Consideraciones Fundamentales en la Implementación de una Solución SSL Exitosa

White Paper

by F5

Introducción

Como animales sociales, a los seres humanos nos cuesta trabajo guardar secretos. Sobrevivimos – y prosperamos – gracias al intercambio de información. Sin embargo, hay información que necesita mantenerse privada, es por ello que la criptografía ha estado presente de una u otra forma desde que el ejército espartano usó el cifrado por transposición para proteger información militar durante sus guerras con los griegos.

Si bien la ciencia de mantener privados a los datos privados correspondía con anterioridad a las agencias de inteligencia gubernamentales, la ubicuidad del Internet ha hecho de la privacidad un tema de interés para todos. Ante un constante flujo de filtraciones de datos, el resguardo de datos en línea se ha convertido en una cuestión de la mayor importancia para empresas alrededor del mundo.

El crecimiento de SSL y el panorama actual de seguridad

Tan sólo hace una década, grandes instituciones financieras y agencias gubernamentales eran las principales organizaciones empleando el protocolo criptográfico conocido históricamente como Secure Sockets Layer (SSL) y ahora llamado Transport Layer Security (TLS). Hoy en día, SSL se -encuentra en todos lados. Organizaciones de todo el mundo están luchando para encriptar la mayoría de su tráfico, incluyendo todo desde email y redes sociales hasta video en streaming. Esta evolución aumenta la seguridad del tráfico web, pero a un precio. El crecimiento del tráfico SSL ha representado una carga extra sobre las organizaciones para que implementen una solución SSL eficiente que le permita a su infraestructura de red responder a los incrementos de carga de trabajo requeridos por la incrementada seguridad.

Las organizaciones se han visto tentadas por el nivel de seguridad que SSL ofrece, pero existen retos involucrados en su implementación como un protocolo de seguridad presente en todo lugar y a todo momento. SSL se ha convertido también en un vector de vulnerabilidades, conforme atacantes lo han comenzado a utilizar como una forma de ocultar malware de dispositivos de seguridad que no pueden ver tráfico encriptado. Los ataques distribuidos de denegación de servicio (denial-of-service; DDoS en inglés) son especialmente problemáticos, dado que aprovechan los costos computacionales relativamente altos asociados con el hospedaje de tráfico de servidores SSL. Además, problemas de implementación como el incidente con Heartbleed pueden resultar en violaciones a la seguridad.

Implementar SSL de forma apropiada es una tarea abrumadora hasta para los administradores más experimentados. Sin embargo, es posible mantenerse por delante de los cambios – al escoger estrategias proactivas en lugar de tácticas reactivas – aprendiendo acerca de las opciones y tendencias más actuales en implementación de SSL en múltiples sitios.

Consideraciones fundamentales al adoptar una estrategia SSL exitosa

Protección de datos y privacidad

El objetivo principal de SSL es proteger los datos en tránsito entre aplicaciones. Al estar resguardadas por SSL las comunicaciones entre un cliente, como un navegador Web, y un servidor serán privadas, y las identidades de ambas partes pueden ser autenticadas. Sin embargo, todo el tráfico que es encriptado con una clave privada está sujeto a una potencial futura decodificación, como aprendimos con las filtraciones de alto perfil de la Agencia de Seguridad Nacional de los Estados Unidos (NSA) por parte de Edward Snowden. Proteger todas las comunicaciones web no es suficiente.

Implemente perfect forward secrecy

SSL tiene una medida defensiva pasiva ante vigilancia externa llamada protección de perfect forward secrecy (PFS; comúnmente traducido al español como Secreto Perfecto hacia Adelante), la cual agrega un intercambio adicional al protocolo de establecimiento de clave entre ambos lados de la conexión SSL. Al generar una clave de sesión única para cada sesión que inicie el usuario, PFS garantiza que un atacante no podrá simplemente recuperar una sola clave y con ella descifrar millones de conversaciones previamente grabadas.

La adopción de PFS podría parecer simple; solamente es necesario activarla dentro del dispositivo de terminación SSL, como lo es un Controlador de Entrega de Aplicaciones (ADC, en inglés). Sin embargo, las organizaciones que utilizan dispositivos pasivos de seguridad, como sistemas de prevención de intrusiones (IPS) o sistemas de detección de intrusiones (IDS), van a encontrarse con problemas dado que estos dispositivos muchas veces requieren estar configurados con una clave privada persistente, que PFS no usa. Como resultado, las organizaciones se ven obligadas a elegir: apagar su IPS/IDS o apagar PFS. Cualquiera de las dos opciones compromete su estrategia global de seguridad.

Existe otra opción. Permita que los IDS/IPS hagan su trabajo descargando todo el tráfico SSL hacia un proxy inverso, como un firewall de aplicación web o ADC. El proxy inverso puede entonces hacerse cargo del cifrado antes de pasar el tráfico descifrado a los IDS/IPS para ser inspeccionado y sanitizado.

Lo que puede hacer: Habilite PFS para proteger la integridad de los datos. Además, considere desplegar un proxy inverso para descargar el tráfico SSL y optimizar el trabajo de los dispositivos de seguridad de red.

Utilice Seguridad de Transporte HTTP Estricta

Habilitar la Seguridad de Transporte HTTP Estricta (HSTS; HTTP Strict Transport Security en inglés) es una de las formas más sencillas y poderosas de mejorar la postura en seguridad de las aplicaciones. Al insertar un encabezado en el tráfico HTTPS, HSTS proporciona una capa de protección contra varios vectores de ataque comunes, incluyendo secuestro de cookies, ataques de intermediario y de degradación. Todos los principales navegadores soportan HSTS actualmente, haciendo de su uso una buena estrategia para asegurarse de que el tráfico se mantenga encriptado.

Lo que puede hacer: Asegurarse de que todas las páginas de todos los dominios tengan el encabezado de HSTS habilitando HSTS para los subdominios. Compruebe que esos subdominios son capaces de soportar el uso de SSL. Revise que la solución SSL permita la rápida y fácil configuración de parámetros HSTS de en todo el sistema. Asegúrese de que el encabezado HSTS tenga una duración de por lo menos seis meses.

Visibilidad y control

Administrar aplicaciones y cerciorarse de que se encuentren seguras requiere de visibilidad al interior del tráfico – o la habilidad de proporcionar esa visibilidad a dispositivos de seguridad como un firewall de aplicaciones web (WAF), un IPS/IDS, o un firewall de nueva generación (NGFW) – para que pueda ser monitoreado en busca de amenazas conocidas. Por definición, sin embargo, SSL también esconde de las soluciones de seguridad los datos siendo comunicados, a pesar de esto existen varias estrategias para mantener la seguridad sin dejar de evidenciar efectivamente el tráfico malicioso.

Emplee descargas y transformación SSL

Encriptar y desencriptar tráfico SSL consume poder de cómputo adicional. Con el crecimiento de SSL, las experiencias de usuario y red pueden verse afectadas por latencia y un rendimiento alentado. Además, algunos protocolos de cómputo intenso no son soportados por algunos de los dispositivos de seguridad actualmente en uso. Un ADC puede liberar esa carga de cómputo al funcionar como un proxy completo para TCP, HTTP, y SSL, lo cual significa que el ADC crea una conexión con el cliente (navegador) y una conexión separada con el servidor. La naturaleza de transformación de un proxy SSL permite que un sitio proporcione características SSL independientes de las capacidades de los servidores de aplicación.

Lo que puede hacer: Despliegue una solución que pueda escalarse. Descargar el trabajo de terminación SSL a un ADC simplifica el cumplimiento de una política consistente de SSL sin afectar el rendimiento, protecciones clave, o visibilidad. Esto aumenta la flexibilidad al permitir que el ADC transforme la interfaz de los servidores web a cualquier protocolo que el ADC soporte, sin importar las opciones de transporte en el back-end. Lo anterior permite que los dispositivos y aplicaciones heredados de mayor importancia en el back end puedan seguir operando sin cambios al mismo tiempo que mantiene una postura de seguridad robusta hacia el exterior.

Además, tener un punto central de control facilita el proceso de actualizar un sitio para protegerlo contra vulnerabilidades emergentes. Finalmente, si cuenta con una arquitectura híbrida, busque una solución que le permita descargar el procesamiento SSL desde máquinas virtuales (VMs) hacia un dispositivo de hardware para reducir las demandas de cómputo sobre la infraestructura y así obtener el máximo de un despliegue virtual.

Neutralice el malware con intercepción SSL

Analistas de seguridad estiman que para 2017, 100 por ciento del nuevo malware usará SSL para ocultar su rastro de los dispositivos de seguridad diseñados para identificarlo y neutralizarlo. Las empresas necesitan monitorear y sanitizar su tráfico web saliente para mitigar amenazas persistentes avanzadas (APTs) como spear phishing o actividad de malware.

Dispositivos de seguridad nuevos están siendo constantemente desarrollados para auxiliar a los administradores en la detección de estas amenazas. Implementando lo que es conocido como estrategia de defensa en profundidad, muchos administradores despliegan dispositivos de seguridad en cadena para que puedan apoyarse uno a otro. Sin embargo, las operaciones de SSL afectan la eficiencia, seguridad y rendimiento de estos dispositivos. Muchas de estas nuevas tecnologías son ciegas al tráfico encriptado o sufren significativa degradación del rendimiento cuando se les requiere inspeccionar el tráfico encriptado. Los firewalls de nueva generación, por ejemplo, pueden experimentar hasta un 80 por ciento de reducción en rendimiento con SSL habilitado. Los autores de malware y spear phishing saben esto y están moviéndose rápidamente hacia encriptar toda la comunicación entre su malware y el mundo exterior.

Lo que puede hacer: Una forma de luchar contra estas amenazas encriptadas es desplegar una solución air gap, la cual consiste en colocar un ADC a cualquier lado de la cadena de visibilidad. EL ADC más cercano a los usuarios desencripta el tráfico de salida y envía las comunicaciones desencriptadas a través de dispositivos de seguridad. Estos dispositivos, que ahora pueden ver el contenido, aplican políticas y controles, detectando y neutralizando malware. Al otro extremo de la cadena, otro ADC vuelve a encriptar el tráfico a medida que sale del centro de datos. Implementar esta solución proporciona la flexibilidad de mantener los dispositivos de seguridad en línea, al mismo tiempo que se asegura de que éstos cumplan con el trabajo para el que fueron construidos.

Una consideración más: Al emplear un detector de amenazas como FireEye o Cisco Sourcefire para proteger la red de ataques de día cero y otros ataques maliciosos, cerciórese de que la solución SSL funcione de la mano de estos productos de seguridad para maximizar la eficiencia.

Mitigue ataques DDoS de fuerza bruta

La complejidad de desplegar SSL, combinada con las dificultades experimentadas por muchos dispositivos de red para obtener visibilidad dentro del tráfico encriptado, hacen de SSL el blanco perfecto para ataques DDoS – un hecho que los atacantes entienden a la perfección. A manera que el volumen total de tráfico SSL legítimo aumenta con rapidez, el tráfico malicioso DDoS se hace cada vez más difícil de detectar para los dispositivos de seguridad.

Lo que puede hacer: Mitigue los ataques DDoS tales como renegociación SSL o inundaciones SSL con una solución SSL comprensiva que pueda identificar eficientemente tráfico DDoS sospechoso y evite que éste impacte la disponibilidad de sitios web. Considere investigar acerca de servicios basados en la nube que puedan ayudar a mitigar el impacto de ataques DDoS basados en SSL.

Revise su seguridad ahora

¿Cómo puede saber si su postura de seguridad SSL se encuentra a la altura? Qualys SSL Labs ofrece una herramienta invaluable que le permite evaluar los certificados y configuración de sus sitios – antes de enfrentar un ataque. También puede evaluar la implementación SSL de su navegador y ver cómo se encuentran otros sitios – y sus competidores – ante estos retos de SSL en constante evolución.

Agilidad de cifrado

Desde el comienzo del protocolo SSL en los 90s, el criptosistema de RSA ha sido la opción preferida para intercambio de claves. Con el tiempo, a medida que los ataques de fuerza bruta se hicieron más viables, la longitud de las claves RSAs tuvo que aumentar. Hoy en día, las claves RSA son tan grandes que el intercambio de claves es una operación de cómputo bastante intensiva.

Para reducir la carga de cómputo al tiempo que se mantienen los estrictos controles de privacidad, nuevos protocolos criptográficos están ganando popularidad. Por ejemplo, la criptografía de curva elíptica (ECC, en inglés) ofrece el mismo nivel de seguridad que algoritmos previos pero requiere de menos procesamiento, lo que también significa que es mucho más amigable con la vida de la batería en dispositivos móviles. Aunque estas opciones criptográficas son prometedoras, las organizaciones están preocupadas por tener que reconfigurar cientos de servidores para ofrecer estos protocolos nuevos, y con razón.

Lo que puede hacer: No es raro tener que cambiar de algoritmos con el paso del tiempo para asegurarse de que la solución SSL tenga agilidad de cifrado – la habilidad de un dispositivo SSL para ofrecer múltiples protocolos criptográficos tales como ECC, RSA2048, y DSA al mismo tiempo, hasta en la misma aplicación web. Además, con la creciente diversidad de cifrado, es esencial que la solución SSL demuestre un historial de mantenerse al tanto del soporte de cifrado.

Administración de claves

Las claves SSL se encuentran entre los elementos de mayor valor para las organizaciones. Un atacante que tenga en su poder claves SSL privadas podría hacerse pasar por las aplicaciones del objetivo y crear el mejor portal de phishing posible. Sin embargo, hay varias formas de proteger estas claves de suma importancia.

Mantenga a salvo claves de alto valor

Un módulo de hardware de seguridad (HSM, en inglés) es un dispositivo hardware y software independiente de seguridad que sigue los estrictos lineamientos de diseño criptográfico FIPS 140-2 para resguardar y administrar las claves criptográficas. Dado que las claves nunca son transferidas fuera del HSM, no hay que preocuparse por vulnerabilidades SSL como Heartbleed.

Lo que puede hacer: La forma más segura de resguardar las claves SSL es usando un HSM. Existen varias posibilidades, como comprar un HSM interno como los incluidos en algunos ADCs. Algunas organizaciones optan por consolidar su administración de claves al usar dispositivos HSM como almacenes centralizados de claves (por ejemplo, un par por cada centro de datos). Estos HSMs de red son accesibles por medio de la red interna a servicios que necesiten desencripción de claves, lo que significa que muchos puntos de terminación SSL pueden utilizar el mismo HSM de red. Una cosa a tomar en cuenta: Hay que asegurarse de que la solución SSL pueda conectarse sin problemas con el HSM de red.

Las organizaciones buscan implementar mejores prácticas de administración de claves y certificados empresariales (EKCM, en inglés) para garantizar la seguridad de las claves SSL. Considere usar un sistema de almacenamiento de claves encriptadas asegurado por hardware, el cual permita el almacenamiento de frases de contraseña en forma encriptada dentro del sistema de archivos de red.

Administre certificados SSL eficientemente

El cimiento de las mejores prácticas EKCM efectivas es la creación de un inventario comprensivo de todos los certificados empresariales, sus ubicaciones, así como la gente responsable de su administración. Cada sitio con SSL habilitado tiene su propio certificado, y cada certificado tiene su propia fecha de caducidad. En una semana cualquiera, uno o más certificados pueden expirar, lo cual va a causar que el sitio web o aplicación asociados dejen de estar disponibles. Administrar todos estos certificados puede ser una tarea laboriosa, pero es esencial para garantizar la alta disponibilidad de sitios críticos. Además, los certificados SSL deberían ser inspeccionados por su longitud de clave (2018 bits o mayor), firma digital (SHA2 o mejor), y en busca de certificados fraudulentos no generados dentro de la PKI interna o por un CA de clave pública. Por último, la conformidad con PCI DSS requiere un certificado documentado y un proceso de administración de claves.

Lo que puede hacer: La mayoría de los administradores en organizaciones medianas a grandes prefieren un sistema externo de administración de certificados porque la organización tiene claves y certificados en varias ubicaciones. En particular, muchos han tenido éxito con dos soluciones externas; Venafi y Symantec. Es importante que cualquiera que sea la solución elegida, ésta tenga APIs abiertas para automatizar la administración y así disminuir la carga operacional.

Conformidad integral

La conformidad es en muchas ocasiones el motor detrás de la adopción de SSL. Las aplicaciones que cumplan con la especificación PCI DSS necesitarán descontinuar el uso de SSLv3 y TLSb1 en el transcurso de los próximos dos años para permanecer en conformidad con PCI 3.0. Nuevas implementaciones de PCI DSS deben de tener deshabilitados SSL 3.0 TLS 1.0.

Lo que puede hacer: Primero, asegurarse de que el firewall de red esté certificado por ICSA Labs. Además, los servicios de transformación SSL proporcionan la habilidad de mantener la conformidad con una política SSL en contacto con el Internet sin tener que aplicar esa política en los servidores individuales. Cerciórese de que la solución SSL está lista para TLS 1.3. Así mismo, las verdaderas ganancias en eficiencia operacional pueden hacerse centralizando la conformidad por medio de un servicio de red descargado hacia un ADC en lugar de intentar resolverlo para cada aplicación individual.

Conclusión

Nos guste o no, el mundo en línea es un lugar peligroso, y proteger la información corporativa sensible de potenciales atacantes se ha convertido en una prioridad para empresas de todos los tamaños. Con violaciones de privacidad haciéndose cada vez más comunes, muchas organizaciones están recurriendo a SSL como una forma de proteger la integridad de sus datos en línea. Sin embargo, la implementación de una estrategia SSL integral viene acompañada de sus propios retos de visibilidad, rendimiento y escala.

Con la planeación y despliegue adecuados, una estrategia SSL fuerte mitiga el riesgo de fallos de seguridad. Una vez que la estrategia está establecida, el sitio estará posicionado para el futuro en cuanto a seguridad, escalabilidad, y confiabilidad, devolviendo la atención a donde realmente importa - impulsar el negocio hacia adelante.

F5 Networks, Inc.
401 Elliott Avenue West, Seattle, WA 98119
888-882-4447 f5.com

Americas
info@f5.com

Asia-Pacific
apacinfo@f5.com

Europe/Middle-East/Africa
emeainfo@f5.com

Japan
f5j-info@f5.com