Sophos Anti−virus Updates on Cisco Security Appliance are Different from Those Available on the Sophos Web Site

Document ID: 117916

Contributed by Jackie Fleming, Cisco TAC Engineer.
Jul 11, 2014

Contents

Introduction

This document describes why the Sophos Anti−Virus updates on the Cisco security appliance are different than those available on the Sophos web site.

Prerequiste

Cisco recommends that you have knowledge of these topics:

- Cisco Email Security Appliance (ESA)
- All versions of AsyncOS

Background

There are two types of updates: updates to the Sophos Anti−Virus engine and updates to the Sophos virus identity files (Integrated Development Environment (IDE) files).

The Sophos Anti−virus engine is fully integrated into the AsyncOS operating system. Sophos generates a new version of their anti−virus scanning engine approximately every month. The new version contains both current virus definitions and any code changes that are required to recognize new types of viruses and to fix known issues. As additional viruses are discovered, Sophos releases virus identity files, called IDE files. These will work with engines that are less than 90 days old.

Sophos updates are managed automatically by Cisco AsyncOS in the C−Series appliance. As Sophos releases new versions of their engine, Cisco qualifies them through a quality assurance (QA) process, and then places them on the Cisco update servers so that your C−Series appliance will automatically download and update them. As IDE virus definition files are released, these move automatically through the service and are placed on the Cisco update servers within a few minutes of their release by Sophos.

Sophos IDE virus signatures are valid and operate with the previous engine versions. All current IDEs will be loaded and will work with the engine version running in the Cisco C−Series appliance.

Configure

Sometimes the files on the Cisco ESA may appear to be out of synchronization with those available directly from Sophos. This can be further complicated by the timezone difference between Sophos and most North American customers. The Sophos web site is managed by Sophos headquarters near Oxford in the UK. The postings on the site are dated with the local timezone, GMT. It is a bit confusing to correlate Sophos IDE files. Not only does the large time difference often cause the dates to seem a day apart, but Cisco uses a different numbering schema for the IDE files. You can try to match these files by checking the Sophos IDE site to see when an IDE was released, as well as how many others were released that day and the day before it, but as Cisco will often pick up incremental changes not posted on this site, this is not the most efficient method. Cisco queries the Sophos website every 10 minutes. The default setting for an appliance is to query the Cisco download site every five minutes. In the worst case there will be a 15 minute delay.

The numbering schema for the IDE files is the date. For example, "Sophos IDE Rules 2004121402 Tue Dec 14 06:27:14 2004" correlates to the thrid update (start counting from zero) on Decemeber 14th, published here.

Cisco recommends that you set the Sophos Automatic Update Interval to the default setting of 15 minutes. Check that you are getting continuous updates from Cisco by using the web−based GUI, on the ***Security Services−>Anti−Virus*** page. This information is also available using the ***antivirusstatus*** CLI command, for example:

```
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
```

If your updates are not successful (you will receive an alert message if this happens), you can try a manual update using the ***Update Now*** button in the GUI, or the ***antivirusupdate*** CLI command. The status of the update is shown in the antivirus log file. For example:

```
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>
```

Updated: Jul 11, 2014 Document ID: 117916