DESCIFRADO: POR QUÉ, DÓNDE Y CÓMO

Por Qué: El Caso para el Descifrado

El crecimiento del tráfico de Internet cifrado o encriptado con los protocolos Secure Sockets Layer (Capa de Puertos Seguros - SSL) o Transport Layer Security (Seguridad de la Capa de Transporte - TLS) es explosivo. De acuerdo al Informe de Transparencia de Google®: "Los usuarios de escritorio cargan más de la mitad de las páginas que ven por HTTPS y pasan dos tercios de su tiempo en páginas HTTPS".[1]

Gracias a los beneficios fundamentales del cifrado (intercambio privado y seguro de información por Internet, así como el cumplimiento de ciertas reglamentaciones como la Health Insurance Portability and Accountability Act, Ley de Transferencia y Responsabilidad de Seguro Médico - HIPAA, y el Payment Card Industry Data Security Standard, Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago - PCI DSS), se espera que la tendencia ascendente en la adopción de SSL continúe. La próxima revisión importante de HTTP 1.1 es HTTP/2 y, aunque el estándar en sí no requiere cifrado, la mayoría de las implementaciones de cliente han indicado que solo admitirán HTTP/2 a través de TLS, que hace que el cifrado sea efectivamente obligatorio. Los exploradores más importantes, incluidos Chrome®, Firefox®, Safari® e Internet Explorer®, se encuentran en diferentes etapas del proceso de marcar las páginas web HTTP como "no seguras".

El cifrado es una forma segura y privada excelente de intercambiar información comercial y es necesario para el cumplimiento. Sin embargo, el tráfico cifrado o encriptado está compuesto básicamente por datos ocultos que no permiten que las organizaciones detecten las amenazas de seguridad que se encuentran en su interior. Lamentablemente, los delincuentes han aprendido a aprovechar esta falta de visibilidad y de identificación para ocultarse de la vigilancia de seguridad dentro del tráfico cifrado y entregar malware. Incluso los sitios web legítimos que usan SSL pueden infectarse con malware. Además, los atacantes usan cada vez más aplicaciones SaaS para entregar malware. Un atacante puede colocar un archivo infectado en una carpeta legítima compartida en una aplicación de almacenamiento de archivos autorizada de una organización, como Box o Dropbox®, y el archivo infectado puede propagarse fácilmente desde allí a los usuarios que sincronicen sus archivos con la carpeta.

Figura 1: Ejemplos de malware transferido a través de tráfico cifrado según la investigación de amenazas de Unit 42 de Palo Alto Networks

Sin la capacidad de descifrar, clasificar, controlar y analizar el tráfico cifrado con SSL, a una organización le resulta imposible proteger correctamente su negocio y sus datos valiosos frente a las amenazas actuales. Este es el punto en el que el descifrado SSL (la capacidad de descifrar, inspeccionar y volver a cifrar el tráfico de Internet antes de enviarlo a su destino) entra en juego. El descifrado, una de las "10 Cosas que su Próximo Firewall Debe Hacer", es necesario para distintas acciones relacionadas con la seguridad, incluso la prevención de amenazas, la prevención avanzada de malware, el bloqueo de archivos, el filtrado de datos y el bloqueo de páginas web malintencionadas.

¿Qué Debe Descifrar? Las Opciones

Hay muchas opciones técnicas disponibles para descifrar el tráfico en su red, incluso proxies web, controladores de entrega de aplicaciones, dispositivos de visibilidad SSL y firewalls de nueva generación. El lugar ideal para descifrar el tráfico SSL depende de la opción que brinde la mayor protección con la menor sobrecarga de gestión, en otras palabras, el máximo retorno de la inversión en seguridad.

Proxies Web

Un proxy web actúa como un "intermediario", que descifra e inspecciona el tráfico saliente antes de volver a cifrarlo y enviarlo a su destino (ver Figura 2). No obstante, los proxies web se limitan a inspeccionar y proteger el tráfico web, que incluye HTTP y HTTPS. Se los suele implementar en puertos web más conocidos como el 80 y el 443. Si una aplicación usa protocolos o puertos que no sean web, los proxies web no pueden ver el tráfico, lo que frustra el objetivo de obtener completa visibilidad y control del tráfico cifrado en su red. Es como si se implementara seguridad aeroportuaria en solo un aeropuerto importante y se dejara expuesto al resto de los aeropuertos. Los proxies también requieren modificar la configuración de proxy de su explorador o usar un archivo de configuración automática de proxy, lo que incrementa la sobrecarga de gestión y agrega otra área por diagnosticar si los usuarios no pueden acceder a Internet.

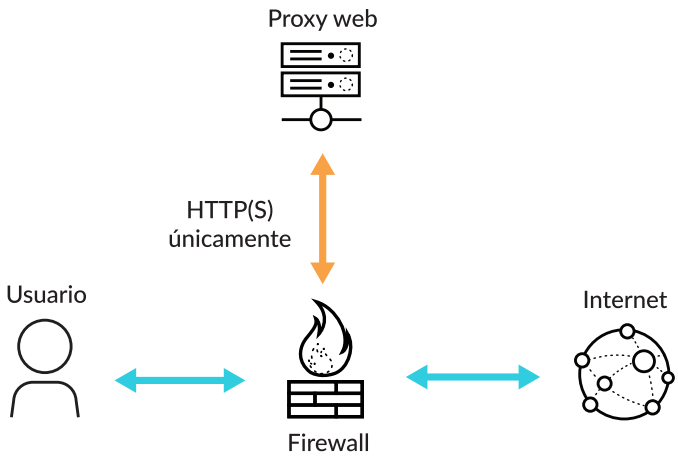

Figura 2: Descifrado y recifrado de un proxy web

Controladores de Entrega de Aplicaciones

La descarga SSL es una de las funciones que ejecutan los Application Delivery Controllers (Controladores de Entrega de Aplicaciones - ADC). En general, una implementación ADC requiere dos dispositivos independientes: uno para descifrar el tráfico y uno para volver a cifrarlo.

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

El problema con las implementaciones ADC es que el tráfico no está cifrado mientras se transporta de un dispositivo ADC a otro, lo que significa que personal de TI irresponsable o cualquiera con acceso a la red física que conecta los dispositivos tendrán un fácil acceso a los datos. Un adversario simplemente puede crear un reflejo del puerto y ejecutar una captura de paquetes para obtener datos confidenciales en texto no cifrado. Esto socava la promesa de la confidencialidad total, que es uno de los propósitos fundamentales del cifrado, y también podría infringir leyes de cumplimiento en algunas industrias y regiones geográficas.

Dispositivos de Visibilidad SSL

Los dispositivos de visibilidad SSL descifran el tráfico y lo ponen a disposición de todas las otras funciones de seguridad de la red que deben inspeccionarlo como proxies web, sistemas de prevención de pérdida de datos y antivirus (ver Figura 3).

El problema es que estos dispositivos incrementan los gastos de capital (capex) y los gastos operativos (opex). Además del costo inicial, un dispositivo de visibilidad SSL se convierte en otro dispositivo más en la red que debe gestionarse, mantenerse y actualizarse, con una configuración y base de reglas totalmente diferente de la de otros dispositivos de seguridad. En cambio, si se utiliza un dispositivo de seguridad para descifrar el tráfico y enviarlo a todos los otros dispositivos complementarios, no es necesario agregar dispositivos de visibilidad SSL.

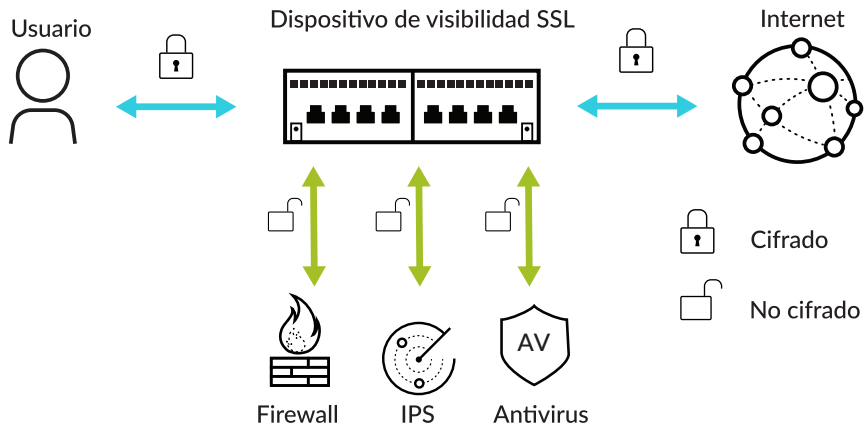

Figura 3: Descifrado a través de un dispositivo de visibilidad SSL

¿Qué Debe Descifrar? La Recomendación

Las organizaciones están reemplazando los firewalls antiguos tradicionales con next-generation firewalls (firewalls de nueva generación - NGFWs) a toda velocidad. De hecho, según Gartner, "firewall empresarial" ahora es sinónimo de NGFW.[2] Los NGFWs incluyen funciones de seguridad como control de aplicaciones y usuarios, sistemas de prevención de intrusiones, filtrado de URLs, antivirus de red y análisis avanzado de malware. Los clientes están utilizando las oportunidades de actualización de firewalls para consolidar múltiples dispositivos de seguridad en un NGFW y aprovechar para ahorrar costos, mejorar la seguridad y facilitar la gestión desde un solo dispositivo. Además, al reducir los dispositivos y consolidar las funciones de seguridad, la complejidad y el consumo de tiempo para solucionar problemas disminuyen considerablemente gracias a que la topología de red es mucho más simple.

Firewalls de Nueva Generación Con y Sin Descifrado		
Casos de Uso Admitidos	**Con Descifrado**	**Sin Descifrado**
Identificar el tamaño de la carga útil, ancho de banda	✓	✓
Identificar el origen del tráfico (de quién y de dónde proviene dentro de la compañía)	✓	✓
Identificar las direcciones IP de origen y de destino, el puerto y el protocolo	✓	✓
Identificar la aplicación utilizada	✓	—
Identificar el tipo de datos enviado	✓	—
Identificar si se infringió la política de uso corporativo	✓	—
Detener la transferencia de tipos de archivo específicos (p. ej., EXE, RAR)	✓	—
Detener la pérdida de datos confidenciales	✓	—
Identificar y detener amenazas en un túnel cifrado	✓	—

Figura 4: NGFWs con y sin descifrado

2. "Cuadrante Mágico para los Firewalls de Redes Empresariales", 10 de julio de 2017, Adam Hils, Jeremy D'Hoinne, Rajpreet Kaur

Los NGFWs son los dispositivos más adecuados para el descifrado del tráfico, ya que proporcionan distintas ventajas:

1. El tráfico descifrado se almacena en la memoria y no se lo envía a otros dispositivos. De esta manera, se cumple con la promesa de confidencialidad de SSL, así como con las reglamentaciones de cumplimiento.
2. Los NGFWs pueden ver y descifrar el tráfico en todos los puertos, lo que otorga visibilidad de todas las aplicaciones, los usuarios, el contenido y las amenazas.
3. Al consolidar múltiples funciones en un solo dispositivo, un NGFW brinda una mayor seguridad. Por ejemplo, puede bloquear amenazas conocidas al utilizar protección de vulnerabilidades, antivirus y firmas antispyware, así como al bloquear sitios web malintencionados. También puede enviar nuevas amenazas potenciales al entorno de análisis avanzado de malware. Si se identifican amenazas, se pueden entregar protecciones nuevas y distribuirlas globalmente en cuestión de minutos.
4. Un NGFW puede enviar el tráfico descifrado a otros dispositivos complementarios adecuados como dispositivos de análisis forense para la retención de registros a largo plazo.
5. Los NGFWs ofrecen una interfaz de gestión fácil de usar que reduce la complejidad y los gastos operativos (opex). Por ejemplo, puede combinar aplicaciones, usuarios, contenido, URLs, prevención de amenazas y análisis avanzado de malware en una sola regla.

Criterios de Compra de un NGFW para Sus Necesidades de Descifrado

No todos los NGFWs son iguales y, lamentablemente, puede ser difícil distinguir entre firewalls que se adjudican características similares. Es importante tener pautas claras para evaluar un NGFW antes de comprarlo. Esto asegurará que el firewall pueda sostener una estrategia integral de prevención de brechas que incluya descifrado SSL.

Consulte la guía "Firewall Buyer's Guide" (Guía para la Compra de un Firewall) para acceder a una lista de todos los requisitos de negocios que su próximo firewall debe cubrir, así como para consejos sobre cómo crear una Request for Proposal (Solicitud de Propuesta - RFP) y un plan de prueba funcional que lo ayudarán en el proceso de selección de proveedores y productos.

Estos son los criterios para comparar las capacidades de descifrado SSL de los NGFWs:

1. **Elegir minuciosamente qué descifrar:** Por cuestiones de privacidad y reglamentarias, su NGFW deberá descifrar el tráfico en forma selectiva sobre la base de criterios lo suficientemente flexibles como para satisfacer sus necesidades. Estos criterios pueden incluir usuarios; URLs; categorías de URLs como finanzas o salud; listas de URLs alojadas externamente para cumplir con las reglamentaciones; origen y destino basados en la dirección IP; puertos; y protocolos. Para detectar el malware potencial, el firewall también debe permitir excluir aplicaciones del descifrado cuando estas se ejecuten en sus puertos predeterminados, pero proseguir con el descifrado de esas mismas aplicaciones cuando se las detecte en puertos no estándares.
2. **Excluir aplicaciones que puedan interrumpirse con el descifrado:** Los proveedores de aplicaciones a veces utilizan HTTP Public Key Pinning (Fijación de Claves Públicas - HTTP), también conocido como fijación de certificados, para evitar la suplantación de identidad de atacantes que utilizan certificados mal emitidos o certificados fraudulentos por otro motivo. Cuando se utiliza esta técnica, los dispositivos de seguridad de red pueden interrumpir algunas aplicaciones durante el descifrado. Su NGFW debe permitirle excluir este tipo de tráfico fácilmente con el nombre de host del sitio web o de la aplicación en la regla de exclusión. Si el NGFW lo obliga a definir exclusiones basadas en nombres distintivos y comunes de certificados, resulta demasiado complejo. Para simplificarlo aún más, el NGFW debería incluir exclusiones predefinidas para las aplicaciones más conocidas que se interrumpan con el descifrado.
3. **Aplicar el estado del certificado:** Querrá eliminar el tráfico para el cual el certificado SSL haya caducado, el emisor del certificado del servidor no sea fiable o el certificado se haya revocado. Su NGFW debe permitirle aceptar o rechazar el tráfico que cumpla con cualquier combinación de estos criterios.
4. **Aplicar conjuntos de cifrado:** Los conjuntos de cifrado incluyen algoritmos de intercambio de claves como RSA, DHE y ECDHE; algoritmos de cifrado como 3DES, RC4 y variantes de AES; y algoritmos de autenticación como variantes de SHA y MD5. El NGFW debe ser compatible con múltiples conjuntos de cifrado y debe permitirle aplicar aquellos que cumplan con sus requisitos de seguridad. Usted debe poder elegir permitir o si bloquear el tráfico que no cumpla con sus conjuntos de cifrado específicos.
5. **Aplicar la versión de protocolo:** Es posible que deba aplicar el uso de versiones específicas de SSL/TLS como TLS 1.2. El NGFW debe ofrecer flexibilidad para aplicar versiones de protocolo específicas y bloquear el tráfico que utilice cualquier versión más débil.
6. **Integrarse con hardware security modules (módulos de seguridad de hardware - HSMs):** Un HSM es un dispositivo físico que gestiona claves digitales, incluso almacenamiento seguro y generación. Brinda una protección tanto lógica como física de estos materiales frente al uso no autorizado y a posibles adversarios. Su NGFW debe integrarse con un HSM para el almacenamiento de claves privadas y claves maestras. Incluso si actualmente su organización no requiere que las claves se almacenen en un HSM, podría necesitar esta funcionalidad en el futuro.
7. **Permitir que los usuarios excluyan el descifrado SSL:** En algunos casos, podría necesitar avisar a los usuarios que el NGFW descifra cierto tráfico web y permitirles terminar las sesiones que no quieran que se inspeccionen. Su NGFW debe permitir la opción de exclusión de SSL para que se les notifique a los usuarios que su sesión está por ser descifrada y que puedan elegir continuar con la sesión o terminarla.
8. **Descifrar el tráfico entrante y saliente:** El NGFW debe tener la capacidad de descifrar el tráfico en ambas direcciones para brindarle la flexibilidad de implementarlo frente a los usuarios o sus servidores web para descifrar el tráfico saliente o el tráfico entrante, respectivamente.
9. **Descifrar SSH:** La mayor parte del tráfico de Internet se cifra mediante SSL/TLS. Sin embargo, Secure Shell (orden segura - SSH) también se puede usar para cifrar y enrutar tráfico dentro de su red. Por ejemplo, algunas aplicaciones internas del centro de datos pueden usar SSH, que está permitido por política. Para evitar que los usuarios usen SSH para evadir sus políticas de uso aceptable o de prevención de amenazas, su NGFW debe admitir el descifrado del tráfico SSH que cumpla con sus criterios.

10. **Usar la aceleración criptográfica por hardware:** El descifrado SSL consume muchos recursos. Su NGFW debe usar la aceleración criptográfica por hardware para mantener un alto rendimiento mientras se descifra el tráfico.
11. **Compartir inteligencia de amenazas y detener las amenazas en todas partes basado en inteligencia de amenazas compartida:** Existen casos en los que el tráfico no es descifrado por el NGFW, por ejemplo, debido a cuestiones de privacidad o a la fijación de certificados. En estos casos, si el NGFW es parte de una plataforma que actúa de acuerdo con la inteligencia de amenazas recopilada de la red, endpoints y nubes, podrá detener las amenazas, incluso si el tráfico no se descifra en la red. Supongamos que una amenaza pasa por la red en tráfico cifrado sin ser detectada y llega al endpoint. La plataforma comparte inteligencia de amenazas entre la red, el endpoint y la nube. Y basada en esta inteligencia compartida, la protección avanzada de endpoints bloquea la amenaza antes de que se concrete el ataque. Además, la información sobre esta amenaza se comparte con toda la plataforma para que la seguridad de las redes y las nubes sea más inteligente. Esta es una ventaja diferencial que no puede brindar un NGFW que funciona solo.

Lo recomendable sería que su proveedor de NGFW tenga planes para admitir las siguientes tendencias con visión de futuro y con probabilidades de tornarse críticas:

- **HTTP/2:** Esta es una revisión importante del protocolo de red HTTP utilizado por la World Wide Web. Se la desarrolló a partir del protocolo experimental inicial SPDY , originalmente creado por Google. Aunque el estándar en sí no requiere cifrado, la mayoría de las implementaciones de cliente han indicado que solo admitirán HTTP/2 a través de TLS, que hace que el cifrado sea obligatorio efectivamente.
- **TLS 1.3:** Habiendo sido aprobado por el Internet Engineering Task Force (Grupo de Trabajo de Ingeniería de Internet), se espera que TLS 1.3 proporcione mayor rapidez y seguridad a todas las conexiones seguras de Internet. Los aspectos destacados en TLS 1.3 incluyen una entrega más rápida de datos, la eliminación del cifrado que no sea AEAD y el intercambio de claves que no sean PFS y la eliminación de la renegociación.

El Impacto en la Seguridad de la Interceptación HTTPS

En 2017, la Universidad de Michigan, la Universidad de Illinois en Urbana-Champaign y otros publicaron un estudio llamado "The Security Impact of HTTPS Interception" (El Impacto en la Seguridad de la Interceptación HTTPS) que analiza el impacto y la prevalencia de la interceptación HTTPS por parte de los dispositivos de seguridad de red. Las conclusiones indican que casi todas las interceptaciones reducen la seguridad de la conexión, incluso muchas generan vulnerabilidades severas.

Esto es una preocupación para los administradores de seguridad de redes, ya que el propósito de la interceptación y del descifrado del tráfico HTTPS es ganar visibilidad y control. El documento indica varias razones sobre por qué las interceptaciones reducen la seguridad de la conexión:

- La configuración predeterminada de muchos de estos dispositivos de seguridad de red debilita la seguridad, por ejemplo, al usar cifrados basados en RC4;
- Muchos dispositivos han interrumpido la validación de certificados;
- Para muchos dispositivos, el proceso de instalación es complicado y propenso a fallas o caídas;
- La configuración de los dispositivos es confusa.

Por lo tanto, es fundamental asegurarse de que su NGFW:

- No habilite los cifrados basados en RC4 de manera predeterminada. La mejor práctica recomendada para la política de seguridad implica evitar los algoritmos débiles como MD5, RC4, SHA1 y 3DES.
- Bloquee los certificados no válidos de manera predeterminada, incluso las sesiones con certificados caducados, certificados de emisores no fiables y certificados con estado desconocido.
- Bloquee sesiones con versiones no compatibles. La mejor práctica recomendada para la política de seguridad bloquea el uso de versiones SSL/TLS vulnerables, incluso TLS 1.0 y SSLv3.
- Use Online Certificate Status Protocol (Protocolo de Estado de Certificado en Línea) y/o listas de revocación de certificado (OCSP y CRLs) para verificar el estado de revocación de los certificados.
- No almacene tráfico descifrado en el disco. Los detalles deben almacenarse solo en la memoria, en cumplimiento con los requisitos de seguridad y regulatorios.

En resumen, solo descifrar el tráfico puede debilitar la seguridad. Sin embargo, habiendo realizado el proceso de diligencia apropiado para comprar un NGFW y al seguir las mejores prácticas, el descifrado no solo le brindará la visibilidad necesaria de todo el tráfico, sino que también lo protegerá de los adversarios que ocultan amenazas en túneles cifrados.

Cómo Habilitar el Descifrado SSL: Personas, Procesos y Herramientas

Para habilitar el descifrado SSL, no solo se tiene que contar con la tecnología correcta, sino que una tríada de personas, procesos y herramientas deben alinearse y trabajar juntos en función del mismo objetivo.

Cómo Habilitar el Descifrado SSL: Mejores Prácticas

Una vez que exista un acuerdo entre los equipos, así como un entendimiento sobre los procesos y las herramientas adecuados, podrá comenzar a descifrar el tráfico. Siga estas mejores prácticas para obtener resultados óptimos y evitar las trampas comunes:

1. **Determinar el tráfico confidencial que no deba descifrarse.** Según las mejores prácticas, se debe descifrar todo el tráfico a excepción de aquel que pertenezca a categorías confidenciales como Salud, Finanzas, Gobierno, Fuerzas Armadas y Compras.

Personas	**Varios equipos deben trabajar juntos:** • El equipo Legal/Cumplimiento decide qué tipo de tráfico puede descifrarse; • El equipo de Recursos Humanos comunica el impacto del descifrado a todos los que usan su red, incluidos empleados, visitantes y contratistas. Además, todas las políticas de uso de computadoras, renuncias a derechos por inicio de sesión de visitantes y políticas de uso de contratistas deben mantenerse actualizadas para mantener el cumplimiento; • El equipo de Gestión de Seguridad administra la public key infrastructure (Infraestructura de Claves Públicas - PKI) ; • El equipo de TI instala certificados en endpoints, además de gestionar el diseño y el dimensionamiento; • El equipo de Servidores garantiza el descifrado del tráfico entrante destinado a los servidores web.
Procesos	**La habilitación del descifrado SSL implica múltiples procesos, como por ejemplo:** • Análisis de rendimiento para el diseño y el dimensionamiento; • Pruebas de impacto en la experiencia del usuario y problemas de implementación, además de escenarios como los certificados caducados y la exclusión de usuarios; • Apoyo de operaciones para abordar posibles problemas relacionados con el descifrado; • Control de cambios e implementación en fases del descifrado.
Herramientas	**La implementación exitosa y el análisis de resultados requieren herramientas para varias funciones, incluso:** • Gestión de certificados; • Análisis de rendimiento de redes; • NGFW para la creación de políticas de descifrado, exclusiones, registro y generación de informes.

2. **Agregar exclusiones para omitir el descifrado en circunstancias especiales:** Deberá omitir el descifrado en ciertas circunstancias como en el caso del tráfico que se interrumpe con el descifrado, usuarios específicos que deban omitir el descifrado por motivos legales o sitios web de socios a los que se les pueda permitir omitir los controles estrictos de certificados. Asegúrese de crear este tipo de exclusiones solo cuando estén justificadas y de procurar hacerlo lo menos posible.
3. **Configurar la verificación del estado de revocación de certificados:** Para verificar el estado de revocación de los certificados, el NGFW utiliza Online Certificate Status Protocols (Protocolos del Estado de Certificado En Línea - OCSPs) y/o Certificate Revocation Lists (Listas de Revocación de Certificados - CRLs). Asegúrese de que los certificados presentados durante el descifrado SSL sean válidos al configurar el firewall para realizar comprobaciones con CRLs/OCSPs.
4. **Configurar conjuntos de cifrado y versiones de protocolo SSL seguros:** Consulte con su equipo de gestión de seguridad para determinar cuáles son los conjuntos de cifrado que deben aplicarse y determinar cuál es la versión mínima aceptable de los protocolos SSL/TLS. Por ejemplo, su equipo de seguridad puede querer usar los algoritmos de intercambio de claves DHE o ECDHE para habilitar perfect forward secrecy (secreto perfecto hacia adelante - PFS), junto con el protocolo TLS 1.2. Como alternativa, el equipo podría querer bloquear el uso de versiones SSL/TLS vulnerables, como TLS 1.0 y SSLv3, y evitar los algoritmos débiles como MD5, RC4, SHA1 y 3DES. Implemente las recomendaciones de su equipo de seguridad en el NGFW.
5. **Implementar el certificado de descifrado de la autoridad de certificación principal de su empresa:** Implemente este certificado en su NGFW para que los usuarios finales no vean los mensajes de advertencia de los certificados SSL.
6. **Descifrar SSH además de SSL:** SSH es un requisito para algunas aplicaciones, pero se lo puede utilizar incorrectamente, tal como lo mencionamos antes. Por este motivo, se recomienda permitir el uso de SSH solo para aplicaciones y usuarios que lo necesiten, además de habilitar el descifrado SSH.

Para conocer más, consulte los siguientes recursos:

- ✓ **SSL Decryption Webpage**
- ✓ **Best Practice Assessment:** Esta evaluación gratuita le ayuda a maximizar las capacidades de su NGFW, como el descifrado SSL, para evitar ciberataques exitosos.

3000 Tannery Way
Santa Clara, CA 95054

Línea principal: +1.408.753.4000
Ventas: +1.866.320.4788
Soporte técnico: +1.866.898.9087

www.paloaltonetworks.com

decryption-why-where-and-how-wp-091918