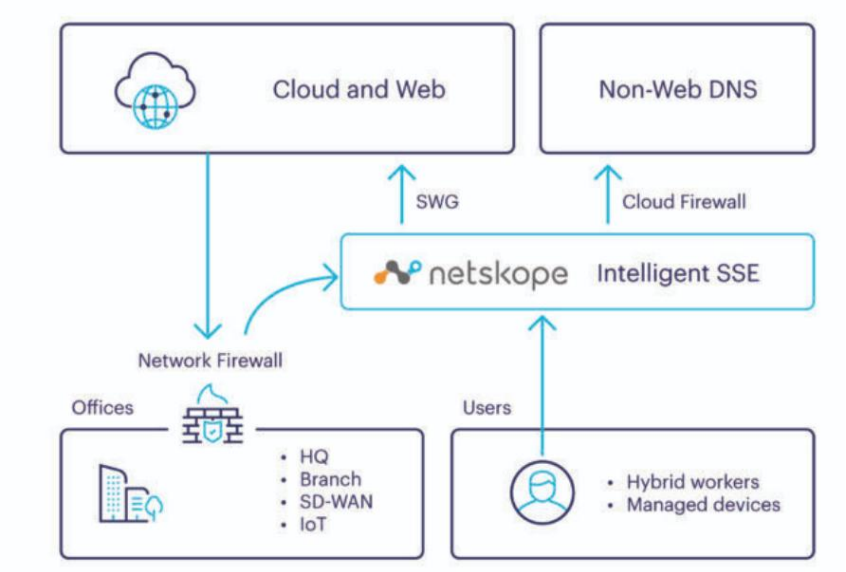


Nota. El diagrama muestra el funcionamiento del Next Generation Secure Web Gateway (NGSWG) de Netskope, ilustrando el flujo del tráfico web desde diferentes entornos y aplicaciones hacia el proxy en la nube para su inspección y control de seguridad. Tomado de Netskope (s. f.).

Proporciona seguridad de red en tráfico saliente a través de todos los puertos y protocolos para usuarios y oficinas. Los controles de política de CFW incluyen 5 tuplas (origen, destino direcciones y puertos con protocolo), además de ID de usuario e ID de grupo, dominios calificados y comodines como destinos, una capa de aplicación de puerta de enlace para FTP y registro de eventos de firewall. Proporciona seguridad de red para el tráfico saliente en todos los puertos y protocolos, para un acceso directo a Internet seguro con el cliente de Netskope en dispositivos gestionados y permite asegurar a los usuarios remotos y a las sucursales con FWaaS usando una consola, un motor de políticas y una plataforma. Asegura Oficinas: Proporcionar seguridad de red para cualquier usuario o dispositivo, para todos los puertos de salida y protocolos, para un acceso directo a Internet seguro a través de GRE e IPsec. Consulte Figura 4.

Figura 4

Diagrama de funcionamiento Cloud Firewall

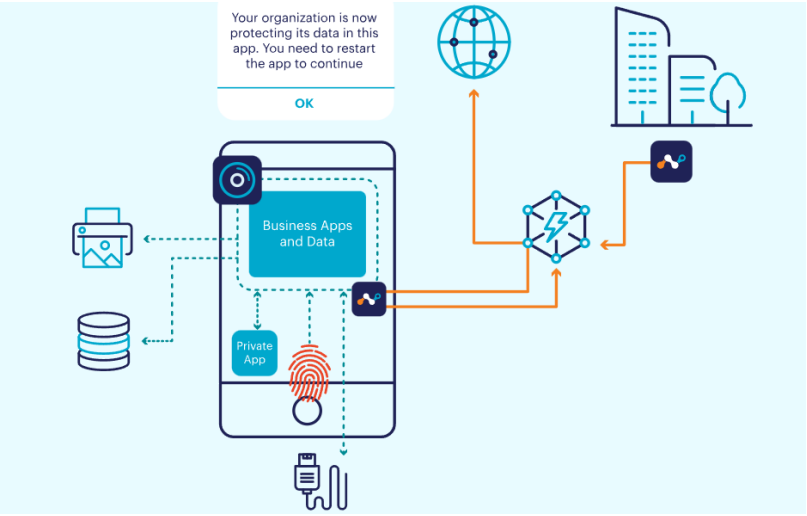


Nota. Representación esquemática de los componentes de una arquitectura de seguridad cloud que habilita acceso seguro a internet. Tomado de Netskope Endpoint DLP Advanced, por Licencias Online. (s. f.).

El licenciamiento de Endpoint Data Loss Prevention de Netskope es una funcionalidad adicional que se integra con el cliente de Netskope para ofrecer protección de datos directamente en los dispositivos finales. Esta característica permite a las organizaciones gestionar y controlar el movimiento de datos sensibles desde y hacia dispositivos USB, impresoras, conexiones Bluetooth y recursos compartidos en la red. Control de Dispositivos: Permite crear políticas detalladas para gestionar qué dispositivos están permitidos y qué usuarios pueden acceder a ellos. Control de Contenido: Utiliza el motor de DLP de Netskope para inspeccionar y controlar el movimiento de datos entre el endpoint y dispositivos USB o impresoras, asegurando que no se transfiera información sensible sin autorización. Es importante destacar que el Endpoint DLP de Netskope es una capacidad opcional que se integra con el cliente de Netskope y no requiere la implementación de un cliente o agente adicional en el endpoint. Ver Figura 5.

Figura 5

Diagrama de funcionamiento EndPoint DLP

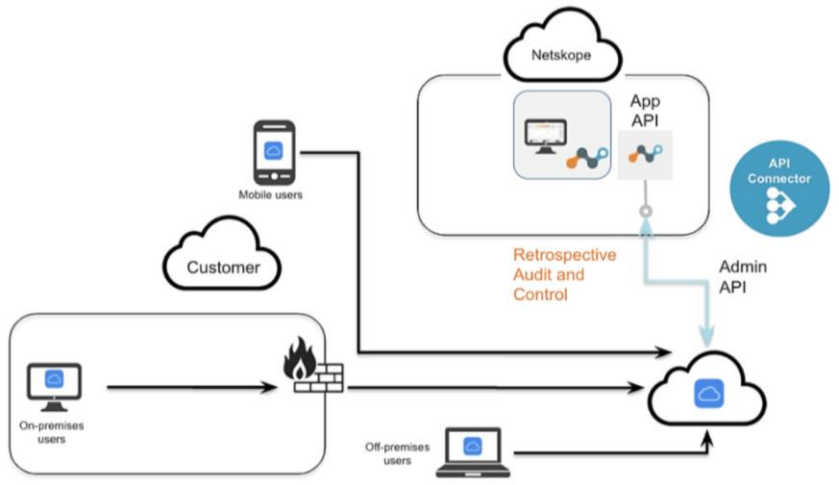


Nota. Arquitectura de seguridad que integra firewall, SWG y SD-WAN para acceso seguro. Tomado de Netskope Endpoint DLP Advanced, por Licencias Online. (s. f.). https://www.licenciasonline.com/ar/es/productos/netskope

Capacidad de la plataforma Netskope para proteger datos en reposo en servicios en la nube gestionados a través de la inspección de APIs. Esta función, parte del módulo Netskope CASB, utiliza tokens OAuth y las API expuestas por los servicios en la nube para conectarse y aplicar políticas de seguridad. Netskope Cloud Inline API permite a las empresas proteger datos en reposo dentro de aplicaciones en la nube gestionadas por TI, como Microsoft 365, Google Workspace, etc. La protección API CASB de Netskope inspecciona el contenido que reside en los servicios gestionados en la nube. La función proporciona visibilidad completa sobre la configuración, el contenido y los patrones de uso dentro de estas aplicaciones, permitiendo la aplicación de políticas para prevenir el intercambio no autorizado y la fuga de datos. Se conecta a las API publicadas por los servicios en la nube utilizando tokens OAuth, permite una implementación fuera de banda sin necesidad de un proxy inline. Ver Figura 6.

Figura 6

Diagrama de funcionamiento CASB-API

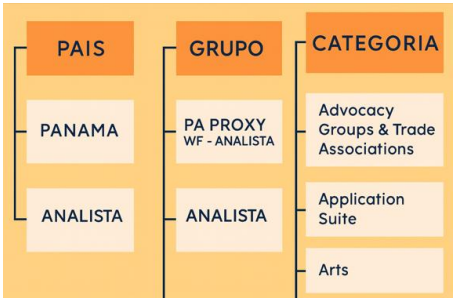


Nota. Implementación fuera de banda mediante API, sin requerir proxy en línea. Tomado de Netskope, por Licencias Online. (s. f.). https://www.licenciaonline.com/ar/es/products/netskope

Finalmente, el cliente remitió las plantillas de configuración correspondientes al servicio de filtrado web. Estos documentos servirán como insumo base para iniciar las configuraciones preliminares dentro de la consola de administración. La información recibida se encuentra segmentada por país, dado que la compañía tiene presencia regional en Centroamérica. En este contexto, se definió un enfoque basado en la restricción de categorías específicas de navegación no autorizadas para los distintos grupos de usuarios, alineándose con el modelo de inspección "allow all" que implementa Netskope, el cual permite todo el tráfico salvo aquellas categorías explícitamente bloqueadas. A continuación, se presenta una imagen referencial del contenido de dichas plantillas. Por razones de seguridad y confidencialidad, no se expone el archivo completo. Véase la Figura 7.

Figura 7

Perfiles de navegación web



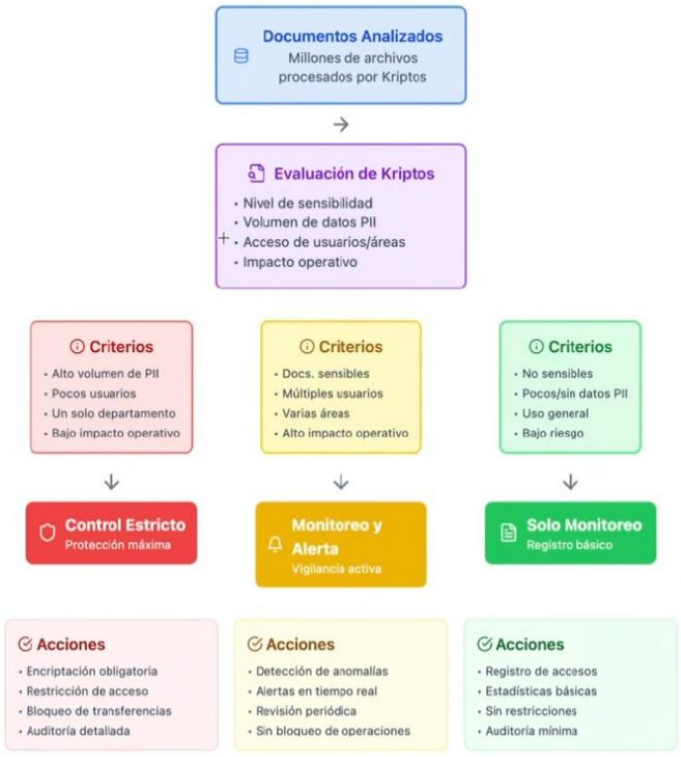
Nota. Ejemplo de la estructura de perfiles de filtrado web por país, grupo y categoría.

De igual manera se socializaron los caos de uso que se desean controlar con el motor DLP avanzado de Netskope, específicamente enfocados al metadato etiquetado que genera la solución de Kriptos y que trabaja de manera fluida y en conjunto con Netskope. En el marco de una alianza tecnológica estratégica firmada en julio de 2020, Kriptos aporta su tecnología de clasificación automática mediante inteligencia artificial para identificar documentos como “confidencial”, “restringido”, “uso interno” o “público” y etiquetarlos con metadatos. Netskope,

por su parte, aprovecha esa clasificación e información contextual para aplicar políticas de protección, como bloqueo, alerta o cifrado, en más de 34 000 aplicaciones en la nube (como OneDrive, Dropbox o Slack) y durante la navegación web. Esta integración potencia una solución de prevención de fuga de información tanto en entornos locales como en la nube, con visibilidad integral y automatización adaptada al contexto de los datos. En la Figura 8 podrá observar la información que el personal de Kriptos solicito priorizar.

Figura 8

Protección de datos recomendada por Kriptos



Nota. Configuraciones sugeridas para la protección de datos mediante la integración con Netskope.

El tenant es un componente fundamental dentro de la plataforma de seguridad en la nube. Netskope Inc, la empresa desarrolladora y proveedora de la plataforma, otorga al banco un tenant

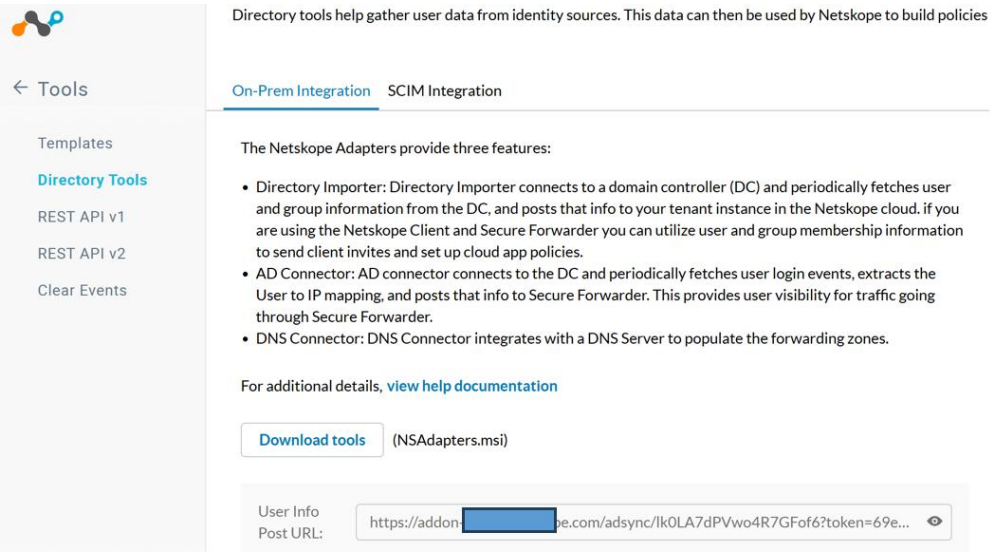
específico al suscribirse a sus productos. Esta plataforma se convierte en el punto central desde el cual la organización puede administrar y proteger sus servicios y aplicaciones en la nube.

Integración de Netskope con el Directorio Activo

La integración entre Netskope y el Directorio Activo se erige como un componente esencial en el proceso de configuración. Este enlace técnico establece una interconexión fluida y estratégica que conlleva varios beneficios cruciales. En primer lugar, posibilita la sincronización coherente de la configuración de usuarios y grupos desde el ecosistema de la compañía hacia la plataforma de Netskope. Este flujo constante de datos garantiza que la herramienta esté siempre actualizada con la estructura organizativa en tiempo real, lo que a su vez facilita la implementación de políticas de seguridad basadas en los usuarios y grupos existentes. Además, esta integración ofrece una solución eficiente para la administración y el cumplimiento de políticas. Al alinear los perfiles de usuarios y grupos entre ambas plataformas, se simplifica la aplicación de políticas específicas a grupos definidos, asegurando un acceso confiable y regulado a los recursos en la nube. Para completar la integración se requiere de un conector On-Premisses que se descarga desde el tenant, en la siguiente ruta: Settings > Tools > Directory tolos > On Prem Integration. Adicionalmente, se copia la URL de post que sirve para establecer la comunicación entre el AD y Netskope. Vease la Figura 9.

Figura 9

Interfaz herramientas de Directory tools

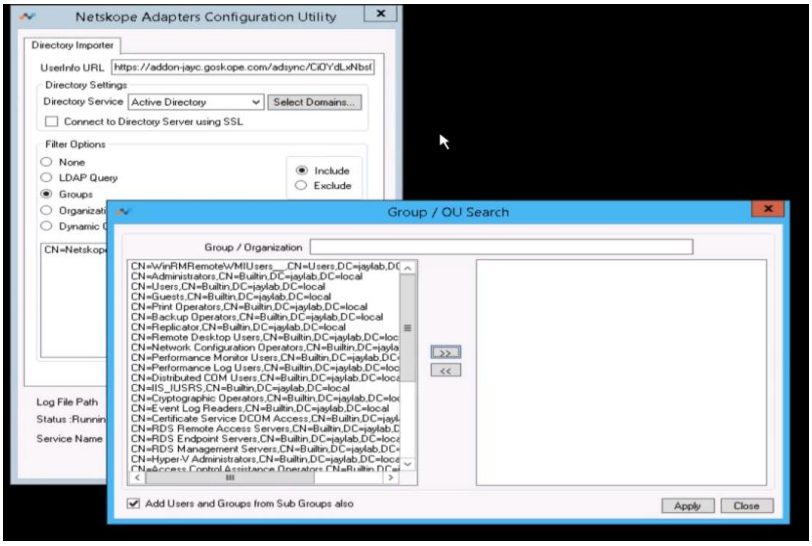


Nota. Vista de la interfaz para la gestión de herramientas de directorio. Tomado de Netskope tenant.

Como se puede observar en la Figura 10, este conector permite seleccionar los grupos o unidades organizacionales que se encuentren configuradas en el AD. Se configura esta aplicación con el propósito de leer los usuarios y grupos, es decir, con ayuda de esta integración se van a administrar. Por ejemplo, en la creación de un nuevo grupo, basta con sincronizar esta aplicación para que se replique el nuevo ajuste en el tenant de Netskope, este proceso se realizó para la configuración del grupo de pruebas.

Figura 10

Integración de AD con Netskope

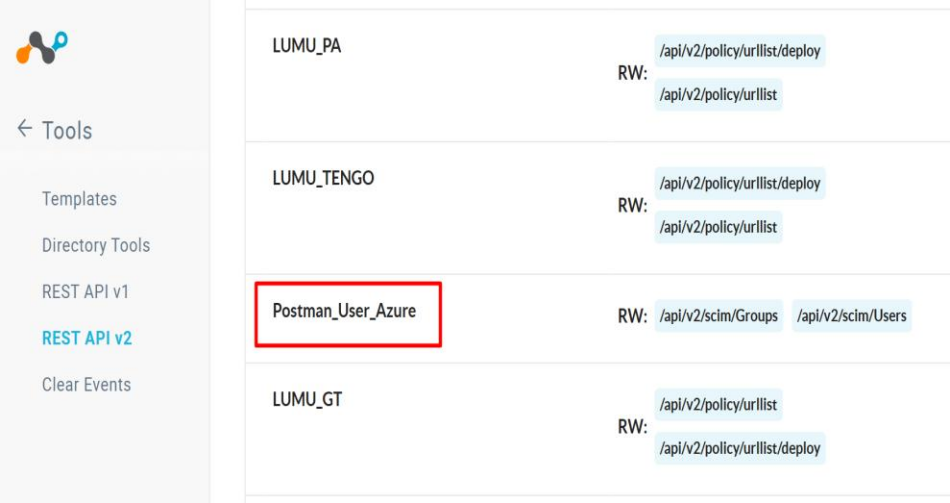


Nota. Diagrama del conector que sincroniza usuarios y grupos desde Active Directory. Tomado de Netskope tenant.

La actividad se realizó mediante un proceso simple que requiere instalar el conector asignarle los usuarios desde el AD y volver a iniciar el proceso del conector desde los servicios de Windows. Por este medio se sincronizaron las Unidades Organizacionales de la compañía, para la creación y sincronización de grupos se empleó una integración SCIM Con Postman. Para completar la integración se requiere de un intercambio de datos a nivel API, adicionalmente se debe contar con el entorno de Postman el cual se puede descargar desde la web. Para obtener las URL de Netskope diríjase a la siguiente ruta: ***Settings > Tools > Directory tolos > SCIM Integration***. Después de generar la URL y copiarla se obtendrá algo como lo mostrado en la Figura 11.

Figura 11

Integración SCIM para Postman



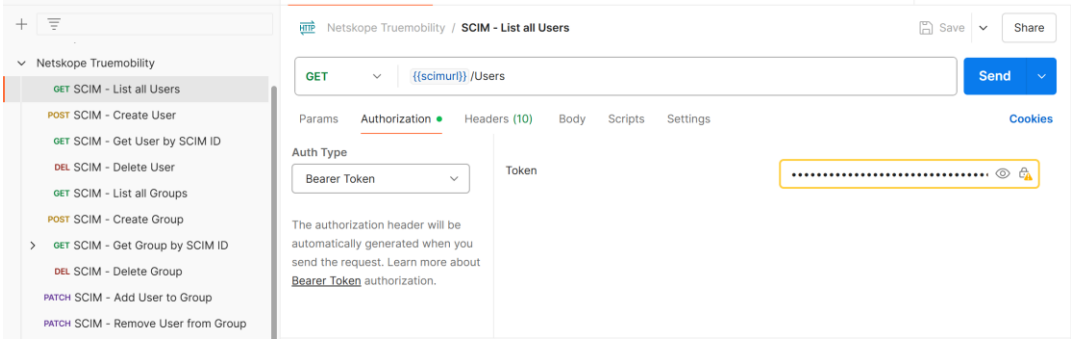
Nota. Esquema de configuración para la gestión automatizada de identidades mediante SCIM. Tomado de Netskope tenant.

Después de intercambiar las credenciales de las API y los tokens generados entre ambas plataformas, se puede proceder con la sincronización de usuarios de manera segura y eficiente. Es fundamental tener en cuenta que Postman opera utilizando REST API v2, por lo que es necesario consultar la documentación específica para asegurarse de que las solicitudes y los endpoints utilizados sean compatibles con las acciones requeridas, tales como la creación de grupos, eliminación de usuarios o cualquier otra tarea de administración que se desee realizar. Esta documentación detallará los parámetros y métodos HTTP que deben ser empleados, así como las mejores prácticas para garantizar que las integraciones se ejecuten de manera óptima y segura. Asegúrese de seguir estas directrices para evitar errores comunes en la implementación y maximizar la eficacia del proceso:

https://truemobility.goskope.com/apidocs/?include_beta_routes=0

Figura 12

Sincronización de usuarios mediante Postman API

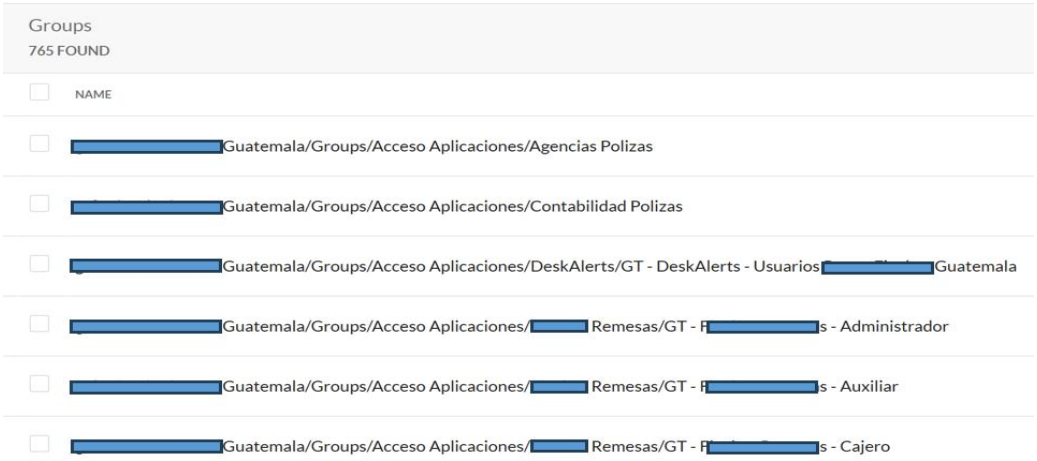


Nota. Proceso de automatización de la gestión de usuarios utilizando la API de Netskope. Tomado de Postman tenant.

La integración de Netskope con Postman, Figura 12 a través de la API permite automatizar tareas repetitivas como la creación de usuarios, asignación a grupos, o eliminación de cuentas. Esto reduce el esfuerzo manual y acelera procesos de gestión, eliminando la necesidad de ingresar manualmente cada cambio en la consola de Netskope. Por otro lado, esta integración permite utilizar los identificadores de los usuarios y sus respectivos grupos en las políticas de protección en tiempo real. La sincronización a través de Postman y la API de Netskope permite monitorear y controlar de manera más precisa los cambios en la estructura de usuarios y grupos. Las respuestas JSON que se obtienen de la API permiten validar que los cambios se realizaron correctamente y facilitan la integración con otras plataformas de monitoreo o auditoría. Simplemente se creó un nuevo grupo y se sincronizo para validar su funcionamiento. A continuación, se muestran algunos de los grupos sincronizados por medio de esta integración que se encuentran en la siguiente ruta: ***Settings > Security Cloud Platform > Netskope Client > Groups.***

Figura 13

Grupos sincronizados



Nota. Listado que muestra los grupos sincronizados desde Active Directory hacia la plataforma. Tomado de Netskope tenant.

En la Figura 13 se pueden apreciar un gran número de grupos sincronizados, en total 7596, Netskope no tiene ninguna limitante con este valor, tampoco con el número de usuarios que se sincronicen. Esto permite adaptar las políticas de seguridad de manera precisa y granular, asegurando una protección efectiva de los activos digitales sin comprometer la experiencia del usuario final. Por otro lado, este valor no necesariamente consume una licencia, esta solo se descuenta cuando es instalado un agente en un dispositivo final. Estas aplicaciones fueron creadas en la primera sesión de trabajo con el personal de TI, se sincronizaron los usuarios de manera correcta y el intercambio de información fue satisfactorio entre el AD y el Netskope. Es un proceso simple que requiere compartir conjuntamente unos certificados, tokens y URL de SAML que se agregan en ambos tenant, al conceder los permisos suficientes de administrador la aplicación podrá sincronizar los grupos, y usuarios hacia la plataforma de Netskope.

Fase II: Configuraciones del Tenant y Políticas de Real Time

El tenant es un componente fundamental dentro de la plataforma de seguridad en la nube. Netskope Inc, la empresa desarrolladora y proveedora de la plataforma, otorga al banco un tenant específico al suscribirse a sus productos. Esta plataforma se convierte en el punto central desde el cual la organización puede administrar y proteger sus servicios y aplicaciones en la nube.

En el contexto del banco, como parte esencial del proceso de configuración inicial de la plataforma, se hace imprescindible llevar a cabo una integración sinérgica con el Directorio Activo en premisa de la compañía. Esta integración reviste una importancia primordial, pues actúa como el puente que permite una sincronización fluida y constante de la configuración de usuarios y grupos desde la infraestructura de la compañía hacia la plataforma Netskope. Esta interconexión tecnológica, en primer término, garantiza una actualización perpetua de la configuración, asegurando que Netskope refleje en tiempo real y con total precisión la compleja estructura organizativa de la empresa. No obstante, su alcance va más allá de la mera sincronización, ya que al amalgamar los perfiles de usuarios y los conjuntos de grupos con Netskope, se desencadena la capacidad para implementar políticas de seguridad y control de acceso que se fundamentan en los grupos preexistentes dentro del dominio organizativo. Esta integración, además, simplifica enormemente la gestión de usuarios al posibilitar la aplicación específica de políticas de seguridad y cumplimiento a cada uno de los grupos definidos. Este enfoque garantiza un acceso óptimo, seguro y altamente gestionado a los distintos servicios y aplicaciones en la nube por parte de los usuarios del banco. En esencia, esta integración con el Directorio Activo desempeña un papel crítico al forjar un vínculo coherente y seguro entre las estructuras internas de la compañía y la robusta plataforma de Netskope, culminando en una administración eficiente y en un entorno en línea altamente seguro. Con Netskope Secure Web Gateway se aplican los beneficios de CASB a toda la web. Al agregar clasificaciones de

categorías específicas a una política de protección en tiempo real, se prohibe a los usuarios el acceso a sitios inapropiados y, además, protege el tráfico de la compañía contra la pérdida de datos y posible malware.

Despliegue del Cliente

El cliente de Netskope proporciona visibilidad y control en tiempo real de los dispositivos gestionados que acceden a la nube y la web desde cualquier parte. En la corporación se desplegó hacia todos los usuarios de la compañía de manera simultánea, esto fue posible por medio de un script que se ejecutó desde el dominio de la compañía a través de una política y con ayuda del software Absolute que incluyo un archivo .bat construido a partir del script que se muestra más adelante. El instalador del agente se puede descargar desde los siguientes enlaces: **Windows**:https://download-[tenant].goskope.com/dlr/win/get, **MacOS**: https://download-[tenant].goskope.com/dlr/mac/get y **Linux**: https://download-[tenant].goskope.com/dlr/linux/get

Por otro lado, se empleó la plantilla de ejecución que se muestra en la Figura 14, que incluye parámetros como "/qn", los cuales posibilitan la instalación silenciosa del agente, ejecutándose en segundo plano sin interacción o notificación al usuario final.

Figura 14

Plantilla de despliegue para Netskope Client

```
msiexec /I [ruta]\NSClient.msi host=addon-[tenant].goskope.com
token=lk0LA7dPVwo4R7Gxxxx mode=peruserconfig autoupdate=on
/norestart /l*v %PUBLIC%\nscinstall.log /qn enrollauthtoken=
f015eff68ff530c25a38ec1ee831xxxx
```

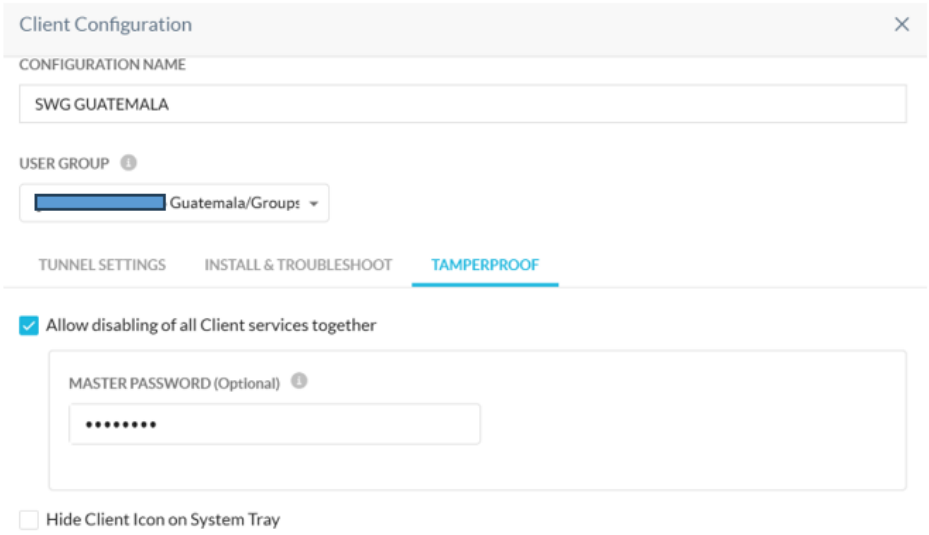
Nota. Comando de instalación silenciosa con parámetros para host, token y registro automático.

Adicionalmente se configuró el netskope client para que no pudiese ser desinstalado u inhabilitado por los usuarios finales; para lograr esto se deshabilito la opción que se subraya en la

siguiente imagen, se habilito la actualización automática que es esencial para mantener el Netskope Client actualizado con las últimas correcciones de seguridad y características. También se habilitó la opción “Enable advanced debug option” para que permitiera la recolección de logs. Finalmente, se configuraron los parámetros de transporte del túnel SSL con el protocolo TLS, para no interferir con infoblox. Vease la Figura 15.

Figura 15

Métricas de seguridad configuradas en el cliente



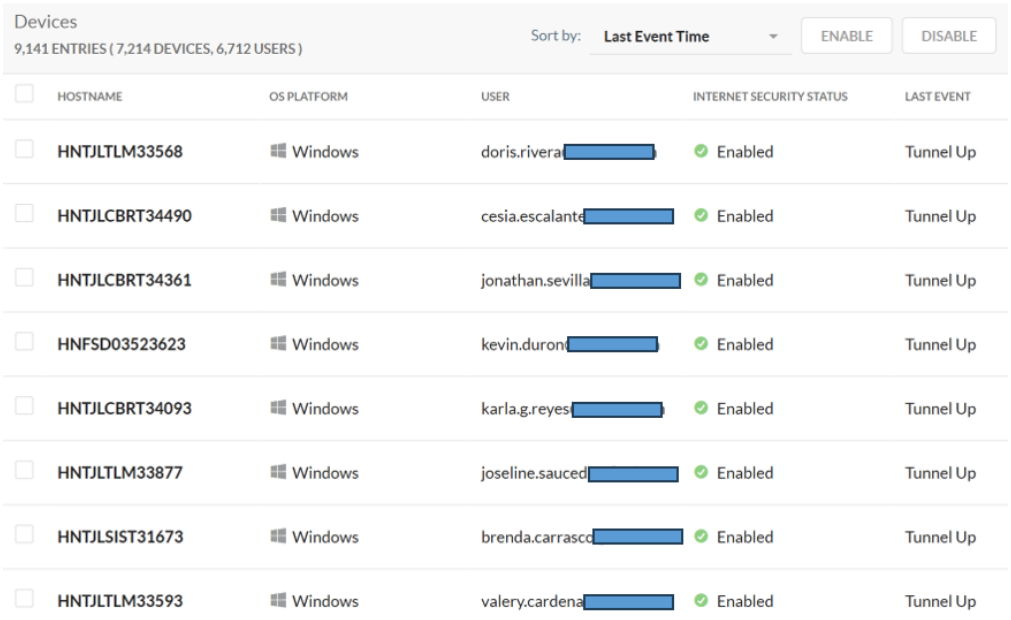
Nota. Panel que muestra las métricas de seguridad habilitadas en el agente desplegado. Tomado de Netskope tenant.

Por otro lado, la densidad de usuarios que tienen instalado el agente de Netskope aun no alcanza el rango esperado, pero se continúan desplegando agentes de manera controlada. Se tienen 6712 usuarios con el agente activo en las últimas semanas del mes de agosto para el año 2025 y con una instalación de agente sobre las máquinas de usuario final cercana a las 7214 máquinas. Si existiera una diferencia de valores tendría sentido porque los clientes activos son diferentes a los instalados, recuerde que para el tenant de Netksope un cliente se encuentra activo cuando en las últimas horas a generado tráfico para consultar recursos en nube y websites. En la

Figura 16, podrá apreciar los usuarios activos y los dispositivos de usuario final que cuentan con el agente instalado y activo.

Figura 16

Cantidad de usuarios instalados



Nota. Resumen del número de usuarios con el agente de Netskope activo en sus dispositivos. Tomado de Netskope tenant.

Cuentas de Usuarios Locales

Como el tenant es suministrado por el fabricante es necesario configurar cuentas de usuario locales que permitan acceder a la plataforma de manera segura y controlada mediante roles de configuración específicos. La creación de estas cuentas se realiza dentro de la consola de ajustes generales, además, se pueden configurar y asignar roles específicos a cada usuario, esto permite acceder solo a los recursos qué sean asignados a un determinado usuario. En la compañía se configuraron los siguientes usuarios locales, véase Figura 17, adicionalmente se incluye una

lista de los 12 roles predefinidos por el fabricante, pero se pueden configurar roles de acuerdo con las necesidades específicas.

Roles Predefinidos

Tenant Admin, Delegated Admin, Application risk analyst, Cloud intelligence analyst, Compliance officer, Directory admin, Enterprise applications admin, IaaS and PaaS admin, InfoSec operations admin, NS technical success, Restricted Admin, Security admin y Security analyst. El alcance de cada uno de estos roles se muestra a continuación:

Figura 17

Roles predefinidos en Netskope

Privilege	Cloud Intelligence Analyst	Application Risk Analyst	Enterprise Applications Admin	Directory Admin	Security Admin	InfoSec Operations Admin	Tenant Admin	Delegated Admin	Restricted Admin	Compliance Officer
View and Manage Administrators	X	X	X	X	X	X	✓	X	X	X
View and Manage Advanced Settings	X	X	X	X	X	X	✓	X	X	X
View and Manage CCI	X	X	✓	X	✓	✓	✓	✓	X	X
View CCI	X			✓	✓	✓	✓	✓	✓	X
View and Manage Events	X	X	X	✓	✓	✓	✓	✓	X	X
View Events	X	X	X	✓	✓	✓	✓	✓	✓	X
View and Manage API-enabled Protection	X	X	X	✓	✓	✓	✓	✓	X	X
View and Manage Policies	X	X	X	X	✓	✓	✓	✓	X	X
View Policies	X	X	X	✓	✓	✓	✓	✓	✓	✓
View Reports	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
View and Manage Settings	X	X	X	X	✓	X	✓	✓	X	X
View and Manage End Users	X	X	X		✓	X	✓	✓	X	X
View and Manage Incidents	✓	X	X	X	✓	✓	✓	✓	X	✓

Nota. Permisos asignados a los roles administrativos predeterminados en la consola. Tomado de Netskope tenant.

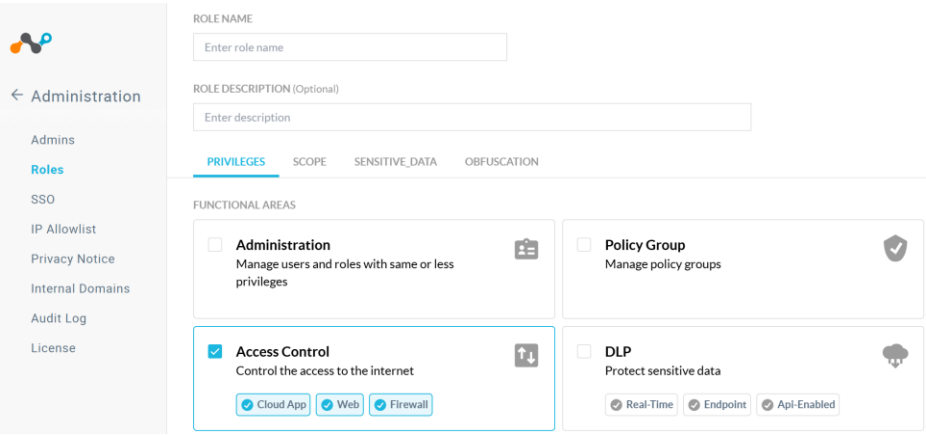
Roles Personalizados

Con la administración basada en roles, puede agregar administradores fácilmente y asignarles roles específicos, con diferentes niveles de acceso a la plataforma Netskope. Se recomienda agregar roles antes de agregar administradores porque deberá seleccionar un rol para

cada administrador que cree, no es posible salvar una cuenta administradora sin antes asignarle un rol. Encontrará el menú que se muestra en la Figura 18. El proceso para crear un rol es bastante simple, solo se debe seguir la ruta, ***Settings > Administration > Roles > New Role.***

Figura 18

Interfaz de creación de roles



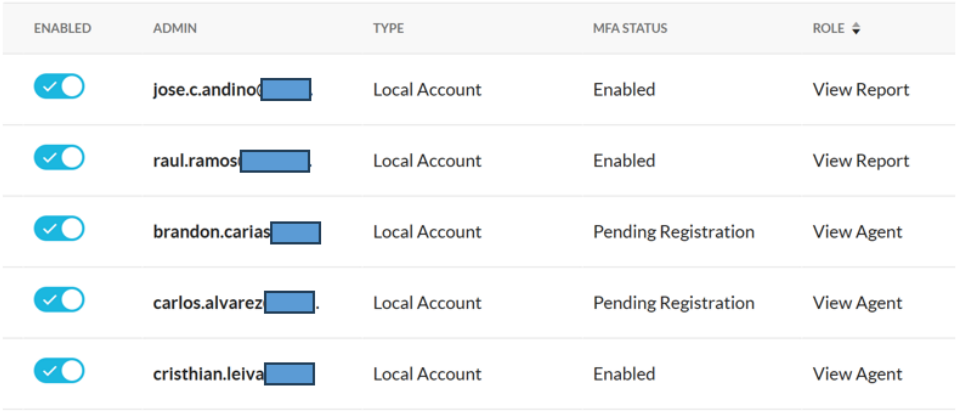
Nota. Pantalla para configurar roles personalizados, definiendo alcance, privilegios y permisos. Tomado de Netskope tenant.

Como se puede apreciar se tienen bastantes opciones para ajustar el rol, incluidas el alcance, privilegios, datos sensibles entre otros, además, si se elimina una cuenta de administrador, no se pierden los distintos permisos asociados con esta cuenta. Simplemente puede reasignar la función de administrador a otro usuario. Por ejemplo, el CISO (Chief Information Security Officer) de su organización puede tener una cuenta de administrador con acceso a todas las políticas relacionadas con la seguridad y al alcance de la organización. Si ese CISO abandona la organización y se elimina su cuenta, las reglas de política que creó no se verían afectadas y permanecerían vigentes. Además, puede asignar fácilmente al siguiente usuario la misma función que al CISO anterior, sin tener que redefinir los permisos desde cero. A

continuación, en la Figura 19, podrá observar las cuentas locales creadas durante la implementación.

Figura 19

Cuentas de usuario locales configuradas en el tenant de Netskope



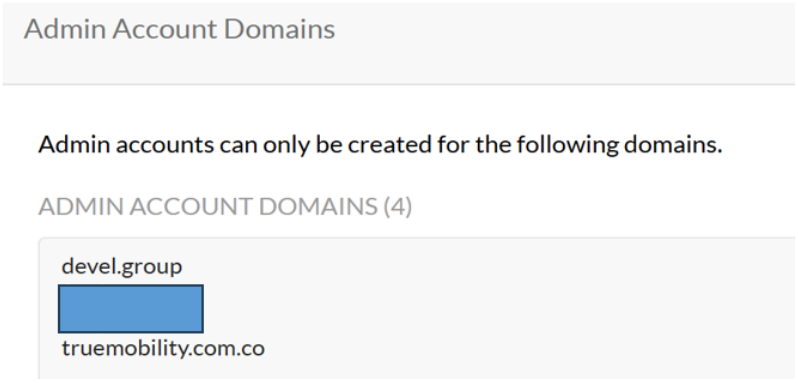
ENABLED	ADMIN	TYPE	MFA STATUS	ROLE
	jose.c.andino[redacted]	Local Account	Enabled	View Report
	raul.ramos[redacted]	Local Account	Enabled	View Report
	brandon.carias[redacted]	Local Account	Pending Registration	View Agent
	carlos.alvarez[redacted]	Local Account	Pending Registration	View Agent
	cristhian.leiva[redacted]	Local Account	Enabled	View Agent

Nota. Listado de usuarios locales creados en la plataforma, mostrando su estado y rol. Tomado de Netskope tenant.

Si llegasen a existir cuentas que tuvieran el icono de candado en la Figura 19, se estaría indicando que se encuentran temporalmente bloqueadas, para desbloquear simplemente se debe dar clic sobre el candado con una cuenta de permisos administrativos. Nótese que las cuentas de usuario locales pertenecen a unos dominios específicos, estos dominios se pueden controlar en ***Settings > Administration > Internal Domains*** y finalmente en la opción de editar se pueden gestionar los dominios que pueden acceder al tenant. Observe los dominios configurados en la Figura 20.

Figura 20

Dominios de cuentas administradoras



Nota. Configuración que restringe la creación de cuentas de administrador a dominios corporativos específicos. Tomado de Netskope tenant.

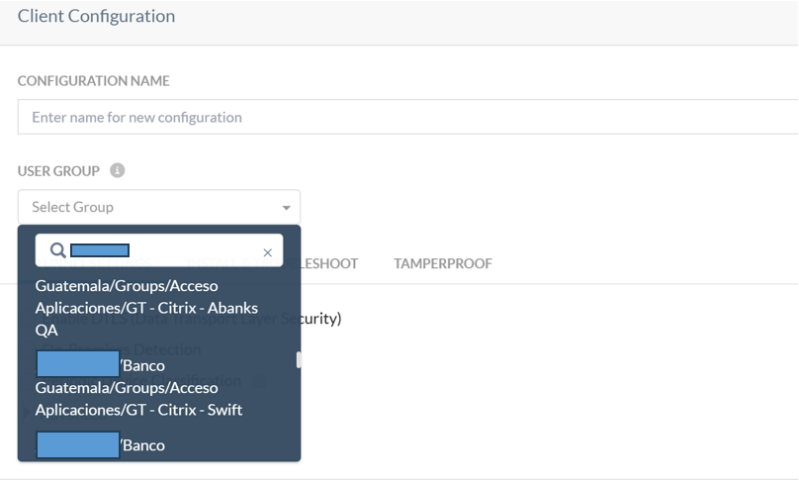
Client Configuration

Es un elemento crítico para garantizar que las políticas y controles de seguridad se apliquen de manera consistente en todos los dispositivos finales dentro de la asociación. Permite a los administradores gestionar y aplicar medidas de seguridad, monitorear la actividad de los usuarios y proteger contra amenazas de seguridad y pérdida de datos. Las configuraciones y parámetros que se aplican al software Netskope Client instalado en dispositivos terminales, como computadoras portátiles, de escritorio o dispositivos móviles, se pueden ajustar en una gran variedad de parámetros de acuerdo con las necesidades específicas de la organización. Puede configurar los ajustes de todo el sistema utilizando el cuadro de diálogo Configuración del cliente, para acceder a este recurso debe dirigirse a la siguiente ruta: ***Settings > Security Cloud Platform > Netskope Client > Client Configuration***. Para realizar de manera correcta la configuración de un nuevo Client Configuration es necesario tener grupos de usuarios o unidades organizacionales disponibles para completar el proceso, no es posible realizar la configuración de manera genérica para todos los usuarios, ya que por defecto Netskope los incluye en sus

ajustes preliminares. Al seguir este enfoque, se garantiza una protección efectiva de los activos digitales de la organización y se optimiza el rendimiento y la experiencia del usuario. En la Figura 21, podrá visualizar el panel principal de configuración, observe que es obligatorio relacionar un grupo de usuarios.

Figura 21

Ventana de configuración de cliente



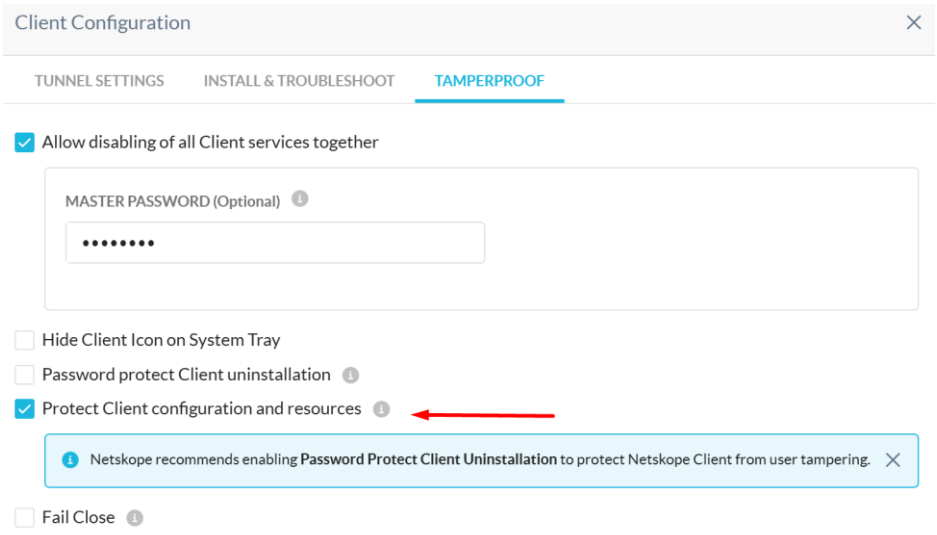
Nota. Interfaz principal para asignar configuraciones específicas a grupos de usuarios. Tomado de Netskope tenant.

Se tienen configurados siete Client Configuration, es un número adecuado y aunque es superior a los valores recomendados, que para efectos prácticos es un total de cinco (5), funciona adecuadamente para el banco y ayuda a gestionar la sepación de roles y tráfico por regional. Para la distribución organizacional del banco siete client configuration son suficientes, uno para cada región y grupo de operaciones, observe que Nicaragua, Panama, Honduras, Guatemala, SWG y Alcance tienen su propio client configuration, finalmente, existe otro con los clientes de producción donde residen la totalidad de los usuarios “All user”. Se debe mantener el enfoque de flujo, es decir, cada uno de los Client Configuration debe estar apuntando a un determinado

Steering Configuration lo que permite tener un control de tráfico sincronizado entre el cliente instalado en la maquina final y la plataforma de seguridad, por buenas prácticas siempre se debe asociar un Steering Configuration a un Client Configuration donde los grupos y usuarios coincidan evitando errores de tráfico. Adicionalmente, las configuraciones preliminares se deben realizar sobre el steering y el client configuration de un grupo de pruebas, luego se aplican los cambios al cliente de producción. Por otro lado, se recomienda configurar el netskope client en su interfaz de **Tamperproof** para que no pueda ser desinstalado u inhabilitado por los usuarios finales, nótese en la Figura 22 que la opción “Allow disabling of Clients” se encuentra inactiva, para bloquear la desinstalación del agente se debe crear una contraseña de protección y habilitar la opción “Protect Client configuration and resources" para garantizar el funcionamiento fluido de Netskope Client en dispositivos de usuario final que ejecutan Windows y MacOS.

Figura 22

Métricas de seguridad configuradas en el cliente

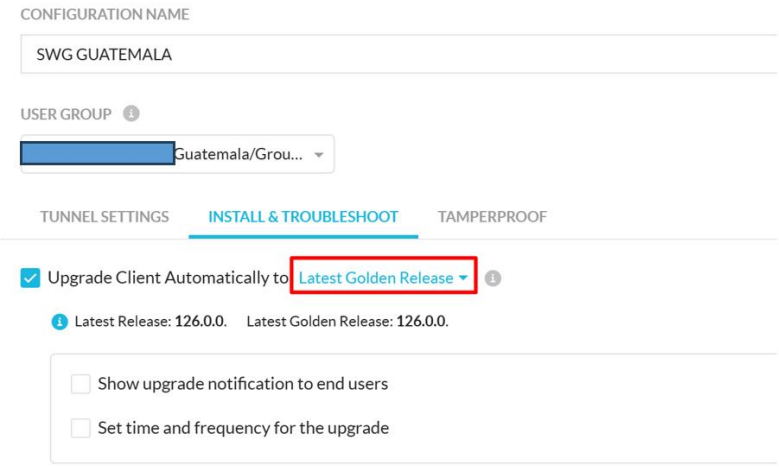


Nota. Panel donde se activan y ajustan las métricas de seguridad que aplicará el agente. Tomado de Netskope tenant.

En la interfaz de Install & Troubleshoot se habilito la actualización automática que es esencial para mantener el Netskope Client actualizado con las últimas correcciones de seguridad y características, también se habilitó la opción “Enable advanced debug option” para que permitiera la recolección de logs con un nivel de detalle mayor, principalmente utilizado con soporte a nivel de TAC. Vease la Figura 23 con la opción de Golden reléase.

Figura 23

Métricas de actualización configuradas en el cliente

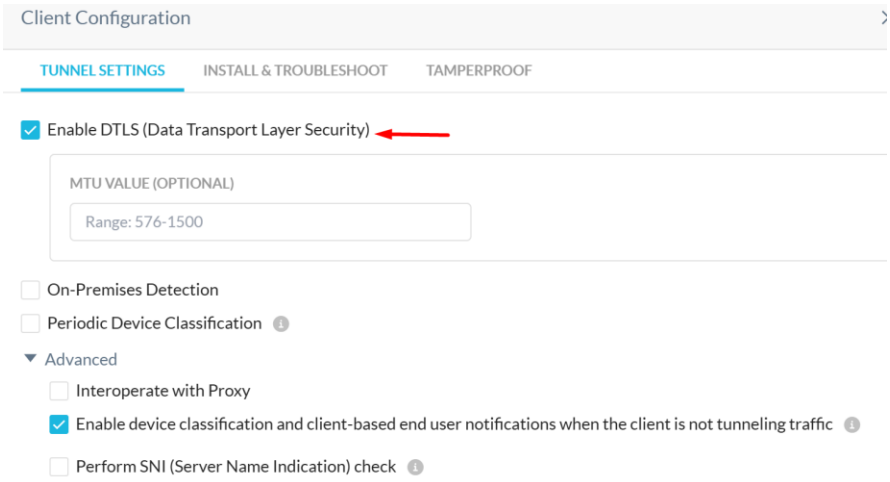


Nota. Configuración de las opciones de actualización automática y versión Golden Release. Tomado de Netskope tenant.

Por último en la interfaz de **Tunnel Settings** que se muestra en la Figura 24 se ajustó el túnel con el protocolo DTLS (Data Transport Layer Security) que mejora la comunicación así como el proceso de red. Contrario al TCP inherentemente que ralentiza el rendimiento general del flujo en la red con una latencia alta y caídas de paquetes, se habilito la opción de “Enable device classification and client-based end user notifications when the client is not tunneling traffic” la cual ayuda a deshabilitar de manera automática el cliente el tráfico se esté tunelizando hacia túneles GRE e IPSec.

Figura 24

Métricas de túnel configuradas en el cliente



Nota. Ajustes del túnel seguro (DTLS) para optimizar rendimiento y cifrado del tráfico. Tomado de Netskope tenant.

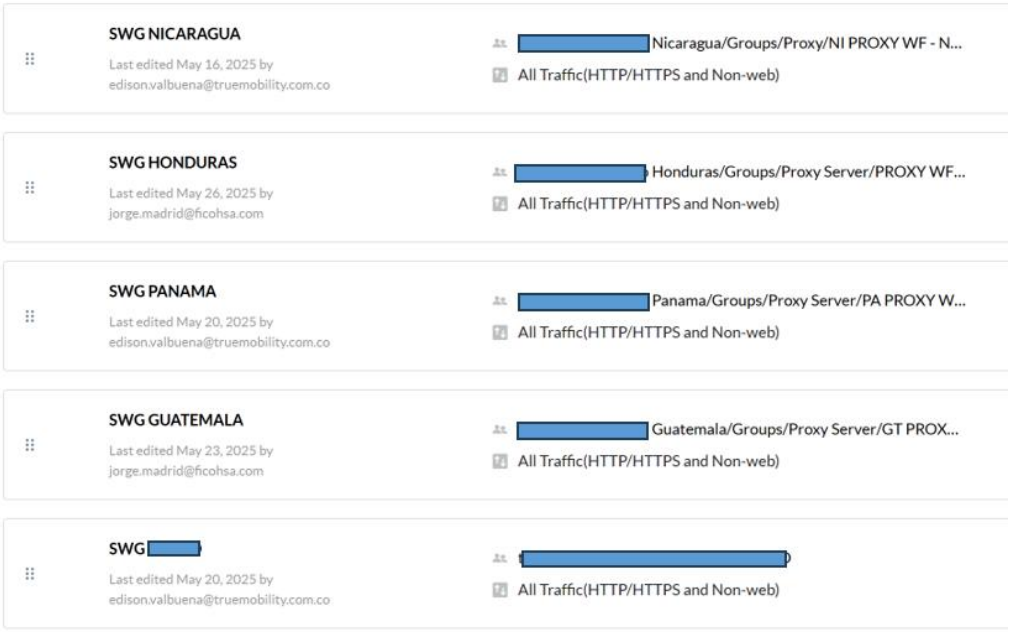
Steering Configuration

Se refiere a la configuración de direccionamiento o enrutamiento que se puede establecer en la plataforma de seguridad en la nube de Netskope. Esta configuración permite a los administradores de Netskope controlar y redirigir el tráfico de red de los usuarios hacia los servicios y aplicaciones en la nube. El steering configuration también puede utilizarse para aplicar políticas de seguridad específicas. Por ejemplo, se pueden establecer reglas para redirigir el tráfico de ciertos usuarios hacia servicios de seguridad adicionales o para bloquear el acceso a determinadas aplicaciones o sitios web, esto se logra mediante los grupos, es decir, se crea un grupo con determinados usuarios y se asocia con un steering configuration especifico, por ende, todos los ajustes de tráfico solo se aplicarán a ese grupo. En conclusión, controla qué tipo de tráfico se dirige a Netskope para un análisis profundo en tiempo real y qué tipo de tráfico se omite. El “Default Tenant Configuration” se aplica a todos los usuarios. Por lo tanto, todos los

usuarios de la compañia que no se encuentren en un steering custom están pasando a través del mismo analizador de tráfico web por defecto, sin embargo, se configuro un steering para las pruebas de tráfico y poder manejar de una manera diferenciada este tráfico antes de pasarlo a producción, este grupo tiene unas configuraciones de bypass diferentes, lo que permitió probar el webfiltering con Netskope. Se recomienda habilitar la opción de Dynamic Steering que permite evaluar los paquetes y determinar si pasan a través del túnel o se omite dicho tráfico. Una vez las configuraciones fueron verificadas con rigurosidad se duplicaron en el entorno de producción. En la siguiente imagen se muestran todos los steering configurados en la corporación.

Figura 25

Steering Configuration



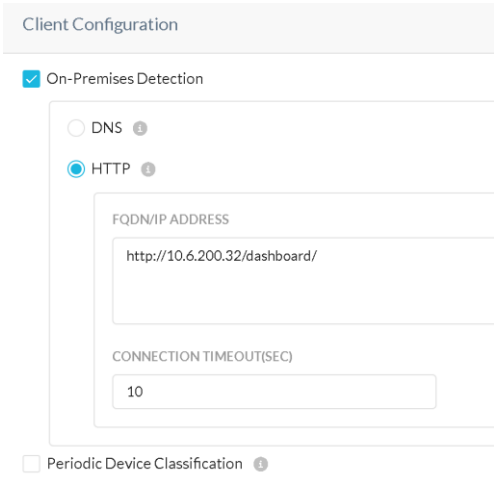
Nota. Configuraciones de enrutamiento definidas para dirigir el tráfico de la red corporativa. Tomado de Netskope tenant.

Como muestra la Figura 25 se tienen siete steering operacionales que apuntan a un especifico cliente, como se mencionó con anterioridad es una buena práctica y permite tener una

organización puntual de la solución. Configurar el Dynamic Steering ayuda a excluir el tráfico del túnel cuando los usuarios finales se encuentran trabajando en Premisa, evitando intermitencias de red o bloqueos hacia sitios excepcionados en la herramienta. La configuración de esta característica requiere de un DNS o una dirección HTTP, con esta dirección Netskope consulta constantemente si el URL/IP es accesible y con base en esto redirecciona el tráfico. Es importante que la configuración de On-Premises sobre el Steering Configuration contenga habilitada la opción de All web traffic, ya en los entornos remotos, es decir, para el Off-Premises se deben tunelizar todos los paquetes, incluyendo los paquetes de las aplicaciones privadas, de esta manera se habilitara el NPA que actúa como una VPN de cero confianzas. Observe en la Figura 26 un ejemplo de configuración de "On-premises detection" con una IP de HTTP.

Figura 26

Ejemplo detección de tráfico



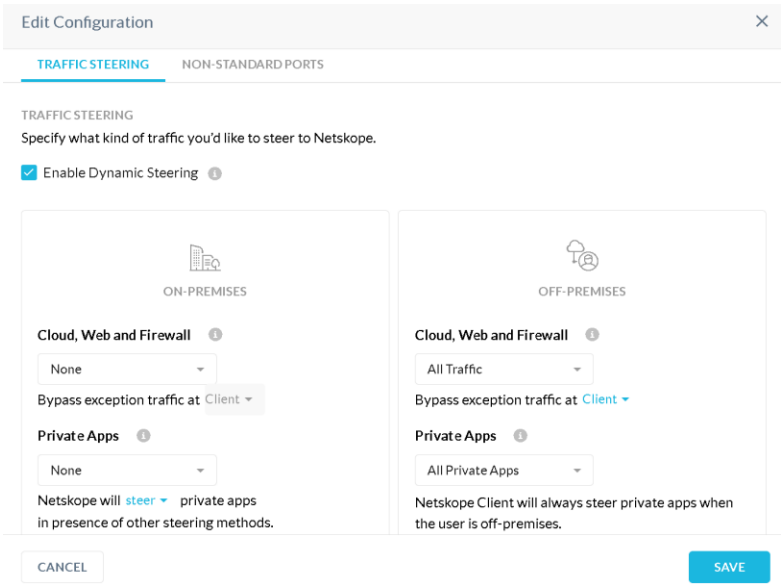
Nota. Configuración de detección local (On-Premises) mediante consultas HTTP a una IP específica. Tomado de Netskope tenant.

Después de realizar este ajuste de detección de tráfico es posible habilitar en el Steering Configuration los perfiles remoto y oficina. En el perfil de On-Premises se habilito el tráfico de

None sin acceso aplicaciones privadas, por otro lado, el perfil de Off-Premises enruta hacia el túnel de Netskope todo el tráfico web y no web así como el tráfico de aplicaciones privadas, observe en la siguiente imagen la configuración detallada de cada perfil, en la izquierda el perfil de oficina y en la derecha el perfil remoto con todo el tráfico permitido. Vea la Figura 27.

Figura 27

Ejemplo de Steering Configuration

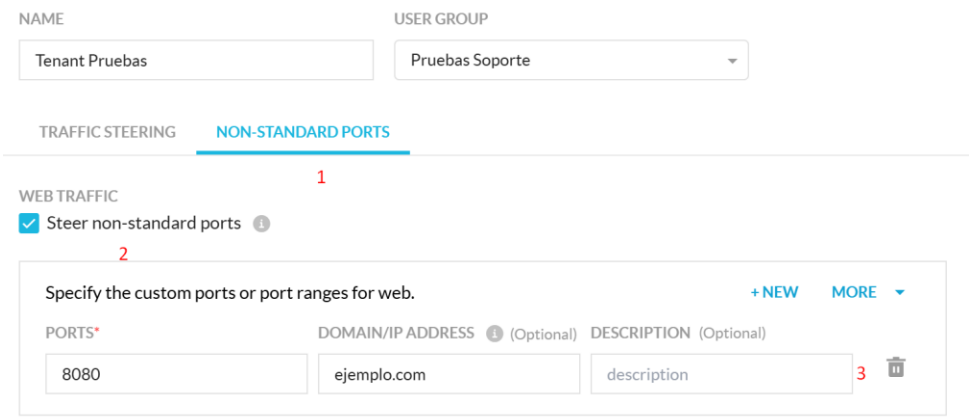


Nota. Comparación de perfiles de enrutamiento: oficina (restringido) y remoto (todo el tráfico permitido). Tomado de Netskope tenant.

En la Figura 28 se puede ver una opción de puertos no estándar la cual permite que el cliente de Netskope dirija el tráfico web (HTTP/HTTPS) en cualquier puerto, como única condición se deben introducir los puertos o dominios que desea dirigir por los puertos personalizados, para lograr esto, haga clic en Non-Standard Ports, luego habilite la opción “Steer non-standard ports” y finalmente agregue el puerto y dominio que quiere tunelizar, se pueden agregar varios puertos.

Figura 28

Agregar puertos no standard

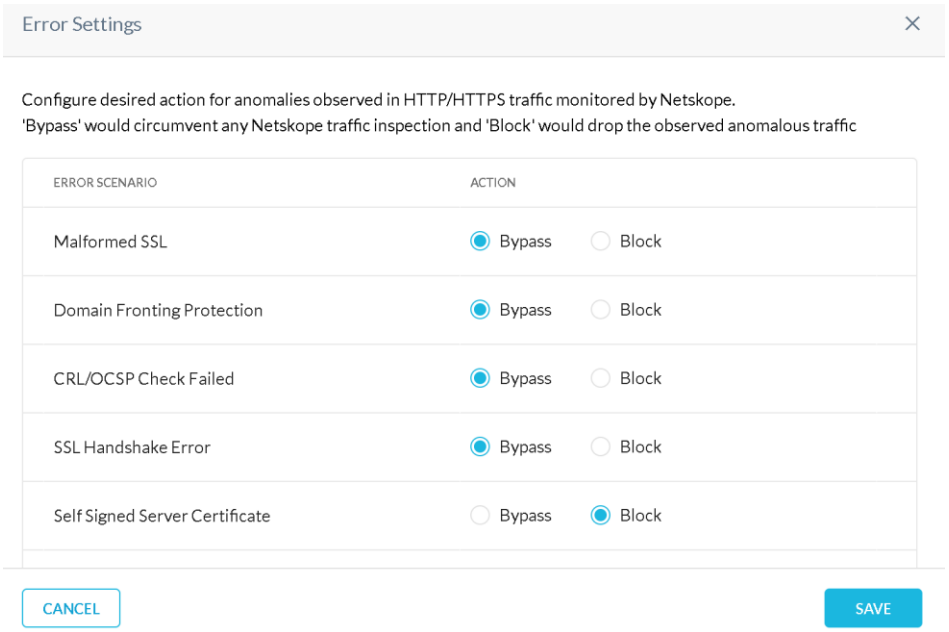


Nota. Configuración que permite añadir puertos personalizados para la detección y gestión del tráfico. Tomado de Netskope tenant.

Para los steering configuration se habilitaron las opciones de anomalías observadas en el tráfico HTTP/HTTPS monitoreado por Netskope. Estas características de error bloquean el tráfico indeseado a nivel de inspección SSL como Malformed SSL, Incomplete Certificate Trust Chain y Untrusted Root Certificate entre otras, Figura 29, por recomendación del fabricante todas estas características de deben encontrar en bloqueo.

Figura 29

Configuración de errores SSL



Nota. Panel para definir la acción (Bypass o Block) ante diferentes anomalías en tráfico SSL/TLS. Tomado de Netskope tenant.

¿Por Qué Ocurre el Error SSL con Netskope?

El error SSL asociado con Netskope se origina en la forma en que esta plataforma de seguridad inspecciona el tráfico cifrado para proteger la información corporativa. Netskope actúa como un proxy “Man-in-the-Middle”, lo que significa que se interpone entre el usuario y los servicios a los que se accede por Internet. Cuando un usuario intenta establecer una conexión segura mediante HTTPS, Netskope intercepta la comunicación y genera un nuevo certificado digital para poder descifrar y analizar el contenido del tráfico. Este proceso es necesario para detectar posibles amenazas, filtraciones de datos o actividades no autorizadas. Sin embargo, si el certificado raíz emitido por Netskope no está previamente instalado o marcado como confiable en el sistema operativo o navegador del usuario, el navegador interpreta que la conexión ha sido

comprometida. Como consecuencia, se genera un error SSL con mensajes como “certificado autofirmado” o “nombre de host no coincide”. Dichos errores no indican necesariamente un fallo de seguridad real, sino la falta de confianza entre el cliente y el proxy. Instalar el certificado raíz de Netskope y asegurarse de que las aplicaciones reconozcan su validez elimina el conflicto y permite mantener la inspección SSL sin alertas ni bloqueos.

La correcta configuración del certificado de Netskope es esencial para garantizar un monitoreo eficaz y libre de errores en el tráfico web corporativo. Una vez que el certificado raíz se importa en los almacenes de confianza del sistema, los navegadores y aplicaciones aceptan las conexiones interceptadas como seguras, manteniendo la confidencialidad y la integridad de los datos. Esto permite a Netskope analizar el contenido cifrado sin interferir con la experiencia del usuario ni generar advertencias visuales. Además, una configuración adecuada posibilita aplicar políticas de seguridad avanzadas, como la detección de malware, la prevención de fuga de información y el control de acceso a aplicaciones en la nube. Si este paso se omite, muchos servicios críticos podrían fallar o mostrar errores de autenticidad, afectando la productividad y la conectividad. Por ello, en entornos corporativos se recomienda desplegar el certificado mediante políticas de grupo.

Políticas de Protección en Tiempo Real

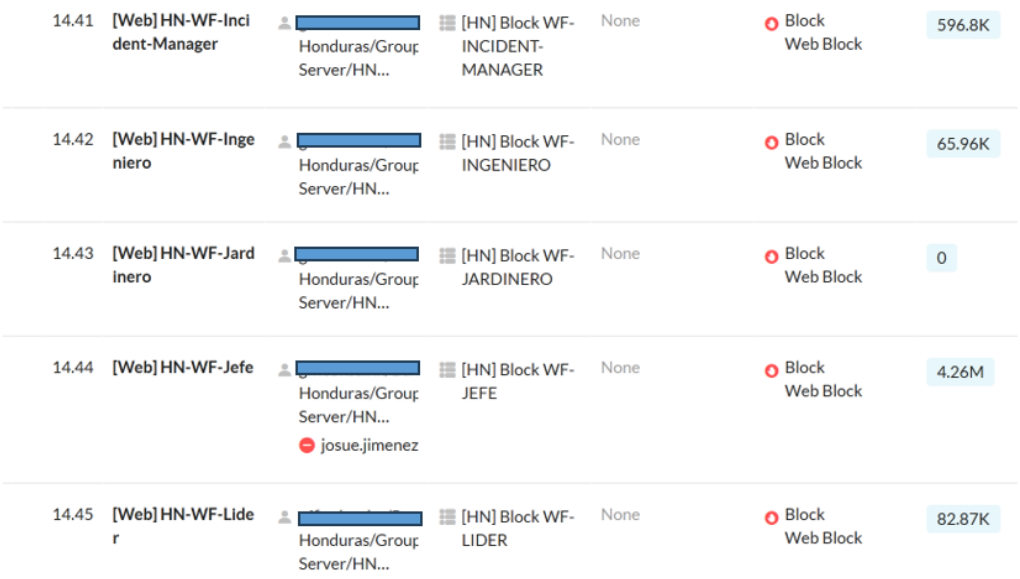
En la compañía bancaria, se ha realizado una configuración exhaustiva de 361 políticas de protección en tiempo real dentro de la plataforma de seguridad en la nube de Netskope, algunas de estas aún se encuentran en estado de prueba. Cada una de estas políticas tiene un objetivo y alcance específicos, abordando diferentes aspectos de seguridad y protección de datos. Estas políticas se implementan para salvaguardar los activos digitales de la compañía y garantizar un entorno seguro para los usuarios. Cada una de las políticas configuradas ofrece un

servicio único y se enfoca en diferentes áreas de protección, por ejemplo, algunas de estas políticas están diseñadas para medir parámetros de protección utilizando perfiles de DLP (Data Loss Prevention) con el objetivo de prevenir la fuga de información sensible. Otras restringen el acceso a aplicaciones no permitidas por la empresa, asegurando que solo las aplicaciones autorizadas y seguras sean utilizadas por los colaboradores. Además, existen políticas que se centran en proteger el tráfico de correo electrónico, detectando y bloqueando amenazas y contenido malicioso. Asimismo, se han configurado políticas para proteger los usuarios contra amenazas latentes presentes en la red, brindando una capa adicional de seguridad. Es importante tener en cuenta que las políticas se ejecutan en orden de configuración, esto significa que la primera política que se aplica es la que aparece en primer lugar en el dashboard de la plataforma, y así sucesivamente hasta que el usuario cumpla con alguna de ellas. Por ende, es fundamental mantener como primera política la de Malware Scan para controlar los archivos de subida y bajada, analizando su contenido en buscas de agentes maliciosos. Si un usuario no se ajusta a ninguna de las políticas establecidas, se le asignará la última política configurada, que suele ser una política de negación de servicios. Esta práctica ayuda a garantizar que todos los usuarios estén sujetos al menos a una política de seguridad. A continuación en la Figura 30, se presenta un listado de todas las políticas creadas hasta el momento, cada una con su objetivo y alcance específicos:

Figura 30

Listado de políticas Web Real time Protection

14.17	[Web] HN-WF-Cajero	[redacted] Honduras/Group Server/HN...	[HN] Block WF-CAJERO	None	Block Web Block	127.1M
14.18	[Web] HN-WF-Cajero-Apoyo	[redacted] Honduras/Group Server/HN...	[HN] Block WF-CAJERO-APOYO	None	Block Web Block	56.09K
14.19	[Web] HN-WF-Chapter	[redacted] Honduras/Group Server/HN...	[HN] Block WF-CHAPTER	None	Block Web Block	212.4K
14.20	[Web] HN-WF-Chef-Ejecutivo	[redacted] Honduras/Group Server/HN...	[HN] Block WF-CHEF-EJECUTIVO	None	Block Web Block	212
14.21	[Web] HN-WF-Chief	[redacted] Honduras/Group Server/HN...	[HN] Block WF-CHIEF	None	Block Web Block	62.36K
14.22	[Web] HN-WF-Cientifico-Datos	[redacted] Honduras/Group Server/HN...	[HN] Block WF-CIENTIFICO-DATOS	None	Block Web Block	0
14.23	[Web] HN-WF-Coe-Lead	[redacted] Honduras/Group Server/HN...	[HN] Block WF-COE-LEAD	None	Block Web Block	24.88K
14.24	[Web] HN-WF-Community-Manager	[redacted] Honduras/Group Server/HN...	[HN] Block WF-COMMUNITY-MANAGER	None	Block Web Block	0
14.25	[Web] HN-WF-Contador	[redacted] Honduras/Group Server/HN...	[HN] Block WF-CONTADOR	None	Block Web Block	7,509
14.26	[Web] HN-WF-Contralor	[redacted] Honduras/Group Server/HN...	[HN] Block WF-CONTRALOR	None	Block Web Block	85.44K
14.27	[Web] HN-WF-Coordinador	[redacted] Honduras/Group Server/HN...	[HN] Block WF-COORDINADOI	None	Block Web Block	171.7K
14.35	[Web] HN-WF-Experto-Datos	[redacted] Honduras/Group Server/HN...	[HN] Block WF-EXPERTO-DATOS	None	Block Web Block	0
14.36	[Web] HN-WF-Facilitador	[redacted] Honduras/Group Server/HN...	[HN] Block WF-FACILITADOR	None	Block Web Block	31.49K
14.37	[Web] HN-WF-Gerente	jesus.britho@fic[redacted] Honduras/Gro... josearturo.alv	[HN] Block WF-GERENTE	None	Block Web Block	968.3K



Nota. imagen que muestra políticas de protección web en tiempo real, su descripción y estado (habilitado/no habilitado). Tomado de Netskope tenant.

Mejoras Clave

Estructuración Técnica:

Segmentación clara de tipos de políticas con viñetas para mejor legibilidad.

Terminología precisa ("exfiltración de información", "amenazas zero-day", "inspección profunda").

Ampliación de Contenido:

Explicación ampliada del rol de DLP ("monitorear y bloquear").

Detalle sobre amenazas de red ("zero-day, phishing").

Contextualización de la política final como "Denegar Todo".

Claridad en Procesos:

Uso de términos como "flujo jerárquico" y "herencia de política".

Explicitación del propósito del Malware Scan ("desarmar amenazas antes de evaluaciones posteriores").

Redacción Profesional:

Sustitución de expresiones genéricas ("brindando" → "proporcionando una capa" → "mitigación de riesgos").

Conectores técnicos ("Este flujo jerárquico hace crítica...").

Eliminación de redundancias ("cada una de estas políticas" → simplificado).

Precisión Conceptual:

"Política de negación de servicios" → "regla de 'Denegar Todo'" (terminología estándar).

"Analizando su contenido en buscas de información sencible" → "inspeccionar exhaustivamente... desarmando amenazas".

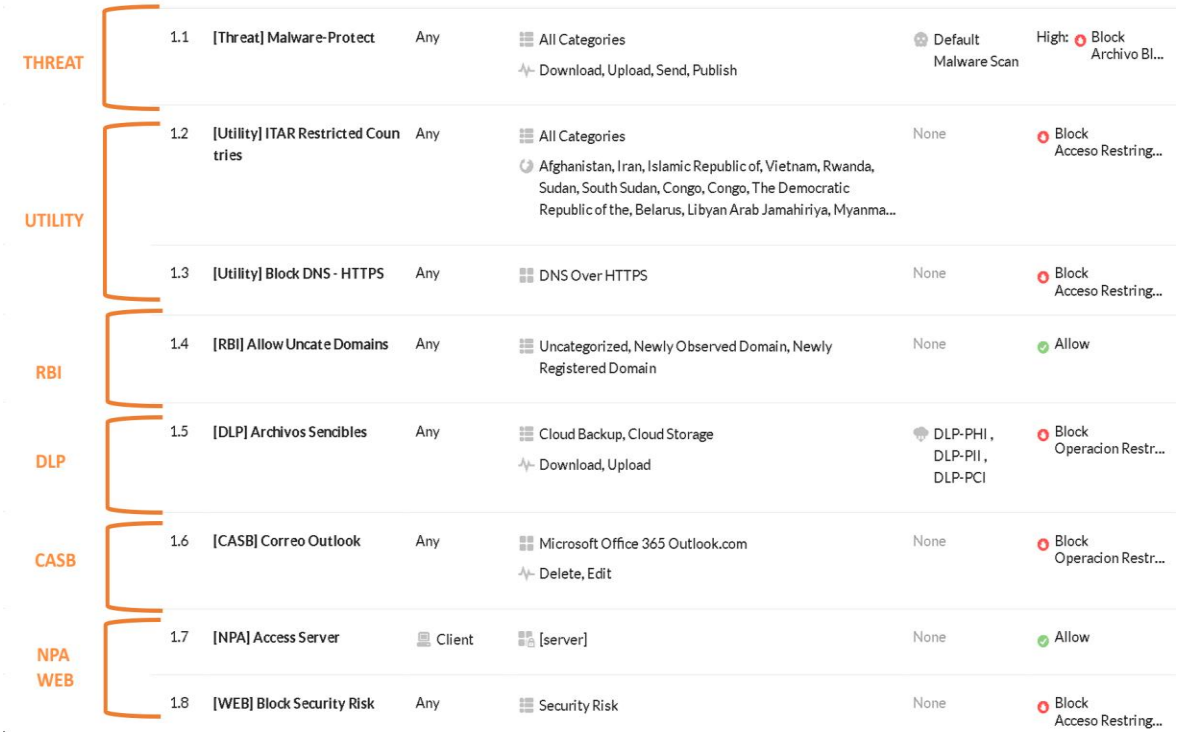
La política de Malware Scan debe ocupar la primera posición para inspeccionar exhaustivamente todos los archivos en tránsito (upload/download), desarmando amenazas antes de evaluaciones posteriores. Si un usuario no activa políticas previas, hereda automáticamente la última política configurada (generalmente una regla de "Denegar Todo"), garantizando cobertura de seguridad universal.

Como se puede apreciar, son bastantes políticas, cada una desempeñando un role específico y suministrando un nivel de seguridad adicional a la navegación web y cloud app. Debido a la estructura organizacional de la compañía se crearon grupos con varias políticas para permitir a los diferentes usuarios de cada dependencia una navegación controlada y eficiente. Netskope ofrece una amplia variedad de políticas de seguridad que se pueden configurar para proteger los datos y las aplicaciones en la nube. A cada política se le pueden adicionar características y parámetros de configuración como: tiempo de uso, acceso por medio de evaluación CCI, app instancias, constraints, reglas de DLP y categorías personalizadas por medio

de listas negras o blancas, todo esto con banners de advertencia para el usuario final. Se mostrarán detalladamente las características configuradas y aplicadas a las políticas anteriormente mencionadas, demostrando cómo cada una contribuye a la protección integral de los activos digitales de la organización y al cumplimiento de las políticas de seguridad establecidas. Se organizaron siguiendo las mejores prácticas tal y como se puede observar en la Figura 31.

Figura 31

Mejores prácticas organización de políticas



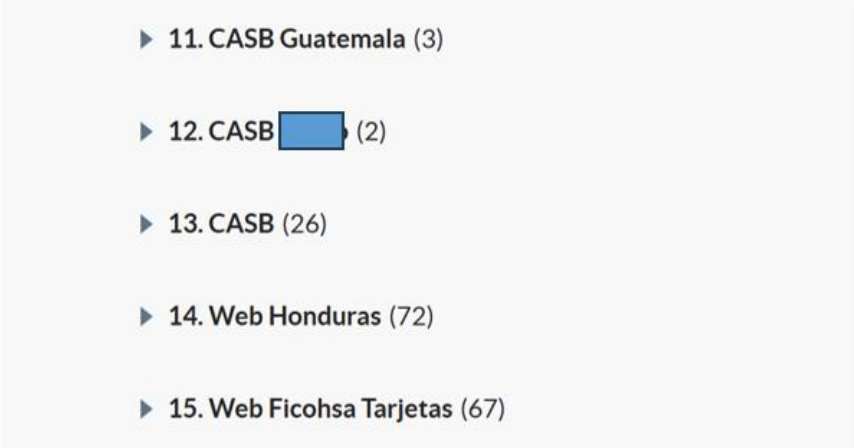
Nota. Ejemplo de estructura jerárquica de políticas agrupadas por categoría funcional (Threat, Utility, RBI, DLP, CASB, NPA). Tomado de Netskope tenant.

Con la funcionalidad de dividir las políticas por grupos se logra obtener un tenant más organizado con un flujo de reglas fácil de interpretar y por ende administrar. Por ejemplo, en la Figura 32 se pueden observar los distintos grupos de reglas que reflejan la división organizativa

del tenant. Cada grupo puede estar asociado a un departamento, equipo o unidad organizativa específica dentro de la empresa, lo que permite una alineación más precisa de las políticas de seguridad con las necesidades y responsabilidades de cada área. La interfaz de usuario de Netskope proporciona acceso completo para implementar y gestionar los derechos de administrador de la solución Netskope. La administración basada en roles de Netskope le permite controlar las funciones de los distintos administradores en la solución. Puede delegar responsabilidades entre los administradores y controlar detalladamente su nivel de acceso a la solución para garantizar que no creen políticas ni configuraciones conflictivas.

Figura 32

Grupos de políticas



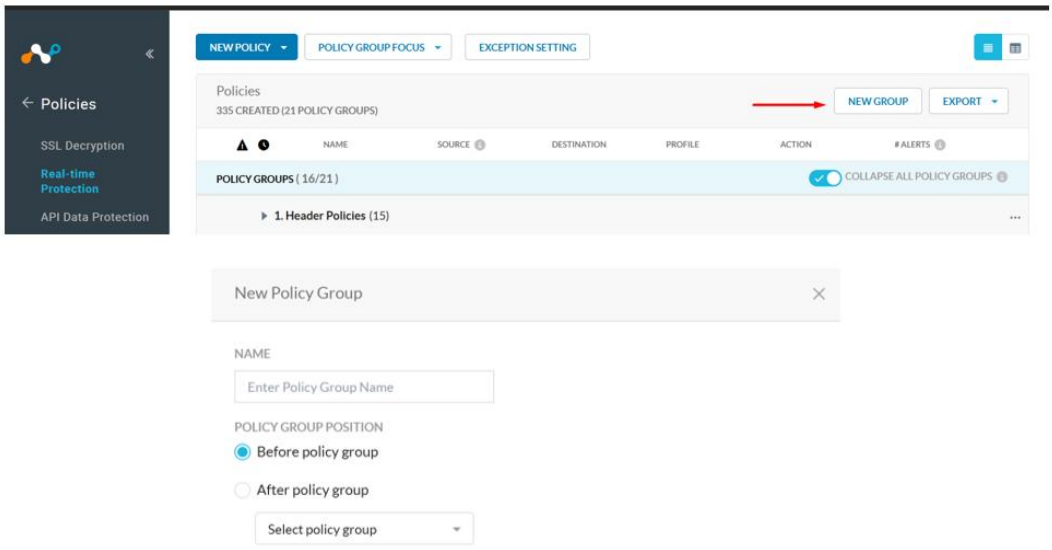
Nota. Listado de grupos de políticas organizados por función (CASB, Web) y región. Tomado de Netskope tenant.

Un grupo es una colección lógica de políticas de protección en tiempo real. Agrupar políticas resulta útil para simplificar el flujo de trabajo, permitiendo acceso preciso a un conjunto de políticas y eliminando cuellos de botella. Por ejemplo, si su empresa tiene cientos de políticas, puede usar grupos para dividirlas por región, unidad de negocio o cualquier función que sea relevante para un grupo de usuarios. Además, crear grupos de políticas facilita a los

administradores la gestión de sus propias políticas. Para crear un grupo de políticas nuevo y mantener el orden administrativo se puede dirigira la siguiente ruta, ***Policies > Real-Time Protection > New Group.*** Ver la Figura 33.

Figura 33

Creación de grupos de políticas



Nota. Interfaz para la creación y gestión lógica de colecciones de políticas. Tomado de Netskope tenant.

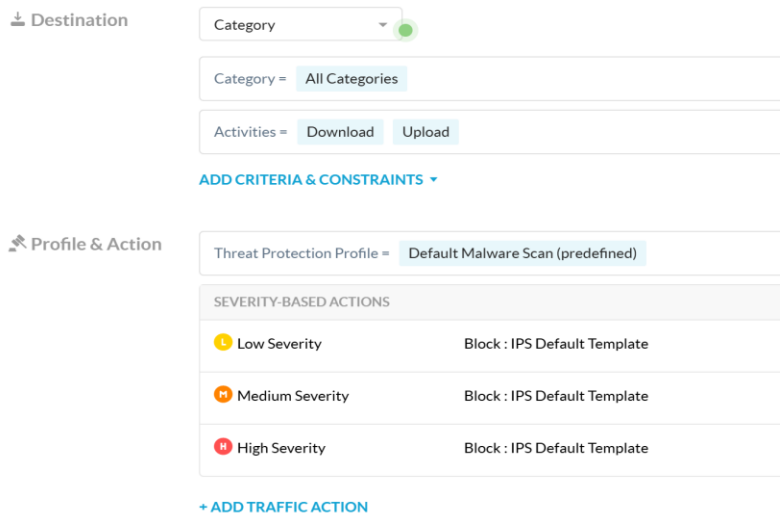
Política 1.1 de Escaneo en Busca de Malware

Utilizando el perfil por defecto de la herramienta se configuro una política deescaneo de malware sobre todas las categorías predefinidas de Netskope para las actividades de Carga y Descarga de archivos. La política de escaneo proactivo contra malware está diseñada para identificar y bloquear cualquier amenaza maliciosa que pueda infiltrarse en la red a través de la transferencia de archivos, ya sea mediante descargas desde fuentes externas o cargas desde dispositivos internos. Esto incluye, entre otros, virus, troyanos, gusanos, ransomware y otras

formas de malware que puedan comprometer la seguridad y el funcionamiento de los sistemas. Ver Figura 34.

Figura 34

Política de Malware Scan



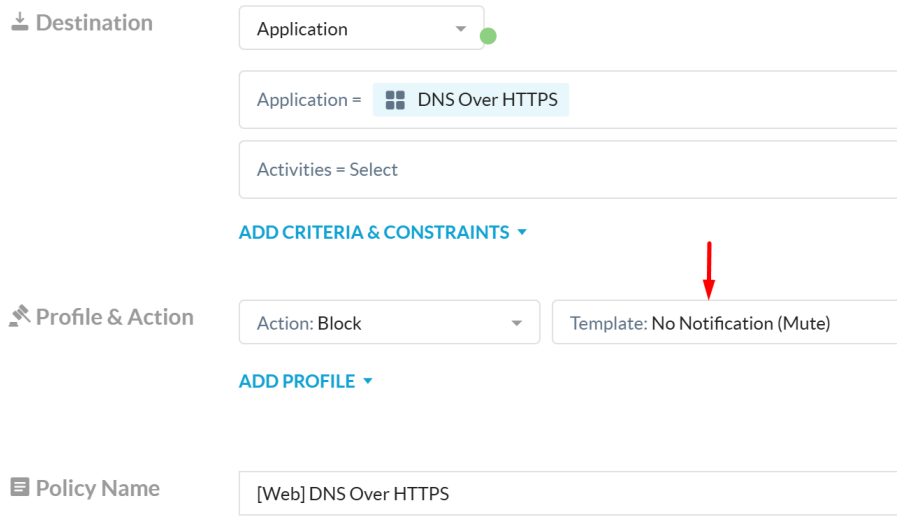
Nota. Configuración de la política para escanear y proteger contra malware. Tomado de Netskope tenant.

Política Utility 1.6 DNS Over HTTPS

DNS sobre HTTPS no es un protocolo compatible para Netskope. Aunque ofrece beneficios de privacidad al cifrar las consultas DNS, también puede ser explotado por malware o actores malintencionados para evadir controles de seguridad y acceder a recursos maliciosos. Dado que DoH no es un protocolo compatible con la solución de seguridad de Netskope, su uso no supervisado puede comprometer la visibilidad y el control de la organización sobre el tráfico de red. Ver Figura 35.

Figura 35

Política Utility DNS



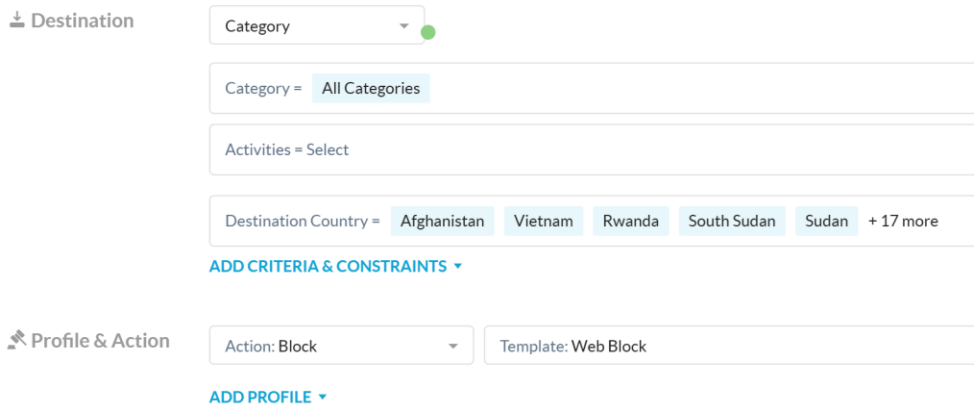
Nota. Regla diseñada para bloquear consultas DNS sobre HTTPS (DoH). Tomado de Netskope tenant.

Política Utility 1.5 ITAR

Con ayuda del mapeo Geo-IP de Netskope para identificar la ubicación geográfica de los servidores de destino. Esta política se centra en bloquear búsquedas, accesos y otras interacciones con páginas web provenientes de países que presentan niveles bajos o nulos de seguridad web, y que son conocidos como principales fuentes de ataques y envío de amenazas en línea. De esta manera, mitigamos el riesgo de exposición a actividades maliciosas y protegemos la integridad de nuestros sistemas y datos sensibles frente a potenciales amenazas externas. Ver Figura 36.

Figura 36

Política Utility ITAR



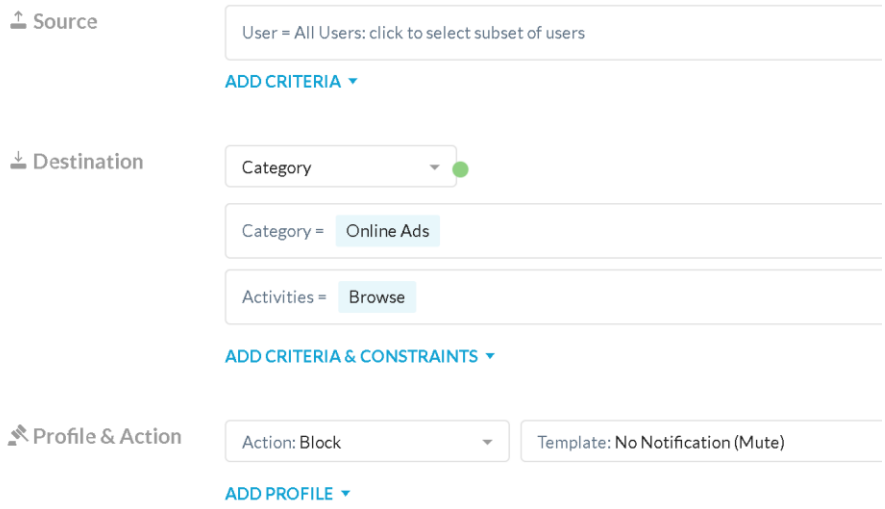
Nota. Política que aplica restricciones basadas en ubicación geográfica (mapeo Geo-IP). Tomado de Netskope tenant.

Política Utility Ejemplo Bloqueo de Publicidad

Esta política se basa en una categoría personalizada que abarca los anuncios en línea y otros contenidos publicitarios considerados como potenciales riesgos para la seguridad y la integridad de nuestros sistemas. Se ha configurado esta categoría en modo de bloqueo para evitar la visualización y la interacción con este tipo de contenido no deseado, que puede representar una amenaza para la seguridad de nuestra red y nuestros datos sensibles. De esta manera, reforzamos nuestra postura de seguridad digital y protegemos proactivamente nuestros activos contra posibles ataques y vulnerabilidades asociadas con la publicidad en línea. Ver Figura 37.

Figura 37

Política Utility Online Ads



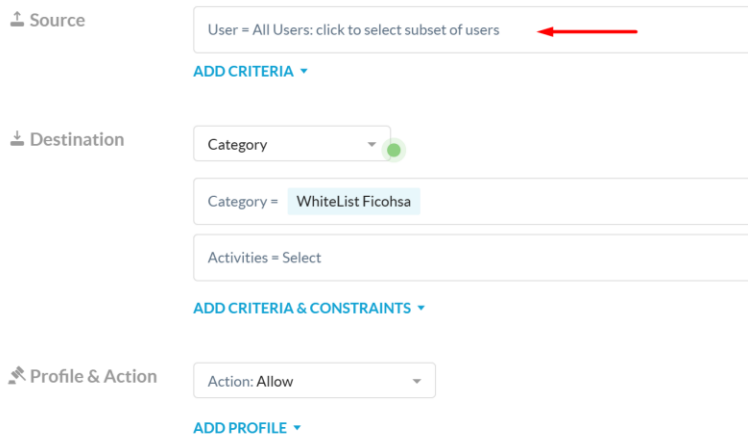
Nota. Regla creada para bloquear anuncios en línea mediante una categoría personalizada. Tomado de Netskope tenant.

Política 1.6 WhiteList

Utilizando una categoría blanca personalizada en nuestra solución de seguridad Netskope. Esta categoría incluye sitios web y servicios en línea que han sido cuidadosamente evaluados y aprobados como seguros y confiables para el acceso por parte de nuestros usuarios. Se ha configurado esta categoría para permitir exclusivamente el acceso a los recursos incluidos en ella, garantizando así que los empleados puedan acceder de manera segura y eficiente a las herramientas y servicios necesarios para realizar sus tareas y laborales. Esta política se encuentra en el grupo de web filtering para no intervenir con el DLP que el banco desea priorizar. Ver Figura 38.

Figura 38

Política de Lista Blanca



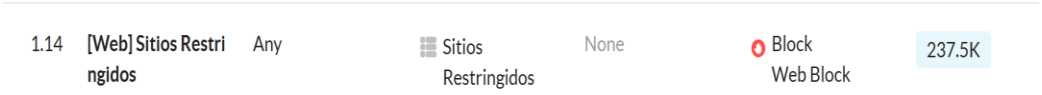
Nota. Configuración que permite tráfico desde dominios o categorías previamente autorizadas. Tomado de Netskope tenant.

Política 1.3 Seguridad Dominios

Se implemento una política de seguridad robusta mediante la configuración de una categoría personalizada que engloba las principales amenazas, tales como páginas de riesgo, malware, contenido violento y obsceno. Esta categoría se ha establecido en modo de bloqueo para prevenir la interacción con este tipo de tráfico considerado de alto riesgo. De esta manera, se fortalecen las defensas de la compañia contra posibles ataques y es posible proteger la integridad de la red y datos sensibles frente a amenazas potenciales. En la parte superior del dashboard se tiene una política que será detallada mas adelante. En la imagen que se muestra enseguida se visualiza la política de protección contra sitios no deseados para el web filtering con una categoría personalizada que engloba todos los sitios que no se deben acceder en la navegación cotidiana de los colaboradores. Ver Figura 36.

Figura 39

Política con categorías prohibidas por la organización

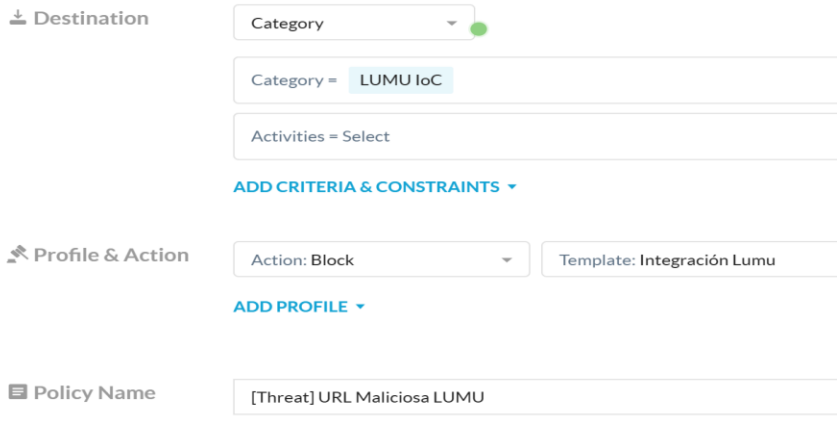


Nota. Regla que bloquea el acceso a sitios restringidos mediante una lista personalizada de categorías y URL. Tomado de Netskope tenant.

Esta otra política forma parte del concepto de seguridad por categorías y dominios, en esta lista personalizada se incluyeron todas aquellas URL que se deben bloquear de manera inmediata para cualquier usuario de la compañía. Observe que se limita a las actividades de búsqueda, descarga, carga e inicio de sesión. A continuación, se muestra la Figura 40, con la política de IoC configurada gracias a la previa integración de LUMU y Netskope.

Figura 40

Política de Dominios maliciosos



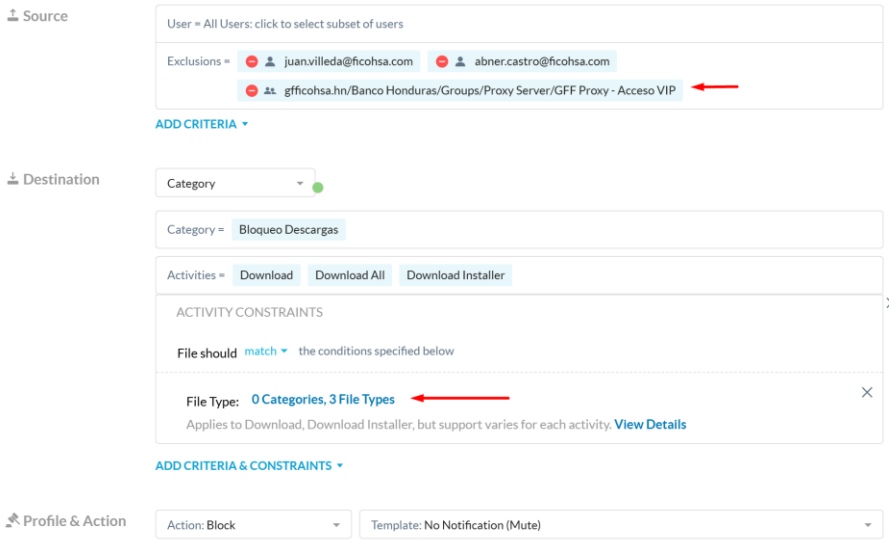
Nota. Configuración de bloqueo basada en indicadores de compromiso (IoC) obtenidos de la integración con LUMU. Tomado de Netskope tenant.

Política Utility Bloqueo Descargas

En la parte de Utility se pueden agregar políticas que aplican de manera general, a un grupo de usuarios o reglas que excluyen a ciertos usuarios, pero en escencia estas políticas sirven para gestionar casos de uso generales que aumentan la seguridad de la organización por medio de parámetros específicos que bloquean, publicidad, permiten el uso de aplicaciones o herramientas de análisis de red o como en el siguiente ejemplo bloquean las descargar de archivos ejecutables. Ver Figura 41.

Figura 41

Política bloqueo descargas



Nota. Regla configurada para impedir descargas desde categorías o dominios considerados de riesgo. Tomado de Netskope tenant.

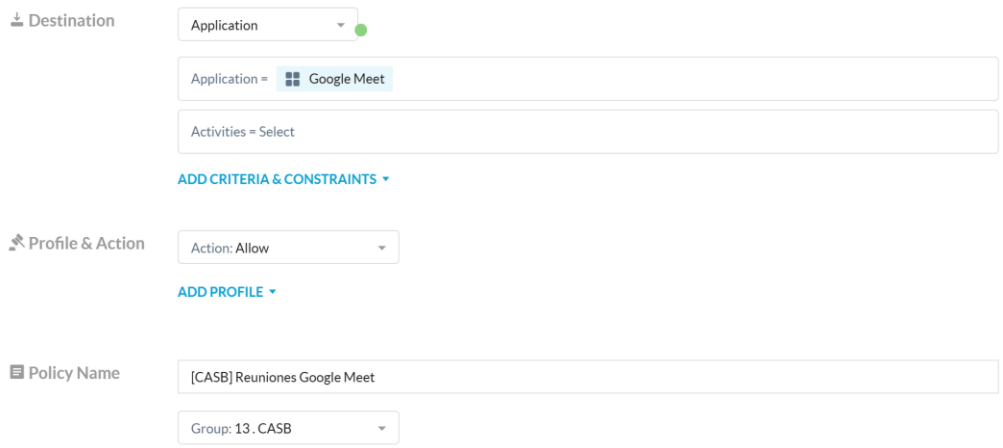
Políticas 3.3 CASB

Se caracterizan por su eficiencia en la detección de conductas de Shadow IT, también son útiles para gestionar otros aspectos de la seguridad en la organización. Puede regular el uso de la nube en su organización con visibilidad y control pormenorizados. En lugar de adoptar un enfoque general mediante el bloqueo de servicios, los CASB le permiten controlar el uso en

función de la identidad, el servicio, la actividad, la aplicación y los datos, véase la Figura 42. El proceso para crear una política de este tipo es bastante simple, solo se debe seguir la ruta, ***Policies > Real-Time Protection > New Policy > Cloud App Access***.

Figura 42

Política de CASB Google Meet



Nota. Regla de control de acceso a aplicaciones en la nube, permitiendo específicamente Google Meet para todos los usuarios. Tomado de Netskope tenant.

En la Figura 42, se puede apreciar una política de CASB que permite el acceso a Google Meet de manera general sin importar la instancia, esta regla se encuentra definida de esta manera para garantizar el correcto funcionamiento de las reuniones internas y externas del banco. No se puede cambiar la política por instancias porque bloquearía el acceso de reuniones gestionadas o administradas por terceros. Es importante mantenerla intacta sin modificaciones o puede generar un impacto significativo en las labores diarias de los colaboradores del banco. En otras palabras, esta configuración asegura que el tráfico hacia la aplicación Google Meet no sea bloqueado ni restringido por Netskope, mientras que otras aplicaciones podrían estar sujetas a políticas más restrictivas o monitoreo más exhaustivo. Es común en despliegues CASB que se definan reglas

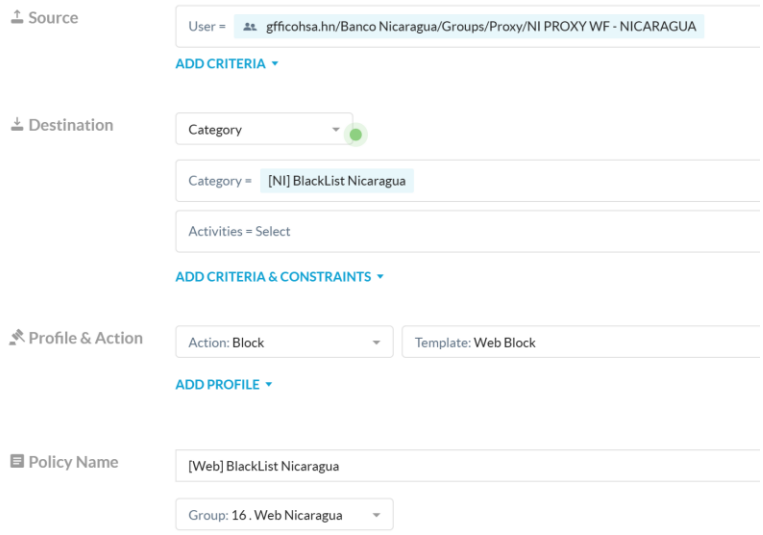
específicas para aplicaciones esenciales colaborativas, permitiéndolas mientras se mantiene la seguridad general.

Políticas 16.2 Web

Están diseñadas para controlar y proteger el acceso web corporativo, proporcionando visibilidad y seguridad detalladas en todo el tráfico HTTP/HTTPS. En lugar de aplicar bloqueos generales, permiten aplicar restricciones según la identidad del usuario, grupos, ubicación, categoría de contenido, servicio, actividad e incluso perfil del dispositivo. Su configuración sigue el flujo de tráfico web definido en la regla. El proceso para crear una política de este tipo es bastante simple, solo se debe seguir la ruta, ***Policies > Real-Time Protection > New Policy >Web Access***.

Figura 43

Política de tráfico Web para Nicaragua



Nota. Regla que bloquea categorías de sitios específicas (Lista Negra Nicaragua) para un grupo de usuarios definido. Tomado de Netskope tenant.

La regla que se muestra en la Figura 43, pertenece al grupo de Web Nicaragua, recuerde que cada país contiene su lista de políticas, esto permite organizar el tenant y mejorar la

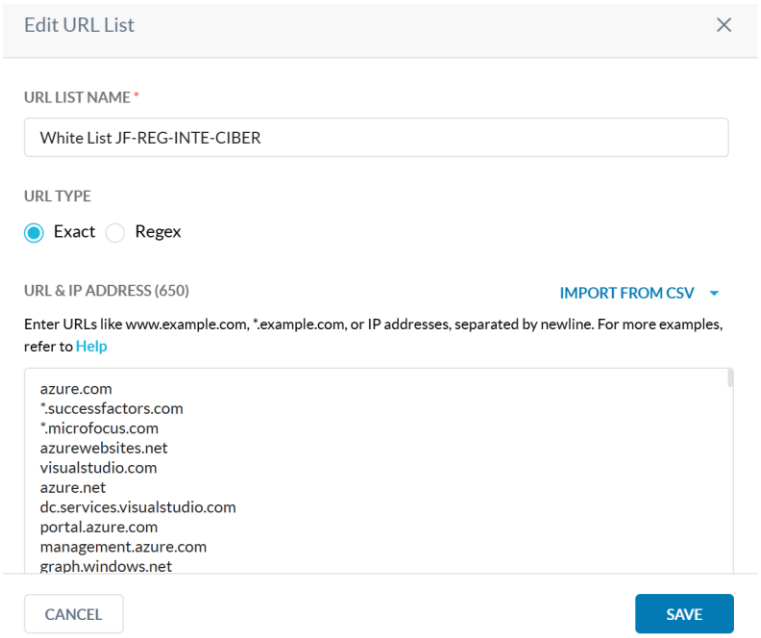
administración de accesos. Específicamente se muestra una regla que bloquea sitios específicos que están definidos dentro de una URL List personalizada que a su vez es llamada por medio de una Custom Category, concepto que se profundizara más adelante. Esto permite bloquear sitios por región sin intervenir de manera genérica para todo el banco en las reglas de cabecera, observe que se relaciona el grupo de NI Proxy WF – Nicaragua únicamente, no todas las regionales cuentan con una lista de bloqueo, la mayoría está manejando los accesos por medio de perfiles predefinidos, que fueron socializados durante varias sesiones y que están construidos por las categorías predefinidas que Netskope reconoce.

URL List

Las listas de URL son un componente de las categorías personalizadas, que ofrecen la flexibilidad de anular la asignación de categorías de URL predefinida de Netskope para una URL determinada. Para crear una lista de URL, seleccione el formato e introduzca las URL deseadas. Antes de comenzar, compile una lista de URL para incluir en un análisis de políticas y, si es necesario, cree otra lista de URL para excluir. Puede introducir las URL individualmente en la interfaz de usuario, crear un archivo CSV con todas las URL o usar la API REST V2. El proceso para crear una categoría es bastante simple, solo se debe seguir la ruta, ***Policies > Profiles > URL List***

Figura 44

URL List configurada



Nota. Interfaz para editar una lista de URL permitidas (lista blanca), mostrando ejemplos de dominios incluidos. Tomado de Netskope tenant.

Como muestra la Figura 44, al agregar URL, puede introducirlas para que coincidan exactamente o usar comodines. También puede definir números de puerto para las URL. Al agregar URL, asegúrese de seguir las reglas de formato. Los dominios comodines (*.dominio.com) incluyen el dominio raíz y todos los subdominios. Tenga en cuenta que si su lista de URL contiene dos o más entradas comodín, subdominios y rutas, el servicio de Netskope utiliza la entrada más larga para la categorización, ejemplos:www.example.com/path/to/resource, example.com, www.example.com,*.example.com, www.example.com:8080, www.example.com:80, 10.10.10.1 y 10.10.10.10/24

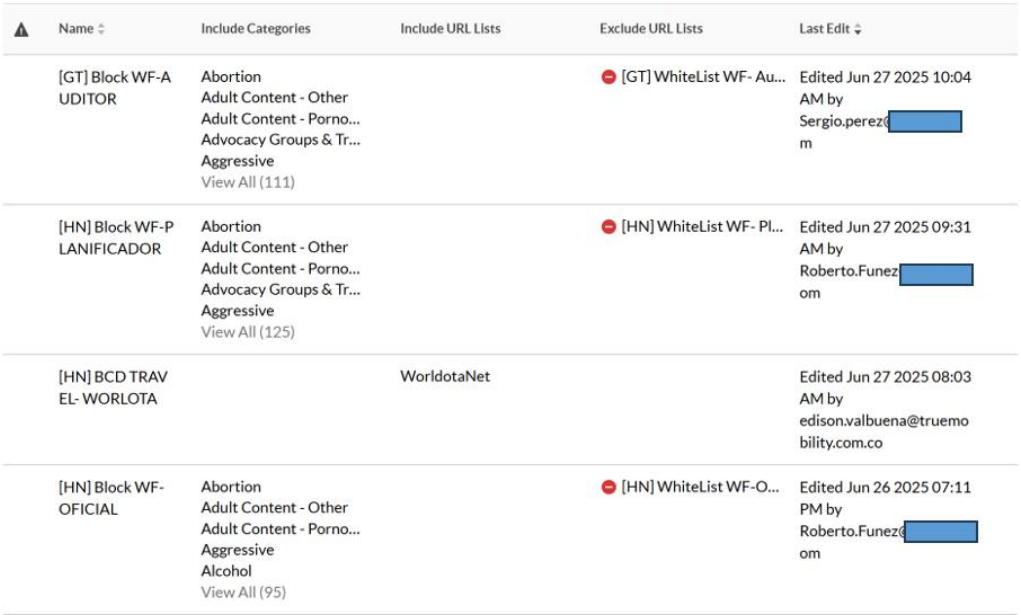
Fase III: Configuraciones Web y DLP

Web Custom Categories

Son categorías que se pueden construir de manera personalizada y basadas en las necesidades de la corporación, puede crear una categoría personalizada para una URL que no esté categorizada, es decir, Netskope no tiene una asignación de categoría para la URL o la categoría predefinida de Netskope no se ajusta a una configuración de política deseada. Además se les pueden incluir listas negras o blancas. Se tienen un total de 280 categorías creadas, por otro lado, el proceso para crear una categoría es bastante simple, solo se debe seguir la ruta, ***Policies > Profiles > Custom Categories.***

Figura 45

Categorías personalizadas



Name	Include Categories	Include URL Lists	Exclude URL Lists	Last Edit
[GT] Block WF-AUDITOR	Abortion Adult Content - Other Adult Content - Porno... Advocacy Groups & Tr... Aggressive View All (111)		[GT] WhiteList WF- Au...	Edited Jun 27 2025 10:04 AM by Sergio.perez[redacted]m
[HN] Block WF-PLANIFICADOR	Abortion Adult Content - Other Adult Content - Porno... Advocacy Groups & Tr... Aggressive View All (125)		[HN] WhiteList WF- Pl...	Edited Jun 27 2025 09:31 AM by Roberto.Funez[redacted]om
[HN] BCD TRAVEL- WORLOTA		WorldotaNet		Edited Jun 27 2025 08:03 AM by edison.valbuena@truemobility.com.co
[HN] Block WF-OFICIAL	Abortion Adult Content - Other Adult Content - Porno... Aggressive Alcohol View All (95)		[HN] WhiteList WF-O...	Edited Jun 26 2025 07:11 PM by Roberto.Funez[redacted]om

Nota. Vista de las categorías personalizadas creadas para la clasificación y filtrado de contenido. Tomado de Netskope tenant.

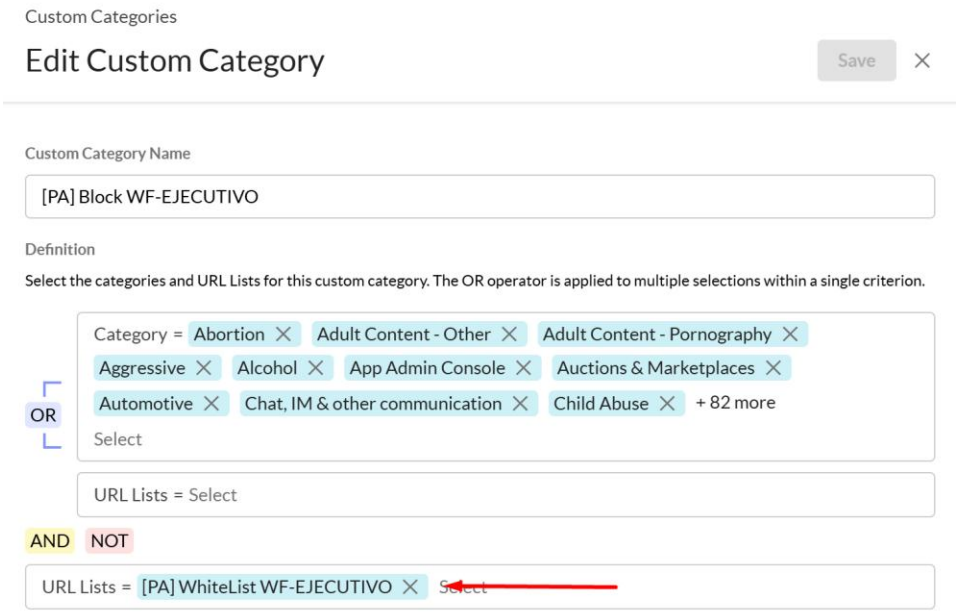
Como se muestra en la Figura 45 durante la implementación fueron configuradas varias categorías personalizadas, en la anterior figura se relacionaron algunas, teniendo en cuenta el número de colaboradores de la corporación y la cantidad de grupos organizacionales fue

necesario segmentar la navegación por listas de acceso personalizadas, estas configuraciones se utilizan en políticas de protección en tiempo real.

La implementación de categorías personalizadas en Netskope se realiza con el objetivo de optimizar el rendimiento y la efectividad de la plataforma de acuerdo con las mejores prácticas sugeridas por el fabricante. Estas categorías personalizadas incluyen listas de acceso tanto blancas como negras, las cuales especifican qué tipos de tráfico deben ser permitidos o bloqueados según los requisitos de seguridad y las políticas de la organización. Para garantizar una configuración precisa y completa, se han generado listas tanto para el tráfico web como para el tráfico no web, que incluye datos pertenecientes a protocolos como TCP, UDP y DNS. Esto asegura que Netskope opere de manera óptima en diversos contextos y escenarios de tráfico, proporcionando una protección integral que abarca tanto la navegación web como otras formas de comunicación y transferencia de datos. Cada categoría personalizada se crea cuidadosamente para incluir las categorías por defecto de la plataforma, lo que permite establecer un nuevo acceso que se ajuste perfectamente a los requerimientos específicos de la organización. Esto significa que se pueden configurar políticas de acceso adaptadas a las necesidades particulares de cada departamento, equipo o unidad organizativa, garantizando un equilibrio óptimo entre seguridad y productividad. La creación de estas categorías se muestra a continuación en la Figura 46.

Figura 46

Categoría personalizada para Panamá



Nota. Configuración de una categoría personalizada que combina múltiples categorías predefinidas y listas de URL para un grupo específico. Tomado de Netskope tenant.

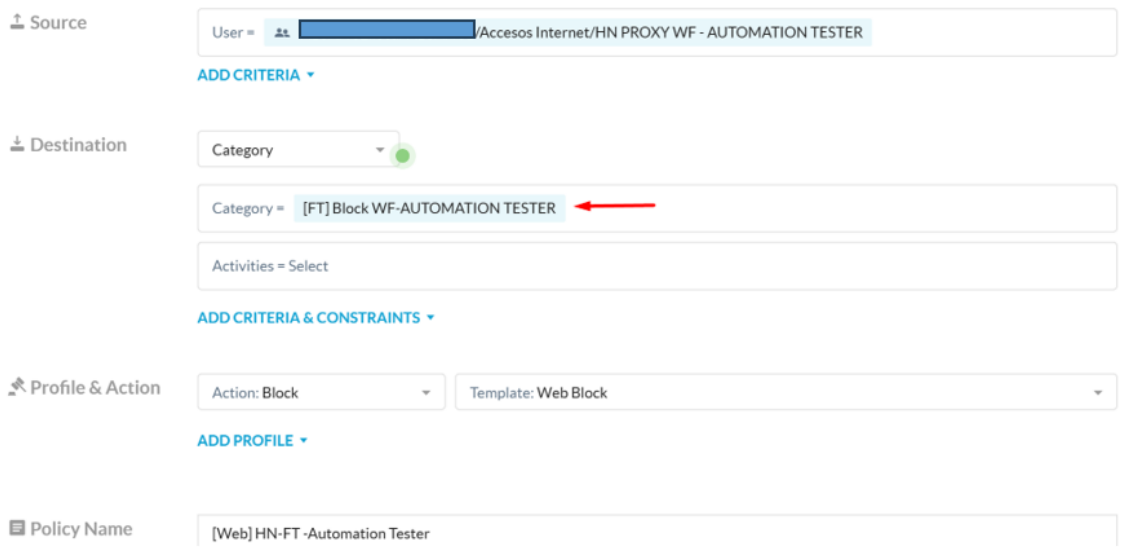
Al crear una categoría personalizada, puede seleccionar una combinación de categorías predefinidas y listas de URL (inclusiones y exclusiones). Netskope considera las categorías personalizadas como categorías independientes de las predefinidas, y debe añadirlas a una política existente o crear una nueva para implementarlas. A manera de ejemplo se mostrará la configuración de una política que utilice categorías personalizadas.

En la Figura 47, se puede observar que en lugar de seleccionar una categoría predeterminada se busca una creada por el administrador del tenant; en el espacio de Destination se agrega la nueva categoría. En el ejemplo se ve una regla que solo está aplicando a un grupo puntual de Honduras Tarjetas, cada categoría personalizada tiene su respectiva etiqueta de inicio

que identifica la regional a la cual pertence: [HN] Honduras, [PA] Panamá, [GT] Guatemala, [NI] Nicaragua y [FT] banco Tarjetas.

Figura 47

Política con categoría personalizada



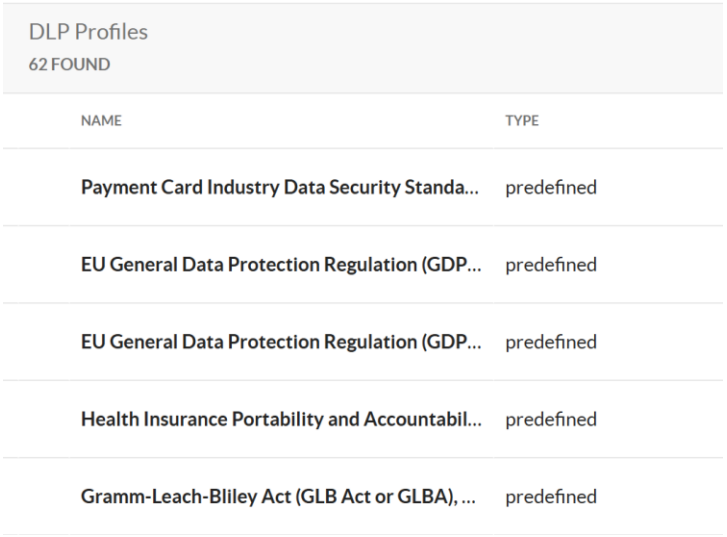
Nota. Regla de seguridad que aplica una categoría personalizada para controlar el acceso o las acciones permitidas. Tomado de Netskope tenant.

Políticas de DLP

Conjunto de prácticas y herramientas destinadas a prevenir la fuga de datos (también conocida como exfiltración de datos) mediante un uso indebido intencional o no. Estas prácticas y herramientas incluyen cifrado, detección, medidas preventivas, ventanas emergentes educativas (para movimientos involuntarios) e incluso aprendizaje automático para evaluar las puntuaciones de riesgo de los usuarios. El proceso para crear un perfil de DLP es bastante simple, solo se debe seguir la ruta, ***Policies > Profiles > DLP > New Profile***. Por defecto vienen configurados 38 perfiles, ver Figura 48.

Figura 48

Perfiles de DLP predefinidos

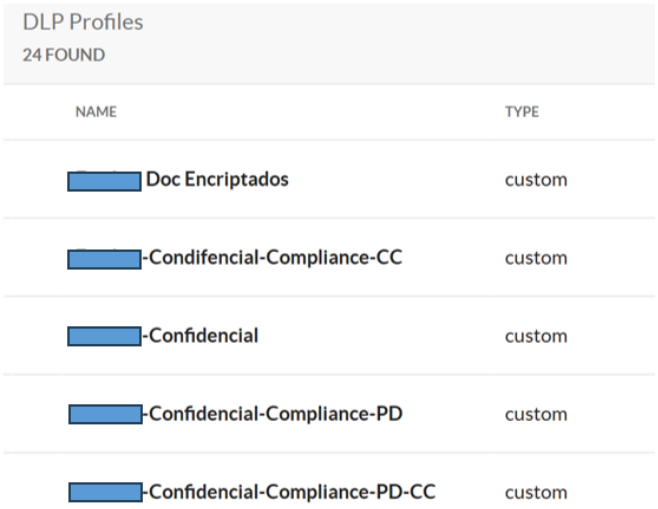


Nota. Lista de perfiles de prevención de pérdida de datos (DLP) estándar disponibles en la plataforma. Tomado de Netskope tenant.

Se puede apreciar por el incremento que se tienen 24 perfiles personalizados. Netskope permite configurar políticas DLP para prevenir la transferencia no autorizada de datos confidenciales y privados. Por ejemplo, se pueden definir políticas que eviten la transferencia de información financiera o de salud a destinos no autorizados. Hay varias políticas de este tipo configuradas, algunas hacia categorías personalizadas, otras con categorías definidas y unas adicionales hacia aplicaciones específicas. Los perfiles custom se muestran en la Figura 49.

Figura 49

Perfiles DLP Custom

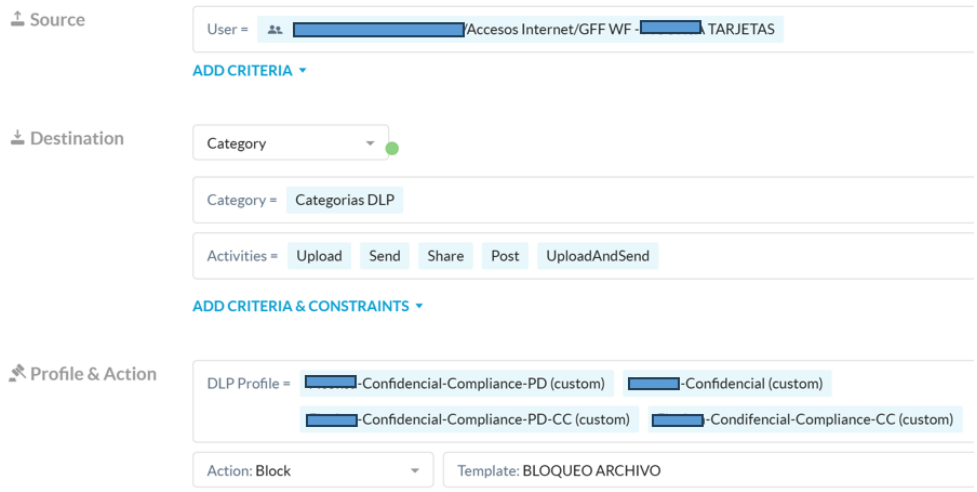


Nota. Perfiles personalizados de prevención de pérdida de datos creados para necesidades específicas de la organización. Tomado de Netskope tenant.

Cada política de DLP protege la información confidencial de los clientes que se trata de compartir de manera irresponsable, adicionalmente y a manera de ejemplo se muestra una política con varios perfiles de DLP personalizados.

Figura 50

Política de Etiquetas



Nota. Regla DLP configurada para actuar basándose en etiquetas de clasificación de datos. Tomado de Netskope tenant.

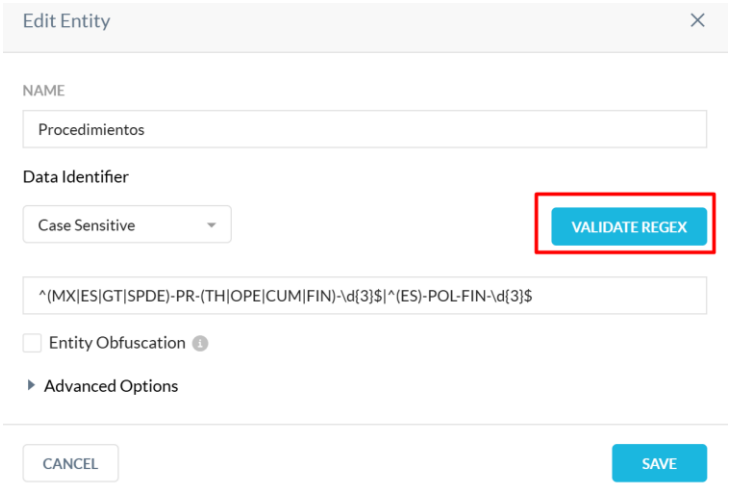
Como muestra la Figura 50 en la sección "Source", es posible seleccionar todos los usuarios, grupos o un usuario específico con el objetivo de proteger la información confidencial en toda la estructura organizativa del banco. Para optimizar la eficacia de la política, se han incluido todas las categorías de Netskope que soportan DLP sobre una custom category y sobre las cuales tiene sentido aplicar este tipo de filtro. Se han definido acciones específicas que deben generar un registro de bloqueo, tales como carga, publicación, envío, compartición y descarga. Esto permite establecer una política robusta que abarca múltiples escenarios y garantiza la confidencialidad de la información sensible, como archivos que contienen bases de datos, información bancaria y que se encuentran con una etiqueta de Confidencial.

Además, se pueden incluir etiquetas de clasificación CCI, las cuales permiten incluir o excluir aplicaciones según las necesidades de la empresa. Generalmente, una regla incorpora etiquetas como “Consumer”, “Departamental” y “Unsanctioned”, asegurando que todas las

aplicaciones empresariales sean excluidas y puedan manipular datos sensibles sin restricciones ni generación de falsos positivos en los registros de eventos. A continuación, se presenta el perfil DLP diseñado para la compra de vehículos, previamente configurado para su uso en la política. Es importante recordar que el flujo de configuración consiste en definir una entidad (regex), asignarla a una regla DLP y, posteriormente, agregar dicha regla a un perfil, el cual se integra finalmente en las políticas de DLP. En la imagen, se muestra un perfil con un "file profile", donde únicamente se requiere su creación y asignación al perfil DLP para su implementación.

Figura 51

Regex para los procedimientos



Nota. Expresión regular utilizada en la definición de una entidad para la detección de contenido sensible. Tomado de Netskope tenant.

La construcción de las reglas DLP inicia con la definición de las Entidades. Se muestra el Regex en la Figura 51 para una de las palabras que se utilizaron en generar la entidad, la construcción de estos caracteres de coincidencia depende de unos símbolos predefinidos por Netskope Inc, con base en esto se construye el Regex necesario que cubra la mayor cantidad de posibilidades, con el propósito de bloquear una palabra escrita de varias maneras y de esta

manera cerrar la detección. En la siguiente documentación encontrara las expresiones regulares que manera el tenant de Netskope y su respectivo propósito:

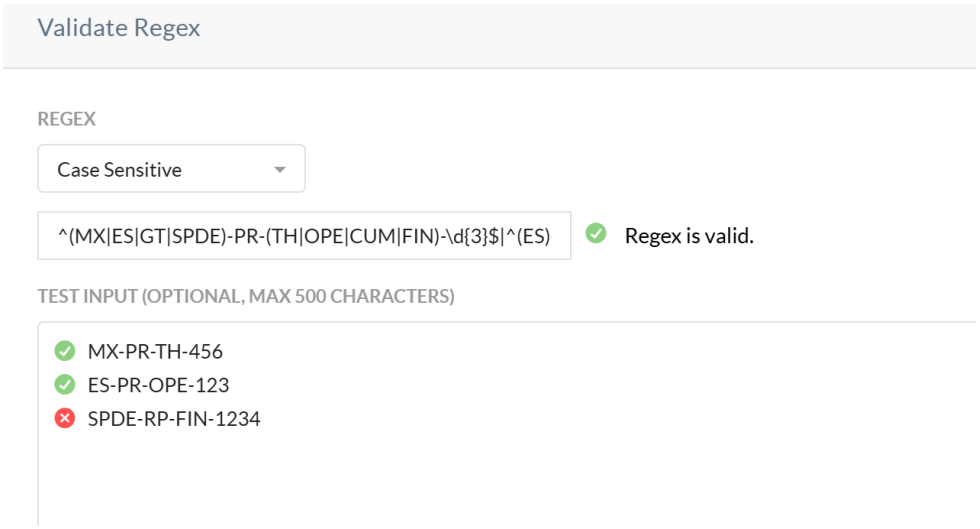
https://docs.netskope.com/en/building-regular-expressions/

Las palabras se construyen en Netskope a través de Regex, la ruta para crear una palabra como la que se muestra en la imagen es la siguiente, Policies > Profiles > DLP > Entities > New Entity. A continuación, se muestra un ejemplo de construcción y validación para la entidad de procedimientos que consta de unos valores iniciales separados por un guión medio y finalizando con tres dígitos.

El propósito de esta construcción es garantizar que, sin importar la forma en que se escriba o manipule la palabra (por ejemplo, con mayúsculas, minúsculas, caracteres intermedios o sustituciones), el sistema sea capaz de detectarla y bloquearla de forma efectiva. Esta estrategia permite cerrar posibles brechas en los mecanismos de detección, asegurando una mayor cobertura en los controles de seguridad. Después de crear la palabra deseada se puede realizar una validación de su funcionamiento con ayuda de la opción “Validate Regex”, se desplegará un cuadro y acto seguido se incluye la palabra que se quiere evaluar, si esta coincide con la entidad configurada se desplegará un icono verde con una paloma de aprobación.

Figura 52

Validación de palabras

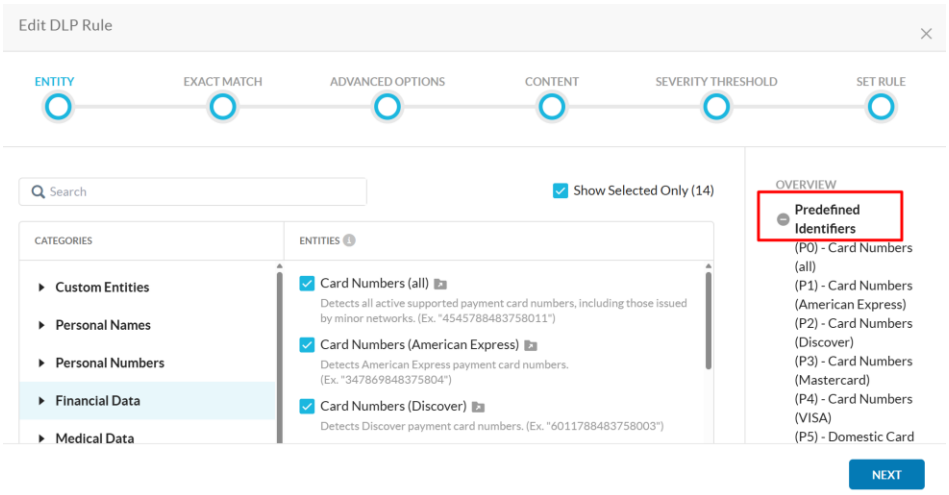


Nota. Herramienta de validación para expresiones regulares (Regex) utilizada en la configuración de entidades DLP. Tomado de Netskope tenant.

Nótese que en la Figura 52, el Regex identifica varios códigos de procedimientos internos de la compañía que se suelen incluir en documentos confidenciales, sin embargo la el ultimo código no es válido, ya que cuenta con cuatro dígitos y su identificador “PR” este escrito mal. Posteriormente, esta Entidad debe ser relacionada en una regla de DLP, las reglas se pueden construir con varias Entidades, las personalizadas y las que vienen predefinidas en la plataforma y su estructura lógica se puede combinar para obtener los resultados esperados. Esta ventana de ajustes se muestra en la Figura 53.

Figura 53

Elaboración de regla DLP

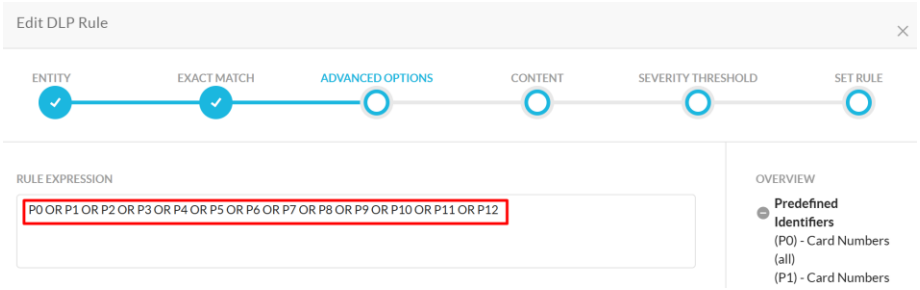


Nota. Proceso de creación de una regla DLP mostrando la selección de identificadores y criterios. Tomado de Netskope tenant.

Lo primero es seleccionar los identificadores y posteriormente con estos construir la expresión lógica que realizará la detección de información. Netskope soporta los siguientes operadores lógicos: **AND, OR, NOT y NEAR.** Vease la Figura 54.

Figura 54

Expresión lógica perfil de DLP.



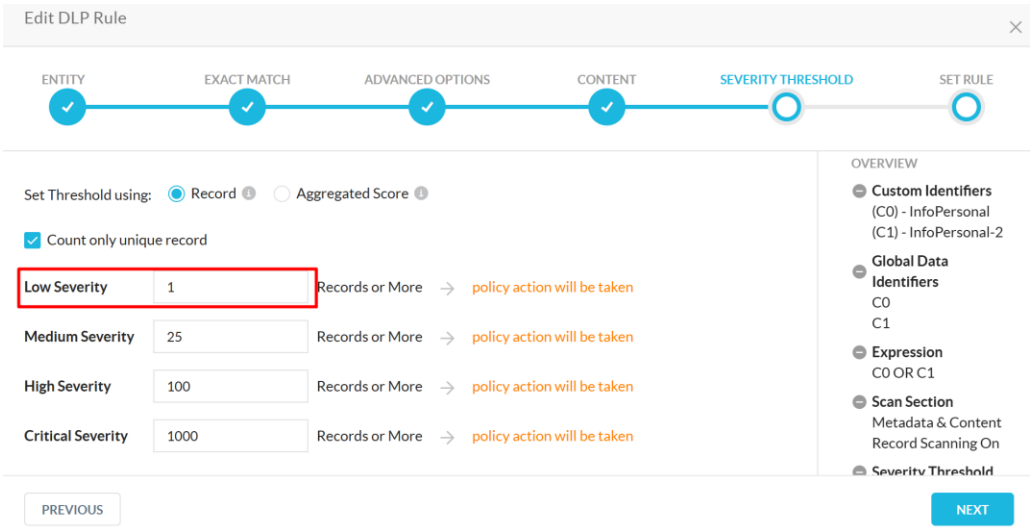
Nota. Interfaz que muestra la configuración de la lógica booleana (AND, OR) para combinar criterios en un perfil DLP. Tomado de Netskope tenant.

Las alertas activadas por la regla de DLP dependen de la gravedad de la infracción. Establezca el número de incidencias que deben coincidir antes de que se active una infracción de DLP y, a continuación, determine el nivel de gravedad que debe activar la alerta. Para establecer un umbral de gravedad:

La opción Puntuación global utiliza la suma de las ponderaciones de cada entidad coincidente para determinar la gravedad de la infracción. La puntuación predeterminada para la mayoría de las entidades es 1. Sin embargo, se pueden usar diccionarios personalizados para asignar otros valores a palabras clave específicas. Ver Figura 55.

Figura 55

Ejemplo severidad de las reglas

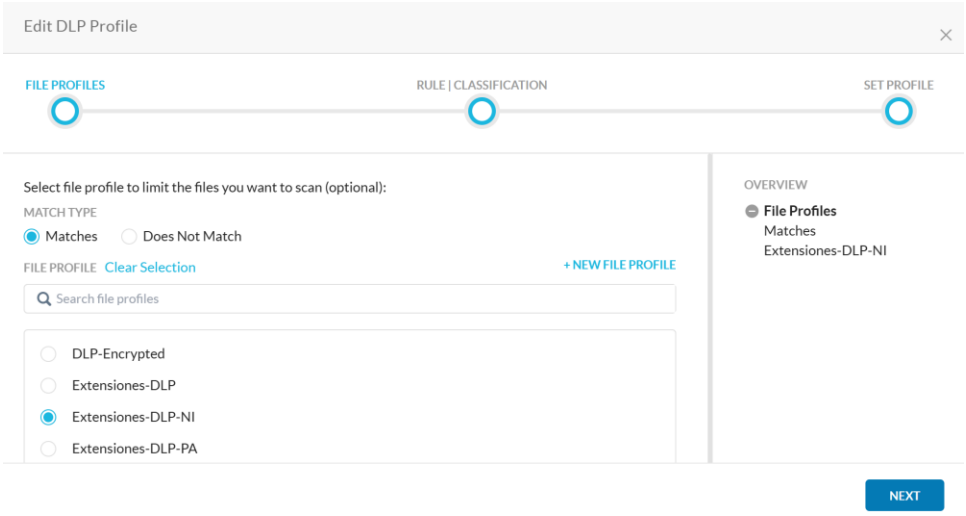


Nota. Configuración de los niveles de severidad y puntuación asignada a las entidades en una regla DLP. Tomado de Netskope tenant.

Contar solo registros únicos: Cuando se activa esta opción, si hay varias incidencias de una palabra clave específica en una infracción de DLP, esta se contabiliza como una sola. Además, al activar esta opción, se borrará el umbral de gravedad preestablecido. Introduzca un número de incidencias para cada nivel de gravedad o simplemente mantenga los valores predeterminados. Cambie o mantenga el nivel de gravedad que activa una acción de política en la lista desplegable. Se enviará una alerta cuando el nivel de gravedad supere el número de incidencias especificado. Finalmente, estas reglas se relacionan en un perfil de DLP y de esta manera queda construido. Ver Figura 56.

Figura 56

Perfil de archivos txt para Nicaragua

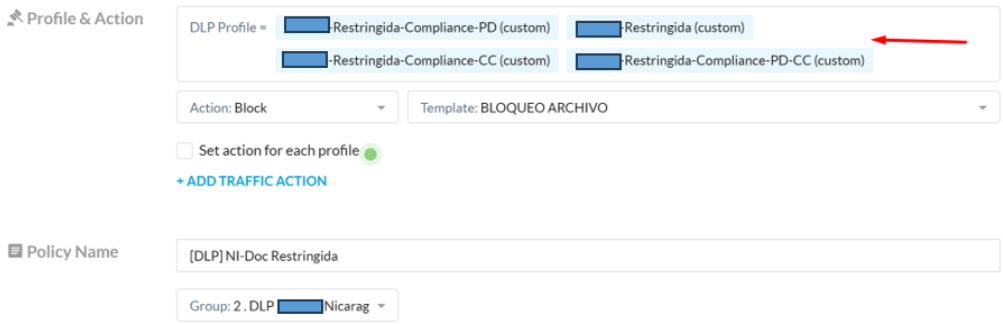


Nota. Configuración de un perfil DLP personalizado para detectar y actuar sobre archivos de texto (.txt) en un contexto regional específico. Tomado de Netskope tenant.

Como se mencionó con anterioridad los perfiles están constituidos por reglas, que también se pueden ajustar a las necesidades de detección específicas de la empresa. En estos mismos perfiles, se pueden agregar cuantas reglas se deseen y estas se pueden personalizar con palabras claves o con niveles de severidad por coincidencia de caracteres, ya sea en documentos, texto plano o imágenes. A continuación en la Figura 57, se puede observar un ejemplo de una regla personalizada que mantiene los niveles de severidad en un estándar bajo, sin permitir la más mínima filtración de información, estos parámetros se pueden ajustar de acuerdo con las necesidades finales. Para revisar con mayor detalle la creación de reglas DLP diríjase al siguiente enlace: https://docs.netskope.com/en/data-loss-prevention/

Figura 57

Política con perfiles de DLP personalizados



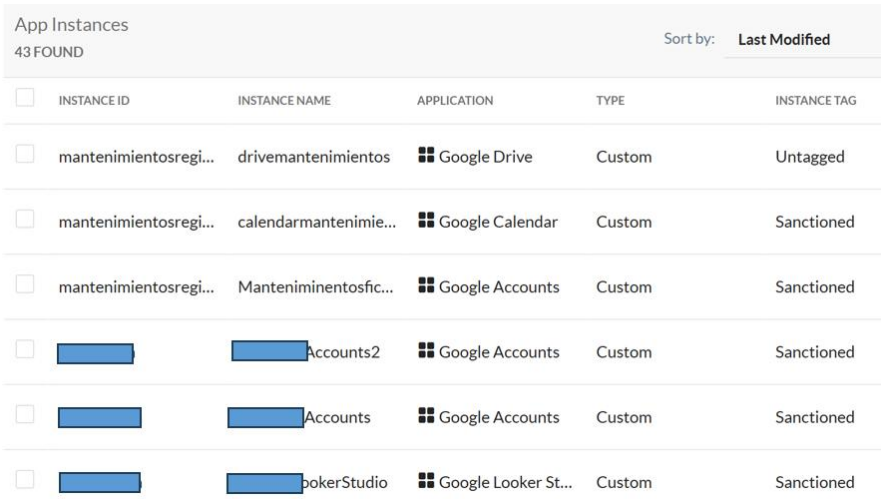
Nota. Regla que aplica perfiles DLP personalizados para el control de transferencia de datos en aplicaciones específicas. Tomado de Netskope tenant.

App Instance

Los perfiles de instancias de aplicaciones le permiten administrar estas instancias de aplicaciones con políticas de protección en tiempo real. Puede crear un perfil de instancia de aplicación especificando el identificador de instancia (ID), el nombre de la instancia y la etiqueta de la instancia, es decir, puede crear sus aplicaciones personalizadas especificando el dominio de su corporación. El proceso para crear una app instance es bastante simple, solo se debe seguir la ruta, ***Policies > Profiles > App Instance > New Custom App Instance.*** Ver Figura 58.

Figura 58

App Instance creadas

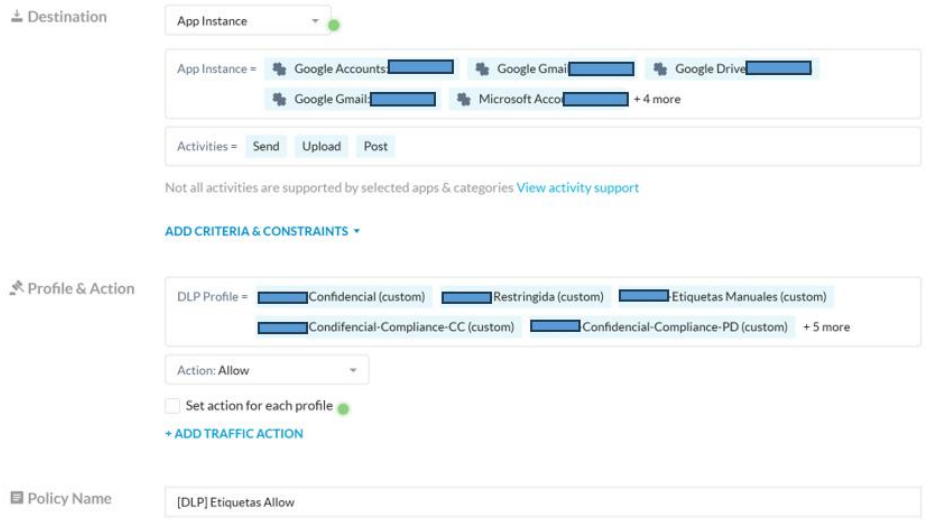


Nota. Lista de instancias de aplicaciones en la nube configuradas para su gestión y control en las políticas. Tomado de Netskope tenant.

Se crearon un total de 43 instancias de aplicaciones en nube, en la anterior imagen se incluyeron algunas a manera de ejemplo, la creación de este objeto de configuración puede ser empleada como criterio de coincidencia en las políticas y permitir el acceso a las aplicaciones con dominios corporativos. A manera de ejemplo se mostrará la configuración de una política en la Figura 59.

Figura 59

Política DLP con uso de una App Instance



Nota. Regla DLP que restringe acciones sobre datos basándose en una instancia de aplicación específica. Tomado de Netskope tenant.

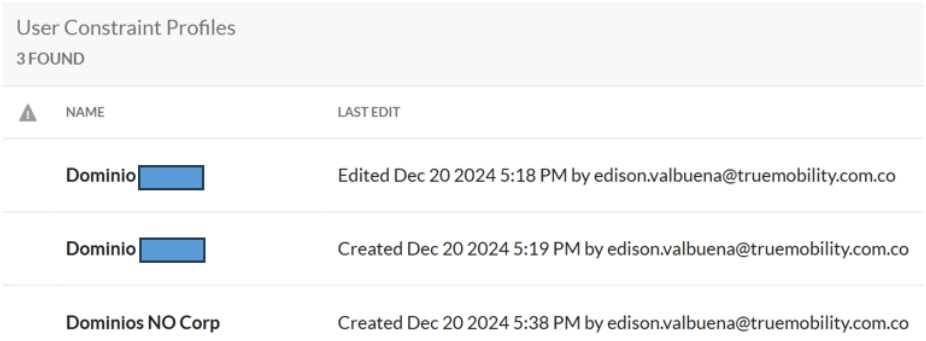
La anterior política que se muestra en la Figura 59 emplea las aplicaciones con Instancia corporativa y los perfiles predefinidos de DLP para indicarle a la plataforma que por medio de estas aplicaciones y con estos destinatarios se puede compartir información con etiquetas Confidencial y Restringida en los entornos corporativos del banco.

Constraint Domain

Se utiliza en políticas de protección en tiempo real. Definen lo que un usuario puede hacer para una actividad específica en una aplicación limitando sus actividades a destinos u orígenes de dominio corporativo y, en el caso de Google Gmail, las restricciones detectan y previenen actividades de filtración de información que intenta ser expuesta hacia dominios externos, como limitante el Constraint por dominio para esta aplicación solo funciona en actividad de “Send”. El proceso para crear un constraint es bastante simple, solo se debe seguir la ruta, ***Policies > Profiles > Constraint > New User Constraint.***

Figura 60

Perfiles de Constraint creados



Nota. Perfiles de restricción configurados para aplicar criterios específicos (como dominios) en las políticas de seguridad. Tomado de Netskope tenant.

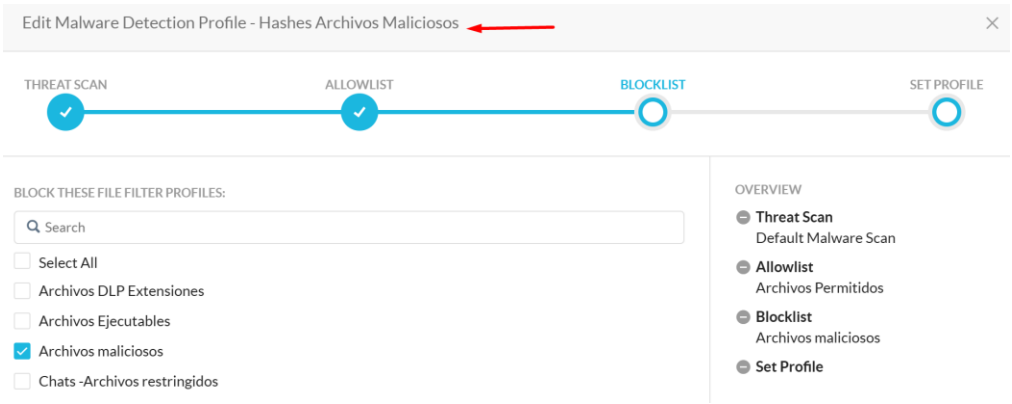
En la Figura 60 se tienen configurados tres (3) dominios para ser empleados en las diferentes políticas, actualmente NO existen políticas que empleen este tipo de criterio de match, porque este concepto de filtración se está monitoreando con las políticas de CASB API, dichas reglas serán revisadas con mayor detalle en la siguiente sección.

Threat Protection Custom

Decodifica e inspecciona el tráfico que otras soluciones de seguridad no pueden, como servicios en la nube no administrados, clientes de sincronización, aplicaciones móviles y sitios web y servicios en la nube cifrados con TLS, para identificar y abordar amenazas, se pueden crear perfiles personalizados, sin embargo, el estándar es bastante completo y es constantemente actualizado. El proceso para crear un perfil de protección es bastante simple, solo se debe seguir la ruta, ***Policies > Profiles > Threat Protection > New Malware Detection Profile.***

Figura 61

Creación de perfil de malware

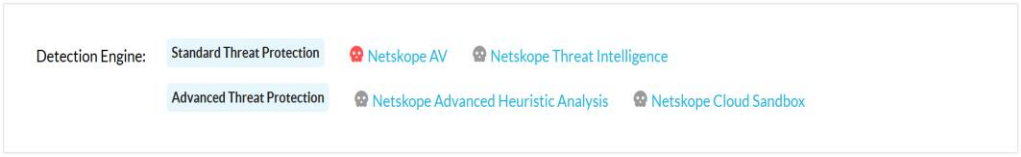


Nota. Interfaz para configurar un perfil personalizado de detección de amenazas (malware). Tomado de Netskope tenant.

Se tienen configurado un perfil personalizado de Threat Protection, Figura 61, para realizar el escaneo de archivos maliciosos, además, se está utilizando el perfil por defecto que es actualizado constantemente por Netskope y tiene en su base de datos los últimos archivos maliciosos, virus o trojanos identificados en la red. Con este perfil se configuro una política de protección que aplica a todos los usuarios y bloquea cualquier archivo corrompido que se intente descargar o cargar en las máquinas de la compañía. Es de las primeras políticas del tenant y evita que se infiltren archivos no deseados en la red local, es de suma importancia no configurar políticas que se ejecuten antes de estas, a continuación, se muestra la política configurada con el perfil de Threat Protection personalizado y los motores de análisis con los cuales cuenta el banco para detectar este tipo de amenazas. Ver Figura 62.

Figura 62

Motores de detección

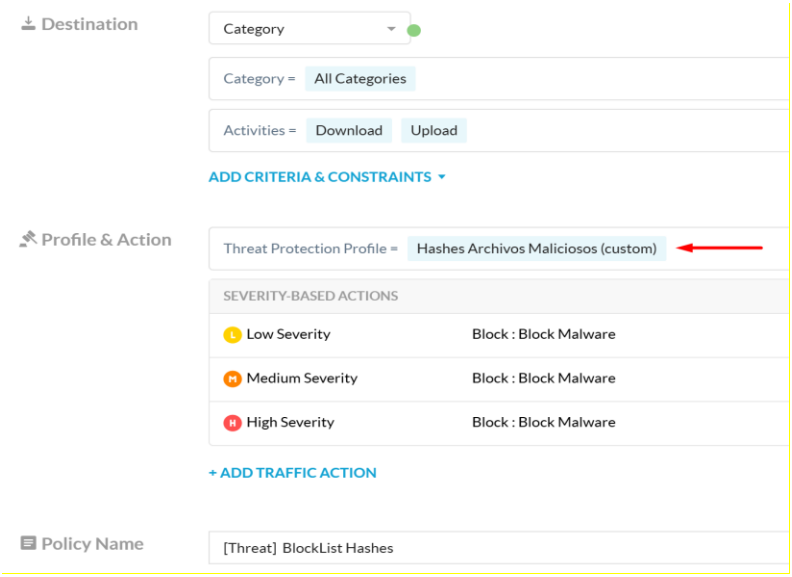


Nota. Configuración de los motores de escaneo (ej. Anti-Malware, Sandbox) utilizados en el perfil de protección contra amenazas. Tomado de Netskope tenant.

Finalmente, se muestra la política configurada con un perfil de Threat Protection custom, diríjase a la Figura 63 para visualizar la regla y observar que se está utilizando el perfil personalizado.

Figura 63

Política 1.2 BlockList Hashes



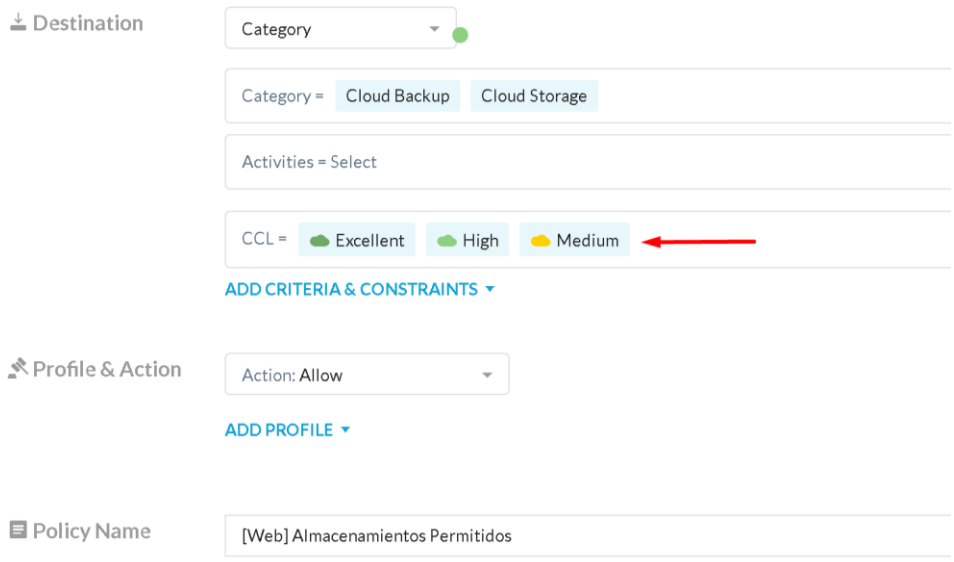
Nota. Regla que utiliza un perfil de amenazas personalizado para bloquear archivos basándose en su hash. Tomado de Netskope tenant.

Cloud Confidence Index

Es una métrica que se utiliza para evaluar el nivel de seguridad de la información en una aplicación. Es un indicador importante para medir la efectividad de las políticas y prácticas de seguridad de una empresa, con este valor que se asigna de manera única a una aplicación SaaS se pueden definir políticas, o se pueden asignar etiquetas. El proceso para crear una etiqueta CCI se puede realizar en la siguiente ruta, ***CCI > Search App > Open App > Tags > New Tag.***

Figura 64

Ejemplo de política con CCL

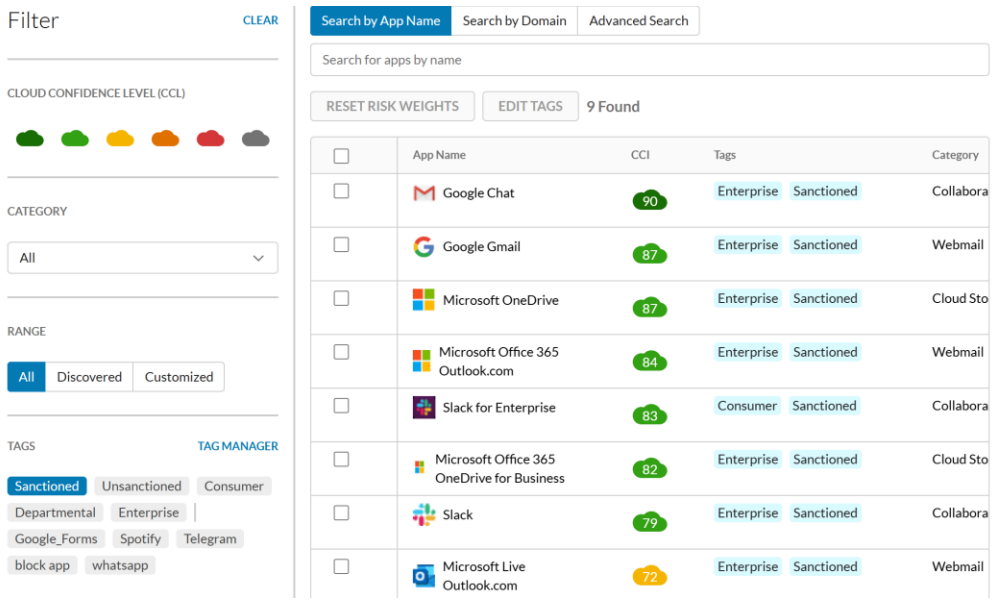


Nota. Regla de seguridad que utiliza el Índice de Confianza en la Nube (CCI) para permitir o bloquear aplicaciones específicas. Tomado de Netskope tenant.

En la Figura 64, se puede observar un ejemplo con una regla que permite solo las aplicaciones con buena reputación de CCL. Este tipo de reglas combina la categoría y la etiqueta de CCL para permitir o bloquear el acceso a una determinada aplicación, es un método útil para gestionar aplicaciones. De igual manera, se puede cambiar la etiqueta por defecto de estas aplicaciones para permitirlas en la política de cloud apps sanctioned. Ver Figura 65.

Figura 65

Aplicaciones Permitidas por etiqueta



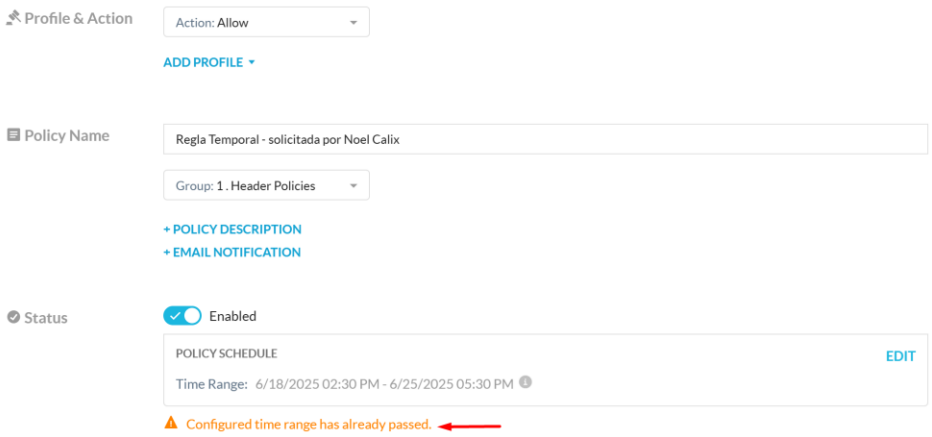
Nota. Política que autoriza aplicaciones en la nube basándose en etiquetas de confianza (CCI) predefinidas. Tomado de Netskope tenant.

Policy Schedule

Permite a las organizaciones tener un mayor control sobre la aplicación de políticas de seguridad en la nube al establecer horarios específicos en los que estas políticas se activan o desactivan automáticamente. Esto es útil para adaptarse a las necesidades cambiantes de seguridad y de la empresa. El proceso para crear un Schedule se puede realizar en la siguiente ruta, ***Policies > Real-time protection > New policy > Policy Schedule.***

Figura 66

Política programada con rango de tiempo

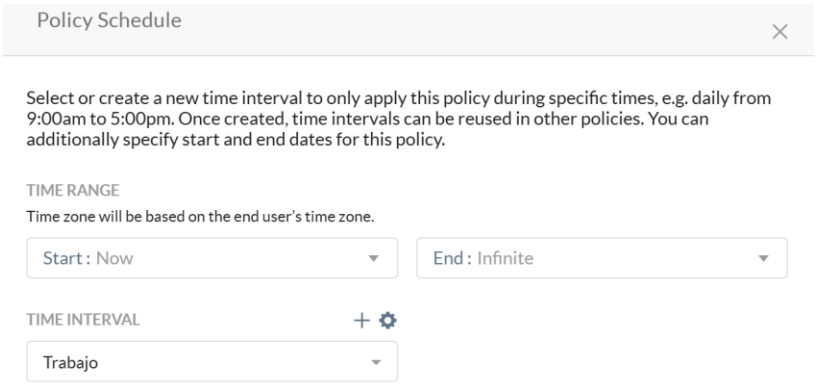


Nota. Regla de seguridad configurada para activarse o desactivarse automáticamente dentro de un horario específico. Tomado de Netskope tenant.

Como se mostraba en la Figura 66, cuando el rango de acción caduca se genera una alerta en color naranja al final de la regla que indica la expiración o validez de la política, cuando esto sucede, se deshabilita automáticamente y no tiene más injerencia en el desempeño del tráfico. También se pueden programar perfiles El perfil de “Trabajo” está configurado para activarse de lunes a viernes desde las 8 AM hasta las 6 PM. Es un ejemplo de cómo se puede configurar una programación y luego aplicar a una política que tendrá funcionabilidad en ese horario. En el banner principal de políticas se agrega un icono de reloj al lado izquierdo del item o numeral de la política.

Figura 67

Perfil de política programada



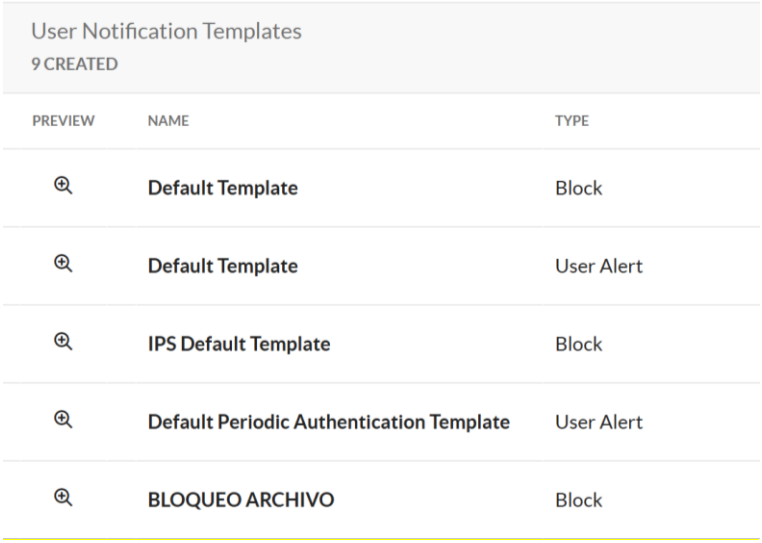
Nota. Configuración del intervalo de tiempo (horario y fechas) durante el cual una política permanece activa. Tomado de Netskope tenant.

Templates

Son los banners que indican cuando se está incumpliendo un parámetro de seguridad, es decir, cada vez que se quiera acceder a un recurso restringido aparecerá en la pantalla del usuario final un mensaje indicándole que no es posible acceder a una página especifica. El proceso para crear un banner se puede realizar en la siguiente ruta, ***Policies > Templates > User Notification > New Template***. Se muestran los mensajes de aviso y notificación configurados durante las diferentes actividades de implementación.

Figura 68

Plantillas configuradas

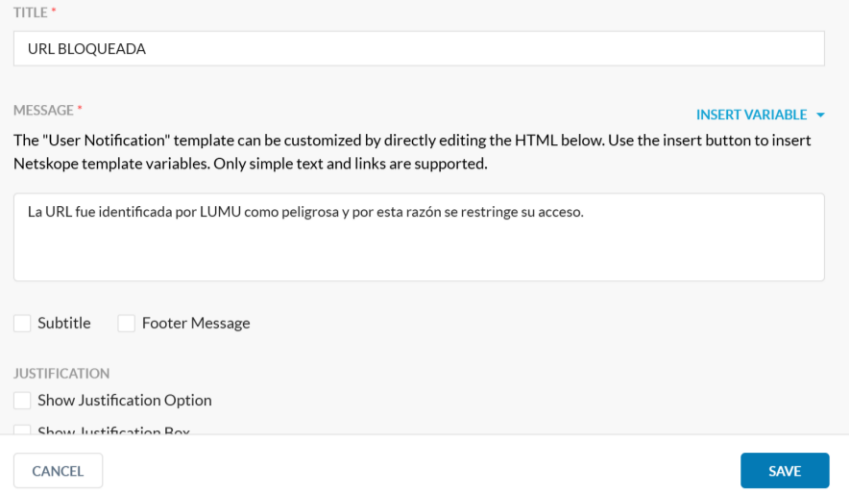


Nota. Lista de plantillas de notificación al usuario (Block, User Alert) creadas y disponibles para su uso en políticas. Tomado de Netskope tenant.

Se tienen configurados cinco (5) templates, ver Figura 68, y vienen por defecto otros cuatro, cada uno de estos se puede utilizar de manera específica en una política o grupo de políticas, por ejemplo, se puede crear un mensaje para la violación de información, otro para accesos no autorizados y uno más para notificación de usuarios. Tal y como se realizó en el Corporación. Esto permite obtener cierto grado de detalle en la administración de la plataforma, manteniendo a los colaboradores informados sobre los bloqueos específicos que se están aplicando. Vease el ejemplo en la Figura 69.

Figura 69

Template de Acceso Restringido

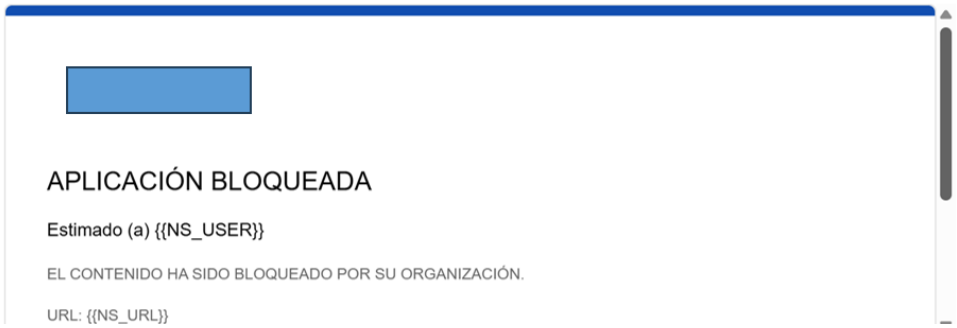


Nota. Ejemplo de personalización de una plantilla de notificación que informa al usuario sobre un bloqueo con mensaje específico. Tomado de Netskope tenant.

Se pueden personalizar los templates, con el logo de la compañía y mensajes específicos, se puede crear uno por política si así se prefiere, en la compañía se configuraron un par de plantillas informativas que son utilizadas en casos de bloqueo y/o accesos no autorizados. Este banner es mostrado a los usuarios que intentan acceder a aplicaciones en línea que no están autorizadas por el grupo de seguridad e IT de la corporación, nótese que corresponde a un texto con parámetros de HTML y variables propias de la plataforma como: nombre de archivo, nombre de política, actividades realizadas etc. Además, se indica un correo electrónico en el cual pueden pedir información adicional o solicitar el acceso al recurso si es necesario. Al usuario final le aparece un banner de este estilo. Vease la Figura 70.

Figura 70

Banner de Aplicación Bloqueada



Nota. Banner personalizado que se muestra al usuario cuando se bloquea el acceso a una aplicación o contenido. Tomado de Netskope tenant.

Fase IV: API Data Protection y Cloud Firewall

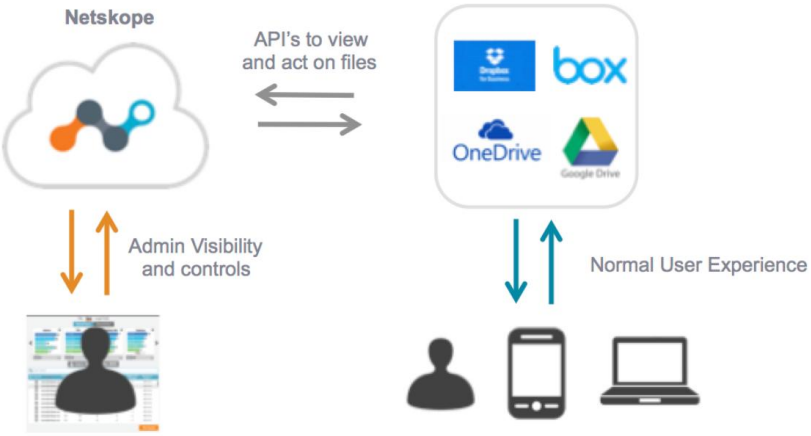
API Data Protection

Las reglas de API Data Protection de Netskope permiten proteger datos sensibles en aplicaciones en la nube mediante la inspección y control de archivos, mensajes y configuraciones de seguridad dentro de servicios SaaS como Microsoft 365, Google Workspace, Box, Slack, Salesforce, Zoom, Jira, entre otros. Durante el proceso de implementación se realizó la configuración API para las aplicaciones SaaS de Google Gmail y Google Drive con esta integración se pueden construir reglas que ayuden a extender el monitoreo DLP del banco. Estas reglas se basan en la integración mediante APIs nativas de cada aplicación SaaS, lo que permite analizar y aplicar políticas sin necesidad de un proxy en línea o agentes en los endpoints. El flujo de funcionamiento inicia con la configuración de la integración en Netskope, donde se autentica la aplicación SaaS mediante OAuth o credenciales API. Una vez integrada, Netskope realiza un descubrimiento continuo de los datos en reposo dentro de la aplicación, identificando archivos, correos, mensajes y configuraciones de seguridad según las políticas establecidas. Las reglas de

protección se basan en perfiles de Data Loss Prevention, donde se definen patrones de datos sensibles como PCI-DSS (tarjetas de crédito), PII (información personal identificable), PHI (datos de salud), secretos de API o credenciales embebidas. Cuando Netskope detecta una violación de política, puede aplicar acciones como alertar, bloquear, poner en cuarentena, cifrar o eliminar contenido, Estas acciones varían de acuerdo con la integración API, por ejemplo: en Google Gmail esta soportada únicamente la acción de Alert, mientras en Google Drive se soportan una variedad más amplia de acciones entre las cuales, se destacan “Delete” y “Restrict Access”. Adicionalmente, puede realizar remediaciones automatizadas como cambiar la configuración de permisos de archivos expuestos públicamente o notificar a usuarios responsables. Un punto clave es la integración con Cloud Access Security Broker para correlacionar eventos de API Data Protection con actividades en tiempo real, proporcionando visibilidad y control unificado, taly como muestra la Figura 71.

Figura 71

CASB API de Netskope



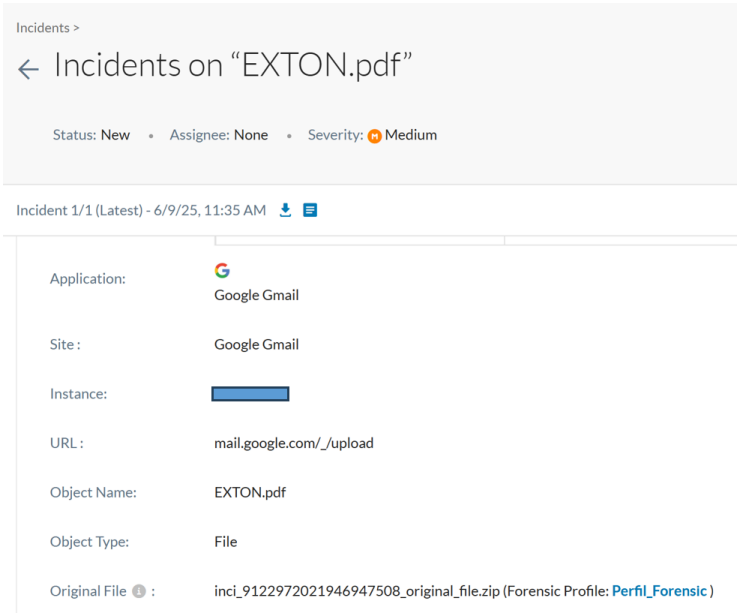
Nota. Diagrama de la arquitectura de protección de datos mediante API para aplicaciones en la

nube. Tomado de Netskope, por Licencias Online. (s. f.). Recuperado de https://www.licenciasonline.com/ar/es/products/netskope

La configuración adecuada de estas reglas es crítica para prevenir fugas de datos, cumplimiento de normativas (GDPR, HIPAA, ISO 27001) y minimizar riesgos de acceso no autorizado. Además, permite auditar y monitorear cambios en archivos y configuraciones que podrían indicar compromisos de seguridad o configuraciones erróneas en la nube, los eventos que se detectan por medio de estas políticas se pueden consultar con bastante detalle en la parte de Incidentes DLP, donde se incluye información precisa como: tipo de archivo, hora, tamaño del archivo, destinatarios y más datos de interés. Ver Figura 72.

Figura 72

Ejemplo de Incidente DLP

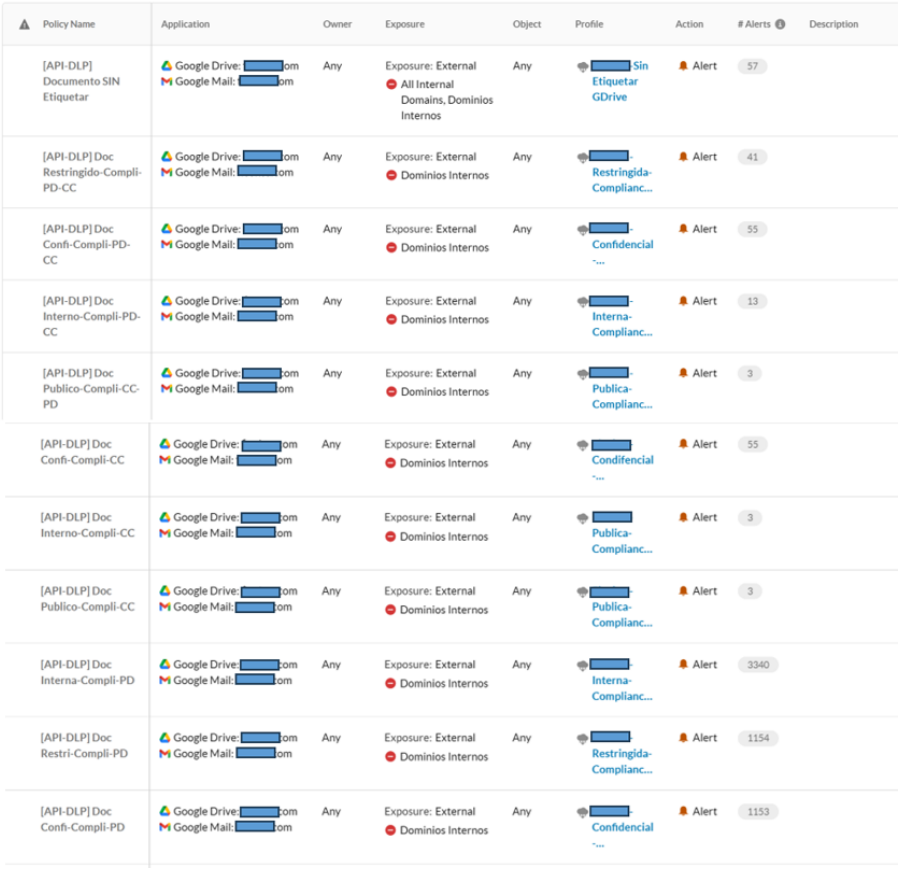


Nota. Detalle de un incidente generado por una política DLP, mostrando la aplicación, archivo y severidad. Tomado de Netskope tenant.

A continuación en la Figura 73, se presenta el listado completo de las políticas de API Data Protection configuradas en la corporación. Estas reglas se diferencian de las de Real-Time Protection en varios aspectos, siendo el más relevante su método de ejecución. A diferencia de las políticas en tiempo real, las reglas de API Data Protection no siguen un orden de prioridad, ya que cada configuración se evalúa de forma independiente y simultánea, sin importar su jerarquía. Además, estas políticas no pueden ser exportadas y cuentan con un conjunto de acciones más limitado. Sin embargo, ofrecen un nivel de análisis más profundo, ya que operan mediante integración directa con las APIs nativas de las aplicaciones en la nube, lo que permite realizar inspecciones exhaustivas sobre datos en reposo y configuraciones de seguridad.

Figura 73

Listado de Políticas API Data



Policy Name	Application	Owner	Exposure	Object	Profile	Action	# Alerts	Description
[API-DLP] Documento SIN Etiquetar	Google Drive: [redacted]om Google Mail: [redacted]om	Any	Exposure: External All Internal Domains, Dominios Internos	Any	[redacted] Sin Etiquetar GDrive	Alert	57	
[API-DLP] Doc Restringido-Compli-PD-CC	Google Drive: [redacted]om Google Mail: [redacted]om	Any	Exposure: External Dominios Internos	Any	[redacted]-Restringida-Complianc...	Alert	41	
[API-DLP] Doc Confi-Compli-PD-CC	Google Drive: [redacted]om Google Mail: [redacted]om	Any	Exposure: External Dominios Internos	Any	[redacted]-Confidencial-...	Alert	55	
[API-DLP] Doc Interno-Compli-PD-CC	Google Drive: [redacted]om Google Mail: [redacted]om	Any	Exposure: External Dominios Internos	Any	[redacted]-Interna-Complianc...	Alert	13	
[API-DLP] Doc Publico-Compli-CC-PD	Google Drive: [redacted]om Google Mail: [redacted]om	Any	Exposure: External Dominios Internos	Any	[redacted]-Publica-Complianc...	Alert	3	
[API-DLP] Doc Confi-Compli-CC	Google Drive: [redacted]om Google Mail: [redacted]om	Any	Exposure: External Dominios Internos	Any	[redacted] Condifencial-...	Alert	55	
[API-DLP] Doc Interno-Compli-CC	Google Drive: [redacted]om Google Mail: [redacted]om	Any	Exposure: External Dominios Internos	Any	[redacted] Publica-Complianc...	Alert	3	
[API-DLP] Doc Publico-Compli-CC	Google Drive: [redacted]om Google Mail: [redacted]om	Any	Exposure: External Dominios Internos	Any	[redacted]-Publica-Complianc...	Alert	3	
[API-DLP] Doc Interna-Compli-PD	Google Drive: [redacted]om Google Mail: [redacted]om	Any	Exposure: External Dominios Internos	Any	[redacted]-Interna-Complianc...	Alert	3340	
[API-DLP] Doc Restri-Compli-PD	Google Drive: [redacted]om Google Mail: [redacted]om	Any	Exposure: External Dominios Internos	Any	[redacted] Restringida-Complianc...	Alert	1154	
[API-DLP] Doc Confi-Compli-PD	Google Drive: [redacted]om Google Mail: [redacted]om	Any	Exposure: External Dominios Internos	Any	[redacted]-Confidencial-...	Alert	1153	

Nota. Tabla que resume las políticas configuradas para la protección de datos a través de API, incluyendo su estado y vigencia. Tomado de Netskope tenant.

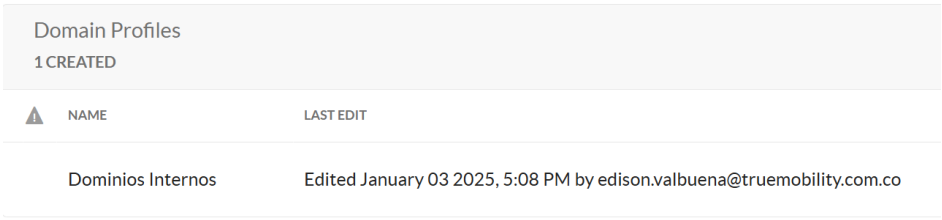
Domain Profile

El perfil de dominio se utiliza para definir cuentas de dominio externo para correo electrónico. El perfil de dominio funciona junto con las aplicaciones API de protección de datos Gmail y Microsoft Office 365 Outlook.com. Como parte del asistente de definición de políticas, puede escanear correos electrónicos enviados a dominios externos como xyz.com o abc.com. El proceso para crear un dominio es bastante simple, solo se debe seguir la ruta, ***Policies > Profiles > Domain > New Domain Profile.***

Con estos dominios es posible evitar que usuarios compartan información confidencial en plataformas de almacenamiento en la nube no aprobadas. Se tienen dos perfiles de dominio configurados para todo lo relacionado con correos corporativos, esto permitió definir políticas específicas para cada categoría, como limitar la carga de archivos a sitios personales de almacenamiento en la nube mientras se permite en cuentas corporativas. Asegurando la aplicación de controles granulares sobre la navegación y el uso de aplicaciones en la nube. A continuación en la Figura 74, se muestran los perfiles de dominio configurados en el banco.

Figura 74

Perfiles de dominio

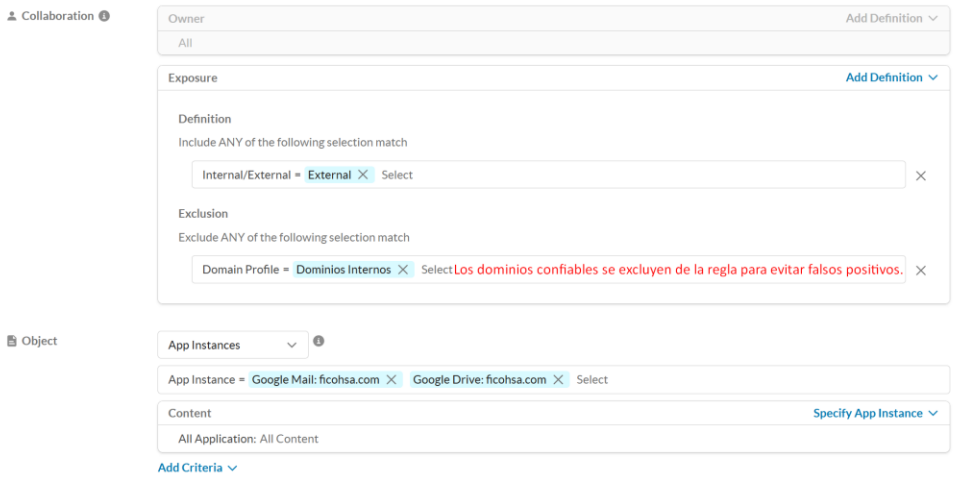


Nota. Configuración de perfiles que definen dominios específicos para aplicar políticas de seguridad en aplicaciones en la nube. Tomado de Netskope tenant.

Todas las políticas de CASB API para Google Gmail y Google Drive configuradas durante la implementación utilizan el criterio de dominio para definir el alcance de la inspección. Dado que el intercambio de información entre colaboradores de la organización no representa un riesgo significativo, su análisis resulta poco relevante. No obstante, es fundamental monitorear este tipo de tráfico cuando los datos se comparten con agentes externos. A continuación, se presenta un ejemplo de política, véase la Figura 75.

Figura 75

Política API-DLP para Google Drive y Google Gmail



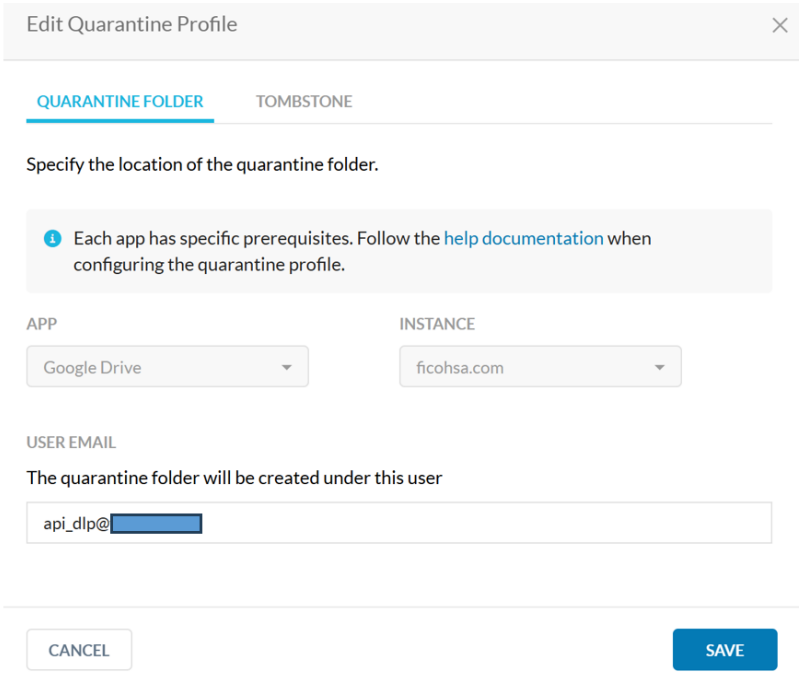
Nota. Regla que combina protección de datos (DLP) mediante API para restringir acciones en aplicaciones de Google. Tomado de Netskope tenant.

Quarentine Profile

Se utiliza para especificar dónde se debe poner en cuarentena el archivo cuando hay una acción de política de Cuarentena. Puede utilizar archivos de desecho para reemplazar el contenido del archivo original, se conservarán el nombre y la extensión del archivo original. También es posible crear un perfil de cuarentena utilizando la plataforma clásica o de próxima generación. En la clásica, las integraciones de aplicaciones se basan en la plataforma de protección de datos API de primera generación. En la próxima generación, las integraciones de aplicaciones se basan en la última plataforma de protección de datos API de próxima generación. Las aplicaciones clásicas se migrarán gradualmente a la próxima generación. El proceso para crear este tipo de perfil es bastante simple, solo se debe seguir la ruta, ***Policies > Profiles > Quarantine > Next Gen > New Quarantine Profile.*** Ver Figura 76.

Figura 76

Perfil de Cuarentena configurado



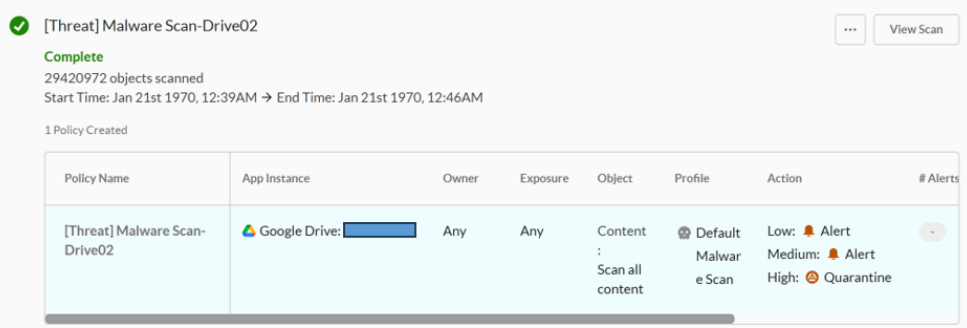
Nota. Configuración de la carpeta de cuarentena en Google Drive donde se aíslan archivos que violan políticas DLP. Tomado de Netskope tenant.

La creación de este perfil permite ejecutar escaneos de datos en reposo, generalmente en archivos almacenados en repositorios como Google Drive, OneDrive o Box. Estos escaneos se clasifican en dos tipos: DLP y Threat Protection. Una vez que la política ha sido configurada e iniciada, el sistema analiza de manera periódica los archivos dentro del repositorio objetivo. Si un archivo coincide con las reglas de detección establecidas, se ejecutan las acciones definidas en la política. Una acción comúnmente utilizada es la cuarentena, en la cual los archivos detectados se trasladan automáticamente a una carpeta de cuarentena designada dentro del mismo repositorio o en un almacenamiento aislado, restringiendo el acceso a los usuarios hasta que se realice una evaluación manual o automática del contenido. En el siguiente ejemplo, se muestra una política configurada específicamente para Google Drive, la cual aplica reglas de

Threat Protection para escanear archivos en reposo y tomar acciones de mitigación en función de los resultados obtenidos tal y como muestra la Figura 77.

Figura 77

Escaneo de malware para datos en reposo



Nota. Política que ejecuta escaneos de amenazas en archivos almacenados (en reposo) en Google Drive. Tomado de Netskope tenant.

Netskope admite múltiples integraciones a nivel de API con diversas plataformas SaaS, lo que permite ampliar la visibilidad, el control y la protección de datos en entornos en la nube. Entre las integraciones compatibles se incluyen: Box, ChatGPT, Cisco Webex, Confluence, Dropbox, Egnyte, GitHub, Google Drive, Google Gmail, Jira, Microsoft Teams, Okta, OneDrive, Outlook, Salesforce, ServiceNow, ShareFile, SharePoint, Slack Enterprise, Workday, Yammer, Zendesk y Zoom. Para habilitar integraciones API de próxima generación y mejorar el alcance y profundidad del análisis en más plataformas, es necesario seguir la siguiente ruta en la consola de Netskope: ***Settings > Configure App Access > Next Gen > CASB API***. El proceso de integración varía según la plataforma, pero generalmente implica los siguientes pasos:

Autenticación y permisos: Se deben generar tokens de autenticación (OAuth o API keys) y proporcionar credenciales de una cuenta con privilegios administrativos en la aplicación SaaS a integrar.

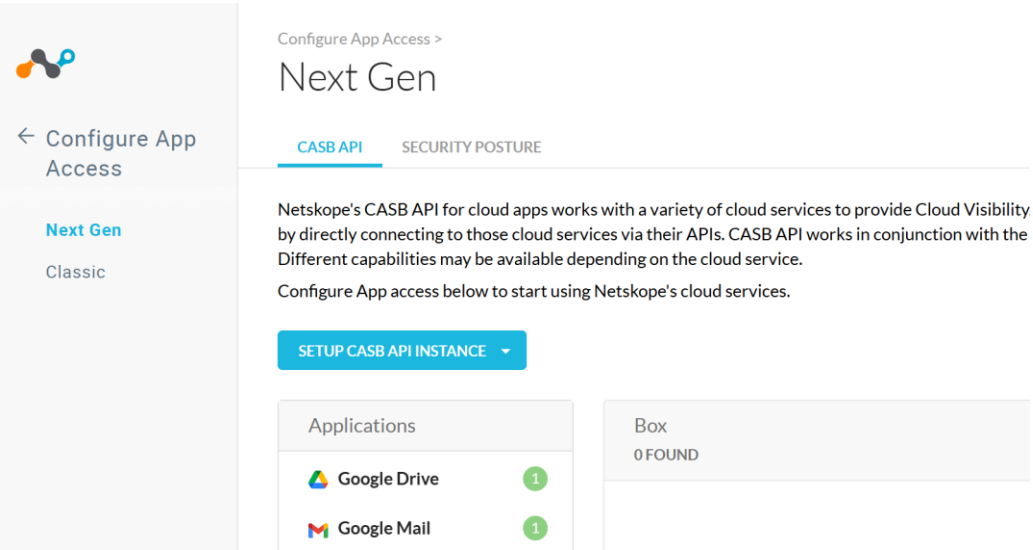
Sincronización y descubrimiento: Netskope accede a la API de la plataforma para sincronizar usuarios, actividades y datos almacenados, permitiendo el monitoreo en tiempo real o por escaneo programado.

Aplicación de políticas: Una vez integrada la aplicación, se pueden configurar políticas de seguridad para detectar amenazas, prevenir la fuga de datos (DLP), aplicar controles de acceso y generar alertas ante actividades sospechosas.

Estas integraciones refuerzan la postura de seguridad en entornos SaaS al proporcionar un control detallado sobre el tráfico y los datos almacenados en la nube, asegurando el cumplimiento normativo y la protección de la información crítica.

Figura 78

Integraciones API configuradas en la organización



Nota. Vista de las aplicaciones en la nube (Box, Google Drive, Gmail) conectadas mediante CASB API para visibilidad y control. Tomado de Netskope tenant.

Cloud Firewall

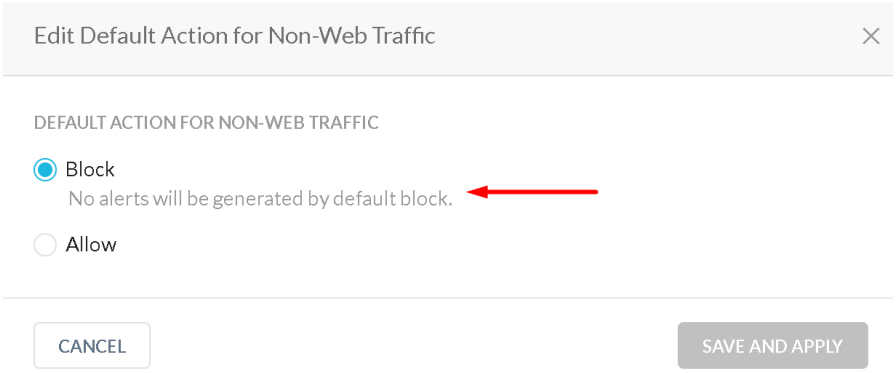
Habilitar el firewall en la nube de Netskope ofrece una solución integral para la administración de la seguridad y el acceso a la red en entornos distribuidos y usuarios en

movimiento. Con esta capacidad, las organizaciones pueden centralizar la administración, obtener visibilidad completa y aplicar políticas consistentes en todas las oficinas y usuarios, sin importar su ubicación física. Esto es fundamental en un entorno empresarial moderno, donde la movilidad y la descentralización son cada vez más comunes. Una de las ventajas principales es la capacidad de proporcionar controles avanzados de seguridad y acceso sin incurrir en los costos, la complejidad y las limitaciones de rendimiento asociadas con los dispositivos de firewall tradicionales, al aprovechar el firewall en la nube de Netskope, el banco pudo establecer políticas granulares para controlar el tráfico saliente no HTTP(S), incluidos los protocolos TCP, UDP e ICMP. Esto le permite proteger sus redes contra una amplia gama de amenazas y vulnerabilidades, incluso en puertos y protocolos no convencionales.

Además, el firewall en la nube de Netskope ofrece una serie de características avanzadas, como controles de políticas basados en 5 tuplas, identificación de usuario y grupo, dominios completamente calificados y comodines como destinos, y una puerta de enlace de capa de aplicación para FTP. Estos elementos proporcionan una flexibilidad excepcional para adaptar las políticas de seguridad a las necesidades específicas de la organización, garantizando al mismo tiempo un nivel óptimo de protección. Como se mostró con anterioridad se habilito todo el tráfico para el entorno Off-Premises y On-Premises, esto quiere decir que el módulo de Cloud Firewall empezó aplicar sobre ese Steering Configuration. Después de realizar un monitoreo del tráfico, que por defecto se encuentra en estado de bloqueo, Figura 79. También es posible construir aplicaciones tipo Cloud Firewall y configurar políticas de navegación en tiempo real.

Figura 79

Acción por defecto tráfico No web



Nota. Configuración que define si el tráfico no web (non-web) se bloquea o permite por defecto en Cloud Firewall. Tomado de Netskope tenant.

Esta configuración por defecto se modificó para que el tráfico fuera permitido mientras se realiza un monitoreo en el Skope IT. Monitorear el tráfico no web en Netskope es crucial por varias razones, por ejemplo, se pueden evidenciar los eventos que están siendo bloqueados en un grupo de usuarios especifico, esto sirve como base para ajustar las redes independientes, crear aplicaciones y proceder con habilitar solo los puertos TCP y UDP que se requieren, asegurando de esta manera la selectividad de las conexiones confiables. Luego de realizar esta actividad durante varias semanas, se pueden empezar a crear las aplicaciones que permitan las conexiones puntuales. El proceso de creación de una Cloud App en Netskope implica seguir una serie de pasos específicos. A continuación, se detalla el proceso: Acceder a la página de configuración de aplicaciones, esto se puede hacer yendo a ***Configuration > Security Cloud Platform > App Definition***. En esta pestaña se debe crear una nueva regla de definición de aplicaciones, para ello, se debe hacer clic en ***New App Definition Rule*** y luego seleccionar ***Firewall App***. En la ventana de Nueva Regla de Definición de Aplicaciones Firewall, se deben seguir los siguientes pasos:

Aplicación: Seleccionar una aplicación de firewall existente o crear una nueva. Es importante proporcionar un nombre significativo para la aplicación.

Dirección IP de Destino: Ingresar una dirección IP válida, un rango de IP, un FQDN (Nombre de Dominio Completo), un PQDN (Nombre de Dominio Parcialmente Calificado) o una máscara de red CIDR separada por comas. Si se deja en blanco, Netskope establecerá la dirección IP de destino como "cualquier".

Protocolo: Elegir el protocolo para la aplicación de firewall. Para TCP, UDP y TCP/UDP, se pueden configurar:

Un puerto específico: por ejemplo, 22.

Un rango de puertos específico: por ejemplo, 1024-2048.

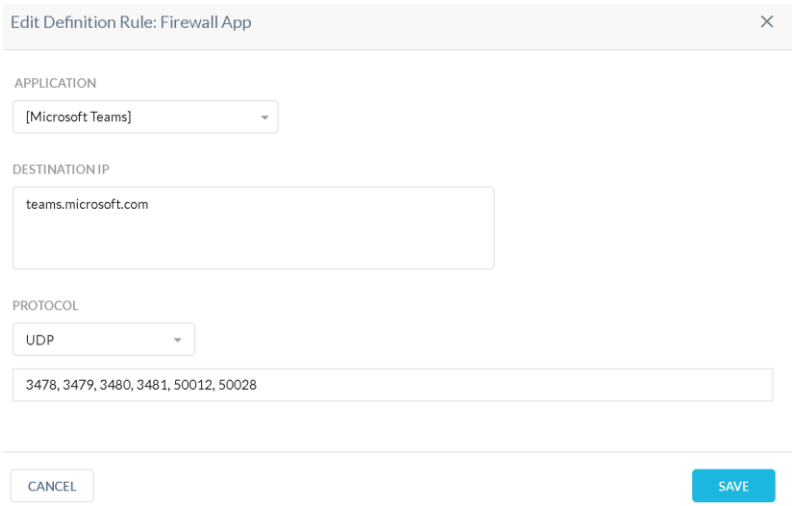
Una combinación de puertos y rangos de puertos: por ejemplo, 22,80,443,1024-2048.

ICMP: No requiere configuración de puerto. Para flujos TCP, se produce un tiempo de espera después de 5 minutos de inactividad. Netskope recomienda utilizar un "keepalive" para protocolos basados en TCP que puedan aprovechar sesiones inactivas más largas, como SSH, FTP, etc.

Puede crear nuevas reglas para que las aplicaciones de firewall se apliquen a las políticas o también se pueden crear varias reglas para la misma aplicación de firewall. Por ejemplo, si crea una aplicación llamada "Allow_FTP" con una determinada IP y protocolo de destino, esta misma aplicación se puede reutilizar para agregar más IP y protocolos de destino. Véase en la Figura 80, una aplicación de tipo Firewall configurada.

Figura 80

Ejemplo de aplicación para Teams

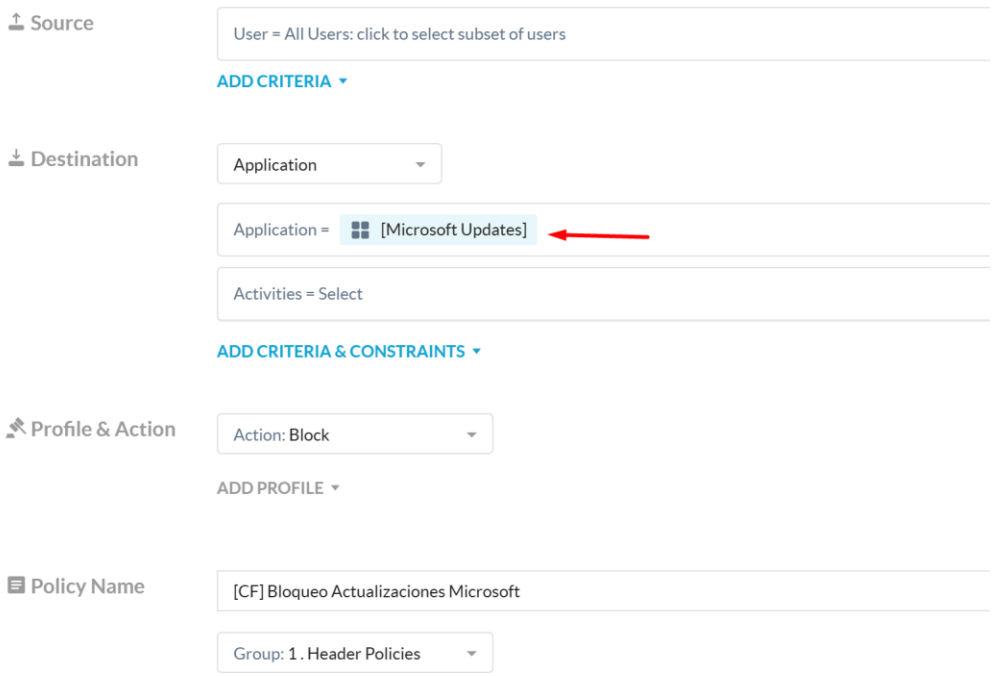


Nota. Configuración de una aplicación tipo Firewall para Microsoft Teams, definiendo protocolos y puertos específicos. Tomado de Netskope tenant.

Se pueden construir políticas de tipo Firewall con aplicaciones preconfiguradas en Netskope, también con aplicaciones personalizadas como se observó con anterioridad para Teams Corporativo y por otro lado, se pueden continuar utilizando las listas URL y las categorías personalizadas para construir políticas más completas, es decir, se tienen varias opciones de configuración todas bastante fáciles de aplicar, sin olvidar los criterios de origen y destino a nivel de direccionamiento, entre otros. En la siguiente regla, que permitió bloquear las actualizaciones de Windows se utilizó una custom category, que se elabora o construye de manera natural, la única diferencia radica en la creación de la regla como tal, que sigue la siguiente ruta, ***Policies > Rela Time Protection > New Policy > Firewall.*** Ver Figura 81.

Figura 81

Política de tipo Firewall

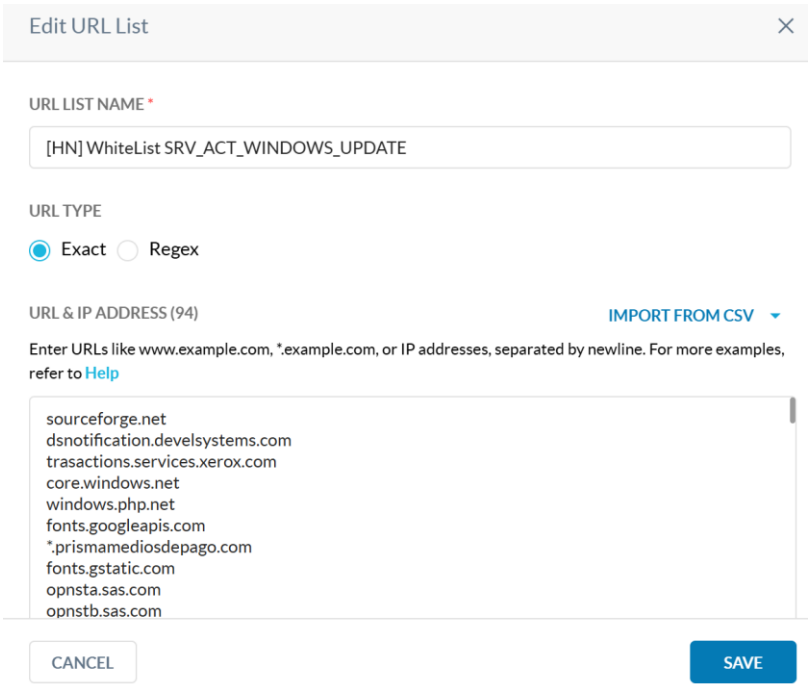


Nota. Regla de Cloud Firewall que bloquea la aplicación "Microsoft Updates" para todos los usuarios. Tomado de Netskope tenant.

Como muestra la Figura 82, para esta política se construyó una URL list con los puertos, direcciones IP y dominios que se identificaron durante la etapa de monitoreo y que son utilizados por Windows para enviar las actualizaciones, de esta manera queda disponible un recurso que puede ser empleado en cualquier momento para adicionar este tipo de información, no se requiere algo adicional más que dirigirse a ***Policies > Profiles > URL List*** y buscar la lista llamada " Windows Updates" , bajo el mismo principio de las listas para el tráfico web se adiciona la información que se requiere bloquear, en este caso la mayoría corresponde a dominios.

Figura 82

Lista de Firewall



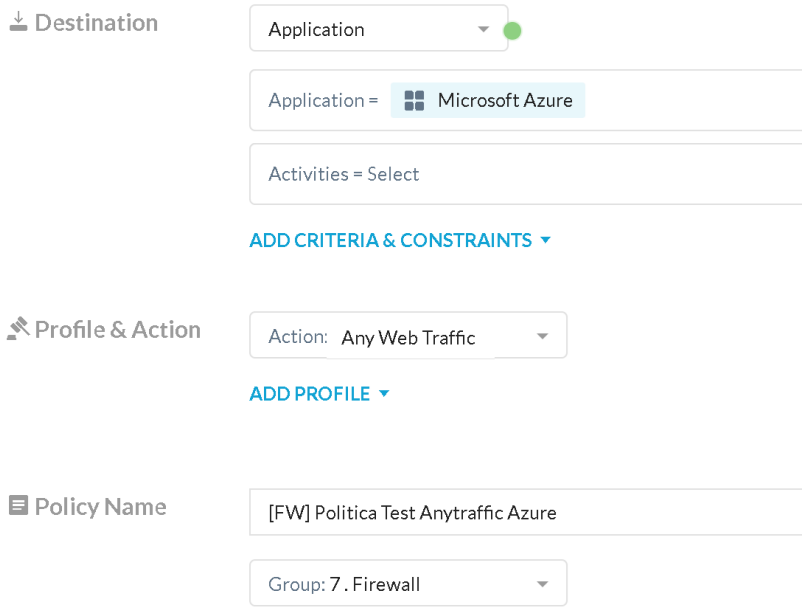
Nota. Lista de URL y direcciones IP configurada como lista blanca para permitir tráfico específico (ej. actualizaciones de Windows). Tomado de Netskope tenant.

Ejemplo Política Firewall 1

Es posible restringir el tráfico no web o por el contrario permitir todo el tráfico para una aplicación especifica, esta configuración cobra sentido cuando se mantiene la configuración de tráfico no-HTTPS por defecto (en Bloqueo). El proceso para crear una política tipo Firewall se puede realizar en la siguiente ruta, Policies > Real-time protection > New policy > Firewall. Ver Figura 83.

Figura 83

Azure permitido en todo el tráfico



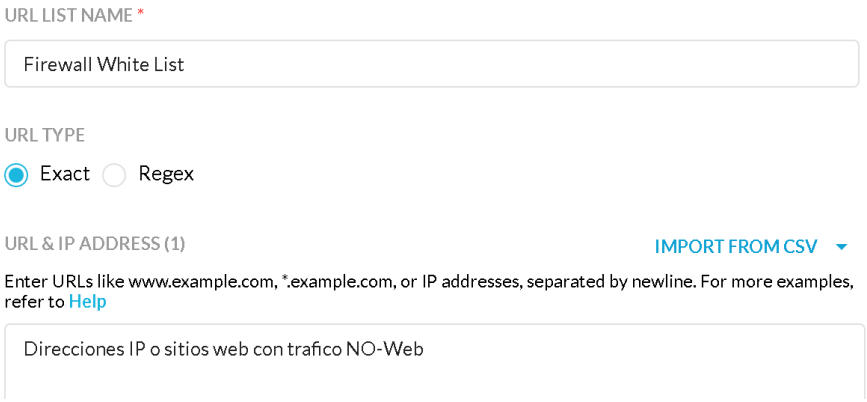
Nota. Regla de Cloud Firewall que permite todo el tráfico hacia servicios de Microsoft Azure. Tomado de Netskope tenant.

Ejemplo Política Firewall 2

También es posible crear una lista blanca para el tráfico de tipo no web, tal cual como se realizó el proceso con la White List general para el tráfico 443 y 80, no se requiere un flujo de configuración diferente, se debe crear una URL List, asociarla a una custom category y crear la política siguiendo el proceso habitual de configuración de reglas. El proceso para crear una política tipo Firewall se puede realizar en la siguiente ruta, ***Policies > Real-time protection > New policy > Firewall.*** Ver Figura 84.

Figura 84

Creación de lista blanca para Firewall

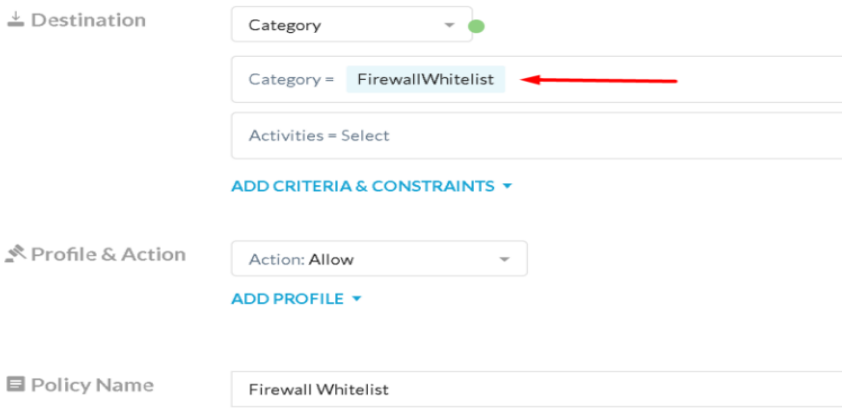


Nota. Interfaz para definir una lista de direcciones IP o dominios permitidos en las reglas de Cloud Firewall. Tomado de Netskope tenant.

Después de asociar la anterior lista a una categoría personalizada se puede crear la política de protección en tiempo real, observe la Figura 85.

Figura 85

Política de lista blanca tipo Firewall



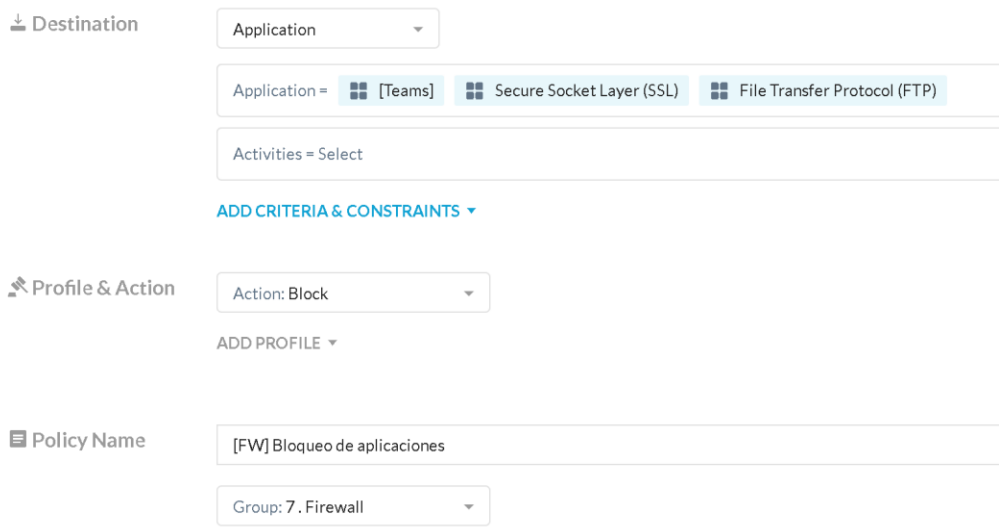
Nota. Regla que permite tráfico hacia destinos incluidos en una categoría personalizada "FirewallWhitelist". Tomado de Netskope tenant.

Ejemplo Política Firewall 3

Por defecto Netskope incluye una gran variedad de aplicaciones que pueden ser empleadas en políticas de este estilo como: File Transfer Protocol, Secure Socket Layer e Internet Message Control Protocol, pero es posible crear nuevas aplicaciones personalizadas que se ajusten a la necesidad como se observa anteriormente para Teams y bloquear puertos específicos. Se muestra un ejemplo de este tipo de reglas, véase la Figura 86.

Figura 86

Bloque de aplicaciones por Firewall



Nota. En la anterior política se combina la regla con aplicaciones por defecto de firewall y la personalizada con puertos específicos para Teams. Tomado de Netskope tenant.

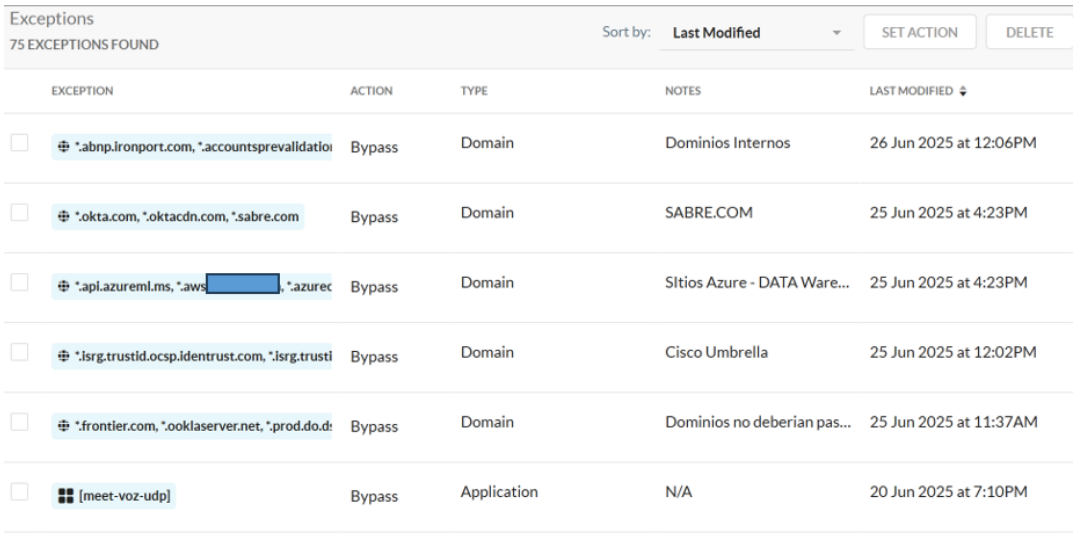
Excepciones de Red

Las excepciones de red son una funcionalidad fundamental cuando se trata de equilibrar la seguridad con la flexibilidad operativa, y es aquí donde la potencia de Netskope se destaca. Netskope ofrece una solución que permite establecer excepciones de red de manera precisa y efectiva, lo que resulta invaluable en situaciones donde se necesitan políticas de seguridad adaptadas a necesidades específicas sin comprometer la integridad de la red. A través de la plataforma de Netskope, es posible definir reglas personalizadas para autorizar el acceso no

restringido o sin inspección a determinados recursos o direcciones IP. Esto es especialmente útil para evitar bloqueos innecesarios o inspecciones intrusivas en casos en los que existan requisitos particulares y necesidades operativas especiales. La capacidad de personalizar estas reglas proporciona un nivel adicional de control, permitiendo a las organizaciones asegurarse de que las políticas de seguridad sean aplicadas de manera precisa y adecuada. El Steering Configuration de Netskope desempeña un papel crucial en esta capacidad. Al dirigir el tráfico hacia la nube, Netskope garantiza que las excepciones de red se integren de manera fluida en la arquitectura general. Sin embargo, es importante destacar que, al definir excepciones en la configuración de dirección, existe la posibilidad de dirigir el tráfico desde fuentes específicas directamente hacia sus destinos correspondientes sin pasar por la nube de Netskope. Esto demuestra la flexibilidad que Netskope ofrece a las organizaciones para optimizar sus flujos de tráfico según sus necesidades. La creación y administración de excepciones en un entorno de seguridad informática es un aspecto crítico que demanda ciertos niveles de autorización y una comprensión detallada de las configuraciones particulares de la implementación. En el caso de Netskope, plataforma de seguridad en la nube líder, esta tarea se vuelve fundamental para garantizar la adaptabilidad y eficacia de las políticas de seguridad sin poner en riesgo la integridad de la red y los datos. Netskope aborda este proceso con un enfoque preciso y detallado que permite establecer excepciones tanto para categorías, dominios, source locations, destination locations, source contries y aplicaciones. La flexibilidad que ofrece Netskope en la gestión de excepciones brinda a las organizaciones la capacidad de adaptar sus políticas de seguridad según las necesidades específicas de su entorno operativo, sin comprometer la coherencia y efectividad de las medidas de protección en tiempo real implementadas. Observe en la Figura 87, algunas de las excepciones más relevantes que se agregaron durante la implementación de los servicios.

Figura 87

Listado de excepciones para Steering Configuration Honduras



Nota. Lista de destinos excluidos del enrutamiento (steering) para tráfico específico de Honduras. Tomado de Netskope tenant.

En los entornos corporativos, especialmente en instituciones financieras, es común que muchas aplicaciones internas —como portales de gestión, sistemas de autenticación, o herramientas de monitoreo— utilicen certificados autofirmados o certificados emitidos por Autoridades Certificadoras (CA) internas. Estos certificados no son reconocidos por las CA públicas, por lo que, al implementar soluciones de inspección SSL/TLS como Netskope Cloud Security Platform, el tráfico hacia estos dominios puede ser interpretado como no confiable. Por defecto, Netskope aplica inspección SSL a todo el tráfico HTTPS para poder analizar amenazas ocultas dentro de conexiones cifradas, realizar controles de políticas DLP (Data Loss Prevention), CASB (Cloud Access Security Broker), y prevenir exfiltración o acceso indebido a datos. Sin embargo, cuando el tráfico está firmado por certificados internos o autofirmados, la inspección falla debido a que Netskope no puede validar la cadena de confianza del certificado.

Como resultado, el tráfico es bloqueado, generando interrupciones en aplicaciones críticas del negocio.

Desactivar globalmente la inspección SSL no es una opción recomendable, ya que esto eliminaría la visibilidad sobre amenazas cifradas, que representan hoy más del 90 % del tráfico web. En lugar de ello, Netskope ofrece una solución granular: las SSL Decryption Policies (políticas de excepción SSL), que permiten excluir de inspección solo los dominios, subdominios o categorías que realmente lo requieran, manteniendo el resto del tráfico bajo inspección activa. Vease la Figura 88.

Figura 88

Excepciones de Netskope

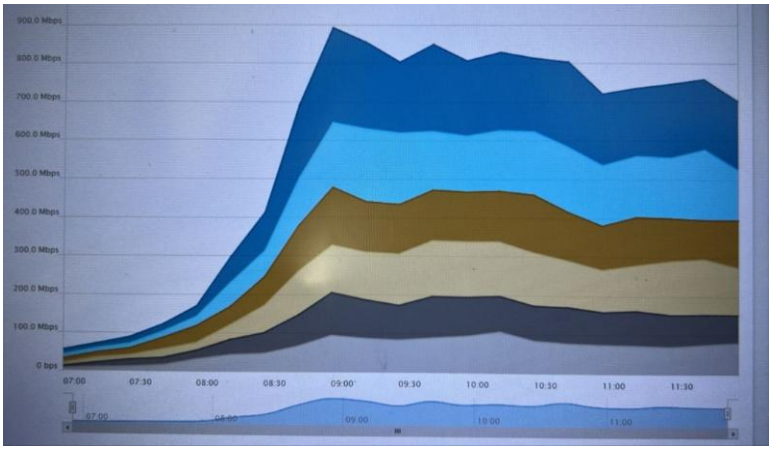
Exception Type	Cloud Traffic	Web Traffic	All Traffic		All DNS Traffic
	Web	Web	Web	Non-Web	DNS(TCP/UDP 53, UDP 5353)
Application	Yes	No	No	Yes	No
Category	No	Yes	Yes	No	No
Certificate-Pinned Application	Yes	Yes	Yes	Yes	No
Domains	Yes	Yes	Yes	Yes	No
DNS	No	No	No	No	Yes
Destination Location	Yes	Yes	Yes	Yes	Yes
Source Location	Yes	Yes	Yes	No	No
Source Countries	Yes	Yes	Yes	No	No

Nota. Tabla que resume los tipos de excepciones y el tráfico al que aplican (web, nube, DNS, etc.). Tomado de Adding Exceptions, por Netskope. https://docs.netskope.com/en/adding-exceptions/

Durante la fase de implementación, se observaron incrementos en el consumo del canal de datos, cuyo ancho de banda había sido previamente controlado. Este aumento, en realidad, no se originó por un tráfico adicional generado por Netskope, sino que se debe a la forma en que la herramienta utiliza el ancho de banda disponible. Netskope no inyecta ni origina tráfico extra; lo que hace es aprovechar al máximo la capacidad que el firewall permite: si se configura 1 GB, Netskope utilizará ese límite siempre que el usuario lo demande. El verdadero origen del problema no fue Netskope, sino los permisos y accesos concedidos a los usuarios. Al estar habilitados ciertos sitios o dominios sin restricciones de tráfico, el cliente permitió que estos flujos utilizaran el canal por completo. Como resultado, el ancho de banda, que antes estaba limitado, de pronto se saturó. Lo que faltaba era un control fino de ancho de banda —una función que Netskope aún no ofrecía directamente al inicio, pero que fue abordada implementando bypass selectivos en dominios que no requerían inspección y que, sin embargo, consumían ancho de banda significativo.

Figura 89

Visualización de tráfico desde el Firewall perimetral



Nota. Panel del firewall que muestra el tráfico de red, volumen y protocolos para análisis de ancho de banda. Tomado de Fortinet tenant.

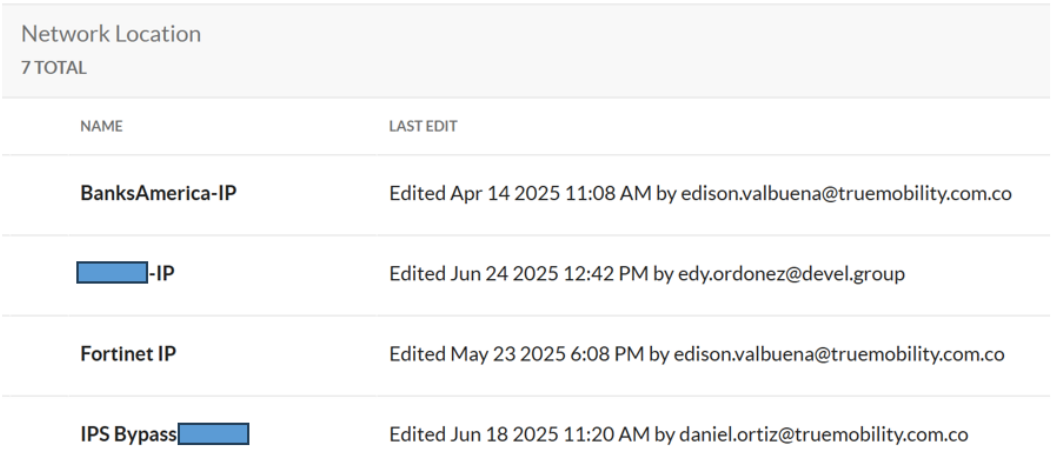
En la Figura 89, se aprecia claramente que, tras implementar Netskope y aplicar bypass a los dominios de actualización (Updates), el tráfico se estabilizó y regresó a los niveles habituales. Esto confirma que la acción de bypass fue efectiva para mitigar el incremento inicial. Al autorizar dominios de actualización sin restricciones, se permitió un pico de ancho de banda cuando esos servicios comenzaron a descargarse o sincronizarse masivamente. Netskope simplemente reflejó ese comportamiento. El incidente se resolvió sin necesidad de reducir la visibilidad o seguridad, solo optimizando las políticas de tunelización.

Network Location

También se crearon varias excepciones de red, la mayoría con dominios o direcciones IP, algunas para aplicaciones específicas que no es necesario analizar el tráfico. Para el servicio de VPN se crearon algunas listas de dominios y direcciones IP que no van a pasar a través del tenant. Estas listas se agregan en Policies > Profiles > Network Location. En esta sección se encuentran las listas con varias direcciones IP que se excluyeron del Steering Configuration de acuerdo con las necesidades de la empresa. Puntualmente se tienen una lista que se excepciona en la sección de Exeptions del respectivo grupo de control de tráfico. Ver Figura 90.

Figura 90

Lista de Network Location configuradas

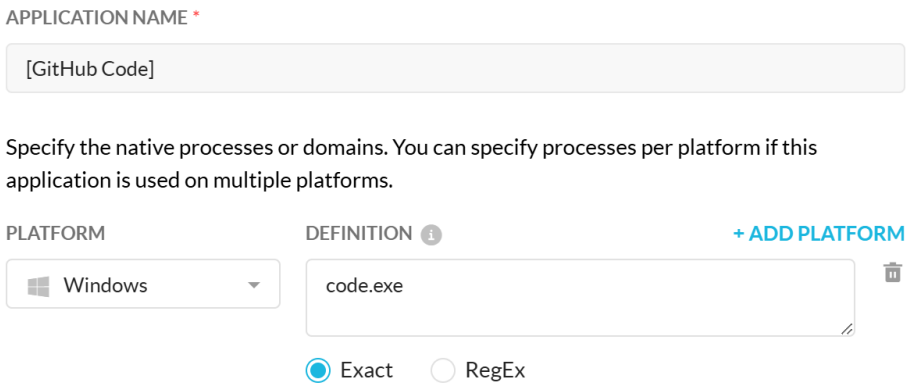


Nota. Configuraciones de ubicaciones de red definidas para el control y excepción del tráfico. Tomado de Netskope tenant.

Para excluir una aplicación como el GitHub Code se crea una excepción de tipo aplicación pinned y se elige la acción de Bypass, es importante incluir los dominios de la app, el tenant de Netskope incluye algunas aplicaciones por defecto, de las cuales, no analiza del todo la encriptación debido a que los aplicativos no soportan este método de análisis y se bloquean o por el contrario cuentan con sus propios certificados seguros y no es necesario un análisis detallado. A continuación se muestra el ejemplo de esta aplicación, para crear más aplicaciones se debe seguir la siguiente ruta. ***Settings > Security Cloud Platform > App definition > Certificate Pinned Apps***. Ver Figura 91.

Figura 91

Excepción para aplicación



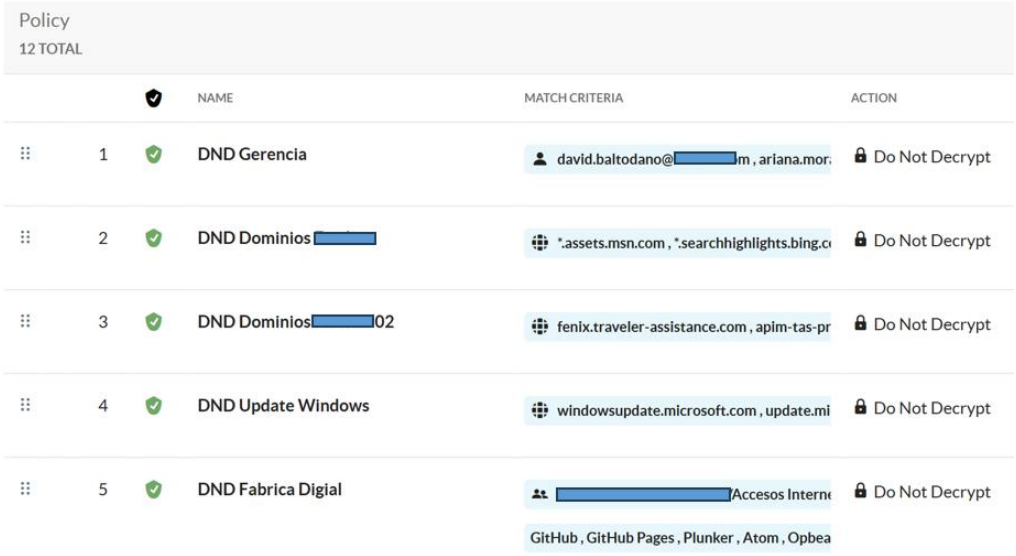
Nota. Configuración de una excepción específica para GitHub Code, definiendo el proceso (code.exe) en la plataforma Windows. Tomado de Netskope tenant.

SSL Decryption

Se pueden crear excepciones de tipo Do not Decrypt, con esto el tráfico no va a ser desencriptado por Netskope. De forma predeterminada, todo el tráfico dirigido a Netskope se descifrará y luego se analizará más a fondo mediante políticas de protección en tiempo real. Si hay algún tráfico que le gustaría dejar cifrado, como el tráfico de invitados anónimos y el tráfico médico/financiero privado, puede especificarlo a través de políticas. El proceso para crear una política DND se puede realizar en la siguiente ruta: ***Policies > SSL Decryption.*** Ver Figura 92.

Figura 92

Políticas de DND y Decrypt configuradas



Nota. Lista de políticas que especifican qué tráfico no debe ser descifrado (Do Not Decrypt), como dominios de actualizaciones o aplicaciones internas. Tomado de Netskope tenant.

Se pueden apreciar diez políticas de este tipo, de hecho, una de estas solía venir configurada por defecto, cuyo principal propósito era omitir la desencriptación del tráfico para algunos dominios web de Microsoft que presentaron inconvenientes durante la implementación de políticas de protección en tiempo real en versiones anteriores de la plataforma, este tráfico sigue pasando a través del túnel de Netskope, solo que no se evalúa el SSL al detalle, por el contrario si se desea realizar una inspección más profunda en las políticas configuradas se debe selección el Decrypt. Observe que son dominios relativamente empresariales y que no deberían representar mayor problema o generar brechas de seguridad. También se pueden agregar políticas de SSL para categorías sin representar una alteración importante, varios de estos dominios vienen agregados como excepciones de tráfico en el tenant, sin embargo, es buena práctica borrarlos de allí y agregarlos en esta sección para tener un monitoreo del tráfico web que

está asociado a estos sitios de red. Al implementar estas políticas de omisión de desencriptación SSL, se logra un equilibrio entre la seguridad y la eficiencia en la red. Se asegura que el tráfico crítico y empresarial pueda fluir sin problemas sin sacrificar la capacidad de monitorear y proteger la red contra posibles amenazas. En resumen, esta estrategia ayuda a garantizar un entorno de trabajo seguro y productivo al tiempo que se toman medidas proactivas para la protección de la red y la privacidad de los datos.

Fase V: Monitoreo de Políticas y Tráfico Web

El principal objetivo del Skope IT es proporcionar información sobre sus aplicaciones, sitios, usuarios y eventos. Netskope ofrece una potente solución de monitoreo a través de su plataforma Skope IT, que proporciona alertas, eventos y análisis de aplicaciones para administrar de manera proactiva el tráfico de la red. Con la capacidad de buscar datos utilizando el lenguaje de consulta de Skope IT, los administradores pueden filtrar análisis por fecha, usuario, ubicación del usuario, dispositivo y actividad, lo que permite un control detallado y personalizado. La importancia del monitoreo en Netskope abarca varios aspectos críticos del entorno de red, incluido el tráfico web, las aplicaciones privadas (NPA) y el tráfico de tipo Firewall, la capacidad de Skope IT para proporcionar información detallada sobre las aplicaciones, sitios web, usuarios y eventos permite a los administradores comprender mejor el comportamiento del tráfico en la red y tomar medidas proactivas para abordar cualquier problema o riesgo potencial. En este contexto, el monitoreo del tráfico web permite a los administradores identificar y gestionar eficazmente las actividades de navegación de los usuarios, mientras que el monitoreo de las aplicaciones ofrece visibilidad sobre el uso de aplicaciones internas críticas para el negocio. Además, el monitoreo del tráfico de tipo Firewall permite detectar y responder

rápidamente a cualquier actividad sospechosa o violaciones de políticas de seguridad. Los siguientes son algunos casos de uso para la página Aplicaciones:

Vea una lista de aplicaciones en la nube descubiertas en las últimas 24 horas.

Determine cuándo los usuarios acceden a una nueva aplicación en la nube y luego supervise el uso de la aplicación.

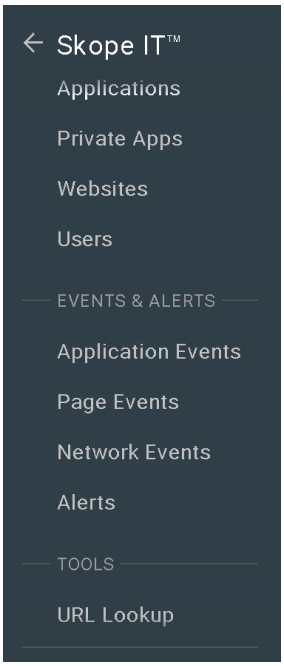
Sepa cuándo una aplicación activa políticas o incidentes de DLP.

Haga clic en la aplicación para comprender todos los detalles de esta aplicación en la nube y verificar el Índice de confianza en la nube (CCI) para evaluar la preparación empresarial de la aplicación.

Vaya a Skope IT para ver todos los eventos de una aplicación en la nube.

Figura 93

Panel de monitoreo



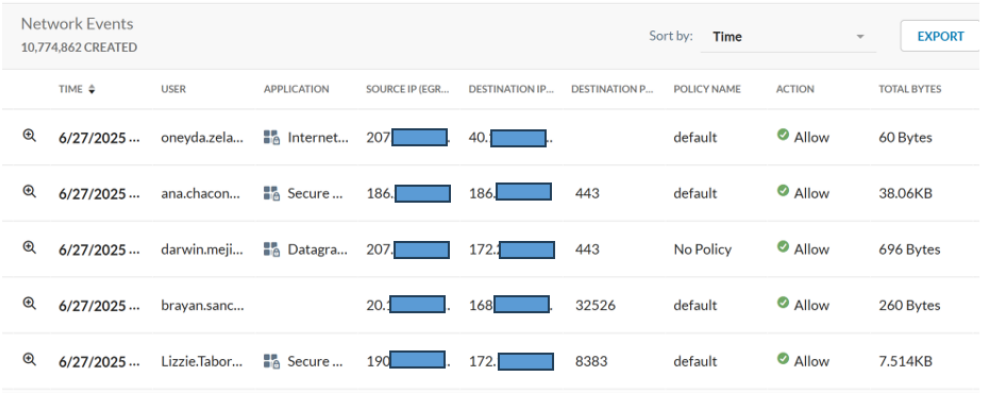
Nota. Vista principal del panel Skope IT, mostrando módulos para monitoreo de aplicaciones, eventos, alertas y herramientas. Tomado de Netskope tenant.

La opción de Skope IT de la Figura 93, ofrece varias subpestañas, cada una proporcionando distintos niveles de información y eventos que permiten supervisar el estado real de la compañía. En la pestaña "Application Events" se espera encontrar todo el tráfico relacionado con los accesos web; "Page Events" brinda información más detallada de las URL accedidas; "Network Events" proporciona datos sobre todas las conexiones de aplicaciones privadas y el tráfico de protocolos UDP y TCP; finalmente, "Endpoint Events" muestra los eventos relacionados con el control por dispositivo y la información que se intenta almacenar en dispositivos USB o imprimir a través de impresoras corporativas o externas.

Es importante realizar un monitoreo constante del tráfico para identificar de manera proactiva las páginas que los usuarios no están accediendo en algún momento y habilitarlas, evitando quejas y la saturación de casos en la mesa de ayuda. Tanto "Application Events" como "Page Events" suministran abundante información sobre los accesos de cada usuario, ya sea a tráfico web o aplicaciones en la nube. Se pueden filtrar los eventos de red y personalizar las columnas que se van a visualizar; existe una gran variedad de opciones que pueden ayudar a resolver problemas de conectividad. Además, es clave observar cómo Netskope está identificando el tráfico para, de esta manera, construir las políticas con las cuales los usuarios realizarán coincidencias. Ver Figura 94.

Figura 94

Skope IT tráfico web

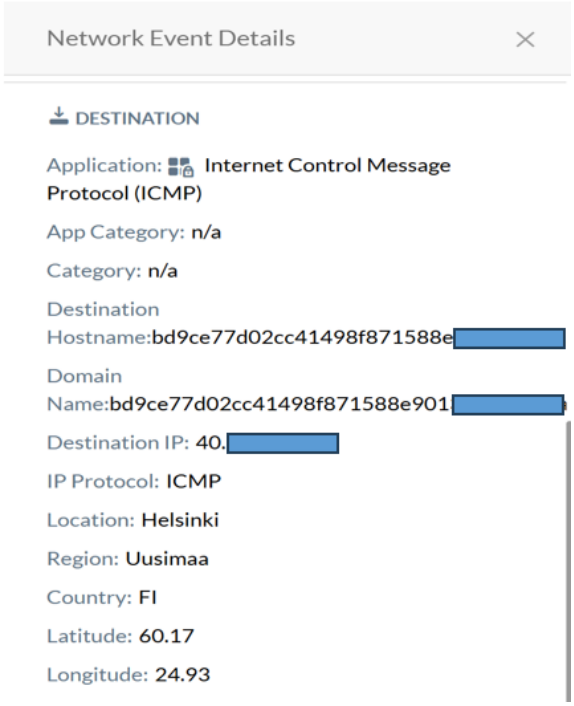


Nota. Panel del Skope IT que muestra el análisis y volumen del tráfico web categorizado. Tomado de Netskope tenant.

Aprovechando la capacidad de Netskope para identificar el tráfico de manera precisa, los administradores pueden crear políticas de seguridad específicas que dictan cómo debe manejarse el tráfico en la red. Estas políticas pueden abordar una amplia gama de escenarios, como el bloqueo de acceso a sitios web maliciosos o la restricción del uso de ciertas aplicaciones en la red. Al establecer estas políticas, las organizaciones pueden mejorar significativamente su postura de seguridad y proteger sus activos digitales contra amenazas potenciales. Para obtener una comprensión más detallada de los eventos de tráfico en la red, Netskope ofrece la posibilidad de visualizar información específica sobre cada evento. Al hacer clic en el icono de lupa con el símbolo de +, los administradores pueden acceder a detalles adicionales sobre el evento, como el tipo de máquina involucrada, el nombre de usuario, la categoría de la aplicación y la valoración proporcionada por la plataforma. Esta funcionalidad permite una mejor comprensión del tráfico y facilita la toma de decisiones informadas en materia de seguridad y cumplimiento. Ver Figura 95.

Figura 95

Detalles de la conexión web



Nota. Vista detallada de un evento de red, mostrando aplicación, destino, ubicación geográfica y metadatos técnicos. Tomado de Netskope tenant.

Observar un evento con mayor detalle permite realizar un análisis más preciso y completo. Esto incluye la capacidad de verificar si el puerto de consulta corresponde a los permitidos por la aplicación, lo cual es crucial para asegurar que el tráfico cumple con las políticas definidas. Además, es posible examinar la dirección IP de origen que realiza la solicitud, así como obtener información detallada sobre la máquina del usuario, como su nombre de host (hostname). Estos parámetros son fundamentales para validar la autenticidad de la petición y asegurar un control riguroso de los accesos. De igual manera, se puede acceder fácilmente a información adicional, como la política que autorizó o denegó el acceso y la cantidad de tráfico permitido durante la sesión o la conexión. Es importante tener en cuenta que,

en este tipo de esquema o topología, los accesos se gestionan y contabilizan por sesiones. El rendimiento del Publisher se ve comprometido únicamente si la cantidad de sesiones TCP o UDP concurrentes supera las 32,000, lo que podría provocar una sobrecarga en su capacidad de procesamiento. Por lo tanto, monitorear y gestionar adecuadamente el número de sesiones es esencial para mantener un desempeño óptimo del sistema.

Categorías de Netskope

Es importante monitorear con frecuencia las categorías de netskope, ya que suelen ser modificadas, agregando nuevos grupos de clasificación o cambiando algunas reglas de categorización. Son un conjunto de clasificaciones que se utilizan para categorizar las aplicaciones y el tráfico web en función de su finalidad y características. Estas categorías se utilizan para establecer políticas de acceso y control de uso de las aplicaciones, así como para detectar y prevenir amenazas de seguridad. En la Tabla 2, se incluyen algunas categorías que continuamente están en edición, para más información diríjase al siguiente enlace: https://docs.netskope.com/en/category-definitions/

Tabla 2

Categorías de Netskope

CATEGORÍA	DESCRIPCIÓN	EJEMPLO URL
Abortion	Web pages that discuss abortion from a historical, medical, legal, or other not overtly biased point of view. Examples are abortion pill, pregnancy termination, fetal abortion etc.	abortion.com, gynpages.com, abortionfacts.com, prochoice.org
Adult Content – Other	Sites with adult content (Sex, Nudity, Gambling,,Gay, Lesbian or Bisexual,Violence) are categorized under this category.	flirtic.rs, mature-sexcontacts.com, frankenladies. de
Adult Content – Pornography	Pornography sites are the ones which allow the portrayal of sexual subject matter.	xvideos.com, youporn.com, chaturbate.com
Advocacy Groups & Trade Associations	Sites that provide information on Industry trade groups, lobbyists, unions, special interest groups and professional organizations.	iso.org, hrw.org, ori.org
Aggressive	Sites that Includes militancy, torture, crime-scene photos, and descriptions or pictures of a violent, bloody or gory nature. Also includes sites that promote	murders.ru, malaprensa.com, alombredelespoir. org

	violence and sedition. Examples are mutilation, crime scenes, massacres etc.	
Alcohol	Web pages that show alcoholic drinks and beers. Examples are whiskey, vodka, ale etc.	thewinecellarinsider.com, johnniewalker.com, carabal.es
App Admin Console	App Admin Console is a collection of apps for which the Netskope NACE can detect administrative actions performed by the app administrator.	NULL
Application Suite	Application Suite indicates that applications listed under this category have multiple products from their respective companies in various other categories.	gsuite.google.com, atlassian.net, axway.com
Arts	Sites that contain creative art judged solely for its intellectual or aesthetic components.	vangoghgallery.com, artble.com, vggallery.com
Auctions & Marketplaces	Sites that discuss on Person to person selling or trading of goods and services through classified, online auctions.	ebay.com, trademe.co.nz, bidorbuy.co.za

Automotive	Sites that provide information about the automotive industry that connects vehicle shoppers with sellers.	ford.com, volvocars.com, mercedes-benz.com
Business	Business sites that contain information on trade, purchase and sale of products or services.	pitneybowes.com, kiewit.com, unilever.com
Business Intelligence and Data Analytics	Business intelligence (BI) sites transform raw data into meaningful and useful information for business analysis purposes. BI technologies can handle large amounts of unstructured data to help identify, develop, and create new strategic business opportunities.	kaggle.com, tensorflow.org, datasciencecentral. com

Nota. Ejemplos de categorías de contenido utilizadas para clasificar y filtrar el tráfico web y de aplicaciones.

Reportes en Netskope

Netskope ofrece una variedad de informes que proporcionan visibilidad y análisis detallados sobre el tráfico de red, las amenazas de seguridad, el cumplimiento de políticas y el uso de aplicaciones en la organización. Estos informes ayudan a los administradores de seguridad a comprender y evaluar el estado de la seguridad y el cumplimiento en la nube, así como a tomar decisiones informadas para proteger mejor los datos y los activos de la empresa. A continuación, se presentan algunos tipos comunes de informes que se pueden generar con Netskope Advanced Analytics:

Informes de actividad y uso de aplicaciones: Estos informes proporcionan información sobre las aplicaciones utilizadas en la red de la organización, incluyendo detalles sobre la cantidad de tráfico, el número de usuarios, el uso de funciones y otras métricas relevantes. Esto ayuda a identificar qué aplicaciones se utilizan más, qué aplicaciones pueden representar un riesgo y permite tomar decisiones informadas sobre las políticas de uso de aplicaciones.

Informes de amenazas y seguridad: Estos informes brindan información sobre las amenazas detectadas y bloqueadas por Netskope, incluyendo malware, phishing, ransomware y otros tipos de ataques. También pueden proporcionar detalles sobre eventos de seguridad, como intentos de acceso no autorizado o violaciones de políticas de seguridad. Estos informes ayudan a comprender el panorama de amenazas y tomar medidas para mitigar riesgos.

Informes de cumplimiento y políticas: Estos informes evalúan el cumplimiento de las políticas de seguridad y cumplimiento establecidas en la organización. Pueden mostrar qué usuarios o grupos de usuarios están cumpliendo o violando las políticas, así como proporcionar información sobre actividades que pueden requerir una revisión o acción adicional. Estos informes son útiles para asegurarse de que se cumplan las políticas internas y las regulaciones externas.

Informes de tráfico y ancho de banda: Estos informes ofrecen información detallada sobre el tráfico de red en la organización, incluyendo la cantidad de datos transferidos, las aplicaciones y servicios que generan el tráfico, y los usuarios o grupos de usuarios que generan el mayor consumo de ancho de banda. Estos informes ayudan a optimizar el rendimiento de la red, identificar posibles cuellos de botella y tomar decisiones informadas sobre la asignación de recursos.

En el siguiente enlace se comparte la guía del fabricante para generar reportes a través de la opción de análisis avanzado. https://docs.netskope.com/en/netskope-help/admin-console/advanced-analytics/

Estos reportes generan gráficas y tablas con la información recopilada por la plataforma. Como el reporte de operaciones y análisis de seguridad que incluye una gráficas, cuadros y tablas con información relevante como: violaciones en políticas de DLP, top de archivos y usuarios, sitios maliciosos entre otra información. Además, estos widgets se pueden personalizar y se pueden combinar para obtener reportes personalizados como muestra la Figura 96.

Figura 96

Reporte de alertas de seguridad

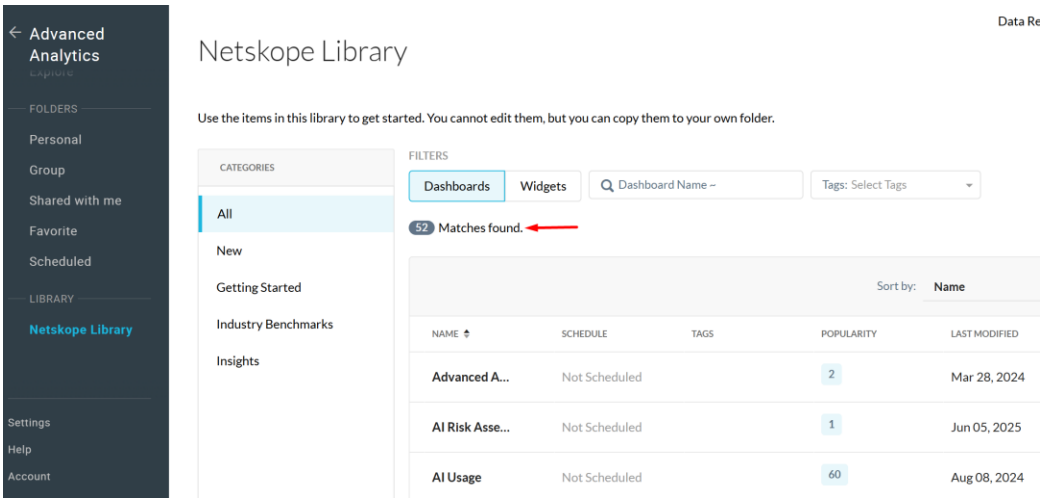
Nota. Vista de un reporte que consolida alertas de seguridad, con opción para exportar en múltiples formatos. Tomado de Netskope tenant.

En la opción que se subraya en la imagen, los tres puntos verticales, se pueden exportar los informes en el formato de preferencia ya sea un archivo. jason, .pdf entre otros. En el dashboard principal se tienen un total de 52 opciones de informes predeterminados y

continuamente se agregan más plantillas, estos se pueden programar periódicamente y se pueden consultar en la sección de “Scheduled”. Ver Figura 97.

Figura 97

Informes predeterminados



Nota. Lista de reportes estándar disponibles en Netskope para auditoría y cumplimiento. Tomado de Netskope tenant.

Conclusiones

Durante la consolidación de este documento, se resaltaron políticas de acceso específicas que demuestran cómo esta capacidad de perfilado y monitoreo mejorado se traduce directamente en la capacidad de diseñar y aplicar políticas que respondan de manera precisa a los requisitos operativos y de seguridad de la organización. En última instancia, esta combinación de análisis detallado y sincronización de grupos permite una gestión de políticas más efectiva y ágil, lo que contribuye directamente a la optimización de la seguridad y la eficiencia operativa en el entorno de red.

La integración de la plataforma Netskope ha representado un avance significativo para la seguridad en la nube de la compañía, es importante mantener el orden de las políticas configuradas, teniendo en cuenta la diferenciación de tráfico que se realiza en el tenant, dándole prioridad al tráfico de aplicaciones que tienen configuradas reglas de DLP. La implementación de políticas de seguridad y cumplimiento ha generado una capa adicional de protección, contribuyendo de manera sustancial a la mitigación de riesgos asociados con posibles fugas de información y amenazas potenciales, donde se incluyó el tráfico No Web para extender el control. A través de estas políticas de seguridad proactivas, se ha fortalecido la defensa de los activos empresariales, asegurando un entorno más resiliente y resistente contra los desafíos emergentes en el panorama de seguridad en la nube.

La herramienta tiene bastantes funcionalidades como se pudo observar durante el proceso de implementación y en lo sintetizado en el documento. Puede parecer compleja la administración de la plaforma, sin embargo, el fabricante ofrece una amplia documentación y el canal de soporte atiende solicitudes complejas, preguntas e incidencias de una manera oportuna.

Las capacidades de personalización y configuración de excepciones permiten a las organizaciones adaptar las políticas de seguridad según sus necesidades operativas y requisitos específicos. Los informes de Advanced Analytics son especialmente útiles para revelar patrones que podrían pasar desapercibidos en análisis superficiales. La aplicación de algoritmos y técnicas avanzadas de análisis de datos ayuda a descubrir correlaciones y causas raíz de eventos, lo que conduce a una comprensión más profunda y precisa de los fenómenos observados.

Es importante revisar detalladamente los logs en la sección de Skope IT antes de realizar ajustes a nivel de políticas o excepciones, es importante que los cambios se realicen primero sobre un grupo de usuarios de pruebas, posteriormente se replican a toda la compañía.

Recomendaciones

Debido a la estructura del banco se debe generar un bypass sobre muchos sitios que empleen SSL, sin embargo, una buena práctica es compartir estos certificados con Netskope y generar la confianza necesaria para que la plataforma de seguridad no restrinja el acceso a estos sitios de vital importancia para la organización. Esto se puede realizar en **Settings > Manage > New Trusted CA > Select file.**

Es fundamental crear Client configuration y Steering Configuration para grupos de red determinados esto facilita el uso de políticas y permite segmentar de cierta manera el tráfico y las reglas que se van a aplicar, no se debe superar el total de cinco (5) Client y Steering, siempre considerando un grupo de pruebas para realizar los ajustes y cambios de configuración previamente. Es importante recargarse en la funcionalidad para obtener una separación de grupos que faciliten la administración.

Netskope permite la configuración de políticas de seguridad personalizadas. Se recomienda aprovechar esta funcionalidad para adaptar las políticas a las necesidades y requisitos específicos de la organización. Esto incluye definir políticas de acceso, bloqueo y protección de datos que reflejen las políticas internas y las regulaciones externas aplicables. Adicionalmente, en la creación de estas políticas se debe priorizar la asignación por grupos y no por usuarios, ya que adicionar más de cinco usuarios a una regla no es practico, por ende, se recomienda organizar los grupos del directorio activo para que sean utilizados en las políticas ya configuradas.

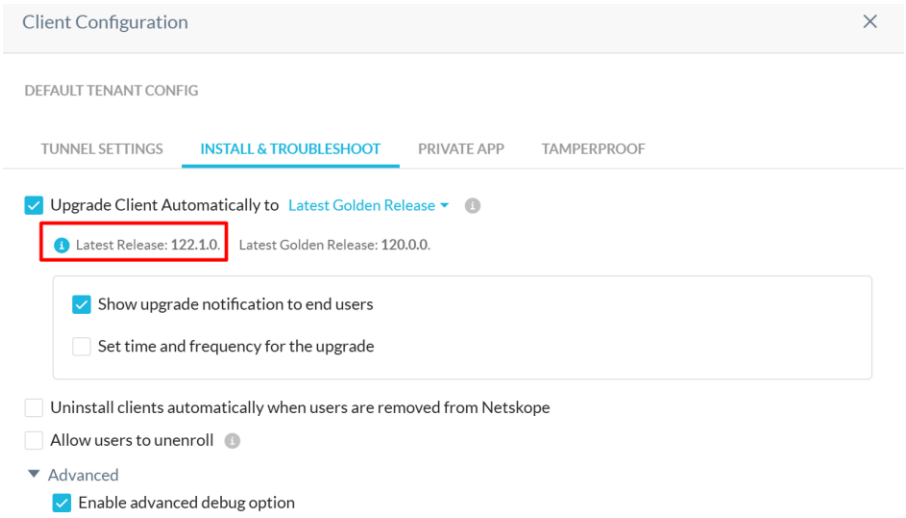
No es recomendable generar excepciones a nivel de usuario en la filtración del tráfico, ya que, Netskope suministra una protección significativa contra amenazas que pueden ser transmitidas en todo el tráfico web.

Antes de proceder con la implementación de una nueva política de control de acceso, es altamente aconsejable realizar una validación exhaustiva del alcance que la herramienta tiene con respecto al aplicativo o categoría específica en consideración. Este análisis se puede llevar a cabo de manera eficiente mediante la funcionalidad de "Search app" en la sección de CCI (Cloud Confidence Index) de Netskope. Al utilizar la opción de "Search app", se obtiene acceso a una valiosa recopilación de información detallada proporcionada por Netskope para el aplicativo en cuestión. Esta información incluye, entre otros aspectos cruciales, los dominios asociados, las actividades soportadas, la calificación CCI, la categoría a la que pertenece, así como información legal pertinente.

Con la opción que suministra Netskope de Cliente Configuration se pueden establecer parámetros de configuración específicos a los clientes, como colocar un password que impida la desinstalación. Una característica que se recomienda es mantener la versión del agente en una distribución Golden, es decir, no tener las actualizaciones programadas a la última versión si no personalizarlas a la penúltima. Se incluye un ejemplo, observe que se especifica la versión y se selecciona la penúltima disponible, esto garantiza un mejor desempeño y evita posibles bugs, sobre todo, en máquinas Mac y Linux. Ver Figura 98.

Figura 98

Configuración de actualizaciones recomendada



Nota. Configuración del cliente para actualizaciones automáticas, notificaciones y protección contra desinstalación. Tomado de Netskope tenant.

Aproveche los identificadores de datos predefinidos de Netskope para detectar información sensible común, como contraseñas, claves privadas y datos codificados en base64. Esto puede simplificar la creación de políticas y mejorar la precisión de la detección. Es importante reconocer que los falsos positivos y negativos son inevitables en las soluciones DLP. Identifique los activos de mayor valor en su organización y construya reglas DLP bien definidas, ajustando los niveles de umbral según los procesos comerciales para minimizar estas incidencias.

El etiquetado de aplicaciones como "Sanctioned" (Autorizadas) en Netskope permite identificar y gestionar de manera efectiva las aplicaciones aprobadas por la organización. Para realizar este etiquetado desde la interfaz del Cloud Confidence Index (CCI), siga estos pasos:

Acceder al CCI: Inicie sesión en la consola de Netskope y navegue hasta la sección del Cloud Confidence Index.

Buscar la Aplicación: Utilice la función de búsqueda para localizar la aplicación corporativa que desea etiquetar.

Evaluar la Aplicación: Revise la puntuación y los atributos de la aplicación proporcionados por el CCI para asegurarse de que cumple con los estándares de seguridad y cumplimiento de su organización.

Etiquetar como "Sanctioned": Una vez evaluada, seleccione la opción para etiquetar la aplicación y asígnela como "Sanctioned". Esto facilitará la aplicación de políticas específicas y el monitoreo de su uso dentro de la organización.

Referencias Bibliográficas

Netskope. (n.d.). Client connection information. Recuperado de https://notskope.com/

Netskope. (n.d.). Community. Recuperado de https://community.netskope.com/

Netskope. (n.d.). Docs. Recuperado de https://docs.netskope.com/

Netskope. (n.d.). Events. Recuperado de https://community.netskope.com/t5/Events/ct-p/events?region=all&language=all

Netskope. (n.d.). Product change notification. Recuperado de https://notify.netskope.com/

Netskope. (n.d.). Recommendations for real time protection policies. Recuperado de https://docs.netskope.com/en/best-practices-for-real-time-protection-policies.html

Netskope. (n.d.). Security checks. Recuperado de https://netskopesecuritycheck.com/

Netskope. (n.d.). Support portal. Recuperado de https://support.netskope.com/s/login/

Netskope. (n.d.). Trust portal. Recuperado de https://trust.netskope.com/