Содержание

Введение

Этот документ описывает, как установить почтовое шифрование на Email Security Appliance (ESA).

Предварительные условия

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Модель: все серии C и серии X
- Шифрование конверта (PostX) Функция установлено

Настройка

Включите почтовое шифрование на ESA

Выполните эти шаги от GUI:

1. Под Сервисами безопасности выберите **Cisco IronPort Email Encryption> Enable Email Encryption** и нажмите **Edit Settings**.

2. **Нажмите Add Профиль Шифрования** для создания нового Профиля Шифрования.

3. Выберите **Cisco Registered Envelope Service** или **Cisco IronPort Encryption Appliance** (если Устройство шифрования куплено) для Типа Ключевого сервиса.

4. Нажмите **Submit и Commit Changes**.

5. После того, как Профиль Шифрования был создан, вам дают опцию для

Инициализации его к серверу Зарегистрированного сервиса конверта Cisco (CRES). Кнопка Provision должна отобразиться рядом с новым профилем. Нажмите **Provision**.

Создайте исходящий фильтр контента

Выполните эти шаги от GUI для создания исходящего фильтра контента для реализации Профиля Шифрования. В следующем примере фильтр инициирует шифрование для любого исходящего сообщения с "Безопасной" строкой: в подчиненном заголовке:

1. Под Почтовой Политикой выберите Outgoing Content Filters и **нажмите Add Фильтр**.

2. Добавьте новый фильтр с условием Подчиненного Заголовка как предмет == "Безопасный": и действие Шифрует и Поставляет Теперь (Заключительное действие). **Нажмите кнопку Submit (Отправить).**

3. Под Почтовой Политикой выберите Outgoing Mail Policies и включите этот новый фильтр в почтовой политике по умолчанию или соответствующей почтовой политике.

4. Изменения передачи.

Проверка

В этом разделе описывается проверить, что работает шифрование.

1. Для проверки генерируйте новую почту с **Безопасным:** в предмете и посылают электронное письмо веб-учетной записи (Hotmail, Yahoo, Gmail), чтобы определить, зашифровано ли это.

2. Проверьте почтовые журналы, как описано в следующем разделе, чтобы гарантировать, что сообщение зашифровано через Исходящий Фильтр контента.

Проверьте обработку фильтра шифрования в Mail_logs

Эти mail_log записи показывают, что сообщения совпали с фильтром шифрования по имени Encrypt_Message.

См. Определение Расположения сообщения ESA для инструкции по тому, как использовать **grep** или **findevent** команды для сбора информации от журналов как показано в этом разделе.

Устранение неполадок

Если фильтр шифрования не инициирует, проверьте почтовые журналы для почтовой политики использование тестового сообщения. Удостоверьтесь, что фильтр включен в этой почтовой политике, и также что нет никакого предыдущего фильтра, включенного в этой политике с **Пропуском, Остающимся** действием **Фильтров контента**.

Гарантируйте, что сообщение (сообщения) в отслеживании сообщений использует корректную строку или определяло маркировку предмета для инициирования шифрования через фильтр контента.