安全防火牆內容更新計畫最佳實踐

問題

通過防火牆管理中心(FMC)管理防火牆威脅防禦(FTD)裝置的組織需要獲得有關應用安全和內容更新的最佳實踐的指導。具體而言，對於必須應用不同更新型別的頻率、是否可以安排更新而不是立即應用更新，以及這些更新對運營有何影響，都存在不確定性。出現此問題的原因是，思科會頻繁發佈內容更新（有時是每週一次），管理員需要瞭解這些更新是必須在發佈後立即應用，還是可以按照組織維護視窗和變更管理策略進行計畫。

環境

- Cisco Secure Firewall Firepower，所有版本
- Firepower管理中心，所有版本

解析

此表顯示了Firepower中每個更新型別的用途。

更新型別	目的	備註
SRU/LSP	入侵規則更新（分別為Snort 2和Snort 3）	維護入侵檢測/防禦規則
GeoDB	IP地址的地理位置資料	用於基於地理定位的流量過濾
VDB	漏洞資訊和主機指紋	用於漏洞評估和風險分析

思科安全防火牆內容更新分為三種不同的型別，每種型別的發佈頻率和建議的計畫做法不同。此表概述了每種更新型別的最佳實踐計畫建議：

更新型別	發佈頻率	建議的計畫	預設FMC計畫	導航路徑（要修改）
SRU/LSP	頻繁	每日	每日	系統>內容更新>規則更新
GeoDB	~每週	每週	每週	系統>內容更新>地理位置更新
VDB	~每月	每週	每週	System > Tools:Scheduling > Weekly Software Download

為了獲得最佳的安全配置和狀態，最佳實踐是在思科發佈這些更新後立即應用這些更新。其中一些更新檔案可能相當大，因此需要考慮頻寬分配。如果使用相同的網路，建議在流量高峰時段之外安裝更大的更新。

SRU/LSP（入侵規則）更新

Snort規則更新(SRU)和輕量級安全包(LSP)包含入侵檢測和防禦規則。必須儘可能頻繁地應用這些更新，以針對新出現的威脅提供保護。

要修改SRU/LSP計畫，請執行以下操作：在FMC介面中導航到System > Content Updates > Rule Updates，以調整時間、日期和頻率設定。

SRU/LSP更新支援自動部署，可以計畫下載和安裝後自動部署。

GeoDB（地理定位資料庫）更新

地理位置資料庫更新提供IP地址的當前地理位置資料，通常每週發佈一次。

修改GeoDB計畫：在FMC介面中導航到System > Content Updates > Geolocation Updates，以調整計畫引數。

GeoDB更新可以計畫下載和安裝，但部署到受管裝置需要手動推送，並且不能像SRU/LSP更新那樣完全自動化。

VDB（漏洞資料庫）更新

漏洞資料庫更新大約每月發佈一次，並作為軟體更新而不是內容更新進行管理。

修改VDB排程：導覽至System > Tools:安排和修改「每週軟體下載」任務以調整下載頻率和時間。

VDB更新屬於軟體更新，不能單獨部署。在執行編譯所有待執行更改的手動部署時包含這些更改。

部署注意事項

部署更新時，FMC會編譯所有掛起的配置更改，並在單個部署操作中包括多種型別的內容更新。某些更新可能會導致在部署過程中短暫的Snort服務重新啟動，在生產過程中計畫更新時必須考慮這一點。

如果短暫的服務中斷是組織運營環境所關心的問題，組織必須使更新計畫與其變更管理策略保持一致，並考慮在維護時段安排更新。

原因

這是一個配置和操作指南請求，而不是技術故障。之所以需要澄清，是因為圍繞更新計畫做法、自動化功能以及思科安全防火牆環境中不同內容更新型別的操作影響存在不確定性。

相關內容

- 思科安全防火牆管理中心管理指南7.6:更新
- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。