Cifrado, privacidad y protección de datos: un acto de equilibrio

Los mandatos comerciales, de privacidad y de seguridad para la inspección SSL/TLS integral

zscaler™

Resumen

El cifrado de clave pública SSL/TLS es el estándar de la industria para la protección de datos y se utiliza para proteger las transacciones web de gran parte de Internet. Su cifrado seguro protege los datos privilegiados en tránsito y brinda confianza y anonimato a los usuarios. Pero también ofrece cobertura para los malhechores que utilizan SSL/TLS para explotar esa confianza y el anonimato para encubrir sus actividades.

Los líderes de TI empresariales deben emplear metodologías completas de inspección SSL/TLS para mitigar los riesgos ocultos en el tráfico cifrado. Este documento técnico examina el riesgo que representan las amenazas cifradas; considera las implicaciones comerciales, de privacidad y de seguridad de administrar ese riesgo; y presenta medidas constructivas para equilibrar las necesidades de seguridad con los derechos de privacidad de los empleados. Al final, la mejor manera para que el liderazgo de TI garantice los derechos de cada empleado es proteger a la organización de amenazas y ataques.

Internet solía ser mucho más simple: un patio de juegos abierto para la élite con conocimientos técnicos ...

Hoy en día, se ha convertido en el lugar donde se producen tanto gran parte de los complejos negocios modernos como de la vida cotidiana. Esta omnipresencia conlleva nuevos riesgos. Por su propia naturaleza, un "Internet para todos" incluye un refugio para los ciberdelincuentes que están decididos a aprovecharse de aquellos de nosotros que lo usamos para hacer negocios y hacer nuestra vida cotidiana.

Los datos privilegiados deben estar protegidos, especialmente cuando están en tránsito. El cifrado ofrece la forma más práctica de hacerlo. Los datos codificados con los protocolos de cifrado SSL/TLS estándar de la industria no pueden ser decodificados de forma práctica (es decir, de forma asequible) por un malhechor que los intercepte. (Consulte la Figura 1 y consulte la barra lateral "Seguridad de la capa de transporte [TLS] y Capa de sockets seguros [SSL]".) El cifrado también ayuda a establecer la confianza y preservar el anonimato. Es esta combinación de capacidades lo que hace que el cifrado SSL/TLS sea ideal para proteger la comunicación a través de Internet, desde la simple navegación web hasta las compras vía comercio electrónico.

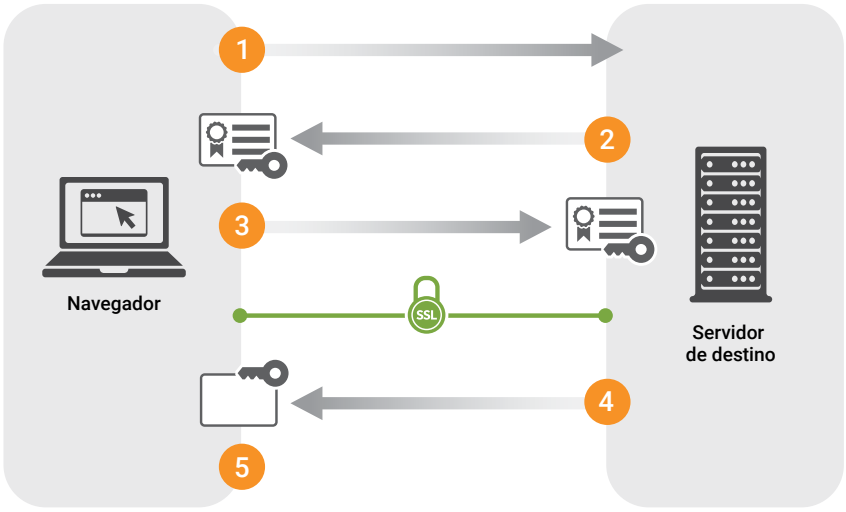
En los entornos comerciales actuales, es esencial proteger los recursos empresariales *y* preservar la privacidad del individuo. SSL/TLS sirve a ambas misiones aparentemente opuestas. Pero en las manos equivocadas, las tecnologías SSL/TLS pueden ser potencialmente peligrosas. ¿Qué sucede cuando los ciberdelincuentes las usan para cifrar malware y ocultar sus actividades? ¿Cómo puede la empresa moderna combatir esta amenaza?

De abierto a seguro: cómo SSL/TLS permite la protección en línea

Internet ha evolucionado. En el pasado, la navegación, ya fuera en Yahoo, Google, Microsoft o el sitio web de su universidad local, no requería privacidad ni protección. Escribir una URL en la barra de direcciones del navegador lo llevaría directamente a ese sitio, sin cookies ni desvíos introducidos, y con poca o ninguna información potencialmente explotable compartida en el camino. Hoy en día, compartimos habitualmente tanto información personal como privada y hacemos negocios en la misma red. Nosotros *vivimos* en Internet. Incluso nuestros hábitos de navegación se han convertido en datos valiosos. Este cambio requiere una forma más privada y segura de interactuar con los servicios web.

Ahí entra en escena la tecnología de cifrado. El cifrado de Capa de sockets seguros (SSL) (y su sucesor, Transport Layer Security, o TLS) establece *túneles seguros* entre un navegador y el sitio de destino utilizando certificados de "clave pública" validados por terceros. Esos certificados, y las relaciones que establecen, crean un conjunto de *cadenas de confianza interconectadas*: "Confío en ti porque alguien en quien confío confía en ti". Cuando una empresa compra dicho certificado a un proveedor de confianza reconocido por el navegador (p. ej. , Verisign, Thawte), esa compañía se convierte en un miembro confiable de esa cadena. Cuando navega a un sitio protegido por SSL/TLS, su navegador y el sitio web intercambian credenciales (el certificado) y parámetros para que la comunicación posterior esté cifrada. Esa comunicación, incluso en el caso de que fuera interceptada, es ininteligible para cualquiera que no sea el navegador y el servidor del sitio web. Los protocolos SSL y TLS llevan proporcionando esta capacidad de cifrado varias décadas.

Cómo funciona SSL/TLS en una conexión navegador-servidor



1. Un usuario abre un navegador y envía una solicitud HTTPS.
2. El servidor de destino devuelve una clave pública cifrada junto con el certificado SSL/TLS.
3. El cliente del navegador valida el certificado, crea y envía una clave cifrada al servidor de destino. (Si el certificado del servidor no está validado, la comunicación finaliza).
4. El servidor de destino descifra la clave recibida y entrega el contenido cifrado (y la clave) al cliente.
5. El cliente descifra el contenido.

Figura 1. Cómo funciona SSL/TLS en una conexión de navegador a servidor de destino.

SSL/TLS proporciona tres características importantes para la navegación web:

Privacidad

Los datos contenidos en el túnel seguro no se pueden ver ni compartir con otra entidad.

Confianza

Se obtiene validación de que el navegador realmente está comunicándose con el servidor/sitio web previsto.

Anonimato

Los comportamientos de navegación del usuario están ocultos a cualquier entidad entre el usuario y el servidor.

Transport Layer Security (TLS) y Secure Sockets Layer (SSL)[1] son protocolos de red destinados a crear un túnel seguro entre dos dispositivos mediante criptografía. Esto proporciona comunicaciones seguras a través de una red informática pública. SSL y TLS protegen los datos a través de métodos criptográficos que utilizan tanto claves públicas como privadas para el cifrado y descifrado y se basan en certificados para autenticar a las partes que se comunican.

[1] https://en.wikipedia.org/wiki/Transport_Layer_Security

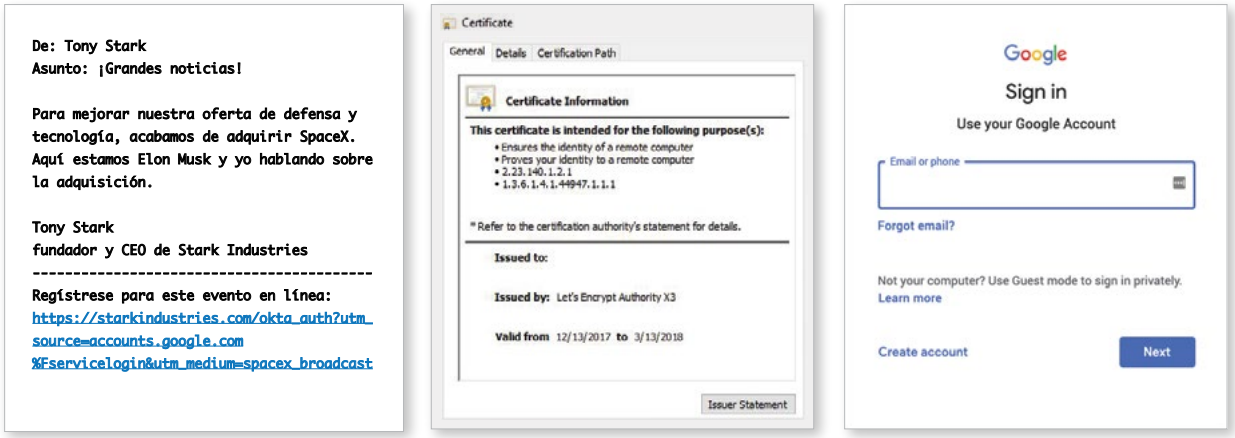
El anonimato protege la información acerca del navegador y la persona tras él, pero no las direcciones IP del navegador ni del servidor. Esta brecha se ha abordado a través de la llegada de proxies anonimizadores[2] y redes de anonimato como TOR.[3]

Riesgo de cifrado número 1: los malhechores se aprovechan de la confianza

El cifrado SSL/TLS ofrece la seguridad de la privacidad: nadie entre su navegador y su destino sabe lo que está viendo o qué datos se comparten. Pero recuerde la cadena de confianza: los malhechores buscan aprovecharse de esta confianza (Ver Figura 1) y han hecho que la confianza inherente a SSL/TLS sea aún más importante que las capacidades de privacidad y anonimato del túnel.

Cómo los ciberdelincuentes se aprovechan de la confianza: ejemplos de ataques furtivos

Objetivos de ejemplo de ataque encubierto: robar credenciales de usuario, exfiltrar datos.
(Todos estos ejemplos se entregaron a través de canales cifrados con SSL).



Spear Phishing
En este ejemplo, un malhechor se hace pasar por un CEO para solicitar clics en una URL de sitio malicioso enmascarado.

Certificado SSL
La legitimidad aumenta con el certificado generado por la autoridad de certificación gratuita.

Ciberocupación de dominios
Un dominio malicioso que se ve y se comporta de manera similar a uno legítimo. Se requiere inicio de sesión.

Figura 2. Ejemplos de cómo los malhechores se aprovechan de la confianza a través de la entrega cifrada SSL/TLS.

Por ejemplo, una simple búsqueda en Internet no puede justificar el cifrado, pero Google lo hace de todos modos. Aunque los datos pueden no ser sensibles, la *certeza* de saber que es Google quien da servicio a la página proporciona ese elemento esencial de confianza. La propia cadena de confianza de cifrado

---

https://en.wikipedia.org/wiki/Anonymizer

https://en.wikipedia.org/wiki/Tor_(anonymity_network)

proporciona esa validación. Al igual que la mayoría de los sitios web modernos, Google ahora entrega todas sus páginas a través de SSL/TLS con URL "HTTPS". La era de la navegación de texto abierto "al natural" está terminando. (En Zscaler, estamos en una posición única para poder observar las tendencias del tráfico de Internet y más del 83 % del tráfico de datos que fluye a través de Zscaler ahora es cifrado a través de SSL/TLS.[4])

El modelo de túnel seguro es, por diseño, seguro. Pero aún es vulnerable, especialmente cuando se trata de la confianza del usuario. Cualquier organización (e incluso un individuo) puede comprar un certificado SSL/TLS. Dicha organización puede usar ese certificado para acaparar o imitar destinos legítimos de Internet (o incluso componentes de una página web legítima), comprometiendo de hecho un sitio con un certificado legítimo. De esta manera, los ciberdelincuentes engañan al humano que se encuentra tras el ordenador y obtienen acceso a datos valiosos del usuario que luego pueden decodificar, *incluso si son cifrados en tránsito.* Los malhechores se hacen pasar por una entidad confiable. Dado que el tráfico está cifrado, su recopilación de datos no se detecta y supera los controles o herramientas empresariales que se implementan para detenerlo.

Riesgo de cifrado número 2: los malhechores ocultan el malware

El aumento de los ataques de phishing, suplantación de identidad y ransomware ha erosionado la confianza en Internet: ¿cómo sé que estoy viendo un sitio legítimo? ¿Cómo sé que algo en el sitio (anuncio, artículo, elemento) no está comprometido? ¿Cómo sé que este sitio aparentemente legítimo no alberga malware cifrado?

Los ciberdelincuentes a menudo vulneran (o suplantan) a proveedores externos como Content Delivery Networks (CDN) que suministran contenido a sitios legítimos, por lo tanto, entregan malware en un sitio legítimo que a todos los efectos está "protegido" por HTTPS.

Los malhechores usan el cifrado SSL/TLS para ocultar su trabajo y la amenaza que presentan está empeorando progresivamente. No se trata de una amenaza nueva. Siempre han tenido la oportunidad de ocultar malware dentro de un código seguro. Es la economía lo que ha cambiado. En los últimos años, ya hay certificados SSL/TLS disponibles *gratuitamente* , lo que reduce en gran medida el coste (y el esfuerzo) de cifrar malware destructivo.

Aquí en Zscaler, hemos visto crecer exponencialmente el volumen de amenazas a través de túneles cifrados en los últimos años. Más del 54 % de las amenazas avanzadas detectadas llegan ahora a través de canales

---

https://www.zscaler.com/threatlabz/encrypted-traffic-dashboard

cifrados SSL/TLS.[5] Y lo que es más preocupante, en 2018 los ataques de phishing cifrados con SSL/TLS aumentaron un 300 %.[6]

Los malhechores usan los mismos protocolos SSL/TLS para cifrar la fuente de su malware (por ejemplo, un sitio cifrado especialmente diseñado para alojar el malware) y las comunicaciones salientes del malware. Ese cifrado presenta la ilusión de datos "confiables", lo que les otorga vía libre para infiltrarse en empresas, acceder a activos y ocultar la filtración de datos.

Riesgo de cifrado número 3: los malhechores enmascaran la exfiltración de datos

Si un ciberdelincuente externo logra infiltrarse en una red corporativa con la intención de robar activos digitales, se enfrenta al desafío de obtener datos fuera del perímetro de seguridad de la empresa. A un malhechor interno se le presenta el mismo problema: ¿cómo obtener información privada fuera de la organización?

Los ciberdelincuentes ocultan el malware dentro de los datos cifrados entrantes. En algunos casos, ese malware estalla dentro de una organización, infectando sistemas internos, y posteriormente se contacta con servidores externos de mando y control (C&C) para filtrar datos corporativos valiosos fuera de la organización.

El cifrado puede enmascarar fugas de datos malintencionadas (e incluso ocasionalmente accidentales). Sin inspección SSL/TLS saliente, ¿cómo puede determinar una investigación de TI si los datos confidenciales permanecen privados? La inspección SSL/TLS debe abordar tanto el tráfico de datos entrantes (mantener alejados a los malhechores) como los salientes (mantener la información privada dentro). En el ejemplo de salida, la inspección SSL es fundamental para prevenir la pérdida de datos e identificar y corregir vulnerabilidades de exfiltración de datos de ataque de día cero.[7]

Equilibrando el acceso y la seguridad en una nueva era de privacidad

La evolución de la conectividad a Internet anuncia una nueva era de privacidad, desde la transmisión de texto sin cifrar a los datos cifrados, desde la confianza implícita a la explícita. Esto se refleja no solo en la demanda de los consumidores por la gestión de datos privados, sino en las pautas regulatorias que definen el derecho de un usuario a la privacidad, como el Reglamento General de Protección de Datos (RGPD)

---

https://www.zscaler.com/resources/solution-briefs/add-advanced-threat-protection-to-close-your-security-gaps.pdf

https://www.zscaler.com/blogs/research/february-2018-zscaler-ssl-threat-report

https://searchsecurity.techtarget.com/definition/zero-day-vulnerability

europeo[8], Ley de Protección de Información Personal y Documentos Electrónicos de Canadá[9]y varias leyes de privacidad estatales existentes en los Estados Unidos (California, Maine, Nevada) y propuestas (Haváii, Illinois, Massachusetts, Mississippi, Nuevo México, Nueva York, Rhode Island, Texas y Washington).

No todo el tráfico de navegación o Internet es igual. En la mayoría de los casos, la privacidad se inclina hacia el individuo. Lo más probable es que un usuario ocasional en un estado democrático navegue de forma privada, mientras que un usuario web en una ubicación con un gobierno autoritario use una red de anonimato como Tor para proteger las comunicaciones de la visibilidad de los censores para comunicarse con su familia en el extranjero. En cada caso, los datos son propiedad del usuario y pocos, con la posible excepción de ese gobierno autoritario, argumentarían en contra de preservar el derecho a la privacidad de cada usuario. Ambos usuarios asumen el riesgo de pérdida de datos o intercepción, un riesgo que se limita a sus propios hogares y dispositivos.

Es otra historia dentro de una empresa, o con acceso a Internet proporcionado por el gobierno. La mayoría estaría de acuerdo en que los usuarios corporativos deberían disfrutar de un derecho a cierto nivel de privacidad en Internet; hay pocas razones por las cuales los hábitos de compra, las opciones de destinos de vacaciones, los pasatiempos o los destinos de navegación de un usuario deberían ser visibles para sus compañeros de trabajo. Las diversas leyes que rigen la privacidad en muchos casos respaldan ese fin. SSL/TLS ha permitido esa privacidad, e incluso el anonimato de navegación, durante años.

Sin embargo, esa privacidad esperada conlleva costes y riesgos: ¿podemos seguir disfrutando de esa privacidad si los malhechores pueden aprovecharse de ese privilegio en su propio beneficio? En un contexto empresarial, el riesgo ya no es solo para el empleado individual, sino para toda la organización. Dentro del contexto de las capacidades de tecnología de cifrado, los líderes de TI de la empresa actuales deben sopesar el riesgo de amenazas entrantes frente a la promesa de privacidad: un acto de equilibrio delicado entre los derechos del empleado individual y el requisito de la empresa de protegerse.

En una organización, la visión del derecho a la privacidad absoluta es menos clara. Cualquier empresa que use Internet (y siendo sinceros, todas las empresas lo usan) tiene una responsabilidad para con sus empleados, accionistas y clientes de protegerse y adherirse a las pautas legales y regulatorias. Los líderes de TI emplean controles técnicos y de procedimiento para prevenir y detectar ataques y comportamientos de riesgo. Para reducir el riesgo y proteger la "casa", dichos controles deben aplicarse a todo el tráfico de datos internos, entrantes y salientes.

---

https://eugdpr.org/

https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

El entorno regulatorio puede agregar complejidad a la gestión de datos corporativos. Algunas jurisdicciones europeas requieren que las corporaciones protejan los datos personales de los empleados para garantizar la privacidad y, en algunos casos, el anonimato, de la navegación web personal. Por ejemplo, la Telekommunikationsgesetz[10] ("Ley de Telecomunicaciones" o TKG) alemana se considera generalmente aplicable a las corporaciones que proporcionan a los empleados acceso a Internet para su uso personal. La TKG requiere específicamente que los usuarios estén sujetos a la "confidencialidad de las telecomunicaciones". También exige que una organización proteja adecuadamente el servicio contra daños y/o intercepción, y proteja los datos de navegación de los usuarios de manera adecuada. Las empresas que cumplen con la TKG deben equilibrar la "confidencialidad de las telecomunicaciones" de los usuarios con la protección de activos.

Según un Informe de transparencia de Google reciente,[11] hasta el 93 % del tráfico del navegador Chrome está cifrado. Con los malhechores utilizando amenazas avanzadas a través de canales cifrados para evadir controles de seguridad de la empresa, ¿cómo puede una empresa protegerse a sí misma y a sus datos y, al mismo tiempo, mantener los derechos de privacidad de los empleados de conformidad con las normas de protección de datos?

Apertura del túnel: descifrado e inspección SSL/TLS

En una empresa, un ataque de malware se limita no solo a un individuo. Una vez que un atacante ha obtenido acceso al dispositivo de un empleado, ese atacante generalmente puede trasladarse a otra parte ("este/oeste[12]") dentro del ámbito de ese empleado e infectar otros sistemas y ordenadores dentro de la red corporativa.

Los controles de ciberseguridad pueden inspeccionar fácilmente la comunicación de texto abierto que entra o sale de una organización, pero el cifrado SSL/TLS de los datos entrantes o salientes complica la inspección. ¿Se puede preservar la presunta privacidad de un túnel seguro si las amenazas cifradas representan un peligro tanto para el usuario individual *como para la* empresa en su conjunto?

La respuesta es SÍ. La lucha contra el riesgo de amenazas cifradas destructivas comienza con la inspección de datos SSL/TLS. Una empresa tiene la obligación institucional y legal de proteger sus activos, y eso incluye proteger las comunicaciones de sus empleados.

---

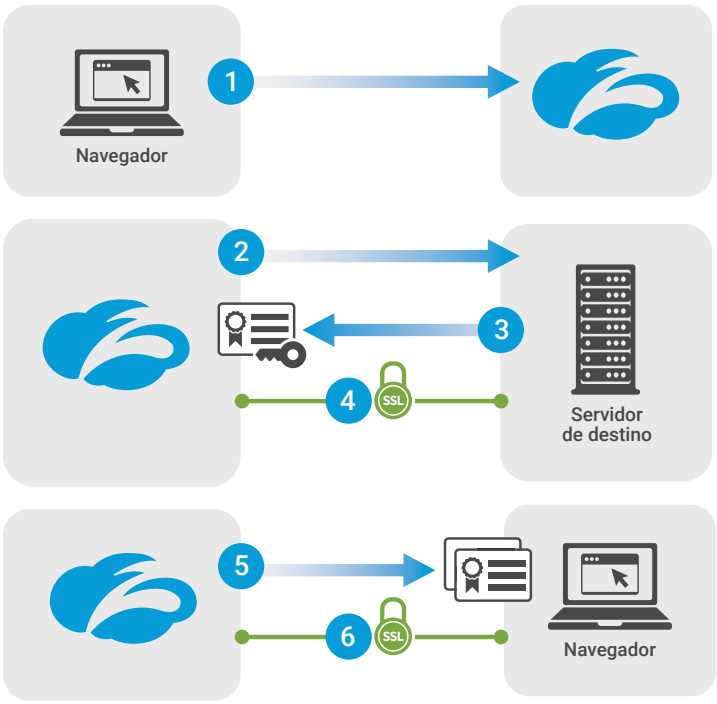
https://germanlawarchive.iuscomp.org/?p=692

https://transparencyreport.google.com/https/overview?hl=en

https://searchnetworking.techtarget.com/definition/east-west-traffic

Para inspeccionar los datos SSL/TLS, la organización debe desviar de manera efectiva esa cadena de confianza de comunicación, interrumpiéndola con un túnel entre el navegador y el dispositivo de inspección y después un túnel posterior entre el dispositivo de inspección y el destino.

Cómo inspecciona Zscaler los datos cifrados SSL/TLS: flujo de trabajo



1. Un usuario abre un navegador y envía una solicitud HTTPS.
2. El servicio Zscaler intercepta la solicitud HTTPS. A través de un túnel SSL separado, el servicio envía su propia solicitud HTTPS al servidor de destino y realiza negociaciones SSL.
3. El servidor de destino envía al servicio Zscaler su certificado con su clave pública.
4. El servicio Zscaler y el servidor de destino completan el protocolo de enlace SSL. Los datos de la aplicación y los mensajes posteriores se envían a través del túnel SSL.
5. El servicio Zscaler lleva a cabo negociaciones SSL con el navegador del usuario. Envía al navegador el certificado intermedio de Zscaler o la raíz intermedia personalizada de su organización, así como un certificado de servidor firmado por la autoridad de certificación intermedia de Zscaler. El navegador valida la cadena de certificados en el almacén de certificados del navegador.
6. El servicio Zscaler y el navegador completan el protocolo de enlace SSL. Los datos de la aplicación y los mensajes posteriores se envían a través del túnel SSL.

Una vez que se completa el protocolo de enlace, el motor de políticas de Zscaler evalúa las reglas de políticas de SSL/TLS, aplica bloqueos o excepciones globales, comprueba los certificados de emisores no fiables y muestra notificaciones (si es necesario).

Figura 3. Proceso de trabajo sobre cómo inspecciona Zscaler los datos cifrados SSL/TLS.[13]

En este ejemplo, la inspección no rompe la relación de confianza entre el individuo y la fuente. El empleado confía en la organización que proporciona el dispositivo de navegación, en lugar de en la fuente de datos. El dispositivo de inspección "verá" el destino y el contenido de los datos.

Entonces la pregunta sigue siendo: *¿Puede una organización realizar esta función esencial de protección mientras respeta las otras dos características del cifrado, el anonimato y la privacidad?* Si se hace de forma correcta, absolutamente sí. La amenaza que representa el malware cifrado hace que la inspección de SSL/TLS sea un requisito de control de ciberseguridad para la empresa moderna y las organizaciones deben equilibrar sus necesidades de seguridad con los derechos de privacidad de sus empleados. Una organización que no

13 https://help.zscaler.com/zia/about-ssl-inspection

inspecciona el tráfico SSL/TLS se expone a riesgos innecesarios, como pérdida de PII, propiedad intelectual robada, espionaje industrial o incluso infecciones de ransomware. (El porcentaje de organizaciones que inspeccionan datos cifrados ha aumentado: entre los clientes empresariales de Zscaler, de los cuales casi la mitad se encuentra en Europa, el 72 % inspecciona el tráfico SSL/TLS).

En una empresa, el anonimato individual en línea se puede preservar ... hasta cierto punto

Al evaluar los modelos de inspección SSL/TLS, primero debemos observar el anonimato. En algunas organizaciones, el suministro de acceso a Internet es un derecho otorgado y regido por el contrato del empleado, establecido y controlado por las políticas de la misma manera que el comportamiento del empleado en el lugar de trabajo se rige por las políticas internas.

La aplicación de esta política requiere supervisión. Un túnel SSL/TLS expone su origen y destino a cualquier cosa, y a cualquier persona, entre el navegador y el servidor. Registrar estas transacciones es esencial para el análisis del comportamiento y la detección de incidentes. Las revisiones de registros pueden ayudar a garantizar el cumplimiento de las políticas y contribuir a la mejora continua de la eficacia de las políticas. (El análisis de registro retrospectivo se utiliza a menudo incluso en investigaciones criminales).

Con un protocolo de inspección SSL/TLS implementado en el lugar de trabajo, los empleados no deben esperar el anonimato completo al navegar en línea, ya que el acceso a Internet es un privilegio otorgado por la organización a sus empleados y se rige por el contrato de trabajo de cada empleado. Para proteger los activos corporativos, la organización puede optar por rastrear las URL de destino, el comportamiento de navegación y el acceso al dispositivo de un usuario. La política corporativa de una organización establece barreras de protección para ese uso de Internet, así como repercusiones por violar dicha política.

Para ser claros, la inspección SSL/TLS no implica el fin del anonimato individual en línea. Las empresas pueden equilibrar las exigencias de privacidad de los empleados con las medidas de ciberseguridad actualizadas. Se requiere un control exhaustivo de los datos para una inspección SSL/TLS efectiva, pero el acceso a los datos que resultan de esa inspección puede ser limitado. Los empleados pueden permanecer en el anonimato durante todo el análisis de registros, incluso durante las investigaciones y la adjudicación (por ejemplo, revisión y respuesta a posibles violaciones de las políticas) hasta que surja la necesidad de intervenir. Este anonimato generalmente se conoce como indexación de registro u ofuscación.

En ocasiones, los líderes de TI deberán inspeccionar y analizar los registros en su totalidad. Por ejemplo, un líder de ciberseguridad revisaría regularmente los registros para identificar devoluciones de llamadas de malware a través del túnel SSL/TLS. Cuando se encuentra uno, la seguridad de TI debe poner en marcha

un flujo de trabajo de limpieza de la máquina, interactuando con el empleado para eliminar el malware del dispositivo específico infectado (o incluso formatearlo o destruirlo). Este proceso se puede implementar para aplicar un enfoque "de cuatro ojos,[14]con un administrador de seguridad y un representante de los trabajadores (por ejemplo, un líder de la asociación de empleados o quizá un abogado externo) revisando los registros de la consola al mismo tiempo.

Cuando los registros identifiquen una infección, un usuario corporativo individual no puede permanecer en el anonimato y debe ser "des-ofuscado" para revelar su identidad de modo que la seguridad de TI pueda poner solución a la amenaza antes de que afecte a la organización en general.

La exfiltración de datos (la "fuga" no deseada de datos de una organización) representa otra situación que puede requerir la des-ofuscación. Por lo general, un proceso de revisión de registros puede determinar que el tráfico SSL/TLS anterior no filtrado puede estar destinado a un sitio web de destino criminal o no aprobado. En este caso, es posible que haya que aplicar la ley y que se deban des-ofuscar datos para apoyar una investigación.

Los empleados deben esperar que la navegación sea anónima para los colegas en el mismo estrato de la empresa, la administración e incluso los equipos de seguridad corporativos ... hasta que un riesgo o una amenaza para las organizaciones desencadene la necesidad de eliminar ese anonimato. En las situaciones anteriores, es esencial que la organización tenga una *necesidad documentada* de des-ofuscar a través de una Política de Uso Aceptable (AUP) que a menudo se incorporaría al contrato laboral del empleado. El uso de Internet a través de dispositivos o redes corporativas debe otorgarse solo cuando el empleado haya accedido a ello (generalmente al comienzo del empleo).

Protección de los datos: descifrado SSL/TLS en un entorno controlado por el RGPD

A simple vista, "la apertura" del túnel de comunicación cifrada SSL/TLS para la inspección de datos y la aplicación de políticas aparentemente hace que los datos dejen de ser privados. Esta es una preocupación habitual planteada por los departamentos jurídicos corporativos y los defensores de la privacidad. Algunos señalan al RGPD como el fundamento para argumentar que el RGPD prohíbe que una organización desencripte e inspeccione datos personales cifrados vía SSL/TLS. En nuestra opinión, esto no es correcto.

Incluso las sesiones normales sin cifrar requerirán que se apliquen exactamente las mismas obligaciones a todas las partes (ISP, proveedor de red, proxy de almacenamiento en caché) entre el navegador y el servidor. Las pautas del RGPD *todavía* requieren que cada parte trate los datos personales con el mismo nivel de

[14] https://whatis.techtarget.com/definition/four-eyes-principle

sensibilidad. El cifrado no cambia las obligaciones impuestas a un controlador de datos o incluso a un procesador. Reduciendo aún más el argumento erróneo, los datos personales están siendo procesados por el dispositivo suministrado por la empresa del empleado de forma no cifrada, *incluso cuando se utiliza un túnel cifrado.* No puede proveerse privacidad absoluta dentro de ese contexto corporativo.

La inspección SSL/TLS se utiliza para hacer cumplir la política e identificar posibles amenazas ocultas en el tráfico de datos cifrados. Para identificar las amenazas, un dispositivo de inspección descifra los datos, los compara con un conjunto de firmas "conocidas como malas" e inspecciona el flujo de datos para determinar el riesgo de amenazas, como la entrada de malware o la salida inadecuada de los datos de la empresa. Si los datos no presentan ninguna amenaza, se vuelven a empaquetar y se envían a su ruta. Realizada de esta manera, la inspección SSL/TLS no reduce la privacidad de los empleados. Los datos no se comparten con nadie, ni se usan de tal manera que infrinjan los derechos de un interesado. El proceso de inspección SSL/TLS protege los activos de la organización de la amenaza de ataque, sin afectar los derechos de privacidad individuales.

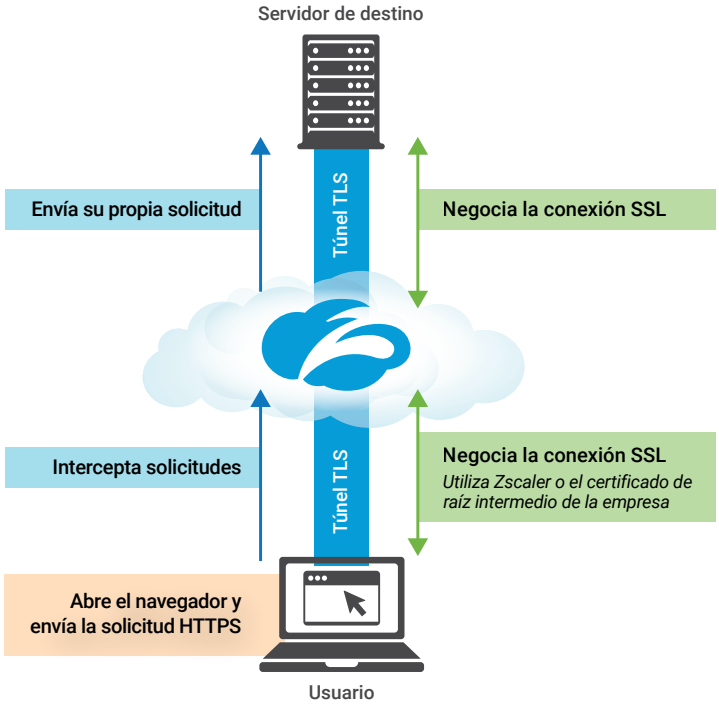
Zscaler ofrece capacidades integrales de inspección SSL/TLS para proteger el tráfico de datos del cliente y proporcionar "perfect forward secrecy (confidencialidad perfecta hacia delante)" (PFS).[15]Zscaler nunca almacena datos en el disco: una vez que se completa la inspección de datos, el flujo de datos continúa sin impedimentos, sin que se conserve ningún registro de los datos de origen más allá del registro de la transacción. Además de proteger los datos en tránsito, Zscaler protege todas las claves SSL/TLS durante la inspección. (Consulte Figuras 3 y 4 para ver cómo inspecciona Zscaler los datos cifrados SSL/TLS. Lea más sobre cómo Zscaler asegura todos los datos y todas las claves de cifrado aquí.[16])

---

https://www.zscaler.com/blogs/corporate/tls-13-busting-myths-and-debunking-fear-uncertainty-doubt

https://help.zscaler.com/zia/safeguarding-ssl-keys-and-data-collected-during-ssl-inspection

Cómo inspecciona Zscaler los datos cifrados SSL/TLS: flujo de trabajo



Zscaler sirve como proxy SSL en línea. Termina la conexión SSL establecida por el cliente y establece una nueva conexión SSL al servidor. Desde la perspectiva del cliente, Zscaler se convierte en el servidor y desde la perspectiva del servidor SSL original, Zscaler se convierte en el cliente.

Inspección Zscaler SSL/TLS basada en la nube:

- Escala para inspeccionar todo el tráfico
- Agiliza la administración de certificados
- Simplifica la administración de la red
- Asegura el tráfico con cifrados AES/GCM/ECDHE para PFS
- Aplica controles de políticas efectivos
- Mantiene los datos del usuario seguros (ya que siguen siendo efímeros, nunca se almacenan en la nube)

Figura 4. Modelo de proxy en línea para la forma en que Zscaler inspecciona los datos cifrados SSL/TLS.[17]

Es útil considerar el derecho a la privacidad como un resultado y revisar la forma en que se logra el resultado, en lugar de desambiguar los pasos individuales que aparentemente afectan a ese resultado. La inspección del tráfico y el resultado binario de bloquear o no bloquear, no es lo mismo que acceder, supervisar o almacenar los datos cifrados.

La inspección exhaustiva SSL/TLS fortalece el cumplimiento del RGPD y la privacidad general de una empresa porque ayuda a proteger la privacidad de la organización, a los empleados de la organización y los activos de la misma. Sin inspección SSL/TLS, el riesgo de exponer datos personales internos/PII es mayor, lo que coloca a la organización en un gran riesgo de incumplimiento.

[17] https://help.zscaler.com/zia/about-ssl-inspection

Las regulaciones de protección de datos apoyan la privacidad *y*seguridad

Regulaciones de privacidad de datos, particularmente la legislación europea como el RGPD,[18el] Reglamento de redes y sistemas de información 2018 (NIS)del Reino Unido[19] y la TKG[20]se implementaron para garantizar que las organizaciones protejan los datos personales al tiempo que se preserva el acceso libre y justo a Internet. Estas regulaciones equilibran los derechos de las personas con los requisitos de que las entidades corporativas implementen medidas de seguridad para proteger los sistemas y los datos. Por ejemplo, las regulaciones de la TKG exigen que las organizaciones apliquen "precauciones técnicas de protección[21]" para evitar la pérdida de datos y evitar ataques externos. La Directiva NIS declara explícitamente que una organización debe habilitar medidas de seguridad apropiadas para garantizar que los sistemas (y los datos que contienen) no puedan verse comprometidos. Y el artículo 5 del RGPD[22] establece que esas organizaciones deben procesar los datos

> *... de tal manera que se garantice la seguridad adecuada de los datos personales, incluida la protección contra el procesamiento no autorizado o ilegal y contra la pérdida accidental, destrucción o daño, utilizando las medidas técnicas u organizativas adecuadas.*

Además, el artículo 32 del RGPD (Seguridad del tratamiento) impone una obligación afirmativa a las organizaciones de implementar medidas de seguridad para el tratamiento de datos personales que "garanticen un nivel de seguridad adecuado al riesgo". Las inspecciones SSL/TLS son muy "apropiadas", dada la magnitud de los riesgos de seguridad que están destinadas a mitigar.

Las amenazas acechan en el tráfico cifrado. Sin inspección, no hay forma de que una empresa pueda distinguir entre datos cifrados SSL/TLS "buenos" y "malos". Ninguna empresa puede cumplir los mandatos de privacidad y seguridad de la TKG, la NIS y el RGPD, y mucho menos proteger a sus empleados e intereses corporativos, sin una inspección exhaustiva del tráfico de datos cifrados.

---

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-gdpr/

http://www.legislation.gov.uk/uksi/2018/506/contents

https://germanlawarchive.iuscomp.org/?p=692

https://germanlawarchive.iuscomp.org/?p=692

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

Conclusiones: cómo implementar la inspección SSL/TLS en su empresa

Las justificaciones de seguridad y protección de datos para la inspección SSL/TLS en la empresa son sólidas e irreprochables. Los líderes de TI deben emplear la inspección SSL/TLS para proteger los datos, los empleados y los activos de su organización. Si no lo hacen, pueden provocar daños irreparables e incluso constituir un incumplimiento del deber.

Los líderes de TI que desean introducir la inspección SSL/TLS en su organización deben tener en cuenta varias consideraciones importantes:

1. **Informar a los empleados.**
   - Asegúrese de que haya una política de uso aceptable válida y que sus políticas se apliquen en el filtro proxy/contenido.
   - Asegúrese de que todos los empleados acepten explícitamente la política de uso aceptable, generalmente a través de su contrato laboral.
   - Asegúrese de que los empleados estén informados de en qué consisten los datos personales y cuánto tiempo los conserva la organización.
   - Asegúrese de que se notifique a los empleados exactamente qué datos se están inspeccionando para que puedan tomar decisiones informadas sobre lo que hacen cuando usan los recursos corporativos.
   - Obtenga el acuerdo y el apoyo de los comités de trabajadores y/o sindicatos, demostrando que la inspección SSL/TLS también redunda en beneficio de los empleados.
   - Socialice la información de lo que se está haciendo y cómo se está haciendo.

2. **Elija una base legal para procesar datos bajo el RGPD.** La regulación no es el enemigo aquí: si una empresa está sujeta a la NIS o similar, la base legal es "obligación legal". Y como se señaló anteriormente, una empresa tiene un "interés legítimo" en proteger a la organización y sus activos.

3. **Obtenga asesoramiento jurídico y de privacidad del equipo interno o de expertos externos, pero esté preparado para discutir los puntos.** Por ejemplo, algunos abogados y profesionales de la privacidad pueden no comprender completamente los servicios que brindan los proveedores o no tener la perspectiva técnica para juzgar si las medidas de seguridad son apropiadas para el riesgo.

4. Asegúrese de que los procesos y controles sean efectivos y apropiados.

- Ofusque u oculte datos de cualquier otro modo de los usuarios normales; asegúrese de que esté disponible solo en la medida en que sea necesario.
- Asegúrese de que haya rigor y un proceso documentado para revisar los datos personales.
- Revise y aplique este flujo de trabajo de forma regular.
- Guarde los datos durante el período de tiempo designado y elimínelos después.
- Mantenga seguros los datos mientras estén en poder de la empresa.

Inspección SSL/TLS: la forma correcta de garantizar el cumplimiento normativo

La inspección SSL/TLS representa las "medidas de seguridad apropiadas" para proteger la privacidad de la empresa, a los empleados de la empresa y los activos de la misma. La inspección SSL/TLS protege a las organizaciones de la amenaza de ataque al tiempo que equilibra los derechos de privacidad individuales y, de esa manera, fortalece el cumplimiento normativo de esas organizaciones.

Las amenazas cifradas son tangibles, destructivas, virulentas y crecen (exponencialmente) en volumen. Los líderes de TI empresariales que eligen no descifrar el tráfico ponen en riesgo tanto la privacidad de sus usuarios como los activos de su empresa, al tiempo que corren el riesgo de no cumplir con diversas regulaciones de protección de datos. En esta era moderna, los líderes de TI deben emplear la inspección SSL/TLS para combatir los riesgos de seguridad para la empresa y preservar la privacidad de sus empleados y usuarios.

Sobre Zscaler

Zscaler se fundó en 2008 con un concepto simple pero poderoso: a medida que las aplicaciones se trasladan a la nube, la seguridad también debe trasladarse allí. En la actualidad estamos ayudando a miles de organizaciones globales a transformarse en operaciones habilitadas para la nube.