paloalto
TECHDOCS

Prácticas recomendadas de descifrado

Version 10.2

docs.paloaltonetworks.com

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Last Revised

January 18, 2022

Table of Contents

Prácticas recomendadas de descifrado

No puede proteger su red contra amenazas que no puede ver e inspeccionar. Gartner señaló que en 2020, alrededor del 70 por ciento de las nuevas campañas de malware utilizaron varias formas de cifrado. De Google Informe de Transparencia muestra que no importa cómo analice el tráfico web de Google, en la mayoría de los casos, hasta el 95 por ciento de él está encriptado. Descifrar ese tráfico para proteger su red contra amenazas ocultas.

Este documento es una lista de comprobación simplificada de los procedimientos recomendados previos a la implementación, la implementación y después de la implementación que puede seguir para implementar el descifrado. Cada sección incluye vínculos a información detallada en la Guía de administración de PAN-OS, incluido cómo configurar las reglas y los perfiles de la directiva de descifrado.

- Planeación de la implementación de las prácticas recomendadas de descifrado SSL
- Implementar el descifrado SSL mediante las prácticas recomendadas
- Siga las prácticas recomendadas de descifrado SSL posteriores a la implementación

Planeación de la implementación de las prácticas recomendadas de descifrado SSL

Preparación para implementar el descifrado mediante el desarrollo de una estrategia de descifrado y un plan de despliegue. Activar el descifrado puede cambiar la forma en que los usuarios interactúan con algunas aplicaciones y sitios web, por lo que la planificación, las pruebas y la educación del usuario son fundamentales para una implementación exitosa.

STEP 1 | Establece metas.

- Planee descifrar tanto tráfico que no sea privado o confidencial como su firewall Recursos permitir. Esto reduce la superficie de ataque al exponer y prevenir amenazas cifradas. Comprenda las leyes y regulaciones locales sobre el tráfico que puede descifrar legalmente y los requisitos de notificación al usuario.
- Migrar de basado en puertos a basado en aplicaciones Seguridad reglas de directiva antes de crear e implementar reglas de directiva de descifrado. Si crea reglas de descifrado basadas en la directiva de seguridad basada en puertos y, a continuación, migra a la directiva de seguridad basada en aplicaciones, el cambio podría hacer que las reglas de descifrado bloqueen el tráfico que desea permitir porque es probable que las reglas de directiva de seguridad usen puertos predeterminados de la aplicación para evitar que el tráfico use puertos no estándar. La migración a reglas basadas en App-ID antes de implementar el descifrado garantiza que cuando pruebe la implementación de descifrado, descubrirá configuraciones erróneas de directivas de seguridad y las corregirá antes de implementar el descifrado para la población general de usuarios.

STEP 2 | Trabajar y educar a las partes interesadas como legal, finanzas, recursos humanos, ejecutivos, seguridad y TI / soporte para desarrollar una estrategia de implementación de descifrado.

- ☐ Obtenga las aprobaciones necesarias para descifrar el tráfico y proteger la empresa.
- ☐ Identifique y priorice el tráfico para descifrar:
  - Decida qué aplicaciones descifrar (sancionadas, no autorizadas). No permita aplicaciones cifradas no autorizadas.
  - Decida qué dispositivos descifrar (corporativos, BYOD, móviles, etc.).

    Las empresas no controlan los dispositivos BYOD. Si permite dispositivos BYOD en su red, descifre su tráfico y sumérjalo a la misma directiva de seguridad que aplica a otro tráfico de red. Para ello, redirija a los usuarios de BYOD a través de un portal de autenticación, indíqueles cómo descargar e instalar el certificado de CA y notifique claramente a los usuarios que su tráfico se descifrará. Eduque a los usuarios de BYOD sobre el proceso e inclúyalo en la política de privacidad y uso de computadoras de su empresa.

  - Decida si desea utilizar la misma directiva de descifrado para diferentes grupos, como diferentes grupos de empleados, contratistas, socios e invitados.
- ☐ Identifica el tráfico que no puedes descifrar:
  - Tráfico que interrumpe el descifrado para razones técnicas como la fijación de certificados, cifrados no compatibles o autenticación mutua.
  - Tráfico que usted Elija no descifrar como finanzas, salud, gobierno y otras categorías sensibles, incluidos usuarios y grupos como ejecutivos.
  - Comprenda completamente el tráfico que usted excepto desde el descifrado. No tiene visibilidad del tráfico cifrado y el firewall no puede aplicar perfiles de prevención de amenazas al tráfico cifrado.
- ☐ Prepare políticas legales y de uso de computadoras de recursos humanos actualizadas para distribuir a todos los empleados, contratistas, socios, invitados y cualquier otro usuario de la red para que cuando implemente el descifrado, los usuarios comprendan que sus datos pueden descifrarse y escanearse en busca de amenazas.
- ☐ Decide cómo manejar la verificación del certificado. Su modelo de negocio puede requerir compensaciones entre la seguridad y la experiencia del usuario. Comprender cómo desea manejar la verificación de certificados ayuda a determinar cómo configurar los perfiles de descifrado de proxy de reenvío SSL.
- ☐ Identifique el tráfico que desea registrar. Tenga en cuenta las diferencias legales y reglamentarias locales, y cómo afectan al tráfico que puede registrar y dónde puede almacenar los registros.

Coloque firewalls donde puedan ver todo el tráfico de red para que ningún tráfico cifrado obtenga acceso inadvertidamente a su red porque omite el firewall.

STEP 3 | Desarrolle un plan para implementar su infraestructura de clave pública (PKI).

- ☐ Si tiene una PKI existente, genere el certificado ssl Forward Trust CA a partir de la CA raíz de empresa como un certificado subordinado. Esto facilita la implementación porque los

dispositivos de red ya confían en la CA raíz de empresa, por lo que no tendrá problemas de certificados. Si no tiene una CA raíz empresarial, considere la posibilidad de obtener una.

Como alternativa, genere un certificado de CA raíz autofirmado en el firewall y cree un certificado subordinado de CA de confianza de reenvío en ese firewall para instalarlo en dispositivos de red. Los certificados autofirmados son los mejores para las pequeñas empresas que no tienen una CA raíz empresarial y para las pruebas de prueba de concepto (POC).

De manera similar a los dispositivos BYOD, las empresas no controlan los dispositivos invitados. Si permite dispositivos invitados en su red, descifre su tráfico y sumérjalo a la misma directiva de seguridad que aplica a otro tráfico de red. Para ello, redirija a los usuarios invitados a través de un portal de autenticación, indíqueles cómo descargar e instalar el certificado de CA y notifique claramente a los usuarios que su tráfico se descifrará. Incluya el proceso en la política de privacidad y uso de computadoras de su empresa.

- Generar ***separar*** Certificados de CA para Forward Trust y Forward Untrust. ¡No utilice la misma CA subordinada de PKI para ambos certificados y no firme el certificado Forward Untrust con la CA raíz de confianza! El certificado Forward Untrust advierte a los usuarios que el certificado que firma el servidor no es legítimo y que no deben dirigirse al sitio. Si la CA raíz de confianza firma el certificado de no confianza, los clientes confían en los certificados que no deberían ser de confianza porque los clientes confían en la CA raíz.
- Genere un certificado de CA de confianza de reenvío subordinado independiente para cada firewall. El uso de CA subordinadas independientes le permite revocar un certificado cuando retira un dispositivo (o par de dispositivos) sin afectar al resto de la implementación y reduce el impacto si necesita revocar un certificado. Los certificados de CA independientes ayudan al soporte técnico a solucionar problemas de usuario porque el mensaje de error del certificado incluye información sobre el firewall que atraviesa el tráfico. Aunque el uso de una CA subordinada de confianza directa en todos los firewalls es más fácil de implementar, el uso de un certificado independiente en cada firewall proporciona la mejor seguridad.
- Si necesita seguridad adicional para sus claves privadas, considere almacenarlos en un HSM.

STEP 4 | Realice una medición de referencia del rendimiento del firewall para comprender el consumo de recursos y los recursos de firewall disponibles para que pueda comparar el rendimiento después de implementar el descifrado y estimar el tamaño de la implementación del firewall necesario para admitir la cantidad de tráfico que desea descifrar.

- Trabaje con su PALO Alto Networks SE/CE para dimensionar la implementación del firewall y evitar errores de tamaño.
- Anote los recursos de firewall disponibles actualmente. En general, cuanto más estricta sea su seguridad, más recursos consumirá el descifrado. Los factores que afectan la cantidad de tráfico que puede descifrar incluyen:
  - La cantidad de tráfico SSL que desea descifrar.
  - Versión del protocolo TLS.
  - Tamaño de la clave.
  - Algoritmo de intercambio de claves. Los algoritmos efímeros de secreto directo perfecto (PFS) como DHE y ECDHE consumen más recursos que RSA, pero proporcionan una mayor seguridad porque el firewall genera una nueva clave de cifrado para cada sesión. Si

un atacante pone en peligro una clave de sesión, PFS impide que el atacante la utilice para descifrar otras sesiones entre el mismo cliente y servidor, mientras que RSA no lo hace.

- Autenticación de certificados. La autenticación de certificados RSA (esto no es lo mismo que el algoritmo de intercambio de claves RSA) consume menos ciclos de CPU que la autenticación de certificados ECDSA, pero ECDSA proporciona el más alto nivel de seguridad.
- Algoritmo de cifrado. El algoritmo de intercambio de claves determina si el algoritmo de cifrado es PFS o RSA.
- El modelo y recursos de firewall. Los modelos de firewall más nuevos tienen más recursos que los modelos más antiguos.

❑ Los tamaños de las transacciones afectan al rendimiento. Mida el tamaño promedio de la transacción de todo el tráfico, luego mida el tamaño promedio de la transacción del tráfico en el puerto 443 (puerto predeterminado para el tráfico cifrado HTTPS) para comprender la proporción de tráfico cifrado en el firewall en relación con su tráfico total y los tamaños promedio de transacción.

La combinación de estos factores determina cómo el descifrado consume los recursos de procesamiento del firewall. Si los recursos del firewall son un problema, use un descifrado más fuerte para el tráfico de mayor prioridad y mayor riesgo y use un descifrado menos intensivo del procesador para descifrar e inspeccionar el tráfico de menor prioridad hasta que pueda aumentar los recursos disponibles.

Dimensione el firewall para incluir espacio para el crecimiento en la cantidad de tráfico a descifrar porque cada día se cifra más tráfico.

STEP 5 | Planeación de una implementación por etapas y priorizada.

❑ Identifique a los primeros usuarios para defender el descifrado y lograr que los gerentes de departamento se unan al plan.

❑ Configure los POC para probar la estrategia de implementación antes de implementarla en la población general de usuarios. Mida la forma en que la implementación de POC de descifrado afecta la utilización de la CPU y la memoria del firewall para ayudar a comprender si el tamaño del firewall es correcto. Los POC también pueden revelar aplicaciones que rompen el descifrado técnicamente.

- Eduque a los participantes de POC sobre los cambios y cómo ponerse en contacto con el soporte técnico.
- Configure un POC de soporte técnico para los POC de descifrado para que el soporte tenga la oportunidad de desarrollar las mejores formas de admitir la implementación.
- Fase en descifrado. Planifique descifrar primero el tráfico más riesgoso (categorías de URL con más probabilidades de albergar tráfico malicioso, como juegos o de alto riesgo) y luego descifre más a medida que gane experiencia. Alternativamente, descifre las categorías de URL que no afectan primero a su negocio (si algo sale mal, no afectará al negocio), por ejemplo, las fuentes de noticias. En ambos casos, descifre algunas categorías de URL, escuche los comentarios de los usuarios, ejecute informes y verifique Registros de descifrado para asegurarse de que el descifrado funciona como se esperaba, y luego descifrar gradualmente algunas categorías de URL más, etc. Plan para hacer exclusiones de descifrado para excluir sitios del descifrado si no puede descifrarlos por razones técnicas o porque decide no descifrarlos.

- Evalúe el éxito de los POC y ajuste las prácticas de implementación.

- Educar a la población de usuarios antes de la implementación general. Los POC ayudan a identificar los puntos más importantes para comunicarse.
- Distribuya políticas legales y de uso de computadoras de recursos humanos actualizadas a todos los empleados, contratistas, socios, invitados y cualquier otro usuario de la red. Asegúrese de que todos entiendan que sus datos se pueden descifrar y analizar en busca de amenazas a medida que implementa el descifrado en cada departamento o grupo.
- Cree programaciones realistas que permitan tiempo para evaluar cada etapa de la implementación.

Implementar el descifrado SSL mediante las prácticas recomendadas

STEP 1 | Generar y distribuir claves y certificados para directivas de descifrado.

- Si tiene una PKI de empresa, genere el certificado de CA de confianza de reenvío para el tráfico de proxy de reenvío desde su CA raíz de empresa. De lo contrario, genere un certificado de CA raíz autofirmado en el firewall, cree una CA subordinada en ese firewall y, a continuación, distribuya el certificado autofirmado a todos los sistemas cliente. Los certificados autofirmados están diseñados para pruebas de laboratorio, implementaciones pequeñas y POC.
- Genere una CA de confianza de reenvío subordinada única para cada firewall (o una CA de confianza de reenvío para todo el firewall, según su planificación—un certificado es más fácil de implementar, pero los certificados separados proporcionan la mejor seguridad y otras ventajas). Las diferentes plataformas PKI tienen diferentes características para escalar la administración de certificados.
- Si no utiliza una CA empresarial, importe el certificado de CA de confianza de reenvío en el almacenamiento de CA de confianza de los sistemas cliente.
- No importar el Forward ***Desconfianza*** El certificado de CA en el almacenamiento de confianza de CA en los sistemas cliente o el certificado de no confianza no actuarán como desencadenador para sitios que no son de confianza. (Sin embargo, si la CA raíz autofirmada del firewall no está instalada como emisor de confianza en los sistemas cliente, puede usar un certificado de confianza de reenvío autofirmado).
- Utilice un método automatizado para distribuir los certificados de forward trust a dispositivos conectados, como el portal GlobalProtect de Palo Alto Networks, los Servicios de certificados de Microsoft AD (mediante objetos de directiva de grupo), las herramientas comerciales o las herramientas de código abierto.
- Si genera el certificado a partir de la CA raíz de empresa, importe el certificado en el firewall.
- Realice una copia de seguridad de la clave privada del certificado de CA de confianza de reenvío del firewall (no la clave maestra del firewall) en un repositorio seguro para que, si se produce un problema, pueda seguir accediendo al certificado de CA de confianza de reenvío.
- Si genera certificados y claves privadas a partir de la CA raíz de la empresa, bloquear la exportación de claves privadas. (Puede instalarlos en nuevos firewalls y panoramas desde la CA de su empresa, por lo que no necesita exportarlos desde PAN-OS).
- Si su plan requiere el uso de un HSM, Almacenar las claves privadas en el HSM.

STEP 2 | Configurar perfiles de descifrado para controlar protocolos, verificación de certificados y manejo de fallas.

- Perfiles de descifrado de proxy de reenvío SSL controlar la verificación de certificados del servidor, los modos de sesión y las comprobaciones de errores para el tráfico saliente. Bloquee sesiones con certificados caducados, emisores que no sean de confianza, versiones no compatibles y conjuntos de cifrado no compatibles. Bloquee las sesiones con autenticación de cliente a menos que una aplicación importante lo requiera, en cuyo caso debe crear un perfil de descifrado independiente que permita la autenticación de cliente y aplicarlo solo al tráfico que requiere autenticación de cliente.

- Perfiles de descifrado de inspección entrante SSL controlar los modos de sesión y comprobar los errores del tráfico entrante. Bloquee sesiones con versiones no compatibles y conjuntos de cifrado no compatibles.
- Configuración del protocolo SSL elementos del conjunto de cifrado de control: versiones de protocolo, algoritmos de intercambio de claves, algoritmos de cifrado y algoritmos de autenticación para el tráfico SSL Forward Proxy y SSL Inbound Inspection. Usa los cifrados más fuertes que puedas. En Proxy de reenvío, establezca el protocolo **Versión Mínima** Para **TLSv1.2** y el **Versión max** Para **Máximo** para bloquear protocolos débiles. Para la inspección de entrada SSL, cree perfiles independientes con la configuración del protocolo que coincida con las capacidades de los servidores cuyo tráfico entrante está inspeccionando.

  Utilice el conjunto de cifrado más fuerte que pueda. Cree políticas y perfiles de descifrado independientes para maximizar la seguridad. Si los sitios heredados que necesita para fines empresariales solo admiten cifrados más débiles, cree un perfil de descifrado independiente para permitir ese tráfico y aplíquelo en una directiva de descifrado solo a los sitios necesarios. Utilice la misma técnica para ajustar la seguridad frente al rendimiento para diferentes categorías de URL.

  *Muchas aplicaciones móviles utilizan certificados anclados. Dado que TLSv1.3 cifra la información del certificado, el firewall no puede agregar automáticamente estas aplicaciones móviles a la lista de exclusión de descifrado SSL. Para estas aplicaciones, asegúrese de que el perfil de descifrado **Versión max** se establece en TLSv1.2 o aplica una directiva de no descifrado al tráfico.*
- Sin perfiles de descifrado controlar la verificación del certificado del servidor para el tráfico que decida no descifrar. Bloquee sesiones con certificados caducados y emisores que no sean de confianza.

  No aplique un perfil sin descifrado al tráfico TLSv1.3. La información del certificado está cifrada, por lo que el firewall no puede bloquear sesiones basadas en la información del certificado.
- Para el proxy de reenvío SSL y el tráfico sin descifrado, configure la lista de revocación de certificados (CRL) y la revocación de estado de certificados en línea (OCSP) revocación de certificados comprueba que los certificados de sitio no se han revocado.
- Perfiles de proxy SSH modos de sesión de control y comprobaciones de fallos para el tráfico tunelizado SSH. Bloquee sesiones con versiones no compatibles y algoritmos no compatibles.

  La práctica recomendada Configuración del perfil de descifrado para el centro de datos y para el perímetro (puerta de enlace de Internet) los casos de uso difieren ligeramente de la configuración general de las mejores prácticas.

STEP 3 | Configurar Reglas de la directiva de descifrado Para definir el tráfico que se va a descifrar y realizar excepciones basadas en directivas para el tráfico que usted ***elegir*** no para descifrar.

- Cree reglas de directiva para exceptuar direcciones IP de destino específicas (por ejemplo, servidores financieros), usuarios y grupos de origen (por ejemplo, ejecutivos o personal de recursos humanos), dispositivos de origen y puertos de aplicaciones que elija no descifrar. Coloque estas reglas en la parte superior de la base de reglas de descifrado, antes de las reglas que descifran el tráfico. Para todo el tráfico excepto el tráfico TLSv1.3, adjunte un perfil

sin descifrado para aplicar SSL controles de verificación de certificados de servidor al tráfico cifrado. Esto evita descifrar inadvertidamente el tráfico que no desea descifrar.

- Use categorías de URL, categorías de URL personalizadas y listas dinámicas externas (EDL) para especificar las URL que no se deben descifrar, como servicios financieros, salud y medicina, gobierno y cualquier otra categoría que no desee descifrar por razones comerciales, legales o reglamentarias. Use un EDL en entornos con direcciones IP que cambian dinámicamente (por ejemplo, Office 365) o cambios frecuentes de pertenencia para actualizar sin tener que confirmar.

  Cree una categoría de URL personalizada o EDL que contenga todas las categorías que elija no descifrar para que solo necesite una regla de directiva de descifrado para ellas.

  Coloque estas reglas por encima de las reglas que descifran el tráfico en la base de reglas de descifrado.
- Configurar registro de descifrado y reenvío de registros.
- Si utiliza Duplicación de descifrado para copiar y enviar tráfico descifrado a una herramienta de recopilación de tráfico, tenga en cuenta las regulaciones de privacidad locales que pueden prohibir la duplicación o controlar el tráfico que puede reflejar.
- Crear una directiva para descifrar el resto del tráfico configurando Proxy de reenvío SSL, Inspección de entrada SSLy SSH Proxy reglas. Siempre descifre las categorías de almacenamiento y copia de seguridad en línea, correo electrónico basado en la web, alojamiento web, sitios personales y blogs, redes de entrega de contenido y URL de alto riesgo. Limitar el proxy SSH a los administradores que administran dispositivos de red, registran todo el tráfico SSH y configuran Autenticación multifactor para evitar el acceso SSH no autorizado.

STEP 4 | Agregar sitios a la Lista de exclusión de descifrado SSL (**Dispositivo** > **Gestión de certificados** > **Exclusión de descifrado SSL**) si rompen el descifrado técnicamente durante las pruebas POC y aún no están en la lista de exclusión. (Descifrar sitios que bloquean el descifrado técnicamente resulta en el bloqueo de ese tráfico).

STEP 5 | En Política de seguridad, bloquear el protocolo Quick UDP Internet Connections (QUIC).

Chrome y algunos otros navegadores establecen sesiones usando QUIC en lugar de TLS, pero QUIC utiliza cifrado propietario que el firewall no puede descifrar, por lo que el tráfico potencialmente peligroso puede ingresar a la red como tráfico cifrado. Cree dos reglas, una para bloquear la aplicación QUIC en puertos estándar y otra para bloquear los puertos UDP 80 y 443. El bloqueo de QUIC obliga al navegador a usar TLS.

STEP 6 | Reenviar el tráfico descifrado a WildFire para inspeccionarlo en busca de malware.

STEP 7 | Implemente el descifrado lentamente.

Descifre algunas categorías de URL, revise los comentarios de los usuarios y ejecute informes para asegurarse de que el descifrado funcione como se esperaba. Descifre gradualmente más categorías de URL hasta que alcance su objetivo. Comience con el tráfico de mayor prioridad (categorías de URL con más probabilidades de albergar tráfico malicioso, como los juegos) y descifre más a medida que aprende de la experiencia y refina el proceso. Una alternativa más conservadora es descifrar primero las categorías de URL que no afectan a su negocio, por ejemplo, las fuentes de noticias.

Siga las mejores prácticas de descifrado SSL posteriores a la implementación

Después de implementar el descifrado, asegúrese de que todo funcione como se esperaba y tome medidas para asegurarse de que siga funcionando como se esperaba.

STEP 1 | Verificar que el descifrado funciona como se esperaba.

STEP 2 | Mida el rendimiento del cortafuegos para asegurarse de que está dentro de las normas aceptables y para comprender el efecto del descifrado en el rendimiento.

Si desea descifrar más tráfico del que admiten los recursos del firewall, aumente la escala para tener suficientes recursos para descifrar todo el tráfico que desea descifrar y proteger su red.

STEP 3 | Instruya a los nuevos empleados a medida que los contrate para que entiendan su política de descifrado y no se sorprendan si no pueden acceder a un sitio en particular porque utiliza conjuntos de cifrado débiles.

STEP 4 | Revise y actualice periódicamente las políticas y los perfiles de descifrado.

STEP 5 | Usar herramientas de solución de problemas de descifrado como el Centro de Comando de Aplicaciones **Actividad SSL** widgets y el registro de descifrado (**Monitor** > **Registros** > **Descifrado**) para monitorear el tráfico de descifrado y resolver problemas de descifrado.

Ejemplos de flujo de trabajo de solución de problemas de descifrado mostrarle cómo usar las herramientas para investigar problemas.

STEP 6 | Cuando necesite cambiar el certificado en un servidor para el que funciona el cortafuegos Inspección de entrada SSL, añadir el nuevo certificado a la regla de política de descifrado para ese servidor antes de realizar el cambio en el servidor. Las reglas de la política de descifrado admiten varios certificados de servidor, por lo que puede conservar el certificado anterior y también agregar el nuevo certificado a la regla. Esto evita cualquier interrupción en el descifrado debido al cambio de certificado en el servidor cuando el cortafuegos solo tiene el certificado anterior. Agregar el nuevo certificado de servidor a la regla de política de descifrado garantiza que cuando cambie el certificado en el servidor, el firewall tenga el certificado correcto para continuar descifrando el tráfico sin problemas.

Asegúrese de eliminar los certificados no válidos de las reglas de la política de descifrado y del cortafuegos después de cambiar los certificados del servidor.

STEP 7 | Utilice la documentación de Palo Alto Networks y otros recursos para obtener más información sobre el descifrado y buscar información:

- los Guía del administrador de PAN-OS proporciona información detallada sobre los cortafuegos de próxima generación de Palo Alto Networks.
- La comunidad de Palo Alto Networks Live tiene un Lista de recursos de descifrado de artículos sobre configuración, instalación y administración de descifrado.
- Para encontrar certificados intermedios faltantes, visite Laboratorios SSL (Qualys).
- Para averiguar qué suites de cifrado admite un servidor, visite Qualys SSL Labs página de prueba SSL del servidor.
- Para consultar estadísticas actualizadas sobre los porcentajes de diferentes cifrados y protocolos en uso en los 150 000 sitios más populares del mundo para que pueda ver tendencias y comprender qué tan extendido es el soporte mundial para cifrados y protocolos más seguros, visite Qualys SSL Labs Página de pulso SSL.