ID документа: 118954

Обновлено: 08 мая 2015

Внесенный Энрико Вернером, специалистом службы технической поддержки Cisco.

Родственные продукты

- Устройство безопасности электронной почты Cisco

Содержание

Введение

Этот документ описывает, как включить Transport Layer Security (TLS) на слушателе на Email Security Appliance (ESA).

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения в этом документе основываются на ESA с любой версией AsyncOS.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Общие сведения

Необходимо включить TLS для любых слушателей, где вы требуете шифрования для входящих подключений. Вы могли бы хотеть включить TLS на слушателях, которые сталкиваются с Интернетом (общие слушатели), но не для слушателей для внутренних систем (частные слушатели). Или, вы могли бы хотеть включить шифрование для всех слушателей. По умолчанию ни частные ни общие слушатели не позволяют TLS подключение. Необходимо включить TLS в таблице доступа к хосту (HAT) слушателя для включения TLS или для входящего (получение) или для исходящий (передача) электронная почта. Кроме того, почтовым параметрам настройки политики потока для частных и общих слушателей выключили TLS по умолчанию.

Настройка

Можно задать три других параметров настройки для TLS на слушателе:

Установка	Значение
Нет	TLS не позволен для входящих соединений. Соединения со слушателем не тре зашифрованных диалогов Протокола SMTP. Это - настройка по умолчанию для слушателей, которых вы настраиваете на устройстве.
Предпочтительный	TLS позволен для входящих соединений слушателю от Агентов передачи сообщений (MTAs).
Требуемый	TLS позволен для входящих соединений слушателю от MTAs, и пока команда STARTTLS не получена, ESA отвечает сообщением об ошибках к каждой коман ни кроме Какой Опции (NOOP), EHLO или ВЫХОД. Если TLS 'Требуется', это означает, что электронной почте, которую отправитель не хочет зашифрованны TLS, откажет ESA, прежде чем это будет передано, который, таким образом, препятствует ему, переданы в ясном.

Включите TLS на Политике Потока Почты HAT для Слушателя через GUI

Выполните следующие действия:

1. От страницы Mail Flow Policies выберите слушателя, политику которого вы хотите модифицировать и затем щелкнуть по ссылке для названия политики для редактирования. (Можно также отредактировать Параметры Политики по умолчанию.) Страница Edit Mail Flow Policies отображена.
2. В "Шифровании и Опознавательном" разделе, для "TLS Использования": поле,

выберите уровень TLS, который вы хотите для слушателя.
3. **Нажмите кнопку Submit (Отправить).**
4. Нажмите **Commit Changes**, добавьте дополнительный комментарий при необходимости, и затем нажмите **Commit Changes** для сохранения изменений.

Примечание: Можно назначить определенный сертификат для TLS подключение отдельным общим слушателям при создании слушателя.

Включите TLS на Политике Потока Почты HAT для Слушателя через CLI

1. Используйте **listenerconfig> команда редактирования** для выбора слушателя, которого вы хотите настроить.
2. Используйте **hostaccess>** команда **по умолчанию** для редактирования параметров настройки HAT слушателя по умолчанию.
3. Введите один из этих выборов для изменения настроек TLS, когда вам предлагают: Обратите внимание на то, что данный пример просит, чтобы вы использовали **certconfig** команду, чтобы гарантировать, что существует подтвержденный сертификат, который может использоваться со слушателем. Если вы не создали сертификатов, слушатель использует демонстрационный сертификат, который предварительно установлен на устройстве. Можно включить TLS с демонстрационным сертификатом для тестирования, но это не безопасно и не рекомендуется для общего использования. Используйте **listenerconfig>, редактируют>** команда **сертификата** для присвоения сертификата на слушателя.Как только вы настроили TLS, установка отражена в сводке слушателя в CLI:
```
Name: Inboundmail
Type: Public
Interface: PublicNet (192.168.2.1/24) TCP Port 25
Protocol: SMTP
Default Domain:
Max Concurrency: 1000 (TCP Queue: 50)
Domain map: disabled
TLS: Required
```
4. Введите команду **передачи** для включения изменения.

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

- Используйте текстовый файл журнала почты и посмотрите этот документ: Определите, является ли ESA Использованием TLS для Доставки или Получения
- Отслеживание сообщений использования: GUI: Монитор> Отслеживание сообщений
- Создание отчетов использования: GUI: Монитор> TLS подключение
- Используйте веб-сайт третьей стороны, такой как checktls.com

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Можно задать, передает ли ESA предупреждение, если согласование TLS отказывает, когда

сообщения переданы к домену, который требует TLS подключение. Сигнальное сообщение содержит название целевого домена для отказавшего согласования TLS. ESA передает сигнальное сообщение ко всему набору получателей для получения Предупреждения предупреждений уровня важности для Системных типов предупреждения. Можно управлять аварийными получателями через страницу System Administration> Alerts в GUI (или через **alertconfig** команду в CLI).

Дополнительные сведения

- Конечный пользователь ведет AsyncOS для электронной почты
- Cisco Systems – техническая поддержка и документация

Связанные обсуждения Сообщества Cisco Support

Сообщество Cisco Support является форумом для вас, чтобы спросить и ответить на вопросы, общие предложения, и сотрудничать с вашими узлами.

См. Cisco Technical Tips Conventions для получения информации об условных обозначениях, используемых в этом документе.

Обновлено: 08 мая 2015
ID документа: 118954