Troubleshoot FMC Automatic Configuration Deployment during FTD Registration that Breaks VPN Connectivity

Contents

Issue

During migration of Firewall Threat Defense (FTD) devices to a new Firewall Management Center (FMC) environment, the FMC automatically deployed configuration immediately upon FTD registration. This automatic deployment occurred before manual VPN policy reattachment and certificate configuration could be completed, resulting in VPN connectivity loss for Secure Client/AnyConnect users and causing an unplanned service outage.

Environment

- Secure Firewall Management Center (FMC).
- FTD configured for Secure Client/AnyConnect VPN services.
- Migration scenario from existing FMC to new FMC environment.

Resolution

The user resolved the immediate connectivity issue through these steps:

Step 1. Reconfigure the device configuration

The user reconfigured the original device configuration and the working VPN settings that were overwritten during the automatic deployment.

Step 2: Reattach policies

Proper policies were manually reattached to ensure VPN functionality was restored and configured correctly for the new FMC environment.

Cause

The automatic deployment behavior during FTD registration to a new FMC is expected functionality, not a defect. The expectation of the user from manual deployment control was based on documentation interpretation, but the default behavior of the system is to deploy configuration automatically upon device registration to ensure policy consistency across the FMC-managed environment.

Tip: Consider using device templates to apply day 2 configuration changes at the time of FTD registration. Device templates were introduced in FMC version 7.6.0.

Related Content

- Cisco Technical Support & Downloads