Guía de Seguridad de las TIC
CCN-STIC 1477

Procedimiento de Empleo Seguro
ZScaler ZIA

Noviembre 2025

Edita:

centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2025.10.29 12:15:47 +01'00'

Fecha de edición: Noviembre 2025

ÍNDICE

1. INTRODUCCIÓN

1. Zscaler es una plataforma de seguridad cloud que proporciona un proxy web seguro para proteger a las organizaciones de las amenazas en línea. El proxy de Zscaler se ejecuta en la cloud y conecta a través de un túnel cifrado con los dispositivos de los usuarios, lo que permite a las empresas proteger sus dispositivos y datos mientras los usuarios acceden a Internet. Ofrece varias características de seguridad, incluyendo filtrado de contenido, detección de amenazas, prevención de intrusiones y cumplimiento normativo. El filtrado de contenido ayuda a evitar el acceso a sitios web maliciosos o inapropiados, mientras que la detección de amenazas utiliza técnicas avanzadas de aprendizaje automático para identificar y bloquear las amenazas en tiempo real. La prevención de intrusiones ayuda a proteger contra ataques de red y la violación de datos, mientras que el cumplimiento normativo ayuda a las empresas a cumplir con las regulaciones y estándares de seguridad.
2. El proxy de Zscaler también ofrece características adicionales, como la capacidad de controlar el acceso a aplicaciones y servicios en la cloud, la protección contra el robo de identidad y el filtrado de correo electrónico. También proporciona una visibilidad detallada y un control granular de las actividades en línea de los usuarios, lo que permite a las empresas detectar y abordar rápidamente cualquier actividad sospechosa. Adicionalmente se integra con soluciones de seguridad, como cortafuegos, sistemas de detección de intrusos y sistemas de gestión de amenazas, permitiendo una protección más completa y una respuesta más rápida a las amenazas.

2. OBJETO Y ALCANCE

3. El objeto del presente documento es servir como guía para realizar una instalación y configuración segura de los dispositivos de **Zscaler Work from Anywhere** con la versión cualificada en la Guía CCN-STIC 105 (Catálogo CPSTIC).
4. Este producto se sitúa dentro de la familia de Proxy de la tipología definida por el CCN (CPSTIC) para la categoría ENS MEDIO.

3. ORGANIZACIÓN DEL DOCUMENTO

5. El documento está estructurado en los siguientes apartados:

- **Apartado 4.** Esta sección incluye recomendaciones para tener en cuenta durante la fase previa a la implementación de la solución.
- **Apartado 5**. Esta sección incluye recomendaciones para tener en cuenta durante la fase de instalación de la solución, poniendo foco en las distintas tareas agrupadas para tener en cuenta.
- **Apartado 6.** Esta sección incluye las tareas recomendadas para la fase de configuración y operación de la solución, poniendo foco en el establecimiento de configuraciones seguras
- **Apartado 7.** Incluye el listado de referencias utilizadas en el documento.
- **Apartado 8.** Incluye el listado de las abreviaturas utilizadas en el documento.
- **Anexo A.** Incluye una tabla con las configuraciones por defecto y recomendadas de cada sección del producto.

4. FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

6. Al completar la adquisición de la solución, la persona de contacto establecida recibirá un correo con las credenciales y la URL de acceso a su *tenant*.
7. Al establecer la conexión se le pedirá la modificación de las credenciales administrativas, pudiendo desde entonces crear usuarios administradores adicionales y asignarles permisos y roles de administración adecuados.
8. Zscaler es un proveedor de servicios de conectividad y seguridad Cloud, como tal no requiere de hardware *on premise* para iniciar el proceso de prestación de servicio, sino simplemente la instalación de software *Zscaler Client Connector (ZCC)* y llegado el caso, la creación de túneles encargados de reenviar el tráfico de aquellos dispositivos donde no se puede instalar el agente ZCC, tales como Servidores o dispositivos IoT/OT.
9. El agente *Zscaler Client Connector*, puede descargarse desde el *Client Connector Portal*, accesible desde la consola de administración de ZIA en la opción *Administration / Client Connect App Store / Registered Devices*. Más información en la sección 5 Fase de instalación. Esta actividad es realizada por el administrador, para luego empujar el binario vía herramientas de distribución de software.
10. Para la instalación del agente de Zscaler se pueden utilizar distintos medios, de forma que podemos integrar la instalación del paquete con herramientas como Microsoft Intune, que se encarguen de su distribución y comprobación de la integridad del proceso.
11. Determinadas arquitecturas pueden requerir, la implementación de nodos privados en la infraestructura de la organización, este caso de uso es especial y requiere de la supervisión del equipo de Zscaler que trabajará con la organización en su diseño y arquitectura.

4.2 ENTORNO DE INSTALACIÓN SEGURO

12. Al tratarse el servicio de Zscaler Internet Access (ZIA) de un servicio Cloud, no necesita instalarse dentro del Centro de Procesamiento de Datos (CPD). Para obtener una explicación en profundidad sobre cómo asegurar su organización, consulte la referencia REF 1 - Guía de arquitectura de referencia de Zscaler.

4.3 REGISTRO Y LICENCIAS

13. Zscaler Internet Access (ZIA), como solución SaaS, se licencia de forma general por usuarios durante una periodicidad anual. Para más información consulte la referencia REF 2 - Licenciamiento Zscaler Internet Access.
14. El coste de la licencia puede variar de acuerdo con la edición de ZIA licenciada y el volumen de usuarios que utilizan el servicio.
15. Una vez adquiridas las licencias, las mismas podrán verse desde el portal de administración de la solución (https://admin.zscaler.net/) al que se accederá con las credenciales administrativas.

4.4 CONSIDERACIONES PREVIAS

16. El enfoque principal previamente a la implementación del servicio ZIA debe considerar los siguientes aspectos:

- **Reenvío de tráfico**
  - Definición del diseño y consideraciones relevantes en la configuración de red para garantizar que el tráfico sea redirigido a los Centros de Datos de Zscaler.
  - Consideraciones necesarias para la implementación de Zscaler Client Connector (ZCC) en los dispositivos de los usuarios, aspectos como configuración de la plataforma de distribución de Software, compatibilidad con herramientas presentes en la estación de trabajo tales como Clientes de VPN, corta fuegos personales o soluciones de protección del puesto de trabajo (Antivirus, cortafuegos personal o EDR).
  - Análisis de la infraestructura de red, identificación del flujo en el proceso de navegación, análisis de la capacidad de la infraestructura para la creación de túneles en caso de necesidad.
- **Autenticación (identificación del usuario)**
  - La identidad del usuario es fundamental para Zscaler de forma que la política de seguridad viaje con la identidad del usuario, en esta fase se deben analizar aspectos como los requerimientos de federación de la aplicación Zscaler Internet Access (ZIA) con el proveedor de identidad existente.
- **Aplicación de políticas**
  - Análisis de las políticas a aplicar, excepciones de tráfico, clasificación de URLs, decodificación de tráfico SSL, etc. Todo ello de acuerdo con la identidad del usuario.
- **Informes + registro**
  - Consideraciones asociadas a la herramienta SIEM existente, retención de registros y ubicación de almacenamiento.

17. Consulte la referencia REF 3 - Guía de configuración paso a paso de ZIA, para obtener una lista más detallada de consideraciones previas a la implementación a tener en cuenta.

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

18. El producto requiere los siguientes componentes para una correcta operación:

- **Proveedor de identidad externo / Microsoft Active Directory / LDAP:** Necesario para autenticar los usuarios y comprobar su identidad como elemento contra el cual se asociará la política de seguridad.
- **Sistema de correlación:** Elemento opcional que permite el registro de información en el servidor SIEM local o cloud de la organización.
- **Elementos de comunicación**, que garanticen la comunicación de los usuarios con los servicios Cloud de Zscaler.

5. FASE DE INSTALACIÓN

19. Zscaler es un servicio Cloud, por lo que el número de elementos a implementar es realmente reducido, si bien es cierto existen ciertos componentes que deben ser implementados y otros que deben configurarse para hacer que el servicio ofrecido se integre con la infraestructura de la organización, a continuación, se definen las tareas a tener en cuenta durante el proceso inicial de implementación, consulte la referencia REF 3 - Guía de configuración paso a paso de ZIA, para más información:

- **Aprovisionamiento del Tenant**
  - Actividad realizada por Zscaler como parte de la contratación del servicio.
- **Asociadas a la autenticación y provisión de usuarios**
  - Integración con el sistema de Identidad. Federación de la aplicación Zscaler Internet Access (ZIA) con el IdP corporativo de la organización:
    - Uso del protocolo SCIM para el aprovisionamiento de usuarios y grupos. Consulte la referencia REF 42 – Entendiendo SCIM, para más información.
    - Uso del protocolo SAML Ver. 2.0 para la autenticación de usuarios. Consulte la referencia REF 36 – configuración de SAML, para más información
  - Instalación del agente Zscaler Client Connector (ZCC) en los puestos de trabajo, consulte la referencia REF 4 - Instalación del agente ZCC en el apartado Downloading & Deployment, para más información sobre el proceso de implementación del agente.
    - Comprobación de que se aplican políticas de exclusión de los procesos de Zscaler Client Connector (ZCC) en los servicios de protección del puesto de trabajo (Endpoint Protection, cortafuegos Personal y/o EDR). Consulte la referencia REF 38 – Lista de procesos permitidos, para una explicación más detallada sobre cómo llevarlo a cabo.
    - En el caso de Zscaler Client Connector conviva, en el puesto de trabajo, con un cliente VPN, que ofrezca al usuario acceso a las aplicaciones remotas cuando se encuentre en movilidad, sólo el tráfico destinado a Internet debe ser inspeccionado por ZIA, siendo necesario excepcionar el tráfico destinado a las aplicaciones privadas que serán gestionadas, desde un punto de vista de comunicaciones, por el cliente VPN. Se deberán crear las excepciones correspondientes en ZCC. Consulte la referencia REF 37 - Interoperabilidad entre clientes VPN y Zscaler Client Connector, para más información.
  - Asociadas a la creación de túneles para el tráfico de servidores
    - En caso de querer proteger el tráfico originado por equipos donde no pueda implementarse Zscaler Client Connector (ZCC) tales como Servidores o dispositivos IoT, se recomienda realizar la configuración de túneles IPSec desde los elementos de infraestructura a los centros de datos de Zscaler. Consulte la referencia REF 40 – Configuración de túneles IPSec, para más información.
    - Creación de las reglas de enrutamiento necesarias para reenviar el tráfico de los servidores a los nodos públicos de Zscaler. Consulte la referencia REF

39 - Mecanismos de reenvío de tráfico, para entender los distintos métodos soportados de reenvío del tráfico.

- Asociadas a los ficheros de configuración de Proxy (PAC)
  - Como parte de las reglas de enrutamiento, si el flujo de la conexión a Internet carece de ruta por defecto, configuración de los ficheros proxy PAC correspondientes. Consulte la referencia REF 41 - Uso de ficheros PAC para el reenvío de tráfico, para más información.
- Asociadas a la configuración de Localizaciones
  - Con el fin de poder aplicar políticas granulares a equipos que no pueden ser autenticados, por ejemplo, servidores o usuarios invitados conectándose desde redes Wifi, creación de localizaciones y aplicación de políticas por Localización. Consulte la referencia REF 43, para más información sobre el uso de localizaciones.
- Implementación de los servicios de logging
  - Aprovisionamiento de la máquina virtual NSS (Nano Streaming Log) para el volcado de los logs en el SIEM corporativo. Consulte la referencia REF 8 - guía de aprovisionamiento de NSS, para más información sobre los distintos entornos soportados y proceso de implementación y configuración.
- Preparación del entorno, configuración de Políticas. Revise la sección FASE DE CONFIGURACIÓN y el ANEXO A. RECOMENDACIONES SOBRE PARÁMETROS DE CONFIGURACIÓN, para más información sobre los valores por defecto y recomendados.
  - Definición de las políticas de seguridad asociadas a la inspección de tráfico SSL
  - Definición de las políticas de seguridad y control de acceso basado en nombres de usuario y pertenencia a grupo o localizaciones
  - Definición y aplicación de las políticas de acceso a aplicaciones y categorías en Internet
  - Protección anti-tampering del Agente de Zscaler Cliente Connector (ZCC) garantizando que no pueda ser desactivado
  - Protección en línea de archivos maliciosos, así como desconocidos usando el servicio de Sandbox
  - Protección bidireccional de amenazas Web como XSS, sitios de phishing, etc.

6. FASE DE CONFIGURACIÓN

20. En esta sección se desarrolla los aspectos a configurar en Zscaler Internet Access. Consulte la referencia REF 1 - Guía de arquitectura de referencia y la referencia REF 3 - Guía de configuración paso a paso de ZIA, para más información.

21. Consultar el ANEXO A. Recomendaciones sobre parámetros de configuración para recomendaciones sobre parámetros de configuración del producto.

22. Las políticas por defecto para la protección del tráfico ya han sido pre configuradas por Zscaler, teniendo en cuenta aspectos de seguridad y experiencia de usuario. Estas configuraciones por defecto, con independencia de que puedan ser variadas, se encuentran siempre disponibles en la consola de administración, pudiendo ser visualizadas a través del enlace Recommended Policy.

23. En la siguiente ilustración se muestra marcado en rojo, la opción de mostrar la configuración recomendada.

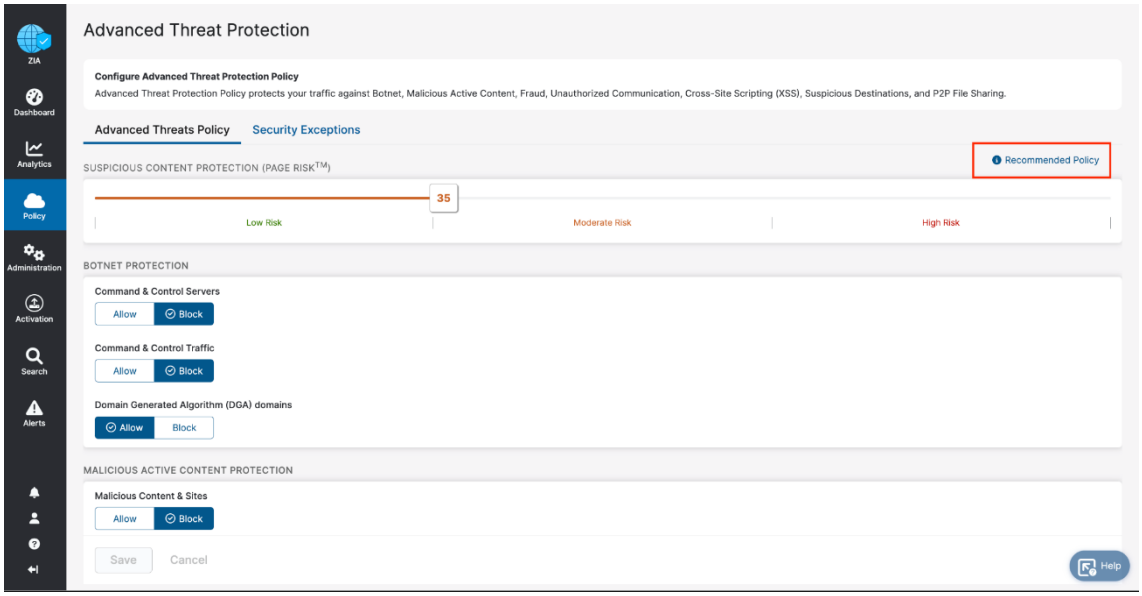

Ilustración 1. Visualización de la configuración recomendada

24. En la siguiente ilustración, se muestra el conjunto de opciones de configuración por defecto recomendadas para la protección contra amenazas avanzadas.

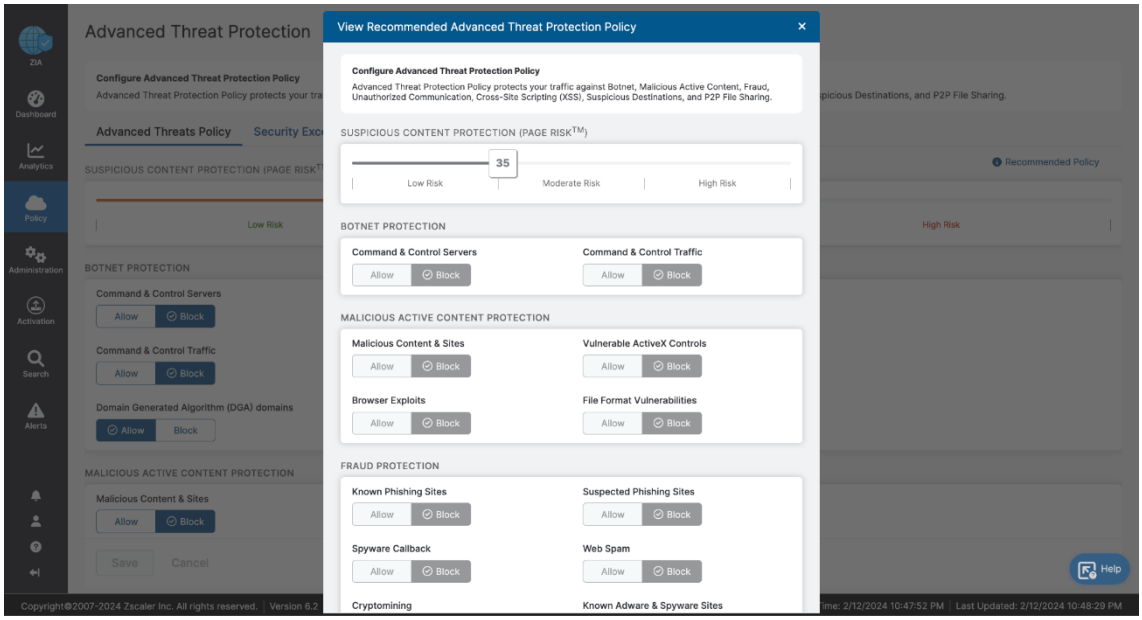

Ilustración 2. Detalle de Configuración recomendada Threat Protection Policy

25. Del mismo modo, todas las secciones de la solución ofrecen una ayuda contextual en línea, pulsando en el botón help ubicado en la esquina inferior derecha, donde se desarrolla en detalle las distintas opciones y en el caso de que aplique la configuración recomendada por defecto.

6.1 AUTENTICACIÓN

26. La identificación de la identidad del usuario es fundamental para la aplicación de políticas que puedan viajar con el usuario independientemente de su localización. Zscaler soporta múltiples métodos de autenticación y verificación de la identidad a continuación se enumeran los más comunes:

- **Federación vía SAML:** Zscaler Internet Access (ZIA) es compatible con todos los proveedores de identidad basados en SAML 2.0
- **Microsoft Active Directory/ LDAP, Secure LDAP**: Zscaler Internet Access (ZIA) es compatible con LDAP para la autenticación e identificación de usuarios, soportando aplicaciones como Microsoft Active Directory o cualquier otro servicio LDAP estándar.
- **Token / One Timelink único:** para las pequeñas empresas, este mecanismo proporciona una manera fácil de enviar un enlace de autenticación o token a la bandeja de entrada de correo electrónico corporativo de los usuarios.
- **Basado en formulario (método no recomendado y por tanto no recogido en esta guía):** Se trata de una autenticación en la que se le presenta al usuario en el navegador un formulario, para que introduzca su usuario y contraseña, estos datos se validan contra la Base de Datos de Zscaler, ya que en este modelo de autenticación no se federa Zscaler Internet Access con ningún proveedor de autenticación externo.
- **Autenticación basada en Kerberos.**

27. Consulte la referencia REF 9 - Métodos de autenticación soportados, para más detalle, así como para revisar otros mecanismos menos comunes de autenticación tales como cookies, etc.

28. Como nota adicional, Zscaler diferencia a los usuarios que navegan a través de Zscaler Internet Access de los administradores encargados de su configuración y mantenimiento, permitiendo, opcionalmente, disponer de IdPs diferenciados. El uso de un proveedor de identidad permite aplicar opciones avanzadas de protección de la identidad a través por ejemplo del uso de múltiples factores de autenticación y mecanismos de fortalecimiento de las credenciales. En la siguiente sección 6.2 administración de Zscaler Internet Access, se desarrolla en más detalle este aspecto.

6.2 ADMINISTRACIÓN DE ZSCALER INTERNET ACCESS

6.2.1 ACCESO A LA INTERFAZ DE ADMINISTRACIÓN

29. La administración del servicio se realiza a través del portal de administración de Zscaler Internet Access (ZIA). Esta aplicación se basa en una interfaz Web accesible vía HTTPS que permite la administración y el mantenimiento del servicio.

30. Consulte la referencia REF 10 - Información sobre el portal de administración, para más información.

31. Para acceder al portal de administración se utilizan los usuarios administradores definidos en el Proveedor de Identidad utilizado por la organización. Zscaler se integra con proveedores de identidad externos que soporten SAML v2, para la validación y el aprovisionamiento de usuarios administradores. En este caso, la solución aplica una validación federada contra el proveedor de identidad asignado, por lo que las credenciales asociadas al usuario administrador no se almacenan localmente en el sistema de información de Zscaler, sino que son gestionadas enteramente por el proveedor de identidad, permitiendo una gestión efectiva de las cuentas administrativas a través del uso de múltiples factores de autenticación tal y como establezca la configuración del proveedor de identidad.

32. Con independencia de lo anterior, determinadas funcionalidades del servicio Zscaler Internet Access (ZIA) pueden ser administradas vía REST API, para ello el sistema utiliza dos posibles mecanismos de autenticación: OAth 2.0, o utilizando las credenciales de un usuario administrador y un API Key/Token de autenticación que se incorporará en la cabecera HTTPS de las subsiguientes llamadas a los distintos endpoints del servicio.

33. Consulte la referencia REF 11 - Llamadas y valores devueltos por la API de ZIA, para entender cómo se desarrollan esas llamadas, así como el proceso de selección OAth 2.0 o usuario y contraseña como metodologías de autenticación contra la API de ZIA.

6.2.2 CONFIGURACIÓN DE USUARIOS ADMINISTRADORES

34. Se recomienda la configuración de roles antes de la creación de usuarios administradores. La administración basada en roles permite controlar qué es lo que los diferentes administradores podrán hacer en la plataforma, permitiendo delegar responsabilidades entre los administradores y estableciendo un control granular que permitirá que las políticas definidas por distintos administradores no entren en conflicto.

35. El detalle de configuración de nuevos usuarios se puede consultar en la referencia REF 44 y en la referencia REF 45, Adición de usuarios administradores y Configuración de Administradores vía SAML respectivamente.
36. Para facilitar la administración basada en roles, cada cuenta de administración se define mediante un role y un ámbito:
    - **El rol** de la cuenta administrador define el conjunto de características disponibles por el administrador en el portal de administración.
    - **El ámbito**, específica las áreas de la organización (por ejemplo, qué departamentos o localizaciones) los administradores tienen permisos, para aplicar los privilegios definidos por su rol.
37. Zscaler ofrece una cuenta de administración por defecto, que ofrece acceso completo al portal de administración y en su ámbito más global. Con la cuenta de administración por defecto se puede:
    - Habilitar o deshabilitar el estado de la cuenta de administración, pero no podemos borrar la cuenta por defecto.
    - Añadir tantos administradores como sean necesarios para cumplir con los requerimientos específicos de la organización.
    - Editar o eliminar cuentas de administrador como sea necesario en cualquier momento.
38. Zscaler permite la adición de hasta 64 roles, en la definición del rol se definirán los permisos funcionales del mismo, es decir tendremos que especificar las características disponibles por cada rol.
39. Consulte la referencia REF 12 - Configuración de roles en ZIA, para más información.
40. Como se ha comentado anteriormente, Zscaler se integra con proveedores de identidad externos como OKTA o Microsoft Azure AD. En estos mismos deberá configurarse una la política de seguridad de contraseñas con los siguientes requerimientos mínimos:
    - Longitud mínima de 12 caracteres.
    - Incluirá mayúsculas, minúsculas, números y símbolos especiales.
    - Número de contraseñas anteriores que no se permite reutilizar: 5.
    - Dos meses como tiempo de expiración de contraseñas.
    - Obligación de cambiar contraseña tras iniciar sesión una vez esta caduque.
    - 10 días deberán transcurrir antes de poder modificar de nuevo una contraseña.

6.2.3 CONFIGURACIÓN DE LA POLÍTICA DE USO ACEPTABLE

41. Zscaler permite definir un mensaje de consentimiento, que le será mostrado al usuario, al iniciar la navegación a través del servicio de Zscaler Internet Access. En este mensaje se le hace saber que la actividad realizada será monitorizada. Como se indica a continuación, esta política de uso aceptable se configura con la frecuencia en la que el mensaje se presentará al usuario y la personalización del mensaje presentado. Las ilustraciones 3 y 4, muestran las opciones de configuración de la política de uso aceptable y la experiencia de uso por parte de los usuarios finales.

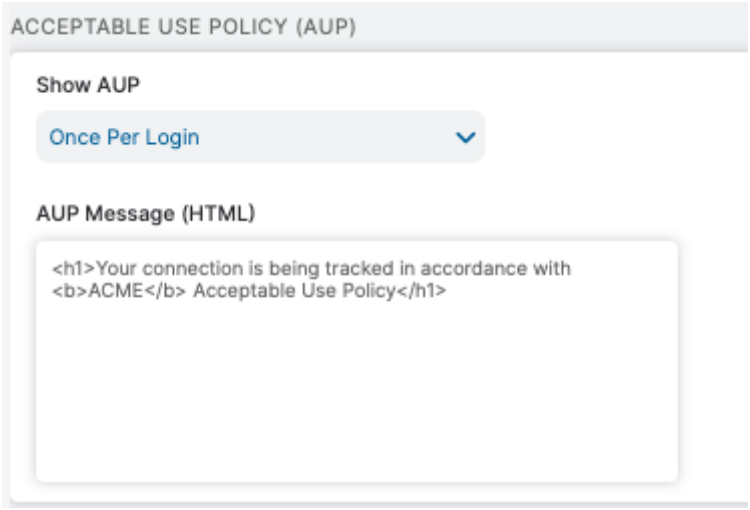

Ilustración 3. Definición de la política de uso aceptable

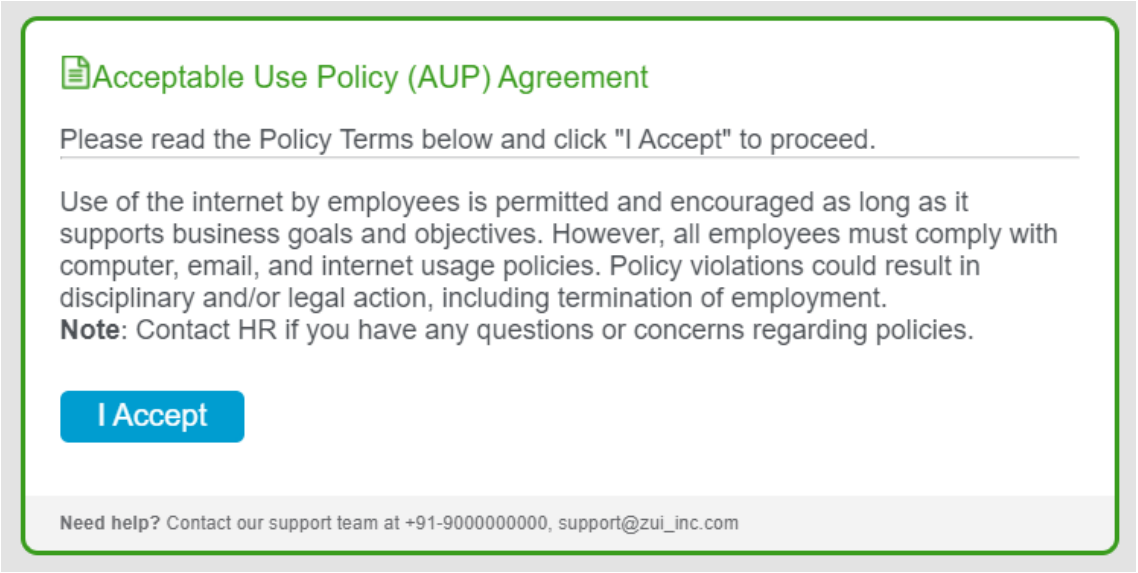

Ilustración 4. Visualización de la notificación de uso aceptable

42. Consulte la referencia REF 14 - Configuración de uso aceptable, para más información.
43. Para configurar la política de uso aceptable, seleccione la opción a Administración > Notificaciones a Usuarios Finales en la consola de Zscaler Internet Access. En la sección Política de uso aceptable (AUP), seleccione mostrar AUP y elija la frecuencia con la que el servicio muestra la página AUP y configúrela en consecuencia. Puede elegir uno de los intervalos predefinidos o personalizar el suyo propio utilizando las siguientes opciones. Se recomienda emplear el valor “una vez por sesión”:
    - Nunca
    - Una vez por sesión
    - Diariamente
    - Semanalmente
    - Una vez por sesión
    - Personalizado

- Día del mes
- Día de la semana

44. El servicio rastrea la hora de aceptación de la AUP y la expiración para cada usuario. El servicio Zscaler establece una cookie AUP cuando un usuario acepta la AUP. Por ejemplo, si selecciona semanalmente, el servicio muestra la página de AUP una semana desde que se estableció la cookie de AUP. Si la cookie de AUP no está presente, el servicio mostrará la página AUP la próxima vez que el usuario inicie sesión.

6.2.4 CONFIGURACIÓN DE LA POLÍTICA DE TIME OUT Y BLOQUEO DE CUENTAS

45. Las sesiones a la consola de administración definen un tiempo predefinido de Time out, momento en el cual el usuario administrador estará forzado a volver a autenticarse, el valor por defecto es 30 minutos, pero puede configurarse entre 5 y 600 minutos. Se recomienda un valor de 5 minutos.

46. Aunque Zscaler se integra con el proveedor de identidad para la gestión de los intentos de autenticación, por defecto la solución bloqueará la cuenta durante 1 minuto, después de 5 intentos de autenticación fallidos, estos parámetros no son configurables.

47. Los eventos asociados a los intentos de autenticación quedarán registrados en el Audit Log de la herramienta, consulte la referencia REF 15 - Acerca de los logs de auditoría, para más información.

6.3 CONFIGURACIÓN DE PROTOCOLOS / ALGORITMOS SEGUROS

48. El producto emplea TLS 1.2 por defecto en las comunicaciones de los administradores con la interfaz de administración y no es necesario llevar a cabo ninguna configuración adicional.

6.3.1 INSPECCIÓN SSL

49. Zscaler, en relación con las **suites de cifrado SSL soportados para la inspección**, soporta inspección basada en hardware con versiones TLS1.3 y 1.2, y también PFS (Perfect Forward Secrecy). Suites de Cifrado en todas las versiones TLS. Para los centros de datos públicos de ZIA, se recomienda la utilización de la versión de TLS más actualizada y de las cipher suites más seguras en el lado de la organización (del esta última al centro de datospúblico de Zscaler). Y también en las conexiones del lado del servidor (centro de datos público de Zscaler al servidor de destino) respectivamente.

50. El detalle de configuración de la inspección SSL se puede consultar en la referencia REF 16 – Inspección SSL.

51. Zscaler soporta inspección TLS 1.3. El detalle de las ciphersuites disponibles se puede consultar en la referencia REF 34 - Ciphersuites soportadas en inspección SSL.

6.3.2 CONFIGURACIÓN SEGURA DE PROTOCOLOS EN EL REENVÍO DE TRÁFICO A ZSCALER

52. Como se ha comentado con anterioridad, existen distintos mecanismos para enviar tráfico a Zscaler para su inspección, revise la referencia REF 39 - Mecanismos de reenvío de tráfico, para más información, los más utilizados son:

- **Zscaler Client Connector (ZCC),** agente ligero que se instala en las estaciones de trabajo y crea un túnel TLS al centro de datos de Zscaler más cercano a su ubicación
- **Túneles GRE / IPSec,** conectividad recomendada para localizaciones fijas como oficinas remotas o headquarters.

53. Zscaler Client Connector, implementa la funcionalidad Túnel 2.0, que consiste en la creación de un túnel DTLS o TLS 1.2, entre la estación de trabajo y el nodo más cercano a la ubicación de la organización, este túnel utiliza el protocolo DTLS por defecto, en el caso de que se desee utilizar TLS 1.2. se deberá modificar el perfil del agente de ZCC de acuerdo con los siguientes pasos:
    - Entrar en el Zscaler Mobile Portal.
    - Ir a la opción Settings y editar el Forwarding Profile aplicado.
    - En la sección Z-Tunnel 2.0 desplegar las opciones haciendo click en Z-Tunnel Transport Settings
    - Finalmente cambiar la selección DTLS por TLS.
54. Estos túneles son creados de forma automática de acuerdo con el perfil de la aplicación que establece los parámetros de geolocalización necesarios para crear túneles contra los centros de datos más cercanos a la ubicación de la organización. Consulte la referencia REF 17 - Mejores prácticas en la implementación de túneles 2.0, para más información.
55. Cuando utilizamos **túneles GRE o IPSec**, realmente se está extendiendo la red de la organización al conjunto de centros de datos elegidos como terminadores de esos túneles. El protocolo GRE no utiliza mecanismos de cifrado, por lo que se recomienda emplear únicamente IPsec.
56. El protocolo IPSec ofrece seguridad a nivel de red para el establecimiento de VPNs, garantizando la confidencialidad, garantizando que la información no pueda ser leída por terceros ajenos al proceso de comunicación, integridad, garantizando que la información no sea adulterada en tránsito y autenticación, verificando la identidad de las partes implicadas en la creación del túnel.
57. Consulte la referencia REF 40 - Configuración de túneles IPSec, para más información sobre como configurar los túneles IPSec.
58. En la referencia REF 35 - Parámetros soportados para la creación de túneles IPSec, se pueden consultar todos los parámetros y algoritmos disponibles. **Se deberá emplear**:
    - Únicamente IKEv2.
    - Grupos Diffie-Hellman: 19, 20 o 21.
    - Cifrado AES-128, AES-192 o AES-256.
    - Algoritmos de integridad SHA-256, SHA-384 o SHA-512.

6.4 GESTIÓN DE CERTIFICADOS

59. El servicio de Zscaler puede inspeccionar el tráfico HTTPS de la organización. Gracias a la decodificación del tráfico SSL en línea, Zscaler puede escanear las transacciones y aplicar políticas de seguridad a los datos transmitidos. Funciona como un completo proxy SSL

man-in-the-middle (MITM). Para llevar a cabo esta inspección, el producto hace uso de certificados.

60. En el proceso de inspección SSL, Zscaler tiene dos opciones: o bien utiliza un certificado intermedio firmado por Zscaler o un certificado intermedio personalizado firmado por la CA de confianza de la organización.

61. Se recomienda emplear certificados firmados por una CA de confianza. El detalle de configuración de los certificados empleados en la Inspección SSL se puede consultar en la referencia REF 21 - Configuración de la inspección SSL. En las referencias REF 19 - Configuración de CAs intermedias y REF 20 - Configuración de cloud HSM se encuentran los pasos para la configuración de certificados intermedios.

62. Se deberán emplear los siguientes parámetros:

- **Key size**: emplear una longitud de clave de, al menos, 3072 bits.
- **Signature algorithm:** el valor por defecto es SHA-256. Se deberá emplear este valor o superiores.

63. Consulte la referencia REF 21 - Configuración de la inspección SSL para más información.

64. El resto de las comunicaciones en las que intervienen certificados son:

- **Comunicación entre el navegador de los administradores y la consola de administración:** Zscaler es un proveedor SaaS que ofrece su servicio SSE a través de una plataforma multi-tenant, el certificado por tanto presentado al navegador es un certificado propiedad de Zscaler y mantenido por Zscaler. No se requiere por tanto ninguna configuración por parte de la organización, no obstante, como se comenta en el apartado 6.3.1 INSPECCIÓN SSL el servicio multi-tenant de Zscaler es compatible con versiones de TLS 1.2 – 1.3, por lo que es recomendable configurar del lado del navegador el nivel de TLS más alto posible para negociar una sesión segura.
- **Comunicación entre los centros de datos públicos de Zscaler y un proxy de terceros (Proxy Chaining):** En este caso Zscaler permite la incorporación de certificados raíz del servicio de proxy de terceros, para firmar con él los certificados MITM generados, consulte la referencia REF 46 – Acerca de certificados raíz para más información.
- **Uso de sesiones de aislamiento:** Uno de los mecanismos de protección contra ciber-amenazas y fugas de información empleados por Zscaler es el uso de sesiones de aislamiento, estas consisten en llevar todo el contenido activo de la navegación a una instancia de aislamiento que corre en los centros de datos públicos de Zscaler de forma que el navegador del usuario sólo recibe un stream de pixeles, relativos al contenido activo que se ejecuta en el entorno aislado. Esta sesión de aislamiento corre una instancia del navegador Chromium, que utiliza conexiones seguras para su comunicación con los centros de datos públicos de Zscaler siendo posible la opción de uso de certificados raíz distintos al de Zscaler, la referencia indicada anteriormente REF 46 – Acerca de certificados raíz, aporta más información al respecto.
- **Comunicación entre ZCC y los nodos públicos de Zscaler:** Zscaler Client Connector utiliza túneles DTLS o TLS para conectar al centro de datosr público de Zscaler más cercanos a la localización de la organización, estos túneles se encuentran cifrados, utilizando para ello certificados que son completamente gestionados por el servicio de Zscaler. Una vez que el túnel se ha creado, para el tráfico de navegación aplica la

información presente en los apartados 58-62 con respecto a la posibilidad de utilizar los certificados por defecto de Zscaler o los de la organización para la inspección de tráfico SSL.

6.5 TIEMPO Y SINCRONIZACIÓN

65. **Se recomienda que todos los sistemas utilizados por la organización se encuentren sincronizados** para permitir una alta fiabilidad en los sistemas de auditoría y logging.
66. En el caso de que Zscaler requiera de alguna máquina local para el desarrollo de sus funciones, esta debe estar correctamente configurada en términos de sincronización horaria.
67. Zscaler utiliza el protocolo Network Time Protocol (NTP) para la sincronización horaria en todos sus componentes de infraestructura. Aquellos dispositivos locales necesarios utilizarán el siguiente procedimiento para la configuración de un servidor NTP local:
    - Ejecutar el siguiente comando como root crontab -e
    - Añadir la siguiente línea: */10 * * * * ntpdate <ntp-server-name>. Reemplazar <ntp-server-name> por el FQDN o la dirección IP del servidor NTP local
    - Grabar los cambios. La línea añadida en el editor del servicio crond se ejecutará cada 10 minutos.
68. Consulte la referencia REF 22 - Configuración NTP server, para más información.

6.6 ACTUALIZACIONES

69. Todos los procesos de actualización o instalación de parches relativos al servicio corren por la cuenta de Zscaler y resultan transparentes para el usuario final. El único componente, ubicado en la estación de trabajo, que tiene que ser actualizado, es el agente Zscaler Client Connector. Este agente, de acuerdo con la política establecida, se actualiza de forma automática y transparente para el usuario final, empujándose la nueva versión, en el siguiente periodo de conexión del agente con el servicio de Zscaler. Llegado el caso el usuario puede acortar ese tiempo forzando manualmente la descarga de la nueva versión definida. Para forzar la conexión del agente con el servicio de Zscaler y aplicar la actualización del agente disponible, el usuario deberá ir a la pestaña “more” del agente instalado en su dispositivo y seleccionar “update app”.

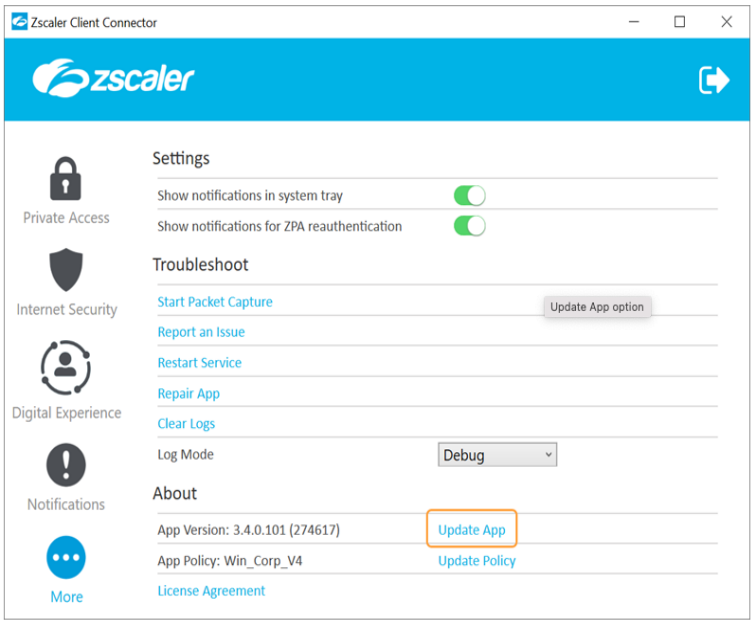

Ilustración 5. Visualización de la opción de actualización manual en ZCC

70. La definición de las políticas asociadas al mantenimiento del agente se realiza desde la consola de administración en la opción Administration / Client Connector App Store / Add configuration desde esta sección se definirá la política relativa al mantenimiento del agente para cada uno de los sistemas operativos soportados.

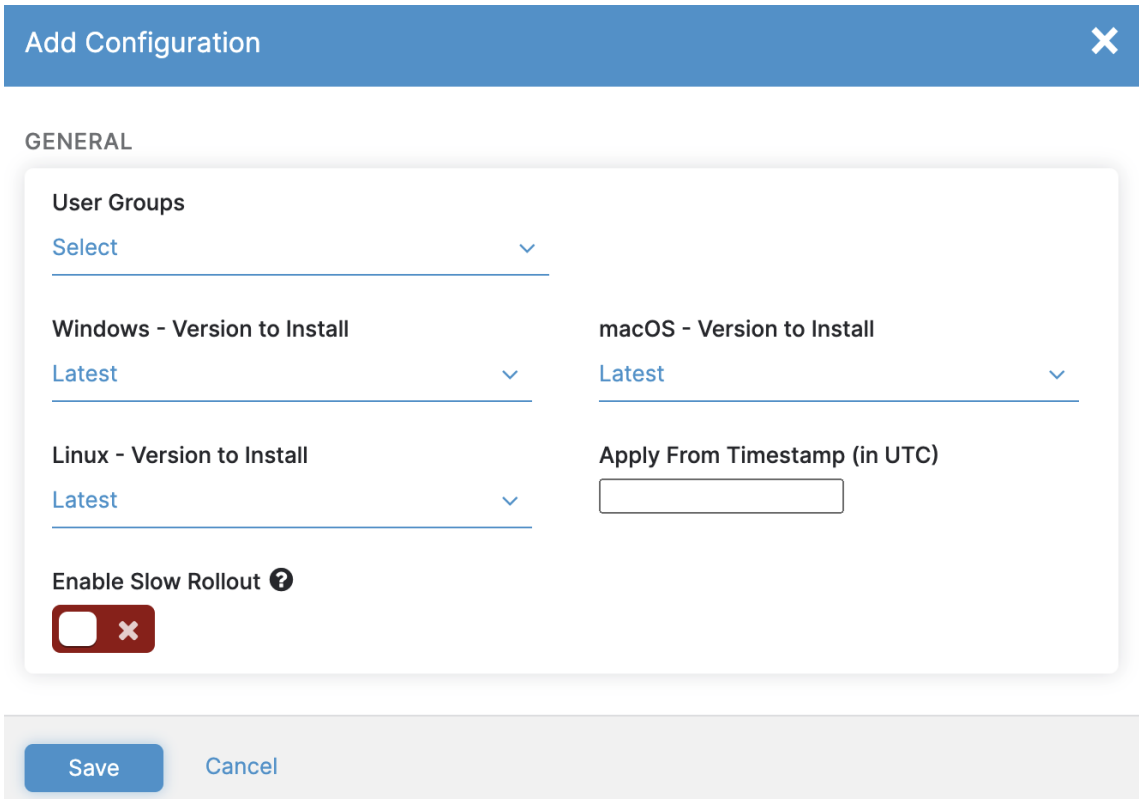

Ilustración 6. Visualización de las opciones de mantenimiento del agente

6.7 SNMP

71. Como servicio Cloud, Zscaler rara vez implementa infraestructura on-premise que requiera de monitorización SNMP v3, si bien es cierto, servicios como los nodos privados o la máquina virtual Nanolog Streaming Service (NSS) comentados en distintas secciones en el documento pueden ser monitorizados mediante MIBs SNMP.

72. El servidor SNMP, las credenciales y los aspectos de seguridad se configuran conectando con el servidor NSS y ejecutando el comando snmp-admin-configure.

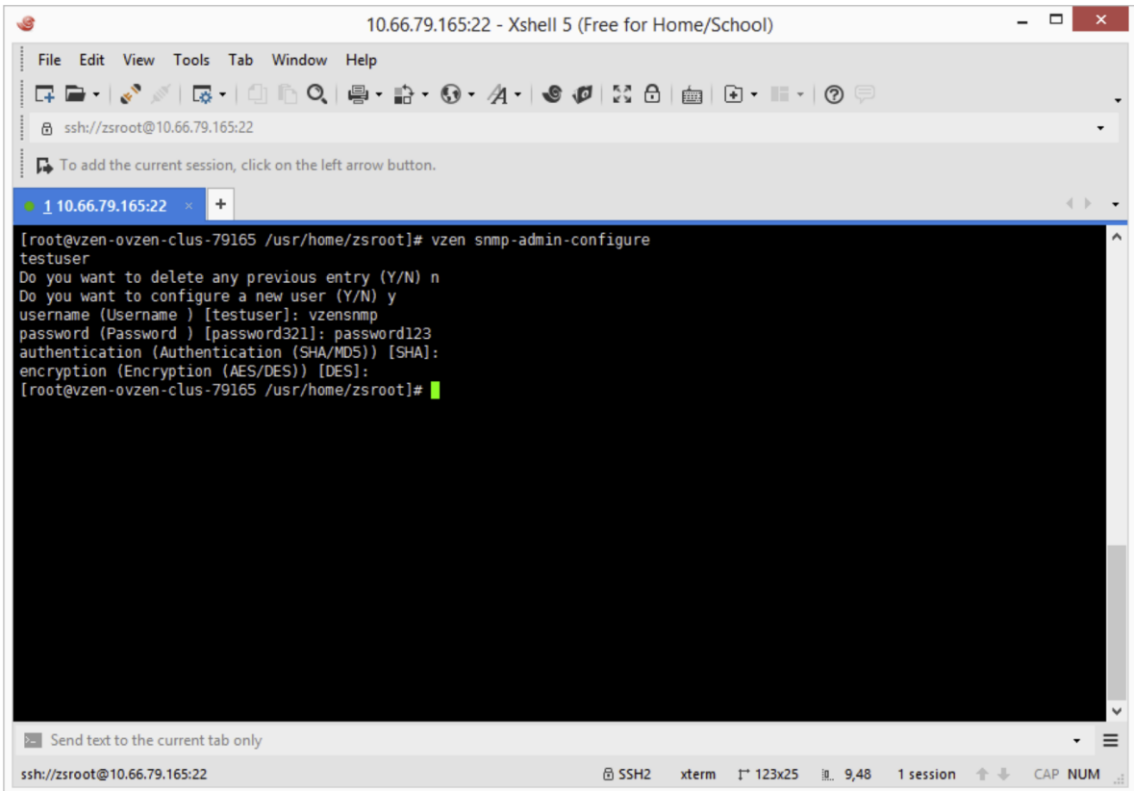

Ilustración 7. Visualización de las opciones de configuración del servicio SNMP

73. Consulte la referencia REF 22 - Zscaler SNMP MIBs, para más información sobre el proceso de carga y monitorización SNMP.

6.8 ALTA DISPONIBILIDAD

74. La arquitectura de Zscaler está diseñada para garantizar una redundancia y resiliencia completa sin puntos de fallo manteniendo nuestro acuerdo de nivel de servicio (SLA) de 99,999%.

75. La creación de un entorno de disponibilidad de cinco 9s es una responsabilidad compartida entre la organización y Zscaler. Por parte de Zscaler, se incorporan mecanismos BGP que permiten enrutar tráfico de un centro de datos a otro en función de parámetros de disponibilidad, por parte de la organización será necesario crear túneles primarios y secundarios a los centros de datos más cercanos a la ubicación de la organización para garantizar el tráfico en caso de degradación de los enlaces de los proveedores de comunicaciones que conectan la organización con los centros de datos de Zscaler.

76. Consulte la referencia REF 23 - Configuración de las funcionalidades de recuperación ante desastres, para más información.

6.9 AUDITORÍA

6.9.1 REGISTRO DE EVENTOS

77. **Logging – Nanolog Streaming Service (NSS):** El servicio Zscaler proporciona la consolidación de registros en tiempo real en todo el mundo, para que pueda ver todas las transacciones realizadas por sus usuarios, independientemente de la ubicación del centro de datos que aplica la política. Los registros se almacenan durante 180 días.

78. El servicio Nanolog Streaming Service (NSS) utiliza una máquina virtual (VM) para transmitir registros de tráfico en tiempo real desde Zscaler a su sistema de gestión de eventos e información de seguridad (SIEM), como por ejemplo Splunk o Microsoft Sentinel, lo que permite alertas en tiempo real y la correlación con los registros de información de otras soluciones ayudando a cumplir de este modo con los requerimientos normativos aplicables. Zscaler ofrece las siguientes suscripciones NSS:

    - NSS for Web: Transmite registros de tráfico web y móvil.
    - NSS for Firewall: Transmite los registros asociados al cortafuegos y al control DNS.

79. Documentación adicional sobre la configuración del servicio Nanolog Streaming Service (NSS). Consulte las siguientes referencias para más información:

    - REF 24 - Documentación asociada servicio NSS
    - REF 25 - Requerimientos de instalación servicio NSS
    - REF 26 - Requerimientos de comunicaciones servicio NSS
    - REF 27 - Guía de configuración NSS y Data Feeds
    - REF 28 - Resolución de incidencias NSS
    - REF 29 - Monitorización de los nodos NSS

80. **Esquema de los Logs generados**: Zscaler ofrece múltiples servicios de seguridad tales como, protección de la navegación con URL filtering, control de Aplicaciones SaaS, protección contra amenazas, corta fuegos de capa 7, control DNS, etc. cada uno de estos componentes genera un log enriquecido que permite la triangulación de los eventos. Estos logs, como se ha comentado anteriormente, son almacenados por Zscaler durante 180 días y se ofrecen herramientas para poder enviarlos a herramientas tipo SIEM existentes.

81. En la sección Insights de la consola de administración de Zscaler Internet Access, podemos obtener los siguientes tipos de registros de información:

    - **Web:** Permite monitorizar las transacciones generadas por cualquier dispositivo (ejemplo. Windows, Mac, IOS, Android, Linux)
    - **Mobile:** Permite ver las transacciones iniciadas por los browsers de dispositivos móviles.
    - **Firewall:** Permite ver detalles, tales como la regla aplicada, los detalles del cliente y servidor y los servicios de red y aplicaciones.

- **DNS:** Peticiones y respuestas DNS
- **Túnel:** Información sobre los túneles establecidos GRE o IPSec, mostrando salud, estado, autenticación y algoritmos de cifrado utilizados.

82. Insights permite la creación de vistas y filtros por cada uno de los campos disponibles en el registro de información capturado. Consulte la referencia REF 30 - Web insights logs filters, para más información sobre los distintos campos capturados y disponibles para filtrar

83. Desde el punto de vista de procesamiento de los logs, Zscaler soporta formatos de log ASCII, y puede transformarlos a cualquier tipo de formato aceptado por el SIEM de la organización o el servidor Syslog utilizado. Las RFC 5424 y la RFC 3164 desarrollan dos de los tipos de syslog soportados, con independencia de lo anterior, Zscaler permite alterar el formato de salida de los logs a formatos tipo Common Event Format (CEF) o Log Event Extended Format (LEEF) por mencionar dos de los formatos más extendidos en su uso en SIEMs comerciales.

84. A continuación, se muestra un ejemplo del formato de logs enviados desde Zscaler al NSS (Nano Streaming Log Service).

    "%s{time}","%s{login}","%s{proto}","%s{eurl}","%s{action}","%s{appname}","%s{appclass}","%d{reqsize}","%d{respsize}","%s{urlclass}","%s{urlsupercat}","%s{urlcat}","%s{malwarecat}","%s{threatname}","%d{riskscore}","%s{dlpeng}","%s{dlpdict}","%s{location}","%s{dept}","%s{cip}","%s{sip}","%s{reqmethod}","%s{respcode}","%s{ua}","%s{ereferer}","%s{ruletype}","%s{rulelabel}","%s{contenttype}","%s{unscannabletype}","%s{deviceowner}","%s{devicehostname}","%s{keyprotectiontype}"\n

6.9.2 ALMACENAMIENTO LOCAL Y REMOTO

85. Los registros de información generados se almacenan en los Clusters Nanolog de Zscaler durante 180 días, pasado este tiempo los registros serán borrados.

86. Zscaler ofrece la posibilidad de exportar estos registros de información a herramientas externas para cumplir con los requerimientos normativos en cuanto a retención de la información establecidos.

87. En la siguiente ilustración se muestran los componentes que intervienen en la integración con un servidor externo tipo Syslog/SIEM ubicado en las instalaciones de la organización (on-prem).

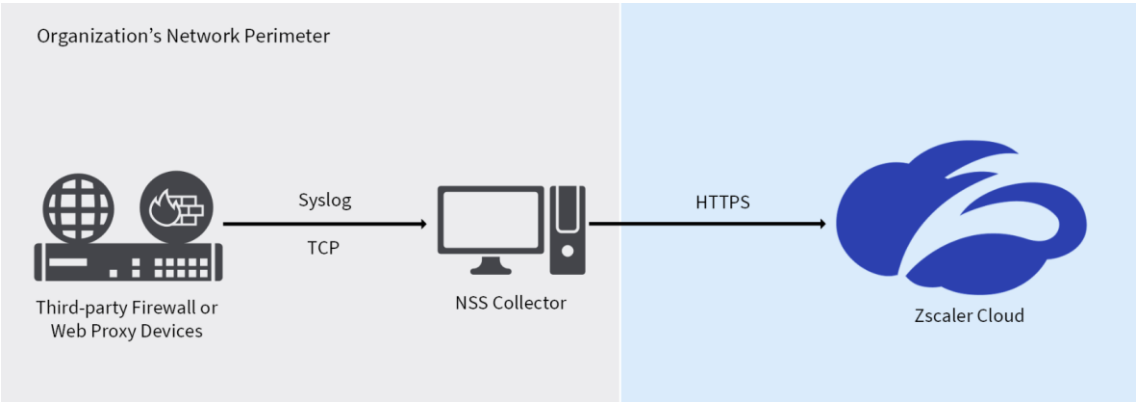

Ilustración 8. Componentes que intervienen en la comunicación con un servidor SIEM externo

88. El proceso consiste en la instalación de un NSS Collector en las instalaciones de la organización. El NSS Collector se suministra como una máquina virtual que deberá implementarse en la infraestructura de computación virtual de la organización. Una vez implementado, se debe configurar en la consola de ZIA un servidor NSS, a través del uso de una clave compartida.

89. La conexión entre el centro de datos de Zscaler y el servidor NSS Collector es es TLS v1.2. La conexión, on-prem entre el NSS Collector y el servidor Syslog es una conexión en claro UDP/TCP. Debido a esto, se recomienda instalar el NSS Collector en la misma red local que el servidor Syslog, o emplear túneles IPsec para el envío de la información.

90. Por último, se establecerá un feed de información, que indicará el tipo de información que se enviará al servidor NSS de acuerdo con los criterios y filtros establecidos.

91. Consulte las referencias REF 31 - Adición de servidores NSS y REF 32 - Entendiendo el servicio Nano Streaming Log Service, para más información sobre el procedimiento de implementación, de un servidor NSS, en función del tipo de hipervisor utilizado y como integrar el servicio NSS con un servidor Syslog externo.

92. Adicionalmente a lo indicado en los párrafos anteriores (párrafos 86 a 90), para aquellas organizaciones que utilicen servidores SIEM Cloud, como por ejemplo Splunk Cloud o Microsoft Sentinel entre otros, Zscaler soporta comunicaciones Cloud to Cloud, consulte la referencia REF 47- Integración con servidores SIEM Cloud, para acceder a las guías de referencia para la integración con los distintos proveedores soportados. En este caso la comunicación entre el centro de datos de Zscaler y el SIEM Cloud se realiza mediante comunicaciones HTTPS basadas en comunicaciones API.

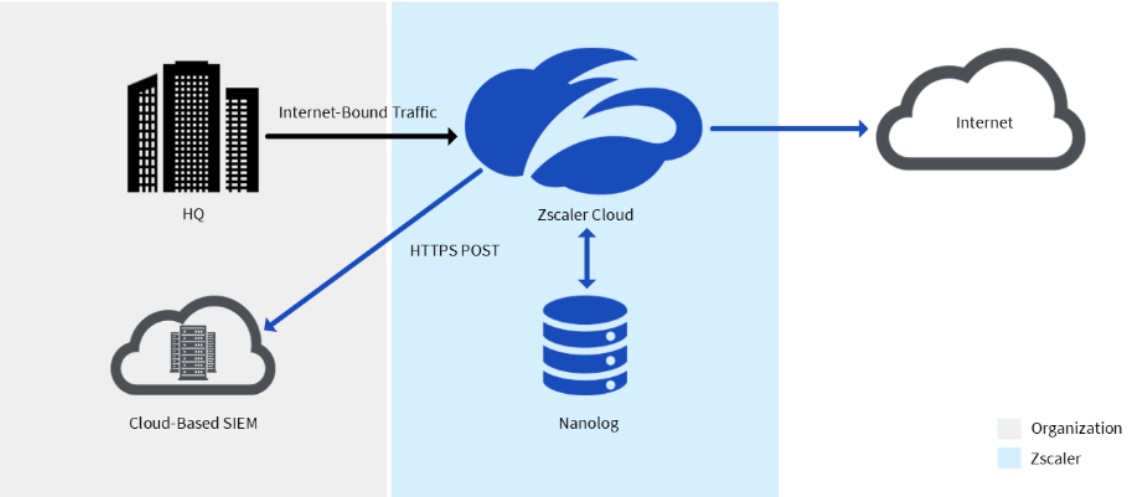

Ilustración 9. Componentes que intervienen en la comunicación con un servidor SIEM cloud y Zscaler

6.10 COPIA DE SEGURIDAD

93. Zscaler permite la creación de una copia de seguridad de políticas y opciones de configuración y restaurarla utilizando un punto de restauración en el tiempo. El punto de restauración representa el momento en el que la acción de copia de seguridad fue realizada y permitirá restaurar las políticas en ese punto concreto. Las copias de seguridad pueden automatizarse estableciendo una frecuencia concreta o bajo demanda utilizando el portal de administración de Zscaler Internet Access (ZIA).

94. Es importante señalar que cuando se restauran políticas y opciones de configuración, se sobrescriben las políticas y configuraciones existentes.
95. Se deberán llevar a cabo copias de seguridad periódicas de la configuración del producto.
96. Consulte la referencia REF 33 - Acerca de la función de backup y restore, para más información sobre la lista de políticas y reglas, así como opciones de configuración.

7. REFERENCIAS

97. A continuación, se muestran las referencias externas realizadas en este documento.

REF 1 Guía de arquitectura de referencia de Zscaler

REF 2 Licenciamiento Zscaler Internet Access

REF 3 Guía de configuración paso a paso de ZIA

REF 4 Instalación del agente ZCC

REF 5 Sistemas operativos soportados en ZCC e instalación

REF 6 Gestión de usuarios y configuración de la autenticación

REF 7 ZCC *Firewall Configuration*

REF 8 Guía de aprovisionamiento de NSS

REF 9 Métodos de autenticación soportados

REF 10 Información sobre el portal de administración

REF 11 Llamadas y valores devueltos ZIA API

REF 12 Configuración de roles en ZIA

REF 13 Configuración de los usuarios administradores en OKTA

REF 14 Configuración de uso aceptable

REF 15 Acerca de los logs de auditoria

REF 16 Inspección SSL

REF 17 Mejores prácticas en la implementación de túneles 2.0

REF 18 Determinando el MTU óptimo para túneles GRE/Ipsec

REF 19 Configuración de CAs intermedias

REF 20 Configuración de cloud HSM para la protección de certificados

REF 21 Configuración de la inspección SSL

REF 22 Configuración NTP *Server*

REF 23 Configuración de las funcionalidades de recuperación ante desastres

REF 24 Documentación asociada servicio NSS

REF 25 Requerimientos de instalación servicio NSS

REF 26 Requerimientos de comunicaciones servicio NSS

REF 27 Guía de configuración NSS y *Data Feeds*

REF 28 Resolución de incidencias NSS

REF 29 Monitorización de los nodos NSS

REF 30 *Web insights logs filters*

REF 31 Adicción de servidores NSS

REF 32 Entendiendo el servicio *Nano Streaming Log Service*

REF 33 Acerca de la función de *backup* y *restore*

REF 34 Ciphersuites soportadas en inspección SSL

REF 35 Parámetros soportados para la creación de túneles IPSec

REF 36 Configuración de SAML

REF 37 Interoperabilidad entre clientes VPN y Zscaler Client Connector

REF 38 Lista de procesos permitidos

REF 39 Mecanismos de reenvío de tráfico

REF 40 Configuración de túneles IPSec

REF 41 Uso de ficheros PAC para el reenvío de tráfico

REF 42 Entendiendo SCIM

REF 43 Acerca de localizaciones

REF 44 Adición de usuarios administradores

REF 45 Configuración de administradores vía SAML

REF 46 Acerca de certificados raíz

REF 47 Integración con servidores SIEM *Cloud*

REF 48 Acerca de la funcionalidad *Admin Rank*

REF 49 Acerca del cumplimiento CIPA

REF 50 Creación de políticas para usuarios no autenticados

REF 51 Listado de aplicaciones ancladas

8. ABREVIATURAS

ZIA	Zscaler Internet Access
ZCC	Zscaler Client Connector
IoT	*Internet of Things* (Internet de las cosas)
OT	*Operational Technology* (Tecnología operacional)
CPD	Centro de Proceso de Datos
URL	*Uniform Resource Locator* (Localizador de recurso uniforme)
SaaS	*Software As a Service* (Software como servicio)
VPN	*Virtual Private Network* (Red Privada virtual)
SSL	*Secure Sockets Layer* (Capa seguridad de conexión)
LDAP	*Lightweight Directory Access Protocol* (Protocolo ligero de acceso a directorios)
SIEM	*Security Information and Event Management* (Información de seguridad y gestión de eventos)
IdP	*Identity Provider* (Proveedor de Identidad)
SCIM	*System for Cross-Domain Identity Management* (Sistema para la gestión de identidades entre dominios)
SAML	*Security Assertions Markup Language* (Lenguaje de marcado de afirmaciones de seguridad)
EDR	*Endpoint Detection and Response* (Detección y respuesta en el puesto de trabajo)
GRE	*Generic Routing Encapsulation* (Encapsulación de rutado genérico)
IPSec	*Internet Protocol Security* (Seguridad de protocolo Internet)
PAC	*Proxy Automatic Configuration* (Configuración de proxy automática)
NSS	Nano Streaming Log Service
XSS	*Cross-Site Scripting* (Secuencia de comandos entre sitios)
FIPS	*Federal Information Processing* Standard (Estándar federal de procesamiento de información)
RSA	Rivest, Shamir, & Adleman
Rest API	*Representational State Transfer* (Transferencia de estado representacional)
Oath	*Open Authentication* (Autenticación abierta)
API	*Application Programming Interface* (Interfaz de programación de aplicaciones)
HTTP	*Hypertext Transfer Protocol* (Protocolo de transferencia de hipertexto)
HTTPS	*Hypertext Transfer Protocol Secure* (Protocolo seguro de transferencia de hipertexto)
TLS	*Transport Layer Security* (Seguridad en la capa de transporte)
AUP	*Acceptable Use Policy* (Política de uso aceptable)
PFS	*Perfect Forward Secrecy* (Reenvío perfecto de secretos)
ECDHE	*Elliptic Curve Diffie-Hellman* (Curva elíptica Diffie-Hellman)
ECDSA	*Elliptic Curve Digital Signature Algorithm (*Algoritmo de firma digital de curva elíptica)
EXP	*Equal Erasure Protection* (Protección contra borrado)
DSS	*Data Security Standard* (Estándar de seguridad de Datos)

RC4	*Ron's Code 4* (Algoritmo de cifrado de clave variable desarrollado por Ron Rivest)
MD5	*Message Digest 5 Algorithm* (Algoritmo de resumen de mensajes)
DES	*Data Encryption Standard* (Algoritmo de cifrado de datos estándar)
CBC	*Cipher Block Chaining* (Encadenamiento de bloques de cifrado)
3DES	*Triple Data Encryption Standard* (168 *Bit*) (Algoritmo estándar de cifrado triple)
IKE	*Internet Key Exchange* (Intercambio de claves por Internet)
AES	*Advanced Encryption Standard* (Algoritmo estándar de cifrado avanzado)
SHA	*Secure Hash Algorithm* (Algoritmo de firma seguro)
GCM	*Galois/Counter Mode* (Modo Galois Contador)
PSK	*Pre-Shared Key* (Clave previamente compartida)
AH	*Authentication Header* (Cabecera de autenticación)
ESP	*Encapsulating Security Payload* (Encapsulado seguro de información)
MITM	*Man in the Middle* (Hombre en el medio)
CA	*Certified Authority* (Autoridad certificadora)
HSM	*Hardware Security Module* (Módulo de seguridad Hardware)
NTP	*Network Time Protocol* (Protocolo de red horario)
FQDN	*Fully Qualified Domain Name* (Nombre de dominio completo)
SNMP	*Simple Network Management Protocol (*Protocolo de gestión de red simple)
MIB	*Management Information Base* (Información de gestión base)
SLA	*Service Level Agreenment* (Acuerdo de nivel de servicio)
BGP	*Border Gateway Protocol* (Protocolo fronterizo)
DC	*Data Center* (Centro de Datos)
VM	*Virtual Machine* (Máquina Virtual)
DNS	*Domain Name Service* (Servicio de nombres de dominio)
ASCII	*American Standard Code for Information Interchange* (Código Estándar Americano para Intercambio de Información)
RFC	*Request for Comments* (Solicitud de comentarios)
CEF	*Common Event Format* (Formato de eventos común)
LEEF	*Log Event Extended Format* (Formato extendido de eventos de registro)
DLP	*Data Loss Prevention* (Prevención de fugas de información)
FTP	*File Transfer Protocol* (Protocolo de transferencias de ficheros)
IPS	*Intrusion Prevention System* (Sistema de prevención de intrusiones)
EUN	*End User Notification* (Notificación de usuario)
UCaaS	*Unified Communications as a Service* (Comunicaciones Unificadas como servicio)
DPI	*Deep Packet Inspection* (Inspección profunda de paquetes)
CIPA	*Children's Internet Protection Act* (Ley de protección infantil en Internet)
OCSP	*Online Certificate Status Protocol* (Protocolo para la comprobación del estado de los certificados en línea)
SSE	*Security Service Edge* (Perímetro de Servicio de Seguridad)
P2P	*Peer to Peer* (Comunicación punto a punto)

ANEXO A. RECOMENDACIONES SOBRE PARÁMETROS DE CONFIGURACIÓN

98. Recomendaciones de seguridad: Security | Malware Protection

Configuración	Recomendación	Valor por defecto	Razón
Inspección de Tráfico	Entrante: Habilitar Saliente: Habilitar	Entrante: Habilitado Saliente: Habilitado	Zscaler inspecciona los archivos subidos (salientes) o descargados (entrantes).
Inspección de protocolo	Inspeccionar HTTP: Habilitar	Inspeccionar HTTP: Habilitado Inspeccionar FTP a través de HTTP: Habilitado Inspeccionar FTP: Deshabilitado	Inspecciona los archivos subidos o descargados vía HTTP, HTTPS, FTP y FTP vía HTTP
Protección contra *malware*	Bloquear todo	Bloquear todo	Bloquea distintos tipos de subidas/descargas de archivos categorizados como *malware*
Protección contra *adware/spyware*	Bloquear todo	Bloquear todo	Bloquea la carga o descarga de paquetes de *spyware* o *adware*
Excepciones de seguridad: archivos protegidos con contraseña	Bloquear Elección: TBD	No establecido	Los archivos ZIP y RAR protegidos con contraseña están permitidos de forma predeterminada. Haga *clic* en Bloquear para evitar que los usuarios carguen o descarguen estos archivos.
Excepciones de seguridad: archivos que no se pueden analizar	Bloquear Elección: TBD	No establecido	Es posible que el servicio no pueda analizar algunos archivos debido a un formato de archivo no reconocido, un tamaño excesivo o una compresión recursiva. Esta opción le permite bloquear dichos archivos no escaneables
Excepciones de seguridad: No analizar el contenido de estas direcciones URL	Configurar las excepciones necesarias	No establecido	Hay varias aplicaciones/servicios financieros que cargan archivos protegidos por contraseña y/o encriptados. Asegúrese de agregar excepciones para esos sitios web por dominio o nombre de *host*

99. Recomendaciones de seguridad avanzadas: Security | Advanced Threat Protection

Configuración	Recomendación	Valor por defecto	Razón
Protección contra contenido sospechoso (*Page Risk TM*)	Rango de 33 a 35	35	Zscaler identifica el contenido malicioso dentro de la página web y asigna una puntuación de riesgo. Bloqueando todas aquellas páginas con un nivel de riesgo superior al establecido.
Protección contra *botnets*	Bloquear todo	Bloquear todo	Bloquea las llamadas a redes de *botnets* por parte de máquinas infectadas
Protección de contenido activo malintencionado	Bloquear todo	Bloquear todo	Bloquea varios tipos de contenido activo malicioso en páginas web
URL maliciosas bloqueadas	Opcional	No establecido	Opcionalmente, puede agregar URL maliciosas que no son detectadas por Zscaler (falsos negativos). Las URLs agregadas en esta sección se bloquearán para toda la organización. Llegado el caso se puede ser más granular aplicando estas URLs en las políticas de filtrado de URLs, pudiendo, en este caso, filtrar el conjunto de usuarios para los que aplica el bloqueo, entre otras opciones de filtrado.
Protección contra el fraude	Bloquear todo	Bloquear todo	Bloquea varios sitios fraudulentos como *phishing* o *spyware call backs* por parte de máquinas infectadas
Protección de comunicaciones no autorizadas	Bloquear todo	Bloquear todo	Bloquea técnicas de evasión de *proxy* como el uso de túneles, anonimizadores, etc.
Protección de secuencias de comandos entre sitios (XSS)	Bloquear todo	Bloquear todo	
Protección de Destinos Sospechosos	Opcional	No establecido	Opcionalmente, puede bloquear las comunicaciones a sitios alojados en la lista de países seleccionados. Zscaler utiliza las coordenadas geográficas de la IP de destino para determinar la ubicación del sitio web
Comunicaciones P2P	*Tor*: Bloquear Bit Torrent: Bloquear Google Talk: Bloquear	*Tor*: Bloquear Bit Torrent: Bloquear Google Talk: Bloquear	

100. Recomendaciones de seguridad avanzadas: Security | Advanced Threat Protection

Configuración	Recomendación	Valor por defecto	Razón
Configuración – *Admin Ranking*	Habilitar	Deshabilitado	Consulte la referencia REF 48 – Acerca de la funcionalidad *Admin Rank*, para más información
Permitir el filtrado de URLs en cascada	Deshabilitar	Deshabilitado	Esta opción muestra la lista de URLs asociadas a las políticas de *URL Filtering* y *Cloud App Control*, de un modo plano. Cambiando el paradigma de administración de la solución.
Tiempo de espera de la sesión de la interfaz de usuario del administrador	5 minutos	30 minutos	Valor a partir del cual la sesión se bloquea en caso de no recibir señal.
Reenvío automático (*proxy forwarding*) para tráficos Web sobre puertos no estándar.	Habilitar	Habilitado	El servicio realizará una inspección profunda de paquetes (DPI - *Deep Packet Inspection*) y detectará la transacción web en puertos no estándar, reenviando ese tráfico al proxy Web, para el desarrollo de los controles de seguridad asociados. La función Zscaler Firewall debe estar habilitada para utilizar esta función
Configuración de excepciones Office 365 *One-Click*	Deshabilitar	Deshabilitado	Se trata de una configuración que permite con un *click* excepcionar el mínimo conjunto de URLs SSL/Auth relativas a *O365* para cumplir con los requerimientos de Microsoft.
Bloqueo de tráfico Web sobre puertos no estándar	Deshabilitar	Deshabilitado	Permite bloquear el tráfico asociado a aquellas aplicaciones que se comunican vía protocolos Web a través de puertos no estándar.
Política para el tráfico no autenticado	Habilitar	Deshabilitado	Habilitar esta función, permite posteriormente, en otras secciones del producto (ejemplo *URL*

			Filtering), aplicar un control granular en la definición de políticas. Existen múltiples razones por las que el tráfico no se autentique, esta funcionalidad permitirá posteriormente aplicar políticas para las distintas casuísticas posibles.

101. Recomendaciones para la definición de políticas avanzadas de navegación || URL & Cloud App Control || Advanced Policy Settings

Configuración	Recomendación	Valor por defecto	Razón
Habilite el cumplimiento de CIPA	Opcional	Deshabilitado	Cuando está habilitada, esta opción crea una política de URL predefinida que bloquea las categorías de URL de acuerdo con la ley de protección infantil en Internet. Esta opción también crea un informe de cumplimiento de CIPA. Consulte la referencia REF 49 – Acerca del cumplimiento CIPA para más información.
Habilitar la búsqueda de dominios recién registrados	Habilitar	Deshabilitado	Cuando está habilitado, Zscaler inicia la búsqueda de antigüedad del dominio a través de la herramienta "*whois*". Cualquier dominio con menos de 30 días se clasificará automáticamente como "Dominio recién registrado". Puede definir una política para permitir/bloquear los dominios recién registrados. Tenga en cuenta que marcar esta casilla no restringirá los dominios recién registrados, necesita una política de URL para hacerlo.
Habilitar la categorización de contenido dinámico	Habilitar	Deshabilitado	Zscaler analiza el contenido de los sitios web sin categorizar para comprobar

			si pertenecen a una de estas categorías: Material para adultos, Drogas, Juegos de azar o Violencia. Si el servicio determina que el sitio pertenece a una de esas categorías, clasificará esos sitios y aplicará la directiva en consecuencia. Dependencias: La inspección SSL es necesaria para aplicar esta directiva para el tráfico HTTPS
SafeSearch	Habilitar	Deshabilitado	Reduce la responsabilidad legal con las búsquedas en la web. Zscaler aplica automáticamente la búsqueda segura en todos los principales navegadores Dependencias: La inspección SSL es necesaria para aplicar esta directiva para el tráfico HTTPS
Habilitar la categorización de sitios incrustados	Habilitar	Deshabilitado	Habilite esta opción para permitir que el servicio aplique la directiva de filtrado de URL para los sitios que se traducen mediante los servicios de traducción en línea, Por ejemplo, cuando esta función está habilitada, si se define una política que bloquea www.gambling.com y un usuario traduce la página a otro idioma mediante el Traductor de Google, el servicio bloqueará la página traducida. Dependencias: La inspección SSL es necesaria para aplicar esta directiva para el tráfico HTTPS
Dominios permitidos para Google *Apps*	Opcional	Deshabilitado	Esta función opcional permite que los usuarios accedan a Gmail y a otras

			aplicaciones de Google solo desde los dominios definidos como corporativos. Esta función se utiliza normalmente para bloquear el uso de la aplicación personal de Gmail/Google
Microsoft *Recommended Office One-Click*	Habilitar	Deshabilitado	Permite de un modo muy sencillo hacer un *bypass* completo del tráfico Office 365 sin necesidad de configurar excepciones o realizar un mantenimiento de posibles URLs cambiantes
Habilitar Office 365, *Tenant Restriction*	Opcional	Deshabilitado	Esta característica opcional permite la aplicación de políticas distintas en función del *tenant* de Office 365. Esta función se utiliza normalmente para bloquear el uso de Office 365 de personal no corporativo.
Skype	Habilitar	Bloquear	Permite el uso de Skype

102. Recomendación para las políticas sobre tráfico no autenticado

Opción de Configuración	**Configuración recomendada**
Habilite la "Política para tráfico no autenticado"	Habilite esta opción en *Administration >> Advanced Settings*. Esto permite a Zscaler aplicar las políticas de URL y *Cloud App Control*, en situaciones donde el tráfico se encuentra sin autenticar (Ejemplo, equipos donde no se puede implementar Zscaler Client Connector, tales como servidores o dispositivos IoT)
Crear políticas para usuarios especiales	Con la opción Política para tráfico no autenticado (explicada anteriormente) habilitada, obtenemos la selección de usuarios especiales al crear las políticas. Este tipo de políticas permite ser muy granular a la hora de definir para que tráfico no autenticado se aplica una política u otra. Consulte la referencia REF 50 - Creación de políticas para usuarios no autenticados para más información sobre las opciones disponibles.
Política creada para el usuario *ANY*	Las políticas que se creen para el usuario *ANY* también se aplicarán a los usuarios especiales (tipos de tráfico no autenticado)

Políticas basadas en la localización	Las directivas basadas en localización se aplican a todo el tráfico de usuarios de la localización determinada (autenticado o no autenticado)

103. Recomendación para la definición de políticas de inspección SSL/TLS. Con el fin de ofrecer el mayor nivel de seguridad posible, se recomienda inspeccionar el mayor tráfico posible cifrado (SSL / TLS). Si bien es cierto, algunas peticiones HTTPS pueden utilizar técnicas como certificate-pinning por lo que este tráfico deberá ser analizado y llegado el caso excluido de la interceptación SSL.

Opción de Configuración	Configuración recomendada	
Certificado TLS	Certificado intermedio personalizado de la organización. Utilizando, en este caso la PKI de la organización, las opciones de configuración se encuentran disponibles en la opción *Advanced SSL Inspection Settings* Consulte la referencia REF 21 - Configuración de la inspección SSL, para más información.	
La acción es: **Inspeccionar**	Certificados de servidor que no son de confianza	**Bloquear**, opcionalmente *Pass Through* permitiendo que el usuario final tome la decisión.
	Bloquear el tráfico no descifrable	**Habilitar** Zscaler puede interceptar casi todo el tráfico TLS. TLS 1.3: puede ser capturado por esta regla, provocando un *Fall Back* a TLS 1.2 por parte de los servidores finales.
	Comprobación de revocación de OCSP	**Habilitar** Habilite esta opción para bloquear el acceso a sitios con certificados revocados. ZIA utiliza OCSP (*Online Certificate Status Protocol*) para obtener el estado de revocación de un certificado. El servicio muestra una notificación al usuario final.
	Versión mínima de TLS de la organización	TLS 1.2
	Versión mínima de TLS del servidor	TLS 1.2
La acción es: **No inspeccionar**	**Evalúe otras políticas** (Evalúe la directiva de *URL Filtering* o *Cloud App. Control*)	Certificados de servidor que no son de confianza: "bloqueados"
		Mostrar *End User Notification* para tráfico bloqueado - "Habilitar"
		Comprobación de revocación de OCSP - "Habilitar"
		Versión mínima de TLS: "TLS 1.2"

	Omitir otras políticas (NO evaluará la directiva de *URL Filtering* ni *Cloud App Control*)	Al seleccionar esta opción, se omitirá la inspección SSL y se omitirán otras directivas configuradas, como el control de URLs y *Cloud App*. Por ejemplo: si un sitio está configurado para ser bloqueado por la directiva de filtrado de direcciones URL o la directiva de control de aplicaciones *cloud*, esta configuración omitirá estas directivas.
La acción es **bloquear**	Mostrar *End User Notification*	**Habilitar** Habilite esta configuración para mostrar las notificaciones del usuario final. Asegúrese de instalar el certificado de CA raíz de Zscaler o el certificado de CA raíz de empresa en el almacén de confianza de sus organizaciones para que el servicio pueda responder o redirigir al usuario a la página de notificación. Si no hay ningún certificado instalado, el explorador mostrará un mensaje de advertencia de certificado no válido. Si esta configuración está deshabilitada, el servicio restablece la conexión con un mensaje genérico de conexión fallida desde el explorador.

Orden de la regla	Nombre de la regla	Criterio	Acción	Descripción
1	Exenciones recomendadas de Zscaler	Categorías de URL - Exenciones recomendadas de TLS	No inspeccionar	Regla generada automáticamente
2	Office 365 *One-Click*	Categorías de URL: *Office 365*, exenciones recomendadas de Zscaler	No inspeccionar	Se genera automáticamente si se activa la opción Microsoft *One-Click*
3	UCaaS *One-Click*	Aplicaciones Cloud: LogMeIn,	No inspeccionar	Generado automáticamente si la

		RingCentral y Zoom		opción UCaaS *One-Click* está configurada
4	Omisión global de SSL	Categorías de URL: Finanzas, Salud, Lista global de omisión de SSL	No inspeccionar	Conjunto de URLs recomendadas para no ser inspeccionadas
5	Inspeccionar usuarios de ZCC	Sistema operativo del dispositivo: MacOS, Windows, Linux, IOS, Android.	Inspeccionar	Posibilidad de aplicar políticas de inspección SSL por dispositivo
6	Inspeccionar el tráfico de un/o conjunto de localizaciones	Grupo de localizaciones	Inspeccionar	Permite aplicar políticas de inspección SSL que afecten a distintas localizaciones
Predeterminado	Regla de inspección SSL predeterminada	Any	No inspeccionar. Evaluar otras políticas	Regla predeterminada para omitir la inspección SSL, pero desencadenar otras directivas como URL y *Cloud App*

104. Recomendación de excepciones en la definición de políticas de inspección SSL

Destino	**Recomendación**	**Razón**
Destinos de IdP, como Azure AD login.microsoftonline.com y .microsoftonline-p.com	No descifrar TLS	Esto ayuda a resolver posibles bucles de autenticación, así como la interceptación de las credenciales de usuario.
Destinos utilizados por dispositivos IoT que no están segmentados encontrándose mezclados con redes de usuarios (Por ejemplo sitios web de impresoras HP, tienda de aplicaciones de Samsung TV)	No descifrar TLS	Los dispositivos IoT no tienen la capacidad de confiar en los certificados raíz, la omisión de TLS para dichos dispositivos resuelve este problema.
Destinos que esperan certificados TLS anclados (*certificate-pinned*) (por ejemplo, la aplicación Box). Para más información consulte la referencia REF 51 – Listado de aplicaciones ancladas.	No descifrar TLS	Estos sitios web no pueden funcionar a través del escaneo TLS, ya que solo confían en certificados de CAs predefinidos

Destinos usados por organizaciones que no pueden presentar cuadros de diálogo de autenticación y usan agentes de usuario conocidos (por ejemplo, cliente de Microsoft Outlook)	No descifrar TLS	La omisión del escaneo TLS para dichas URL también omite la autenticación
Destinos que necesitan la conservación de la IP de origen (*ip anchoring*)	No reenviar a Zscaler	Algunas aplicaciones cloud pueden requerir direcciones IP de salida pertenecientes a la organización para la autenticación
Dominios internos o alojados en la empresa (por ejemplo, IdP alojado internamente)	No reenviar a Zscaler	Los sitios web alojados internamente no deben pasar por el servicio SSE de Zscaler mejorando de este modo la latencia, el rendimiento, la interoperabilidad y el enrutamiento