

Integrazione dei certificati Sectigo per Cisco Firepower Threat Defense (FTD)

Cisco FTD è una soluzione di sicurezza aziendale completa e ampiamente diffusa. Sebbene Cisco FTD protegga le reti da numerose minacce, una gestione efficace dei certificati SSL/TLS è fondamentale per garantire la trasmissione sicura dei dati e l'autenticazione dei dispositivi. Senza una corretta gestione dei certificati, le reti rimangono vulnerabili ad attacchi e accessi non autorizzati. L'emissione e la gestione dei certificati SSL/TLS per la protezione di Cisco FTD devono essere completamente automatizzate e altamente scalabili.

Nella scelta di una piattaforma di gestione del ciclo di vita dei certificati (CLM – Certificate Lifecycle Management), gli utenti Cisco FTD devono dare la priorità alla visibilità e all'automazione all'interno della propria infrastruttura. La piattaforma deve migliorare la visibilità e l'efficienza operativa attraverso flussi di lavoro automatizzati, garantire la scalabilità futura e offrire servizi di supporto e manutenzione affidabili per assicurare un funzionamento continuo, sicuro ed efficiente.

Di seguito sono riportati alcuni criteri chiave per la scelta di una piattaforma CLM efficace:

- ✓ Censire, registrare, sostituire e rinnovare i certificati SSL/TLS in modo rapido e affidabile.
- ✓ Automatizzare i flussi di lavoro per gestire volumi crescenti di certificati su vasta scala.
- ✓ Supportare l'automazione tramite tecnologie moderne come API REST e SDK.
- ✓ Centralizzare il controllo e la visibilità senza uscire dall'ecosistema Cisco.
- ✓ Fornire un supporto completo per varie tipologie di certificati SSL/TLS, inclusi certificati wildcard e multi-dominio.
- ✓ Garantire un supporto clienti affidabile e aggiornamenti regolari.

Il supporto di Sectigo

Grazie all'integrazione tra Sectigo e Cisco FTD, è possibile gestire facilmente i certificati e proteggere l'infrastruttura di rete utilizzata per la decifratura SSL, il tutto senza mai uscire dall'ecosistema Cisco. Questa integrazione offre una soluzione scalabile per registrare, rinnovare, sostituire e monitorare i certificati server SSL/TLS, grazie al supporto di API REST e Software Development Kit (SDK).

Il connettore Sectigo per Cisco FTD

Il connettore Sectigo per Cisco FTD è progettato per semplificare e automatizzare la gestione dei certificati digitali impiegati nella funzionalità di decifratura SSL. Il connettore gestisce le diverse operazioni del ciclo di vita dei certificati, come la registrazione, il rinnovo e la sostituzione, garantendo comunicazioni SSL/TLS del tutto sicure.

Supportando sia Autorità di Certificazione (CA) pubbliche che private e gestendo un'ampia gamma di tipologie di certificati, il connettore Sectigo rafforza l'infrastruttura di sicurezza dei sistemi Cisco FTD, rappresentando un elemento indispensabile per una difesa di rete avanzata.

L'adozione del connettore Sectigo per Cisco FTD offre ai team IT i seguenti vantaggi:



Emissione scalabile di certificati SSL/TLS

Sectigo consente agli amministratori IT di automatizzare l'emissione e l'installazione di certificati validi sugli apparati Cisco FTD.



Rinnovo automatizzato dei certificati

Sectigo mette a disposizione tecnologie di automazione che rinnovano e installano automaticamente i nuovi certificati all'approssimarsi della scadenza, garantendo sicurezza continua ed eliminando il rischio di fermi macchina.



Gestione completa del ciclo di vita dei certificati

Oltre al rinnovo, Sectigo offre funzionalità di sostituzione dei certificati, necessarie ad esempio in caso di variazione della dimensione della chiave, dell'algoritmo o dei nomi alternativi del soggetto (SAN).



Sicurezza avanzata per le credenziali di integrazione

Maggiore flessibilità nella protezione delle credenziali di integrazione contro accessi non autorizzati grazie a funzionalità di cifratura avanzata (AES-256).



Visibilità migliorata

Monitoraggio semplice di tutte le operazioni sui certificati, tracciamento del loro utilizzo e accesso a dettagli sulle versioni dei pacchetti, senza uscire dall'ambiente operativo di riferimento.



Configurazione semplice

L'integrazione di Sectigo per Cisco FTD supporta API REST e SDK, consentendo un'attivazione e una gestione fluide sia con CA private che pubbliche.



Supporto completo

Sectigo gestisce un'ampia gamma di certificati SSL/TLS, tra cui certificati wildcard, singolo dominio e certificati RSA, soddisfacendo ogni esigenza di sicurezza.

Il vantaggio di Sectigo: L'integrazione di Sectigo CLM con Cisco FTD garantisce numerosi vantaggi, tra cui il rinnovo automatico e trasparente dei certificati in scadenza, che assicura una protezione senza interruzioni. La nostra soluzione scalabile supporta gli ambienti Cisco FTD e semplifica le attività operative tramite l'emissione automatizzata basata su configurazioni predefinite, riducendo le attività amministrative.

Inoltre, abbiamo implementato algoritmi di cifratura avanzati in AES-256 per garantire la massima sicurezza delle credenziali di integrazione e dei dati sensibili. Insieme, queste caratteristiche offrono una soluzione di sicurezza completa ed efficiente, aumentando la protezione complessiva dell'ambiente Cisco.

I certificati SSL/TLS e la piattaforma CLM di Sectigo aiutano a garantire una solida protezione crittografica, a mantenere la conformità e a prepararsi all'era crittografica post-quantistica, mantenendo semplice la gestione su vasta scala. L'integrazione con Cisco FTD automatizza l'emissione e il ciclo di vita dei certificati, eliminando i processi manuali causa di disservizi.

Per ulteriori informazioni sull'integrazione Sectigo per Cisco FTD, sui certificati SSL/TLS o sulla gestione dei certificati in generale, contattare il team commerciale di Sectigo all'indirizzo: sales@sectigo.com.



Informazioni su Sectigo

Sectigo è un provider leader nella gestione del ciclo di vita dei certificati (CLM), che aiuta le organizzazioni a proteggere le identità umane e macchina riducendo al contempo i rischi nascosti della moderna fiducia digitale. Con l'aumento dei volumi di certificati e la riduzione della loro durata, i certificati non gestiti stanno diventando causa di disservizi, vulnerabilità di conformità e interruzioni operative. Sectigo sfrutta l'automazione orchestrata per offrire semplicità su vasta scala (Simplicity at Scale) tramite la sua piattaforma CLM cloud-native, unendo visibilità, controllo e gestione del ciclo di vita in ambienti complessi. Con oltre 700.000 clienti, tra cui il 65% delle aziende Fortune 500, Sectigo è una delle Autorità di Certificazione più grandi e consolidate, con oltre 20 anni di eccellenza nella fiducia digitale.

Per ulteriori informazioni, visita il sito www.sectigo.com o seguici su [LinkedIn](https://www.linkedin.com/company/sectigo).

