セキュアファイアウォールコンテンツ更新スケジューリングのベストプラクティス

お問い合わせ内容

Firewall Management Center(FMC)を使用してファイアウォール脅威対策(FTD)デバイスを管理している組織では、セキュリティとコンテンツの更新を適用するためのベストプラクティスに関するガイダンスが必要です。具体的には、異なる更新タイプを適用する頻度、更新を即時に適用するのではなくスケジュールできるかどうか、更新による運用上の影響は不明です。問題が生じる原因は、シスコがコンテンツの更新を頻繁に（場合によっては毎週）リリースしており、管理者は、更新をリリース後すぐに適用する必要があるのか、組織のメンテナンスウィンドウと変更管理ポリシーに従ってスケジュールを設定できるのかを理解する必要があるためです。

環境

- Cisco Secure Firewall Firepower（全バージョン）
- Firepower Management Center(FMC)、すべてのバージョン

解決策

次の表に、Firepowerの各更新タイプの目的を示します。

更新の種類	目的	注意事項
SRU/LSP	侵入ルールの更新（それぞれSnort 2およびSnort 3）	侵入検知/防御ルールの維持
GeoDB	IPアドレスの位置情報	位置情報ベースのトラフィックフィルタリングに使用される

VDB	脆弱性情報とホストフィンガープリント	脆弱性アセスメントとリスク分析に使用

Cisco Secure Firewallのコンテンツアップデートは、それぞれ異なるリリース頻度と推奨されるスケジューリング方法を持つ3つのタイプに分類されます。次の表に、各アップデートタイプのベストプラクティスのスケジューリング推奨事項の概要を示します。

更新の種類	リリース頻度	推奨スケジュール	デフォルトのFMCスケジュール	ナビゲーションパス（変更対象）
SRU/LSP	頻度	日次	日次	[システム] > [コンテンツの更新] > [ルールの更新]
GeoDB	~ 毎週	毎週	毎週	[システム] > [コンテンツの更新] > [位置情報の更新]
VDB	~ 月1回	毎週	毎週	[システム] > [ツール]: [スケジュール] > [ソフトウェアの週次ダウンロード]

最適なセキュリティ設定とポスチャを実現するには、シスコがリリースするとすぐに、これらのアップデートを適用することがベストプラクティスです。これらの更新ファイルの中には非常に大きいものもあり、帯域幅の割り当てを考慮する必要があります。同じネットワークを使用している場合は、トラフィックのピーク時間外に大規模なアップデートをインストールすることを推奨します。

SRU/LSP（侵入ルール）のアップデート

Snort Rule Updates(SRU)およびLightweight Security Package(LSP)には、侵入検知および防御ルールが含まれています。新たな脅威に対する保護を維持するため、これらのアップデートは運用上可能な限り頻繁に適用する必要があります。

SRU/LSPスケジュールを変更するには、FMCインターフェイスでSystem > Content Updates > Rule Updatesの順に移動し、時刻、日付、および頻度の設定を調整します。

SRU/LSPアップデートは自動導入をサポートし、ダウンロードおよびインストール後に自動的に導入するようにスケジュールできます。

GeoDB（位置情報データベース）の更新

位置情報データベースのアップデートでは、IPアドレスの現在の地理的位置データが提供され、通常は週に1回リリースされます。

GeoDBスケジュールを変更するには、FMCインターフェイスでSystem > Content Updates > Geolocation Updatesの順に移動し、スケジューリングパラメータを調整します。

GeoDBの更新は、ダウンロードとインストールのスケジュールを設定できますが、管理対象デバイスへの導入には手動プッシュが必要で、SRU/LSPの更新のように完全に自動化することはできません。

VDB（脆弱性データベース）の更新

脆弱性データベースのアップデートは、ほぼ毎月リリースされ、コンテンツのアップデートではなく、ソフトウェアのアップデートとして管理されます。

VDBスケジュールを変更するには、System > Tools: Schedulingの順に選択し、Weekly Software Downloadタスクを変更して、ダウンロードの頻度とタイミングを調整します。

VDBのアップデートはソフトウェアアップデートに該当するため、単独で導入することはできません。すべての保留中の変更をコンパイルする手動展開を実行する際に含まれます。

導入に関する考慮事項

更新を展開する場合、FMCは保留中のすべての構成変更をコンパイルし、1回の展開操作で複数のタイプのコンテンツ更新を含めることができます。一部の更新は、導入時に短時間のSnortサービス再起動を引き起こす可能性があります。これは、実稼働時間中に更新をスケジュールするときに考慮する必要があります。

更新スケジュールを変更管理ポリシーに合わせ、短いサービス中断が運用環境で懸念される場合は、メンテナンス時間帯に更新をスケジュールすることを検討する必要があります。

原因

これは、技術的な不具合ではなく、設定と運用ガイダンスの要求でした。明確化の必要性は、アップデートのスケジューリング方法、自動化機能、およびCisco Secure Firewall環境のさまざまなコンテンツ更新タイプの運用上の影響に関する不確実性から生じました。

関連コンテンツ

- Cisco Secure Firewall Management Centerアドミニストレーションガイド7.6：アップデート
- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。