Prácticas recomendadas de descifrado

Version 10.0 (EoL)

docs.paloaltonetworks.com

techDOCS paloalto NETWORKS

Contact Information

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

About the Documentation

- To ensure you are viewing the most current version of this document, or to access 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

October 28, 2020

Table of Contents

Prácticas recomendadas de descifrado

No es posible proteger la red de amenazas que no se puede ver o inspeccionar. Gartner predice que en 2020, más del 70 por ciento de las nuevas campañas de malware utilizarán varias formas de cifrado. El Informe de transparencia de Google muestra que no importa cómo analice el tráfico web de Google, en la mayoría de los casos, más del 90 por ciento está cifrado. Descifre el tráfico para proteger su red de amenazas ocultas.

Este documento es una lista de comprobación mejorada de las prácticas recomendadas de implementación previa, implementación e implementación posterior que puede seguir para implementar el descifrado. En cada sección, se incluyen enlaces a información detallada en la Guía del administrador de PAN-OS, entre lo que se incluye cómo configurar perfiles y reglas de política de descifrado.

- Planificación de implementación de práctica recomendada de descifrado SSL
- Implementación de descifrado SSL mediante prácticas recomendadas
- Siga las prácticas recomendadas de descifrado SSL posteriores a la implementación

Planificación de implementación de práctica recomendada de descifrado SSL

Prepárese para implementar el descifrado mediante el desarrollo de una estrategia de descifrado y un plan de implementación. Activar el descifrado puede cambiar la forma en que los usuarios interactúan con algunas aplicaciones y sitios web, por lo tanto, la planificación, prueba y capacitación de los usuarios son etapas críticas para una implementación exitosa.

STEP 1 | Establezca objetivos.

- ❑ Planifique el descifrado de tanto tráfico que no sea privado o sensible como le permitan los recursos de su cortafuegos. Esto reduce la superficie de ataque al exponer y prevenir amenazas cifradas. Comprenda las leyes y disposiciones locales sobre el tráfico que puede legalmente descifrar y los requisitos de notificaciones al usuario.
- ❑ Realice la migración desde las reglas de políticas de seguridad basadas en puertos hasta las basadas en la aplicación antes de crear e implementar reglas de política de descifrado. Si crea reglas de descifrado sobre la base de una política de seguridad basada en puertos y, luego, realiza la migración a la política de seguridad basada en la aplicación, el cambio podría provocar que las reglas de descifrado bloqueen el tráfico que intenta permitir. Esto se debe a que las reglas de política de seguridad probablemente usen puertos predeterminados de la aplicación para evitar que el tráfico use puertos no estándar. Realizar la migración a reglas basadas en App-ID antes de implementar el descifrado garantiza que cuando pruebe la implementación del descifrado, descubrirá errores de configuración de la política de seguridad y deberá repararlos antes de implementar el descifrado en la población general de usuarios.

STEP 2 | Brinde capacitación y trabaje con las partes interesadas, como los miembros del departamento de legal, Recursos Humanos, ejecutivos, seguridad y TI/soporte técnico 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 que desea descifrar:
  - Decida qué aplicaciones descifrará (aprobadas, no aprobadas). No permita aplicaciones cifradas no aprobadas.
  - Decida qué dispositivos descifrará (corporativos, personales [BYOD], móviles, etc.).

    Las empresas no controlan los dispositivos BYOD. Si permite dispositivos BYOD en su red, descifre su tráfico y sométalo a la misma política de seguridad que aplica en otro tráfico de red. Para hacerlo, redirija a los usuarios de BYOD por un portal cautivo, indíqueles cómo descargar e instalar el certificado de CA y notifíqueles claramente que su tráfico se descifrará. Informe a los usuarios de BYOD sobre el proceso e inclúyalo en la política de uso del ordenador y privacidad de su empresa.
  - Decida si desea usar la misma política de descifrado para diferentes grupos, como distintos grupos de empleados, contratistas, socios e invitados.
- ❑ Identifique el tráfico que no es posible descifrar:
  - El tráfico que interrumpe el descifrado por motivos técnicos, como el uso de un certificado fijado, cifrados no compatibles o una autenticación mutua.
  - El tráfico que elige no descifrar, como categorías del sector de finanzas, salud, gobierno y otras categorías sensibles, incluidos los usuarios y grupos, como los ejecutivos.

- Comprenda por completo el tráfico que espera del descifrado. No tiene visibilidad del tráfico cifrado y el cortafuegos no puede aplicar los perfiles de prevención de amenazas al tráfico cifrado.

- ❑ Prepare políticas de uso de ordenador del departamento legal y de recursos humanos para distribuir a todos los empleados, contratistas, socios, invitados y los demás usuarios de red de manera que cuando implemente el descifrado, los usuarios comprendan que sus datos pueden descifrarse y analizarse en busca de amenazas.
- ❑ Decida cómo administrar la verificación de certificados. El modelo de su empresa puede exigir que llegue a un término medio entre la seguridad y la experiencia el usuario. Comprender cómo desea administrar la verificación de certificados ayuda a determinar cómo configurar los perfiles de descifrado de proxy SSL de reenvío.
- ❑ Identifique el tráfico que desea registrar. Tenga en cuenta las diferencias reglamentarias y legales locales, y cómo estas afectan el tráfico que puede registrar y dónde puede almacenar los logs.

Coloque cortafuegos donde estos puedan ver todo el tráfico de red, de modo que el tráfico cifrado no obtenga acceso a su red porque omite el cortafuegos.

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

- ❑ Si tiene una PKI existente, genere el certificado de CA confiable de reenvío SSL de su 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, de modo que no enfrentará problemas con los certificados. Si no tiene una CA raíz de empresa, considere obtener una.

  De manera alternativa, genere un certificado de CA raíz autofirmado en el cortafuegos y cree un certificado de CA confiable de reenvío en ese cortafuegos para que se instale en los dispositivos de red. Los certificados autofirmados son la mejor opción para las empresas pequeñas que no tienen un CA raíz de empresa y para las pruebas de concepto (POC).

  

  De manera similar que con los dispositivos BYOD, las empresas no controlan los dispositivos invitado. Si permite dispositivos invitados en su red, descifre su tráfico y sométalo a la misma política de seguridad que aplica en otro tráfico de red. Para hacerlo, redirija a los usuarios invitados por un portal cautivo, 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 uso de ordenadores y privacidad de su empresa.
- ❑ Genere certificados de CA *diferentes* para el reenvío confiable y el reenvío no confiable. No use la misma CA subordinada de PKI para ambos certificados y no firme el certificado de reenvío no confiable con la CA raíz confiable. El certificado Forward Untrust advierte a los usuarios que el certificado que firma el servidor no es legítimo y que no deben ir al sitio. Si la CA raíz de confianza firma el certificado Untrust, entonces los clientes confían en los certificados que no deberían confiar porque los clientes confían en la CA raíz.
- ❑ Genere un certificado de CA de reenvío confiable subordinado distinto para cada cortafuegos. El uso de CA subordinadas independientes le permite revocar un certificado cuando retira un dispositivo (o un par de dispositivos) sin afectar el resto de la implementación y reduce el impacto en caso de que necesite revocar un certificado. Los certificados de CA separados ayudan al soporte técnico a solucionar problemas que el usuario emite porque el mensaje de error del certificado incluye información sobre el tráfico que atraviesa el cortafuegos. A pesar de que usar una CA subordinada confiable de reenvío en todos los cortafuegos es fácil de implementar, usar un certificado diferente en cada cortafuegos proporciona la mejor seguridad.
- ❑ Si necesita seguridad adicional para sus claves privadas, considere almacenarlas en un HSM.

STEP 4 | Tome una medida de referencia del rendimiento del cortafuegos para comprender el consumo de los recursos y los recursos de cortafuegos disponibles para comparar el rendimiento después de implementar el descifrado, y calcule el tamaño requerido de la implementación del cortafuegos para admitir la cantidad de tráfico que desea descifrar.

- ❑ Trabaje con SE/CE de Palo Alto Networks para medir el tamaño de la implementación del cortafuegos y evitar problemas de capacidad.
- ❑ Tenga en cuenta los recursos del cortafuegos disponibles actualmente. En general, cuanto mayor es su seguridad, mayor será el consumo de recursos del cortafuegos. Los factores que afectan cuánto tráfico puede descifrar incluyen los siguientes:
  - La cantidad de tráfico SSL que desea descifrar.
  - Versión de protocolo TLS.
  - Tamaño de clave.
  - Algoritmo de intercambio de clave. Los algoritmos efímeros de la Confidencialidad directa total (PFS) como DHE y ECDHE consumen más recursos que RSA, pero brindan mayor seguridad porque el cortafuegos genera una nueva clave de cifrado para cada sesión. Si un atacante pone en riesgo una clave de sesión, PFS evita que este la use para descifrar otras sesiones entre el mismo cliente y servidor, mientras que RSA no lo hace.
  - Autenticación del certificado. La autenticación de certificados de RSA (que no es lo mismo que el algoritmo de intercambio de claves de RSA) consume menos ciclos de CPU que la autenticación de certificados de ECDSA pero esta brinda el nivel de seguridad más alto.
  - Algoritmo de cifrado. El algoritmo de intercambio de claves determina si el algoritmo de descifrado es PFS o RSA.
  - El modelo y los recursos del cortafuegos. Los modelos de cortafuegos más nuevos tienen más recursos que los anteriores.
- ❑ El tamaño de las transacciones afecta el rendimiento. Mida el tamaño de la transacción promedio de todo el tráfico, luego mida el tamaño de la transacción promedio del tráfico en el puerto 443 (puerto predeterminado para el tráfico cifrado de HTTPS) para saber la proporción del tráfico cifrado en el cortafuegos en relación con el tráfico total y los tamaños de transacción promedio.

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

Mida el cortafuegos para incluir un margen para el crecimiento del volumen de tráfico para descifrar porque cada vez se descifra más tráfico.

STEP 5 | Planifique una implementación en etapas con prioridades.

- ❑ Identifique a los primeros usuarios que respaldarán el descifrado e integre a los administradores del departamento al plan.
- ❑ Configure las pruebas de concepto para probar la estrategia de implementación antes de implementarla en la población general de usuarios. Determine la forma en que la implementación de POC del descifrado afecta las CPU del cortafuegos y el uso de la memoria para ayudarlo a comprender si el tamaño del cortafuegos es correcto. Las POC también pueden revelar aplicaciones que interrumpen el descifrado en términos técnicos.
  - Capacite a los participantes de la POC sobre los cambios y cómo comunicarse con el soporte técnico.
  - Configure una POC de soporte técnico para las POC de descifrado, de modo que el soporte técnico tenga la oportunidad de desarrollar mejores formas de admitir la implementación.
  - Introduzca progresivamente el descifrado. Planifique descifrar primero el tráfico más peligroso (las categorías de URL con mayor probabilidad de tener tráfico malicioso, como los juegos o de alto riesgo) y luego, descifre más a medida que gane experiencia. Como alternativa, descifre primero las categorías de URL que no afecten a su empresa (si algo no funciona, no afectará a la empresa), por ejemplo, las fuentes de noticias. En ambos casos, descifre algunas categorías de URL, escuche los comentarios del usuario, ejecute informes y compruebe los logs de descifrado para garantizar que el descifrado funciona según lo esperado y, luego, descifre de manera gradual

algunas categorías de URL, etc. Planifique realizar exclusiones de descifrado para excluir sitios del descifrado si no puede descifrarlos por motivos técnicos o porque decide no hacerlo.
    - Determine el nivel de éxito de las pruebas de concepto (POC) y ajuste las prácticas de implementación.
- Capacite a la población de usuarios antes de la implementación general. Las pruebas de concepto ayudan a identificar los puntos más importantes para comunicarse.
- Distribuya las políticas de uso actualizadas de equipos informáticos para recursos humanos y jurídicos a todos los empleados, contratistas, socios, invitados y cualquier otro usuario de la red. Asegúrese de que todos comprendan que sus datos se pueden descifrar y analizar en busca de amenazas a medida que implementa el descifrado en cada departamento o grupo.
- Cree programas realistas que le den tiempo para evaluar cada etapa de la implementación.

Implementación de descifrado SSL mediante prácticas recomendadas

STEP 1 | Genere y distribuya claves y certificados para las políticas de descifrado.

- Si tiene una PKI de empresa, genere un certificado de CA confiable de reenvío para reenviar el tráfico proxy de su CA raíz de empresa. De lo contrario, genere un certificado de CA raíz autofirmado en el cortafuegos, cree una CA subordinada en ese cortafuegos y, luego, distribuya el certificado autofirmado a todos los sistemas cliente. Los certificados autofirmados tienen como objetivo realizar pruebas de laboratorio, implementaciones pequeñas y pruebas de concepto.
- Genere una CA de envío de confianza subordinada única para cada cortafuegos (o una CA de envío de confianza para todos los cortafuegos, según su planificación; un certificado es más fácil de implementar, pero los certificados separados brindan la mejor seguridad, además de otros beneficios). Las diferentes plataformas de PKI tienen distintas funciones para escalar la gestión de certificados.
- Si no utiliza una CA empresarial, importe un certificado de CA de confianza de reenvío al almacenamiento de CA fiable de los sistemas cliente.
- No importe el certificado de CA *no confiable* de reenvío en el almacenamiento de CA confiable en los sistemas cliente o el certificado no confiable no actuará como un activador de sitios no confiables. (Sin embargo, si el certificado de CA raíz autofirmado del cortafuegos no está instalado como un emisor de confianza en los sistemas cliente, puede usar un certificado no fiable de reenvío autofirmado).
- Use un método automatizado para distribuir los certificados confiables de reenvío en los dispositivos conectados, como el Portal de GlobalProtect de Palo Alto Networks, los servicios de certificado AD de Microsoft (con los objetos de política de grupo), herramientas comerciales o herramientas de código abierto.
- Si genera el certificado a partir de su CA raíz de empresa, impórtelo al cortafuegos.
- Realice una copia de seguridad de la clave privada del certificado de CA confiable de reenvío (no la clave principal del cortafuegos) en un repositorio seguro de modo que si ocurre un problema, pueda acceder al certificado de CA confiable de reenvío de todas maneras.
- Si genera certificados y claves privadas desde su CA raíz de empresa, bloquee la exportación de claves privadas. (Puede instalarlos en nuevos cortafuegos y Panoramas desde la CA de empresa, por lo que no necesita exportarlas desde PAN-OS).
- Si su plan requiere el uso de un módulo de seguridad de hardware (HSM), almacene las claves privadas en el HSM.

STEP 2 | Configure perfiles de descifrado para el control protocolos, la verificación de certificados y la gestión de fallas.

- Los perfiles de descifrado de proxy SSL de reenvío controlan la verificación de certificados del servidor, los modos de sesión y las verificaciones de fallas del tráfico saliente. Bloquee las sesiones con certificados caducados, emisores no confiables, versiones no compatibles y conjuntos de cifrados no compatibles. Bloquee sesiones con autenticación del cliente salvo que así lo requiera una aplicación importante, en tal caso debe crear un perfil de descifrado diferente que permita la autenticación de cliente y aplicarlo solo en el tráfico que necesita esta autenticación.
- Los perfiles de descifrado de inspección de entrada SSL controlan los modos de sesión y las verificaciones de fallas del tráfico entrante. Bloquee las sesiones con versiones no compatibles y conjuntos de cifrados no compatibles.
- La configuración del protocolo SSL controla los elementos del conjunto de cifrado, las versiones de protocolo, los algoritmos de intercambio de claves, los algoritmos de cifrado y los algoritmos de autenticación para al Proxy SSL de reenvío y el tráfico de inspección de entrada SSL. Utilice los cifrados más potentes que pueda. Para el proxy de reenvío, establezca el protocolo **Min Version**

(Versión mínima) en **TLSv1.2** y el protocolo **Max Version (Versión máxima)** en **Max Version ((Versión máxima)** para bloquear protocolos débiles. Para la inspección de entrada SSL, cree perfiles diferentes con una configuración de protocolo que coincida con las capacidades de los servidores cuyo tráfico entrante inspecciona.

Utilice el conjunto de cifrado más potente que pueda. Cree políticas y perfiles de descifrado independientes para maximizar la seguridad. Si los sitios antiguos que necesita para fines comerciales solo admiten cifrados más débiles, cree un perfil de descifrado independiente para permitir ese tráfico y aplíquelo en una política de descifrado solo en 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. Debido a que TLSv1.3 cifra la información del certificado, el cortafuegos no puede añadir automáticamente estas aplicaciones móviles a la Lista de exclusión de descifrado SSL. Para estas aplicaciones, asegúrese de que la Versión máxima del perfil de descifrado esté configurada en TLSv1.2 o aplique una política de No descifrado al tráfico.

- Los perfiles de No descifrado controlan la verificación de certificados del servidor para el tráfico que decide no descifrar. Bloquee las sesiones con certificados vencidos y emisores no fiables.

No aplique un perfil de No descifrado al tráfico TLSv1.3. La información del certificado está cifrada, por lo que el cortafuegos no puede bloquear sesiones basándose en la información del certificado.

- Para el tráfico sin descifrar y el proxy SSL de reenvío, configure ambas verificación de revocación de certificados de la Lista de revocación de certificados (Certificate Revocation List, CRL) y el Protocolo de estado de certificado en línea (Online Certificate Status Protocol, OCSP) a fin de verificar que no se hayan revocado certificados del sitio.
- Los perfiles de proxy SSL controlan los modos de sesión y las verificaciones de fallas del tráfico SSL de transmisión mediante túneles. Bloquee las sesiones con versiones y algoritmos no compatibles.

La configuración recomendada del perfil de descifrado para el centro de datos y los casos de uso para el perímetro (puerta de enlace de Internet) difieren un poco de la configuración general recomendada.

STEP 3 | Configure las reglas de la política de descifrado para definir el tráfico que se descifrará y para realizar excepciones basadas en la política para el tráfico que ***elige*** no descifrar.

- Cree reglas de políticas para excluir direcciones IP de destino específicas (por ejemplo, servidores financieros), grupos y usuarios de origen (por ejemplo, ejecutivos o personal de Recursos Humanos), dispositivos de origen y puertos de aplicación que elige 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 de No descifrado para aplicar controles de verificación de certificados de servidor SSL al tráfico cifrado. Esto evita que se descifre tráfico innecesario de manera inadvertida.
- Utilice Categorías de URL, Categorías de URL personalizadas y Listas dinámicas externas (EDL) para especificar las URL que no desea descifrar, como servicios financieros, salud y medicina, gobierno y cualquier otra categoría que no quiera descifrar para motivos de negocios, legales, o reglamentarios. Use una EDL en entornos con direcciones IP dinámicas (por ejemplo, Office 365) o cambios frecuentes de pertenencia para actualizar sin tener que confirmar.

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

  Coloque estas reglas encima de las reglas que descifran el tráfico en la base de reglas de descifrado.
- Configure el registro de descifrado y reenvío de logs.

- Si usa un reflejo de descifrado para copiar y enviar el tráfico descifrado a una herramienta de compilación, tenga en cuenta las disposiciones de privacidad locales que podrían prohibir el reflejo o control del tráfico que puede realizar.
- Cree políticas para descifrar el resto del tráfico mediante la configuración de reglas de proxy SSL de reenvío, inspección de entrada SSL y proxy SSH. Siempre descifre las categorías de URL de almacenamiento y copia de respaldo en línea, correo electrónico basado en la Web, hosting web, sitios y blogs personales, redes de entrega de contenido y URL de alto riesgo. Limite el proxy SSD a los administradores que gestionan los dispositivos de red, registre todo el tráfico SSH y configure la autenticación de múltiples factores para evitar el acceso SSH no autorizado.

STEP 4 | Añada sitios a la lista de exclusión de descifrado SSL [**Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **SSL Decryption Exclusion (Exclusión del descifrado SSL)**] si interrumpen el descifrado desde el punto de vista técnico durante la prueba de POC y no están en la lista de exclusión. (El descifrado de sitios que bloquean el descifrado técnicamente resulta en el bloqueo de ese tráfico).

STEP 5 | En la política de seguridad, bloquee el protocolo de Conexiones UDP rápidas en Internet (QUIC).

Chrome y algunos otros exploradores establecen sesiones con QUIC en lugar de TLS, pero QUIC usa cifrado de propiedad que el cortafuegos no puede descifrar, por lo que tráfico potencialmente peligroso puede entrar en la red como tráfico cifrado. Cree dos reglas, una para bloquear la aplicación de QUIC en los puertos estándar y otra para bloquear los puertos UDP 80 y 443. El bloqueo de QUIC obliga al navegador a utilizar TLS.

STEP 6 | Reenvío tráfico descifrado a WildFire para inspeccionarlo en busca de software malintencionado.

STEP 7 | Implemente el descifrado lentamente.

Descifre algunas categorías de URL, revise los comentarios del usuario y ejecute informes para garantizar que el descifrado funciona como se esperaba. Descifre gradualmente más categorías URL hasta que alcance su objetivo. Comience con el tráfico de mayor prioridad (categorías de URL con más probabilidades de tener tráfico malicioso, como los juegos) y descifre cada vez más a medida que gane experiencia y mejore el proceso. Una alternativa más conservadora es descifrar primero las categorías de URL que no afectan a su empresa, por ejemplo, las fuentes de noticias.

Siga las prácticas recomendadas de descifrado SSL posteriores a la implementación

Luego de que implemente el descifrado, asegúrese de que todo funcione con el nivel esperado y realice los pasos necesarios para garantizar que siga siendo así.

STEP 1 | Verifique que el descifrado funcione con el nivel esperado.

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

Si desea descifrar más tráfico del que permiten los recursos del cortafuegos, amplíe de forma que tenga suficientes recursos para descifrar todo el tráfico que desea descifrar y proteger su red.

STEP 3 | Dé formación a los nuevos empleados a medida que los contrata para que comprendan su política de descifrado y no se sorprendan si no pueden llegar a un sitio específico porque utiliza conjuntos de cifrado débiles.

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

STEP 5 | Utilice herramientas de resolución de problemas de descifrado como los widgets de **SSL Activity (Actividad SSL)** del Centro de comando de aplicaciones y el Log de descifrado [**Monitor (Supervisar)** > **Logs** > **Decryption (Descifrado)**] para supervisar el tráfico de descifrado y resolver problemas de descifrado.

Los Ejemplos de flujo de trabajo de resolución de problemas de descifrado le muestran cómo utilizar las herramientas para investigar problemas.

STEP 6 | Use la documentación de Palo Alto Networks y otros recursos para aprender más sobre el descifrado y buscar información:

- La Guía del administrador de PAN-OS proporciona información detallada sobre los cortafuegos de próxima generación de Palo Alto Networks.
- La comunidad Palo Alto Networks Live tiene una lista de recursos de descifrado con artículos sobre los ajustes, configuración y administración el descifrado.
- Para buscar certificados intermedios faltantes, visite SSL Labs (Qualys).
- Para conocer los conjuntos de cifrado que admite un servidor, visite la página de pruebas el servidor SSL de Qualys SSL Labs.
- Para revisar las estadísticas actualizadas sobre los porcentajes de diferentes cifrados y protocolos en uso en los 150 000 sitios más populares del mundo, de modo que pueda ver las tendencias y comprender lo amplio que es el soporte en el mundo de protocolos y cifrados más seguros, visite la página web SSL Pulse de Qualys SSL Labs.