

Intégration des certificats Sectigo pour Cisco Firepower Threat Defense (FTD)

Cisco FTD est un équipement de sécurité complet très largement adopté par les entreprises. Bien que Cisco FTD protège contre de nombreuses menaces, une gestion efficace des certificats SSL/TLS est essentielle pour garantir la transmission sécurisée des données et l'authentification des équipements. Sans une gestion adéquate des certificats, les réseaux restent vulnérables aux attaques et aux accès non autorisés. L'émission et la gestion de vie des certificats (CLM) SSL/TLS protégeant Cisco FTD doivent être entièrement automatisées et hautement évolutives.

Lors du choix d'une plateforme de gestion du cycle de vie des certificats (CLM – Certificate Lifecycle Management), les utilisateurs de Cisco FTD doivent donner la priorité à la visibilité et à l'automatisation au sein de leur infrastructure. La plateforme doit renforcer l'efficacité opérationnelle grâce à des flux de travail automatisés, s'adapter à l'évolution future du parc et offrir des services d'assistance et de maintenance fiables pour garantir un fonctionnement continu, sécurisé et efficace.

Voici quelques critères essentiels lors du choix d'une plateforme CLM efficace :

- ✓ Répertorier, enrôler, remplacer et renouveler les certificats SSL/TLS rapidement et de manière fiable.
- ✓ Automatiser les flux de travail pour gérer à grande échelle des besoins croissants en certificats.
- ✓ Prendre en charge l'automatisation via des technologies modernes comme les API REST et les SDK.
- ✓ Centraliser le contrôle et la visibilité sans quitter l'écosystème Cisco.
- ✓ Offrir une prise en charge complète de divers certificats SSL/TLS, notamment les certificats génériques (wildcard) et multi-domaines.
- ✓ Proposer un support client fiable et des mises à jour régulières.

Sectigo peut vous aider

Grâce à l'intégration entre Sectigo et Cisco FTD, vous pouvez facilement gérer vos certificats et protéger l'infrastructure réseau utilisée pour le déchiffrement SSL, le tout sans quitter l'écosystème Cisco. Cette intégration offre une solution évolutive pour enrôler, renouveler, remplacer et répertorier sans effort vos certificats serveurs SSL/TLS, grâce à une API REST et un kit de développement logiciel (SDK).

Le connecteur Sectigo pour Cisco FTD

Le connecteur Sectigo pour Cisco FTD est conçu pour simplifier et automatiser la gestion des certificats numériques utilisés par la fonctionnalité de déchiffrement SSL. Le connecteur facilite diverses opérations du cycle de vie des certificats, telles que l'enrôlement, le renouvellement et le remplacement, garantissant ainsi des communications SSL/TLS totalement sécurisées.

En prenant en charge les autorités de certification (CA) privées et publiques, tout en s'adaptant à un large éventail de types de certificats, le connecteur Sectigo renforce l'infrastructure de sécurité des déploiements Cisco FTD, ce qui en fait un atout indispensable pour une défense réseau robuste.

L'exploitation du connecteur Sectigo pour Cisco FTD permet à vos équipes informatiques de bénéficier de :



Émission évolutive de certificats SSL/TLS

Sectigo permet aux administrateurs informatiques d'automatiser l'émission et l'installation de certificats valides sur les équipements Cisco FTD.



Renouvellement automatisé des certificats

Sectigo propose des technologies d'automatisation transparentes qui renouvellent et installent automatiquement les nouveaux certificats à l'approche de leur expiration, garantissant une sécurité continue et éliminant les risques de panne.



Gestion complète du cycle de vie des certificats

En plus du renouvellement, Sectigo offre des capacités de remplacement de certificats, indispensables par exemple en cas de modification de la taille des clés, des algorithmes ou des noms alternatifs du sujet (SAN).



Sécurité renforcée des identifiants d'intégration

Une flexibilité accrue pour protéger vos identifiants d'intégration contre tout accès non autorisé grâce à des fonctionnalités avancées de chiffrement et de déchiffrement (AES-256).



Visibilité accrue

Surveillez facilement toutes les actions sur les certificats, suivez leur utilisation et accédez à des rapports détaillés sur les versions des packages, sans quitter votre environnement habituel.



Configuration simple

L'intégration de Sectigo pour Cisco FTD prend en charge les API REST et les SDK, permettant une configuration et une exploitation fluides avec les CA privées comme publiques.



Prise en charge globale

Sectigo prend en charge un large éventail de certificats SSL/TLS, notamment les certificats génériques (wildcard), mono-domaine et RSA, répondant ainsi à l'ensemble de vos besoins de sécurité.

L'avantage Sectigo : En intégrant Sectigo CLM à Cisco FTD, vous bénéficiez de nombreux avantages, notamment le renouvellement automatique et fluide des certificats expirés, garantissant une protection ininterrompue. Notre solution évolutive prend en charge les environnements Cisco FTD et simplifie le déploiement grâce à l'émission automatisée basée sur des configurations prédéfinies, réduisant ainsi la charge administrative.

De plus, nous avons mis en œuvre des capacités de chiffrement avancées en AES-256 pour garantir la sécurité des identifiants d'intégration et des données sensibles. Ensemble, ces fonctionnalités offrent une solution de sécurité complète et rationalisée, renforçant la protection et l'efficacité de votre environnement Cisco.

Les certificats SSL/TLS et la plateforme CLM de Sectigo vous aident à imposer une sécurité cryptographique robuste, à maintenir votre conformité et à vous préparer au monde post-quantique, tout en maintenant la simplicité des opérations à grande échelle. L'intégration de Sectigo avec Cisco FTD automatise l'émission et le cycle de vie des certificats, éliminant définitivement les processus manuels à l'origine des pannes.

Pour plus d'informations sur l'intégration de Sectigo pour Cisco FTD, les certificats SSL/TLS ou la gestion des certificats en général, veuillez contacter l'équipe commerciale de Sectigo à l'adresse : sales@sectigo.com.



À propos de Sectigo

Sectigo est un leader mondial de la gestion du cycle de vie des certificats, aidant les organisations à sécuriser les identités humaines et machines tout en réduisant les risques invisibles de la confiance numérique moderne. À mesure que le volume de certificats augmente et que leur durée de vie diminue, les certificats non gérés deviennent une source d'interruptions de service, de risques de non-conformité et de perturbations opérationnelles. Sectigo utilise l'automatisation orchestrée pour offrir une simplicité à grande échelle via sa plateforme CLM native dans le cloud, réunissant visibilité, contrôle et gestion du cycle de vie au sein d'environnements complexes.

Avec plus de 700 000 clients, dont 65 % des entreprises du Fortune 500, Sectigo est l'une des autorités de certification les plus importantes et les plus anciennes, forte de plus de 20 ans d'expertise dans la fourniture d'une confiance numérique inégalée.

Pour plus d'informations, visitez www.sectigo.com ou suivez-nous sur [LinkedIn](#).

