Secure Firewall Content Update Scheduling Best Practices

Issue

Organizations managing Firewall Threat Defense (FTD) devices with Firewall Management Center (FMC) require guidance on best practices for applying security and content updates. Specifically, there is uncertainty around how frequently different update types must be applied, whether updates can be scheduled rather than applied immediately, and what the operational impacts of these updates are. The question arises because Cisco releases content updates frequently, sometimes weekly, and administrators need to understand if these must be applied immediately upon release or if they can be scheduled according to organizational maintenance windows and change management policies.

Environment

- Cisco Secure Firewall Firepower, all versions
- Firepower Management Center, all versions

Resolution

This table shows the purpose of each update type in Firepower.

Update Type	Purpose	Notes
SRU / LSP	Intrusion rule updates (Snort 2 and Snort 3 respectively)	Maintains intrusion detection/prevention rules
GeoDB	Geolocation data for IP addresses	Used for geolocation-based traffic filtering
VDB	Vulnerability information and host fingerprints	Used for vulnerability assessment and risk analysis

Cisco Secure Firewall content updates are categorized into three distinct types, each with different release frequencies and recommended scheduling practices. This table outlines the best practice scheduling recommendations for each update type:

Update Type	Release Frequency	Suggested Schedule	Default FMC Schedule	Navigation Path (To Modify)
SRU / LSP	Frequent	Daily	Daily	System > Content Updates > Rule Updates
GeoDB	~Weekly	Weekly	Weekly	System > Content Updates > Geolocation Updates
VDB	~Monthly	Weekly	Weekly	System > Tools: Scheduling > Weekly Software Download

For optimal security configurations and posture, the best practice is to apply any of these updates as soon as they are released by Cisco. Some of these update files can be fairly large and bandwidth allocations need to be considered. It is suggested to install the larger updates outside of peak traffic hours, if using the same network.

SRU/LSP (Intrusion Rules) Updates

Snort Rule Updates (SRU) and Lightweight Security Packages (LSP) contain intrusion detection and prevention rules. These updates must be applied as frequently as operationally feasible to maintain protection against emerging threats.

To modify the SRU/LSP schedule: Navigate to **System > Content Updates > Rule Updates** in the FMC interface to adjust the time, date, and frequency settings.

SRU/LSP updates support automated deployment and can be scheduled to deploy automatically after download and installation.

GeoDB (Geolocation Database) Updates

Geolocation Database updates provide current geographic location data for IP addresses and are typically released weekly.

To modify the GeoDB schedule: Navigate to **System > Content Updates > Geolocation Updates** in the FMC interface to adjust the scheduling parameters.

GeoDB updates can be scheduled for download and installation, but deployment to managed devices

requires manual push and cannot be fully automated like SRU/LSP updates.

VDB (Vulnerability Database) Updates

Vulnerability Database updates are released approximately monthly and are managed as software updates rather than content updates.

To modify the VDB schedule: Navigate to **System > Tools: Scheduling** and modify the **Weekly Software Download** task to adjust the download frequency and timing.

VDB updates fall under software updates and cannot be deployed independently. They are included when performing manual deployments that compile all pending changes.

Deployment Considerations

When deploying updates, the FMC compiles all pending configuration changes and can include multiple types of content updates in a single deployment operation. Some updates can cause brief Snort service restarts during deployment, which must be considered when scheduling updates during production hours.

Organizations must align update schedules with their change management policies and consider scheduling updates during maintenance windows if brief service interruptions are a concern for their operational environment.

Cause

This was a configuration and operational guidance request rather than a technical malfunction. The need for clarification arose from uncertainty around update scheduling practices, automation capabilities, and the operational impact of different content update types in Cisco Secure Firewall environments.

Related Content

- Cisco Secure Firewall Management Center Administration Guide, 7.6: Updates
- Cisco Technical Support & Downloads