Managing Certificates on Cisco, Palo Alto, and Fortinet Routers

Network security appliances from Cisco, Palo Alto Networks, and Fortinet sit at the center of a huge share of enterprise network infrastructure, and each vendor handles certificate management through its own distinct tooling and conventions. This article covers the practical realities of managing certificates across these three major platforms, building on the general router certificate best practices covered elsewhere in this series.

Cisco: IOS and Firepower Certificate Management

Cisco devices running IOS or IOS-XE typically manage certificates through the command-line interface, using crypto PKI trustpoint configurations that define how a device requests, stores, and uses certificates, whether through manual enrollment, SCEP-based automated enrollment, or importing certificates generated externally. Firepower devices, Cisco's next-generation firewall platform, add a graphical management interface through Firepower Management Center, which simplifies certificate deployment somewhat but still benefits considerably from API-driven automation for organizations managing certificates across many devices rather than configuring each one individually through the console.

Palo Alto Networks: Panorama-Centralized Management

Palo Alto firewalls integrate certificate management into their broader policy and configuration framework, commonly managed centrally through Panorama for organizations running more than a handful of devices. Panorama allows administrators to push certificate updates across an entire fleet of managed firewalls from a single console, which considerably simplifies what would otherwise be a per-device manual task, and supports integration with external certificate authorities through APIs for organizations building automated issuance pipelines rather than relying on manual certificate uploads through the graphical interface.

Fortinet: FortiGate and FortiManager

FortiGate appliances handle certificates through their own web-based management console or command-line interface, with FortiManager serving a similar centralized role to Cisco's Firepower Management Center or Palo Alto's Panorama for organizations managing certificates across a large fleet of FortiGate devices. Fortinet devices commonly serve both server-side certificates, for administrative access and VPN termination, and support certificate-based authentication for site-to-site and remote access VPN configurations, both of which need their own tracked renewal schedule within whatever centralized certificate inventory an organization maintains.

The Common Thread Across All Three Platforms

Despite their different interfaces and terminology, all three platforms share the same underlying challenges covered throughout this series: avoiding reliance on default self-signed certificates for administrative access, ensuring the full certificate chain is properly installed rather than just the end-entity certificate, and moving away from manual, console-driven certificate updates toward automated issuance and deployment wherever the platform's tooling supports it. Organizations running a mixed environment of Cisco, Palo Alto, and Fortinet devices particularly benefit from a centralized certificate management platform that can abstract across these vendor-specific differences, rather than managing three entirely separate certificate workflows in parallel.

Automating Across Multi-Vendor Network Environments

Most enterprise networks run more than one of these vendors simultaneously, whether through acquisition, regional deployment differences, or deliberate multi-vendor strategy, which makes a unified certificate management approach considerably more valuable than vendor-specific manual processes repeated three different ways. Certificate lifecycle management platforms with API integrations across multiple network vendors let security teams manage renewal, deployment, and monitoring from one system, regardless of which specific appliance ultimately consumes the certificate.

AI-Assisted Network Security Operations

AI-driven security operations tooling increasingly integrates with these platforms to monitor configuration drift, flag anomalous traffic, and in some deployments, assist with automated remediation across Cisco, Palo Alto, and Fortinet environments simultaneously. These AI-assisted tools themselves typically need properly authenticated, certificate-secured API access into each vendor's management platform, meaning the certificate hygiene of the management interfaces described above directly affects the reliability of any AI-driven network monitoring layered on top of them.

The Countdown Is Already Running: 200 Days, 100 Days, 47 Days

Every certificate conversation in 2026 eventually arrives at the same clock, and it is worth closing on it here. The CA/Browser Forum's Ballot SC-081v3 is not a proposal under discussion; it is an approved, already-in-motion schedule. Maximum public TLS certificate lifetimes fall from 398 days to 200 days on March 15, 2026. They fall again to 100 days on March 15, 2027. By March 15, 2029, they drop to just 47 days, with domain validation itself needing to be re-proven roughly every 10 days.

01

Translate that into operational terms and the picture gets stark quickly. An organization currently renewing certificates a few times a year will be handling renewal events on the order of every couple of weeks by the end of this countdown, across every endpoint it operates. Manual tracking, calendar reminders, and a spreadsheet somebody checks once a month will not survive contact with that cadence. What has always been an occasional chore is becoming a continuous, automated operation, whether an organization plans for it or not.

02

Certificates on network appliances from any of these vendors are just as bound by the shrinking public lifetime schedule below as a web server's certificate, and multi-vendor environments in particular need centralized automation to keep pace as renewal frequency climbs toward every 47 days across every platform simultaneously.

03

The 200-day, 100-day, and 47-day milestones are not distant hypotheticals; the first has already arrived. Organizations that build the automation loop now, generating keys, vaulting them securely, brokering issuance across Certificate Authorities through APIs, and rebinding certificates to live endpoints without manual intervention, will meet each deadline without disruption. Organizations that wait will be rebuilding their certificate operations under deadline pressure, with far less room for error and far less time to get it right. The countdown is the call to action. The only real decision left is whether to automate on your own schedule, or on the CA/Browser Forum's.