Содержание

Вопрос

Как вы автоматизируете регистрационные передачи?

Среда

Cisco Email Security Appliance (ESA), Web Security Appliance (WSA), устройство управления безопасностью (SMA) и все версии AsyncOS.

Многие различные типы журналов созданы на Устройстве безопасности. Можно хотеть иметь устройство, автоматически передают определенные журналы другому серверу.

Эта настройка может быть сделана через GUI или CLI с помощью протоколов SCP или FTP. Считайте специфические особенности ниже:

GUI

1. Перейдите **к Администрированию системы-> Регистрационные Подписки**.
2. Нажмите регистрационное название журнала, вы хотите модифицировать под 'Регистрационным Названием' Поле.
3. Под 'Методом поиска' можно выбрать 'FTP on Remote Server' или 'SCP on Remote server'.
4. Введите правильные значения в соответствующий сценарий, который вы выбираете. Если вы не знакомы с правильными значениями, свяжитесь со своими системами / администратор сети, поскольку они могут помочь вам определять, какие серверы доступны в вашей сети.

CLI (интерфейс командной строки)

Посмотрите следующую последовательность CLI:

Выберите метод, который вы желаете установить. От этой точки CLI обойдет вас посредством тех же настроек соединения, которые доступны в GUI.

Это следующие:

FTP

- Интервал максимального времени между передачей: 3600 секунд
- Хост FTP: Имя хоста / IP-адрес сервера FTP
- Каталог: Удаленный каталог на сервере FTP (относительно входа в систему FTP. Как правило, '/')
- Имя пользователя: Имя пользователя FTP
- Password: Пароль для FTP

SCP

- Интервал максимального времени между передачей: 3600 секунд
- Протокол: SSH1 или SSH2
- Хост SCP: Имя хоста / IP-адрес Сервера SCP
- Каталог: Удаленный каталог на сервере SCP (относительно входа в систему SCP. Как правило, '/')
- Имя пользователя: Имя пользователя SCP
- Включите проверку ключа хоста
- Автоматически просмотр
- Войдите вручную

Примечание: FTP является протоколом открытого текста, означая, что уязвимые данные могут быть читаемыми кем-то, кто осуществляет сниффинг сетевого трафика. SCP является зашифрованным протоколом, таким образом делая сниффинг неэффективного в snooping данных. Если данные чувствительны, и безопасность является беспокойством, рекомендуется, чтобы SCP использовался вместо FTP.