安全防火墙内容更新计划最佳实践

问题

使用防火墙管理中心(FMC)管理防火墙威胁防御(FTD)设备的组织需要有关应用安全和内容更新的最佳实践的指导。具体而言，对于必须应用不同更新类型的频率、是否可以安排更新而不是立即应用更新，以及这些更新对运营有何影响，都存在不确定性。出现此问题的原因是，思科经常发布内容更新，有时是每周发布一次。管理员需要了解这些更新是必须在发布后立即应用，还是可以按照组织维护窗口和变更管理策略进行安排。

环境

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

分辨率

下表显示了Firepower中每种更新类型的用途。

更新类型	目的	备注
SRU/LSP	入侵规则更新（分别为Snort 2和Snort 3）	维护入侵检测/防御规则
GeoDB	IP地址的地理定位数据	用于基于地理定位的流量过滤
VDB	漏洞信息和主机指纹	用于漏洞评估和风险分析

Cisco Secure Firewall内容更新分为三种不同的类型，每种类型的发布频率和推荐的计划做法不同。此表概述了每种更新类型的最佳实践计划建议：

更新类型	发布频率	建议时间表	默认FMC计划	导航路径（修改）
SRU/LSP	频繁	每天	每天	System > Content Updates > Rule Updates
GeoDB	~每周	每周	每周	System > Content Updates > Geolocation Updates
VDB	~每月	每周	每周	System > Tools:Scheduling > Weekly Software Download

为了获得最佳的安全配置和状态，最佳实践是在思科发布这些更新后立即应用这些更新。其中一些更新文件可能相当大，需要考虑带宽分配。如果使用相同的网络，建议在流量高峰时段之外安装较大的更新。

SRU/LSP（入侵规则）更新

Snort规则更新(SRU)和轻型安全包(LSP)包含入侵检测和防御规则。必须尽可能频繁地应用这些更新，以针对新出现的威胁提供保护。

修改SRU/LSP计划的步骤：在FMC界面中导航到System > Content Updates > Rule Updates以调整时间、日期和频率设置。

SRU/LSP更新支持自动部署，可计划在下载和安装后自动部署。

GeoDB（地理定位数据库）更新

地理位置数据库更新提供IP地址的当前地理位置数据，通常每周发布一次。

修改GeoDB调度的步骤：在FMC界面中导航到System > Content Updates > Geolocation Updates以调整调度参数。

可以安排GeoDB更新进行下载和安装，但部署到受管设备需要手动推送，不能像SRU/LSP更新那样完全自动化。

VDB（漏洞数据库）更新

漏洞数据库更新大约每月发布一次，并作为软件更新而不是内容更新进行管理。

修改VDB调度的步骤：导航到System > Tools:安排和修改每周软件下载任务以调整下载频率和时间。

VDB更新属于软件更新，不能单独部署。执行手动部署时包含这些更改，这些手动部署会编译所有待处理的更改。

部署注意事项

部署更新时，FMC会编译所有待处理的配置更改，并在单个部署操作中包含多种类型的内容更新。某些更新可能会导致在部署过程中短暂的Snort服务重新启动，这必须在生产过程中计划更新时予以考虑。

如果运营环境需要考虑短暂的服务中断，组织必须根据变更管理策略调整更新计划，并考虑在维护时段安排更新。

原因

这是一个配置和操作指南请求，而不是技术故障。由于更新计划做法、自动化功能以及思科安全防火墙环境中不同内容更新类型的操作影响存在不确定性，因此需要澄清。

相关内容

- 思科安全防火墙管理中心管理指南7.6:更新
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。