Cisco Security Appliance의 Sophos Anti-virus 업데이트는 Sophos 웹 사이트에서 제공하는 업데이트와 다릅니다.

목차

소개

이 문서에서는 Cisco 보안 어플라이언스의 Sophos Anti-Virus 업데이트가 Sophos 웹 사이트에서 제공되는 업데이트와 다른 이유를 설명합니다.

프리레퀴스트

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco ESA(Email Security Appliance)
- 모든 버전의 AsyncOS

배경

업데이트에는 두 가지 유형이 있습니다.Sophos Anti-Virus 엔진에 대한 업데이트와 Sophos 바이러스 ID 파일(IDE(통합 개발 환경) 파일)에 대한 업데이트

Sophos Anti-virus 엔진은 AsyncOS 운영 체제에 완전히 통합됩니다.Sophos는 약 매월 안티바이러스 검사 엔진의 새 버전을 생성합니다.새 버전에는 최신 바이러스 정의 및 새로운 유형의 바이러스를 인식하고 알려진 문제를 해결하는 데 필요한 모든 코드 변경 사항이 모두 포함되어 있습니다.추가 바이러스가 발견되면 Sophos는 IDE 파일이라는 바이러스 ID 파일을 릴리스합니다.90일 미만의 엔진으로 작동됩니다.

Sophos 업데이트는 C-Series 어플라이언스의 Cisco AsyncOS에 의해 자동으로 관리됩니다 .Sophos가 새로운 버전의 엔진을 릴리스할 때 Cisco는 QA(Quality Assurance) 프로세스를 통해 해당 엔진을 검증한 다음 Cisco 업데이트 서버에 배치하여 C-Series 어플라이언스가 자동으로 다운로드하여 업데이트합니다.IDE 바이러스 정의 파일이 릴리스되면 이러한 파일은 서비스를 통해 자동으로 이동하며 Sophos가 릴리스한 후 몇 분 이내에 Cisco 업데이트 서버에 배치됩니다.

Sophos IDE 바이러스 서명은 유효하며 이전 엔진 버전에서 작동합니다.모든 현재 IDE가 로드되고 Cisco C-Series 어플라이언스에서 실행 중인 엔진 버전과 함께 작동합니다.

구성

Cisco ESA의 파일이 Sophos에서 직접 사용 가능한 파일과 동기화되지 않은 경우가 있습니다.이는 Sophos와 대부분의 북미 고객 간의 시간대 차이로 인해 더욱 복잡해질 수 있습니다.Sophos 웹 사이트는 영국 옥스퍼드에 위치한 Sophos 본사에서 관리합니다.사이트의 게시물은 현지 표준 시간대인 GMT와 맞춰져 있습니다.Sophos IDE 파일의 상관 관계를 파악하는 것은 약간 혼동됩니다.시간이 크게 달라지면 날짜가 하루 떨어져 있는 것처럼 보일 뿐만 아니라 Cisco에서는 IDE 파일에 대해 다른 번호 매기기 스키마를 사용합니다.Sophos IDE 사이트를 확인하여 IDE가 릴리스된 날짜 및 그 날 이전에 릴리스된 항목 수를 확인하도록 시도할 수 있습니다. 그러나 Cisco는 이 사이트에 게시되지 않은 증분 변경 내용을 자주 선택하므로 가장 효율적인 방법은 아닙니다.Cisco는 10분마다 Sophos 웹 사이트를 쿼리합니다.어플라이언스의 기본 설정은 5분마다 Cisco 다운로드 사이트를 쿼리하는 것입니다.최악의 경우에는 15분 지연이 있을 것이다.

IDE 파일의 번호 매기기 스키마가 날짜입니다.예를 들어, "Sophos IDE Rules 2004121402 Tue December 14 06:27:14 2004"는 12월 14일에 게시된 세 번째 업데이트(0부터 시작)와 관련이 있습니다.

Sophos Automatic Update Interval(Sophos 자동 업데이트 간격)을 기본 설정인 15분으로 설정하는 것이 좋습니다.Security Services(**보안 서비스**)**->Anti-Virus(안티바이러스)** 페이지에서 웹 기반 GUI를 사용하여 Cisco로부터 지속적인 업데이트를 받고 있는지 확인합니다.이 정보는 다음과 같이 antivirusstatus **status** CLI 명령을 사용하여 사용할 수도 있습니다.

```
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
```

업데이트가 성공하지 못한 경우(이 경우 경고 메시지가 표시됨), GUI에서 **Update Now(지금 업데이트)** 버튼 또는 antivirusupdate CLI 명령을 사용하여 수동 업데이트를 시도할 수 있습니다.업데이트 상태는 안티바이러스 로그 파일에 표시됩니다.예:

```
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>
```