Cisco セキュリティ アプライアンス上の Sophos Anti-Virus の更新が Sophos の Web サイトで入手できるものと異なる

目次

概要

このドキュメントでは、シスコ セキュリティ アプライアンス上の Sophos Anti-Virus 更新が Sophos Web サイトで入手可能なものと異なる理由について説明します。

前提条件

次の項目に関する知識が推奨されます。

- Cisco E メール セキュリティ アプライアンス（ESA）
- AsyncOS のすべてのバージョン

背景説明

次の 2 種類の更新があります。 Sophos Anti-Virus エンジンの更新と Sophos ウイルス ID ファイル（統合開発環境（IDE）ファイル）の更新。

Sophos Anti-Virus エンジンは、AsyncOS オペレーティング システムに完全に統合されています。 Sophos は、ほぼ毎月、ウイルス対策スキャン エンジンの新しいバージョンを生成します。 新しいバージョンには、最新のウイルス定義と、新しいウイルスの種類を認識し、既知の問題を修正するために必要なコード変更が含まれています。 新たなウイルスが検出されると、Sophos は IDE ファイルと呼ばれるウイルス ID ファイルをリリースします。 これらは、過去 90 日以内のエンジンで動作します。

Sophos の更新は、C シリーズ アプライアンス内の Cisco AsyncOS によって自動的に管理されます。 Sophos がエンジンの新しいバージョンをリリースすると、シスコは品質保証（QA）プロセスを通してそれらを認定してから、シスコ アップデート サーバに配置し、C シリーズ アプライアンスが自動的にダウンロードして更新できるようにします。 IDE ウイルス定義ファイルがリリースされると、それらのファイルがサービスを通して自動的に移動し、Sophos のリリースから

数分以内にシスコ アップデート サーバに配置されます。

Sophos IDE ウイルス署名は有効で、以前のエンジン バージョンで動作します。 最新の IDE がすべて読み込まれ、Cisco C シリーズ アプライアンスで実行しているエンジン バージョンで動作します。

設定

Cisco ESA 上のファイルは、Sophos から直接入手可能なファイルと同期していないように見える場合があります。 このことは、Sophos とほとんどの北米のお客様の間のタイムゾーンの違いによってさらに複雑になる可能性があります。 Sophos Web サイトは、英国のオックスフォードの近くの Sophos 本社で管理されています。 サイトへの投稿は、ローカル タイム ゾーンの GMT に基づいて日付が設定されます。 Sophos IDE ファイルを関連付ける場合に少し混乱が起きます。 日付が 1 日ずれるような大きな時間差が生じることがあるだけでなく、シスコでは IDE ファイルに対して別の番号付け方式を採用しています。 Sophos IDE サイトをチェックして、IDE がリリースされた日時と、その日とその前の日に他にいくつのファイルがリリースされたかを確認することによってそれらのファイルを照合することができますが、シスコはこのサイトに投稿されていない増分変更を受け取る場合があるため、これはあまり有効な方法とは言えません。 シスコでは 10 分ごとに Sophos Web サイトを照会しています。 アプライアンスのデフォルト設定は 5 分ごとにシスコ ダウンロード サイトを照会することです。 最悪、15 分の遅延が発生します。

IDE ファイルの番号付け方式では日付を使用します。 たとえば、"Sophos IDE Rules 2004121402 Tue Dec 14 06:27:14 2004" は、ここで公開された 12 月 14 日の 3 つ目の更新（0 から数えて）に対応します。

Sophos の自動更新間隔を 15 分のデフォルト設定に設定することをお勧めします。 [Security Services] -> [Anti-Virus] ページで Web ベースの GUI を使用して、シスコから連続的に更新を入手していることをチェックします。 この情報は、次のように **antivirusstatus** CLI コマンドを使用することによっても入手できます。

```
mail3.example.com> antivirusstatus
    SAV Engine Version        4.03
   IDE Serial                2006031503
   Last Engine Update        Tue Mar 14 01:01:49 2006
   Last IDE Update           Thu Mar 16 06:33:50 2006
   Last Update Attempt       Thu Mar 16 09:18:51 2006
   Last Update Success       Thu Mar 16 06:33:50 2006
```

更新が成功しない（アラート メッセージが表示される）場合は、GUI の [Update Now] ボタンまたは **antivirusupdate** CLI コマンドを使用して手動更新を試すことができます。 更新のステータスはウイルス対策ログ ファイルに表示されます。 次に、例を示します。

```
smtp.example.com> tailCurrently configured logs:
1. "antivirus" Module: thirdparty Format: Anti-Virus
2. "avarchive" Module: mail Format: Anti-Virus Archive
3. "bounces" Module: bounces Format: Bounces
4. "brightmail" Module: thirdparty Format: Symantec Brightmail Anti-Spam
5. "cli_logs" Module: system Format: CLI Audit Logs
6. "error_logs" Module: mail Format: IronPort Text
7. "ftpd_logs" Module: ftpd Format: IronPort Text
8. "gui_logs" Module: gui Format: IronPort Text
9. "mail_logs" Module: mail Format: IronPort Text
10. "rptd_logs" Module: rptd Format: IronPort Text
```

```
11. "sntpd_logs" Module: sntpd Format: IronPort Text
12. "status" Module: mail Format: Status Logs
13. "system_logs" Module: system Format: IronPort Text
Enter the number of the log you wish to tail.
[]> 1Press Ctrl-C to stop.
Thu Mar 16 09:08:50 2006 Info: Current IDE serial=2006031503. No update needed.
Thu Mar 16 09:13:50 2006 Info: Checking for Sophos Update
Thu Mar 16 09:13:50 2006 Info: Current SAV engine ver=4.03. No engine update needed
Thu Mar 16 09:13:50 2006 Info: Current IDE serial=2006031503. No update needed.
Thu Mar 16 09:18:50 2006 Info: Checking for Sophos Update
Thu Mar 16 09:18:50 2006 Info: Current SAV engine ver=4.03. No engine update needed
Thu Mar 16 09:18:50 2006 Info: Current IDE serial=2006031503. No update needed.
Thu Mar 16 09:23:50 2006 Info: Checking for Sophos Update
Thu Mar 16 09:23:50 2006 Info: Current SAV engine ver=4.03. No engine update needed
Thu Mar 16 09:23:50 2006 Info: Current IDE serial=2006031503. No update needed.
^C
smtp.example.com>
```