在Cisco安全设备的Sophos抗病毒更新是与在Sophos网站的那些联机不同

目录

简介

本文描述在Cisco安全设备的Sophos抗病毒更新为什么跟在Sophos网站的那些联机不同。

Prerequiste

Cisco 建议您了解以下主题：

- 思科电子邮件安全工具(ESA)
- AsyncOS所有版本

背景

有更新的两种类型：对Sophos抗病毒引擎的对Sophos病毒标识文件的更新和更新(集成开发环境(IDE)文件)。

Sophos抗病毒引擎充分地集成到AsyncOS操作系统。Sophos近似每个月生成他们的抗病毒扫描引擎新版本。新版本包含要求识别病毒新类型和调整已知问题的两个当前病毒定义和所有代码更改。因为另外的病毒是已发现， Sophos发表病毒标识文件，呼叫IDE文件。这些与少于90天是年纪的引擎一起使用。

Sophos更新由在C系列设备的思科AsyncOS自动地管理。因为Sophos发布他们的引擎新版本，思科通过质量保证(QA)进程在思科更新服务器合格他们，然后放置他们，以便您的C系列设备将自动地下载并且更新他们。当IDE病毒定义文件发布，这些通过服务在思科更新服务器自动地移动和被放置在几分钟内他们的版本由Sophos。

Sophos IDE病毒签名有效并且运行与上一个引擎版本。所有当前(IDEintegrated device electronics)将装载和与在思科C系列设备的引擎版本运行一起使用。

配置

有时在思科ESA的文件可能看来是出于与那些可得到的同步直接地从Sophos。这可以由在Sophos和多数北美洲客户之间的时区区别进一步复杂化。Sophos网站由在牛津附近的Sophos总部管理UK的。在站点的投稿定日期与本地时区， GMT。它有点混淆关联Sophos IDE文件。不仅大时差经常导致日期分开似乎一个天，但是思科使用一不同的编号模式IDE文件。您能设法通过检查Sophos IDE站点发现匹配这些文件，当IDE发布，以及多少天和在它的前一天，而是作为思科经常将拾起在此站点没张贴的递增更改，这不是多数高效的方法的其他发布。思科查询Sophos网站每10分钟。设备的默认设置是查询思科下载站点每五分钟。在最坏的情况下将有15分钟延迟。

IDE文件的编号模式是日期。例如， “Sophos IDE规则2004121402星期二十二月对第三次更新的14 06:27:14 2004"相互关系(请开始计数从零)在Decemeber第14，发布此处。

思科建议您设置Sophos自动更新间隔为15分钟默认设置。检查通过使用基于Web的GUI，您从思科得到连续更新，在**安全Services->Anti-Virus**页。例如此信息也是可用的使用CLI命令的**antivirusstatus**， ：

```
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
```

如果您的更新不是成功的(您将收到警报消息，如果这发生)，使用在GUI的**更新**按钮您能**当前**尝试一次手工的更新或者CLI命令的**antivirusupdate**。更新的状况在防病毒日志文件显示。例如：

```
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>
```