

Integración de certificados Sectigo para Cisco Firepower Threat Defense (FTD)

Cisco FTD es un dispositivo de seguridad integral adoptado ampliamente por las empresas. Aunque Cisco FTD protege contra diversas amenazas, una gestión eficaz de los certificados SSL/TLS es esencial para garantizar la transmisión segura de datos y la autenticación de dispositivos. Sin una gestión adecuada de los certificados, las redes quedan expuestas a ataques y accesos no autorizados. La emisión y gestión de certificados SSL/TLS para proteger Cisco FTD debe estar totalmente automatizada y ser altamente escalable.

Al seleccionar una plataforma de gestión del ciclo de vida de certificados (CLM – Certificate Lifecycle Management), los usuarios de Cisco FTD deben priorizar la visibilidad y la automatización dentro de su infraestructura. La plataforma debe mejorar la visibilidad y la eficiencia operativa mediante flujos de trabajo automatizados, adaptarse a la escalabilidad futura y ofrecer servicios de soporte y mantenimiento fiables para garantizar un funcionamiento continuo, seguro y eficiente.

A continuación se presentan algunas consideraciones clave al elegir una plataforma CLM eficaz:

- ✓ Registrar, inscribir, sustituir y renovar certificados SSL/TLS de forma rápida y fiable.
- ✓ Automatizar los flujos de trabajo para gestionar necesidades crecientes de certificados a gran escala.
- ✓ Ofrecer soporte mediante tecnologías de automatización como API REST y SDK.
- ✓ Centralizar el control y la visibilidad sin salir del ecosistema de Cisco.
- ✓ Proporcionar soporte integral para varios tipos de certificados SSL/TLS, incluidos certificados comodín (wildcard) y multidominio.
- ✓ Ofrecer un soporte al cliente fiable y actualizaciones periódicas.

Cómo ayuda Sectigo

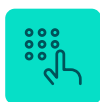
Con la integración de Sectigo y Cisco FTD, puede gestionar fácilmente sus certificados y proteger la infraestructura de red dedicada a la inspección y descifrado SSL, todo ello sin salir del ecosistema de Cisco. Esta integración ofrece una solución escalable para inscribir, renovar, sustituir y listar sus certificados de servidor SSL/TLS sin esfuerzo, respaldada mediante API REST y un kit de desarrollo de software (SDK).

Conector Sectigo para Cisco FTD

El conector Sectigo para Cisco FTD está diseñado para simplificar y automatizar la gestión de certificados digitales utilizados en la función de descifrado SSL. El conector facilita diversas operaciones del ciclo de vida, como la inscripción, renovación y sustitución, garantizando comunicaciones SSL/TLS totalmente seguras.

Al admitir tanto autoridades de certificación (CA) públicas como privadas y adaptarse a una amplia variedad de tipos de certificados, el conector Sectigo refuerza la infraestructura de seguridad de los despliegues de Cisco FTD, convirtiéndose en un activo indispensable para una defensa de red sólida.

El uso del conector Sectigo para Cisco FTD permite a sus equipos de TI beneficiarse de:



Emisión escalable de certificados SSL/TLS

Sectigo permite a los administradores de TI automatizar la emisión e instalación de certificados válidos en dispositivos Cisco FTD.



Renovación automatizada de certificados

Sectigo ofrece tecnologías de automatización transparentes que renuevan e instalan automáticamente los nuevos certificados cuando se acerca su caducidad, garantizando la seguridad continua y eliminando el riesgo de caídas del servicio.



Gestión completa del ciclo de vida de certificados

Además de la renovación, Sectigo proporciona capacidades de sustitución de certificados, necesarias por ejemplo cuando cambia el tamaño de clave, el algoritmo o los nombres alternativos del sujeto (SAN).



Seguridad reforzada para credenciales de integración

Mayor flexibilidad para proteger sus credenciales de integración frente a accesos no autorizados gracias a capacidades avanzadas de cifrado y descifrado (AES-256).



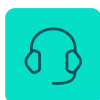
Visibilidad mejorada

Monitoree fácilmente todas las acciones sobre los certificados, rastree su uso y acceda a información detallada sobre las versiones de los paquetes, sin salir de su entorno habitual.



Configuración sencilla

La integración de Sectigo para Cisco FTD admite API REST y SDK, lo que permite una configuración y funcionamiento fluidos con CA privadas y públicas.



Soporte integral

Sectigo admite una amplia gama de certificados SSL/TLS, incluidos certificados comodín (wildcard), dominio único y certificados RSA, garantizando la cobertura de todas sus necesidades de seguridad.

La ventaja de Sectigo: Al integrar Sectigo CLM con Cisco FTD, disfrutará de múltiples beneficios, como la comodidad de la renovación automática y transparente de los certificados a punto de caducar, lo que garantiza una protección ininterrumpida. Nuestra solución escalable admite entornos Cisco FTD y simplifica el despliegue mediante la emisión automatizada basada en configuraciones predefinidas, reduciendo la carga administrativa.

Además, hemos implementado capacidades avanzadas de cifrado mediante AES-256 para proteger la seguridad de las credenciales de integración y los datos sensibles. En conjunto, estas funciones proporcionan una solución de seguridad completa y optimizada, mejorando la protección general y la eficiencia de su entorno Cisco.

Los certificados SSL/TLS y la plataforma CLM de Sectigo le ayudan a aplicar solidez criptográfica, mantener el cumplimiento normativo y prepararse para el mundo poscuántico, todo ello manteniendo la simplicidad operativa a gran escala. La integración con Cisco FTD automatiza la emisión y el ciclo de vida de los certificados, eliminando los procesos manuales que provocan interrupciones del servicio.

Para obtener más información sobre la integración de Sectigo para Cisco FTD, certificados SSL/TLS o gestión de certificados en general, póngase en contacto con el equipo de ventas de Sectigo en: sales@sectigo.com.



Acerca de Sectigo

Sectigo es un proveedor líder en la Gestión del Ciclo de Vida de Certificados (CLM), que ayuda a las organizaciones a asegurar las identidades humanas y de máquinas mientras reduce los riesgos ocultos de la confianza digital moderna. A medida que el volumen de certificados aumenta y sus periodos de validez se reducen, los certificados no gestionados se convierten en una fuente de interrupciones del servicio, vulnerabilidades de cumplimiento y problemas operativos. Sectigo utiliza la automatización orquestada para ofrecer simplicidad a gran escala (Simplicity at Scale) a través de su plataforma CLM nativa en la nube, unificando la visibilidad, el control y la gestión del ciclo de vida en entornos complejos.

Con más de 700.000 clientes, incluido el 65 % de las empresas del Fortune 500, Sectigo es una de las autoridades de certificación más grandes y con mayor trayectoria, ofreciendo una confianza digital inigualable desde hace más de 20 años.

Para más información, visite www.sectigo.com o siganos en [LinkedIn](#).

