Содержание

Введение

Этот документ описывает, почему Антивирусные обновления Sophos на устройстве Безопасности Cisco являются другими, чем доступные на веб-сайте Sophos.

Prerequiste

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Cisco Email Security Appliance (ESA)
- Все версии AsyncOS

Общие сведения

Существует два типа обновлений: обновляет к Антивирусному механизму Sophos и обновлениям идентификационных файлов вируса Sophos (файлы Интегрированной среды разработки (IDE)).

Антивирусный механизм Sophos полностью интегрирован в операционную систему AsyncOS. Sophos генерирует новую версию их механизма сканирования антивируса приблизительно каждый месяц. Новая версия содержит и текущие определения вируса и любые изменения кода, которые требуются, чтобы распознавать новые типы вирусов и исправлять известные неполадки. Поскольку дополнительные вирусы обнаружены, Sophos освобождает идентификационные файлы вируса, названные файлами IDE. Они будут работать с механизмами, которые меньше чем 90 дней.

Обновлениями Sophos управляет автоматически Cisco AsyncOS в устройстве Серии C. Поскольку Sophos освобождает новые версии их механизма, Cisco квалифицирует их посредством процесса обеспечения качества (QA), и затем размещает их в серверы обновления Cisco так, чтобы ваше устройство Серии C автоматически загрузило и обновило их. Поскольку файлы определения вируса IDE освобождены, они перемещаются автоматически через сервис и размещены в серверы обновления Cisco в течение нескольких минут после их выпуска Sophos.

Сигнатуры вируса IDE Sophos допустимы и работают с предыдущими версиями механизма. Весь текущий IDEs будет загружен и будет работать с версией механизма, работающей в Cisco устройство Серии C.

Настройка

Иногда файлы на ESA Cisco, может казаться, вне синхронизации с доступными непосредственно от Sophos. Это может быть далее осложнено различием в часовом поясе между Sophos и большинством североамериканских клиентов. Веб-сайтом Sophos управляет главный офис Sophos под Оксфордом в UK. Регистрации на узле датированы с локальным часовым поясом, GMT. Немного сбивает с толку коррелировать файлы IDE Sophos. Мало того, что большая разница во времени часто заставляет даты казаться на расстоянии в один день, но Cisco, использует другую схему нумерации для файлов IDE. Можно попытаться совпасть с этими файлами путем проверки узла IDE Sophos для наблюдения, когда IDE был освобожден, а также сколько других было освобождено в тот день и за день до него, но поскольку Cisco будет часто брать инкрементные изменения, не зарегистрированные на этом узле, это не большая часть эффективного метода. Cisco делает запрос веб-сайта Sophos каждые 10 минут. Настройка по умолчанию для устройства должна сделать запрос сайта для скачивания Cisco каждые пять минут. В наихудшем случае будет 15-минутная задержка.

Схема нумерации для файлов IDE является датой. Например, "Правила IDE Sophos 2004121402 вторник 14 декабря 6:27:14 2004" коррелята к третьему обновлению (начинают рассчитывать от нуля) на Decemeber, 14-м, публикованном здесь.

Cisco рекомендует установить Интервал Автоматического обновления Sophos в настройку по умолчанию 15 минут. Проверьте, что вы получаете непрерывные обновления от Cisco при помощи находящегося на web GUI на странице **Security Services-> Anti-Virus**. Этой информацией является также доступное использование **antivirusstatus** команды CLI, например:

Если ваши обновления не будут успешны (то вы получите сигнальное сообщение, если это произойдет), можно попробовать ручное обновление с помощью кнопки **Update Now** в GUI или **antivirusupdate** команды CLI. Статус обновления показывают в антивирусном файле журнала. Пример: