Всестороннее руководство по установке для TLS на ESA

Содержание

Введение
Предварительные условия
Требования
Используемые компоненты
Общие сведения
Обзор функциональных возможностей и требования
Принесите свой собственный сертификат
Обновите текущий сертификат
Разверните подписанные сертификаты
Генерируйте подписанный сертификат и CSR
Предоставьте подписанный сертификат CA
Загрузите подписанный сертификат к ESA
Задайте сертификат для использования с сервисами ESA
Входящий TLS
Исходящий TLS
HTTPS
LDAP
Фильтрация URL-адресов
Резервное копирование конфигурация устройства и сертификат (сертификаты)
Активируйте входящий TLS
Активируйте исходящий TLS
Устранение неполадок
Промежуточные сертификаты
Включите уведомления для требуемых сбоев TLS подключение
Найдите успешные сеансы подключения TLS в почтовых журналах
Дополнительные сведения

Введение

Этот документ описывает, как создать сертификат для использования с Transport Layer Security (TLS), активировать входящий и исходящий TLS и решить основные проблемы TLS на Cisco Email Security Appliance (ESA).

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

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

Реализация TLS на ESA предоставляет конфиденциальность для передачи "точка-точка" электронных почт через шифрование. Это позволяет администратору импортировать сертификат и секретный ключ от сервиса Центра сертификации (CA), или использовать подписанный сертификат.

Cisco AsyncOS для Безопасности электронной почты поддерживает расширение *STARTTLS* к Протоколу SMTP (*Безопасный SMTP по TLS*).

> **Совет:** Для получения дополнительной информации о TLS, обратитесь к RFC 3207.

> **Примечание:** Этот документ описывает, как установить сертификаты на кластерном уровне с использованием функции *Централизованного управления* на ESA. Сертификаты могут быть применены на уровне машины также; однако, если машина будет когда-либо удалена из кластера и затем добавит назад, то сертификаты машины уровня будут потеряны.

Обзор функциональных возможностей и требования

Администратор мог бы желать создать подписанный сертификат на устройстве по любой из этих причин:

- Для шифрования диалогов SMTP с другими MTAs, которые используют TLS (и входящие и исходящие диалоги)
- Для включения сервиса HTTPS на устройстве для доступа к GUI через HTTPS
- Для использования в качестве сертификата клиента для Упрощенных протоколов доступа к каталогам (LDAP) (LDAP), если Сервер LDAP требует сертификата клиента
- Для разрешения безопасной связи между устройством и Диспетчером предприятия алгоритма цифровой подписи райвеста шамира адлемана (RSA) для Защиты потери данных (DLP)
- Для разрешения безопасной связи между устройством и Устройством Сетки Угрозы Усовершенствованной вредоносной защиты (AMP) Cisco

ESA прибывает предварительно сконфигурированный с демонстрационным сертификатом, который может использоваться для установления TLS подключение.

> **Внимание. :** В то время как демонстрационный сертификат достаточен для установления безопасного TLS подключение, знать, что это не может предложить соединение поддающееся проверке.

Cisco рекомендует получить X.509 или Конфиденциальность Расширенная Электронная почта (PEM) сертификат от CA., как который Это могло бы также упоминаться как сертификат *Apache*. Сертификат от CA выбираем по подписанному сертификату, потому что подписанный сертификат подобен ранее упомянутому демонстрационному сертификату, который не может предложить соединение поддающееся проверке.

> **Примечание:** Формат сертификата PEM далее определен в RFC 1421 через RFC 1424. PEM является форматом контейнера, который может включать только общий сертификат (такой как с установками Apache и файлами сертификата CA*/etc/ssl/certs*) или вся цепочка сертификатов, для включения открытого ключа, секретного ключа и корневых сертификатов. *PEM* названия из отказавшего метода для безопасной электронной почты, но формат контейнера, который это использовало, все еще активен и является трансляцией base64 ключей ASN.1 X.509.

Принесите свой собственный сертификат

Опция для импорта собственного сертификата доступна на ESA; однако, требование - то, что сертификат находится в формате *PKCS#12*. Этот формат включает секретный ключ. У администраторов не часто есть сертификаты, которые доступны в этом формате. Поэтому Cisco рекомендует, чтобы вы генерировали сертификат на ESA и подписали ее должным образом CA.

Обновите текущий сертификат

Если сертификат, который уже существует, истек, пропустите *Развертывающийся* раздел *Подписанных сертификатов* этого документа и оставьте сертификат, который существует.

> **Совет:** См. Возобновление Сертификата на Документе Cisco Устройства Безопасности электронной почты для получения дополнительной информации.

Разверните подписанные сертификаты

В этом разделе описывается генерировать подписанный сертификат и Запрос подписи сертификата (CSR), предоставьте подписанный сертификат CA для подписания, загрузите подписанный сертификат к ESA, задайте сертификат для использования с сервисами ESA и резервное копирование конфигурация устройства и сертификат (сертификаты).

Генерируйте подписанный сертификат и CSR

Для создания подписанного сертификата через CLI введите **certconfig** команду.

Выполните эти шаги для создания подписанного сертификата от GUI:

1. Перейдите к **Сети>, Сертификаты> Добавляют Сертификат** от GUI устройства.

2. Нажмите **Создать** раскрывающееся меню **Подписанного сертификата**.

   Когда вы создаете сертификат, гарантируете, что *Общее имя* совпадает с именем хоста интерфейса прослушивания, или что это совпадает с именем хоста интерфейса доставки.

   Интерфейс *прослушивания* является интерфейсом, который связан со слушателем , который настроен под **Сетью> Слушатели**.

   Интерфейс *доставки* автоматически выбран, пока явно не настроено от CLI с **deliveryconfig** командой.
3. Для входящего подключения поддающегося проверке проверьте, что совпадают эти три элемента:

   Запись MX (имя хоста Системы доменных имен (DNS))

   Общее имя

   Интерфейсное имя хоста

   Примечание: Системное имя хоста не влияет на TLS подключение в отношении того, чтобы быть поддающимся проверке. Системное имя хоста показывают в верхнем правом углу GUI устройства, или от CLI **sethostname** выходные данные команды.

   Внимание. : Не забудьте **отправлять** и **передавать** ваши изменения, прежде чем вы экспортируете CSR. Если эти шаги не будут выполнены, то новый сертификат не посвятит себя конфигурации устройства, и подписанный сертификат от CA не может подписаться или применен к, сертификат, который уже существует.

Предоставьте подписанный сертификат CA

Выполните эти шаги для отправки подписанного сертификата CA для подписания:

1. Сохраните CSR к локальному компьютеру в формате PEM (**Сеть> Сертификаты> *Запрос подписи сертификата Загрузки* Name> Сертификата**).

2. Передайте генерируемый сертификат к распознанному CA для подписания.

3. Запросите, чтобы X.509/PEM/Apache отформатировал сертификат, а также промежуточный сертификат.

CA тогда генерирует сертификат в формате PEM.

Примечание: Для списка поставщиков CA обратитесь к статье Wikipedia Центра сертификации.

Загрузите подписанный сертификат к ESA

После того, как CA возвращает доверяемый общий сертификат, который подписан секретным ключом, необходимо загрузить подписанный сертификат к ESA. Сертификат может тогда использоваться с общим или частным слушателем, сервисом HTTPS IP - интерфейса, Интерфейсом LDAP или всеми исходящими TLS подключение к целевым доменам.

Выполните эти шаги для загрузки подписанного сертификата к ESA:

1. Гарантируйте, что доверяемый общий сертификат, который получен формат PEM использования или формат, который может быть преобразован в PEM перед загрузкой его к устройству. **Совет:** Можно использовать OpenSSLtoolkit, программу открытых программных средств, для преобразования формата.
2. Загрузите подписанный сертификат:

   Перейдите к **Сети> Сертификаты**.

   Нажмите название сертификата, который передавался CA для подписания.

   Введите путь к файлу на локальном компьютере или сетевом томе.

   Примечание: При загрузке нового сертификата он перезаписывает текущий сертификат. Промежуточный сертификат, который отнесен к подписанному сертификату, может также быть загружен.

   Внимание. : Не забудьте **отправлять** и **передавать** изменения после загрузки подписанного сертификата.

Задайте сертификат для использования с сервисами ESA

Теперь, когда сертификат создан, подписался и загрузил к ESA, он может использоваться для сервисов, которые требуют certificate usage.

Входящий TLS

Выполните эти шаги для использования сертификата для входящих сервисов TLS:

1. Перейдите к **Сети> Слушатели**.
2. Нажмите название слушателя.
3. Выберите название сертификата от раскрывающегося меню *Сертификата*.
4. **Нажмите кнопку Submit (Отправить).**
5. Повторите Шаги 1 - 4 по мере необходимости для любых дополнительных слушателей.

6. **Передайте** изменения.

Исходящий TLS

Выполните эти шаги для использования сертификата для исходящих сервисов TLS:

1. Перейдите для **Отправки по почте Политики> Целевые Средства управления**.
2. Нажмите **Edit Global Settings...** в разделе *Глобальных параметров*.
3. Выберите название сертификата от раскрывающегося меню *Сертификата*.
4. **Нажмите кнопку Submit (Отправить).**
5. **Передайте** изменения.

HTTPS

Выполните эти шаги для использования сертификата для сервисов HTTPS:

1. Перейдите к **Сети> IP - интерфейсы**.
2. Нажмите имя интерфейса.
3. Выберите название сертификата от раскрывающегося меню *Сертификата HTTPS*.
4. **Нажмите кнопку Submit (Отправить).**
5. Повторите Шаги 1 - 4 по мере необходимости для любых дополнительных интерфейсов.
6. **Передайте** изменения.

LDAP

Выполните эти шаги для использования сертификата для LDAP:

1. Перейдите к **Администрированию системы > LDAP**.
2. **Нажмите кнопку Edit Settings (Изменить настройки)...** в разделе *Глобальных параметров LDAP*.
3. Выберите название сертификата от раскрывающегося меню *Сертификата*.
4. **Нажмите кнопку Submit (Отправить).**
5. **Передайте** изменения.

Фильтрация URL-адресов

Выполните эти шаги для использования сертификата для фильтрации URL-адресов:

1. Введите **websecurityconfig** команду в CLI.

2. Продолжитесь через командные строки. Гарантируйте выбор **Y** при достижении этого приглашения:

   ```
   Do you want to set client certificate for Cisco Web Security Services Authentication?
   ```

3. Выберите номер, который привязан к сертификату.

4. Введите команду **передачи** для фиксации изменений конфигурации.

Резервное копирование конфигурация устройства и сертификат (сертификаты)

Гарантируйте, что конфигурация устройства сохранена в это время. Конфигурация устройства содержит завершенный сертификат, работают, который был применен через ранее описанные процессы.

Выполните эти шаги, чтобы сохранить файл конфигурации устройства:

1. Перейдите к **Администрированию системы> Файл конфигурации> файл Загрузки к локальному компьютеру, чтобы просмотреть или сохранить**.

2. Экспортируйте сертификат:

   Перейдите к **Сети> Сертификаты**.

   Нажмите **Export Certificate**.

   Выберите сертификат для экспортирования.

   Введите имя файла сертификата.

   Введите пароль для файла сертификата.

   Нажмите **Export**.

   Сохраните файл к локальной или сетевой машине.

   Дополнительные сертификаты могут быть экспортированы в это время или нажать **Cancel** для возврата к **Сети>** местоположение **Сертификатов**.

   Примечание: Этот процесс сохраняет сертификат в формате PKCS#12, который создает и сохранил файл с защитой пароля.

Активируйте входящий TLS

Для активации TLS для всех входящих сеансов соединитесь с веб-GUI, выберите **Mail Policies> Mail Flow Policies** для настроенного входящего слушателя, и затем выполните эти шаги:

1. Выберите слушателя, для которого должна модифицироваться политика.

2. Щелкните по ссылке для названия политики для редактирования его.

3. В разделе *Характеристик безопасности* выберите один из них *Шифрование и Параметры проверки подлинности* для установки уровня TLS, который требуется для того слушателя и почтовой политики потока:

   Выключено – Когда эта опция выбрана, TLS не используется.

   Предпочтенный – Когда эта опция выбрана, TLS может выполнить согласование от удаленного MTA до ESA. Однако, если удаленный MTA не выполняет согласование (до приема *220* ответов), транзакция SMTP продолжается *в ясном* (не зашифрованный). Никакая попытка не предпринята, чтобы проверить, происходит ли сертификат из доверенного центра сертификации. Если ошибка происходит после того, как 220 ответов получены, то транзакция SMTP не переключается на открытый текст.

   Требуемый – Когда эта опция выбрана, о TLS можно выполнить согласование от удаленного MTA до ESA. Никакая попытка не предпринята для проверки сертификата домена. Если согласование отказывает, никакое электронное письмо не послано через соединение. Если согласование успешно выполняется, то почте отправляют через шифрованный сеанс.
4. **Нажмите кнопку Submit (Отправить).**

5. Нажмите кнопку **Commit Changes**. Можно добавить дополнительный комментарий в это время при желании.

6. Нажмите **Commit Changes** для сохранения изменений.

Почтовая политика потока для слушателя теперь обновлена с параметрами настройки TLS, которые вы выбрали.

Выполните эти шаги для активации TLS для входящих сеансов, которые поступают от избранного набора доменов:

1. Соединитесь с веб-GUI и выберите **Mail Policies> HAT Overview**.

2. Добавьте отправителя (отправителей) к соответствующей Sender Group.

3. Отредактируйте параметры настройки TLS почтовой политики потока, которая привязана к Sender Group, которую вы модифицировали в предыдущем шаге.

4. **Нажмите кнопку Submit (Отправить).**

5. Нажмите кнопку **Commit Changes**. Можно добавить дополнительный комментарий в это

время при желании.

6. Нажмите **Commit Changes** для сохранения изменений.

Почтовая политика потока для Sender Group теперь обновлена с параметрами настройки TLS, которые вы выбрали.

Совет: См. следующую статью для получения дополнительной информации о том, как ESA обрабатывает проверку TLS: Каков алгоритм для Проверки сертификата на ESA?

Активируйте исходящий TLS

Для активации TLS для сеансов исходящего соединения соединитесь с веб-GUI, выберите **Mail Policies> Destination Controls**, и затем выполните эти шаги:

1. **Нажмите Add назначение....**

2. Добавьте целевой домен (такой как *domain.com*).

3. В *Разделе поддержки TLS* нажмите раскрывающееся меню и выберите одну из этих опций для включения типа TLS, который должен быть настроен:

   Ни об одном – Когда эта опция выбрана, TLS, не выполняют согласование относительно исходящих соединений от интерфейса до MTA для домена.

   Предпочтенный – Когда эта опция выбрана, о TLS выполняют согласование от интерфейса ESA до MTA для домена. Однако, если согласование TLS отказывает (до приема 220 ответов), транзакция SMTP продолжается *в ясном* (не зашифрованный). Никакая попытка не предпринята, чтобы проверить, происходит ли сертификат из доверяемого CA., Если ошибка происходит после того, как 220 ответов получены, то транзакция SMTP не переключается на открытый текст.

   Требуемый – Когда эта опция выбрана, о TLS выполняют согласование от интерфейса ESA до MTA для домена. Никакая попытка не предпринята для проверки сертификата домена. Если согласование отказывает, никакое электронное письмо не послано через соединение. Если согласование успешно выполняется, то почте отправляют через шифрованный сеанс.

   Предпочтенный - Проверяют – Когда эта опция выбрана, о TLS выполняют согласование от ESA до MTA для домена, и устройство пытается проверить доменный сертификат. В этом случае эти три результата возможны:

   О TLS выполняют согласование, и сертификат проверен. Почте отправляют через шифрованный сеанс.

   О TLS выполняют согласование, но не проверен сертификат. Почте отправляют через шифрованный сеанс.

Никакой TLS подключение не сделан, и сертификат не проверен. Сообщение электронной почты отправлено в открытом тексте.**Требуемый - Проверяют** – Когда эта опция выбрана, о TLS выполняют согласование от ESA до MTA для домена, и проверка доменного сертификата требуется. В этом случае эти три результата возможны:

О TLS подключение выполняют согласование, и сертификат проверен. Сообщение электронной почты отправлено через шифрованный сеанс.

О TLS подключение выполняют согласование, но сертификат не проверен доверяемым CA., которого не отправляют почте.

О TLS подключение не выполняют согласование, но почте не отправляют.

4. Внесите дальнейшие изменения, которые необходимы к *Целевым Средствам управления* для целевого домена.

5. **Нажмите кнопку Submit (Отправить).**

6. Нажмите кнопку **Commit Changes**. Можно добавить дополнительный комментарий в это время при желании.

7. Нажмите **Commit Changes** для сохранения изменений.

Устранение неполадок

В этом разделе описывается решить основные проблемы TLS на ESA.

Промежуточные сертификаты

Когда текущие сертификаты обновлены вместо нового создания сертификата, необходимо искать двойные промежуточные сертификаты, особенно. Промежуточный сертификат (сертификаты), возможно, изменился или, возможно, был неправильно объединен в цепочку, и сертификат, возможно, загрузил множественные промежуточные сертификаты. Это может представить проблемы объединения в цепочку и проверки сертификата.

Включите уведомления для требуемых сбоев TLS подключение

Можно настроить ESA для передачи предупреждения, 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 всем получателям, которые собираются получить предупреждение предупреждений уровня важности для *Системных* типов предупреждения.

Примечание: Это - глобальный параметр, таким образом, он не может быть установлен на основе на домен.

Выполните эти шаги для включения предупреждений TLS подключение:

1. Перейдите для **Отправки по почте Политики> Целевые Средства управления**.

2. Нажмите **Edit Global Settings**.

3. Проверьте **Передачу предупреждение, когда требуемый TLS подключение откажет** флажок.

   Совет: Можно также настроить эту установку с **destconfig>** команда CLI **настройки**.

ESA также регистрирует экземпляры, для которых TLS требуется для домена, но не мог использоваться в журналах почты устройства. Когда любое из этих условий соблюдают, это происходит:

- Удаленный MTA не поддерживает ESMTP (например, это не поняло команду *EHLO* от ESA).
- Удаленный MTA поддерживает ESMTP, но команда *STARTTLS* не была в списке расширений, которые это объявило в его ответе *EHLO*.
- Когда ESA передал команду *STARTTLS,* удаленный MTA объявил расширение *STARTTLS*, но ответил ошибкой.

Найдите успешные сеансы подключения TLS в почтовых журналах

TLS подключение зарегистрированы в почтовых журналах, наряду с другими значительными действиями, которые отнесены к сообщениям, таким как действия фильтрации, антивирусные и вердикты для защиты от спама и попытки доставки. Если будет успешный TLS подключение, то в почтовых журналах будет запись *успеха* TLS. Аналогично, отказавший TLS подключение производит *подведенную* запись TLS. Если сообщение не имеет связанной записи TLS в файле журнала, то сообщение не было передано TLS подключение.

Совет: Для понимания почтовых журналов обратитесь к Документу Cisco Определения Расположения сообщения ESA.

Вот пример успешного TLS подключение от удаленного хоста (прием):

```
Wed Jul 20 19:47:40 2005 Info: New smtp ICID 282204970 interface mail.example.com
(10.2.3.4) address 10.3.4.5 reverse dns host unknown verified no
Wed Jul 20 19:47:40 2005 Info: ICID 282204970 ACCEPT SG None match SBRS None
Wed Jul 20 19:47:40 2005 Info: ICID 282204970 TLS success
Wed Jul 20 19:47:40 2005 Info: Start MID 200257070 ICID 282204970
```

Вот пример отказавшего TLS подключение от удаленного хоста (прием):

```
Tue Jun 28 19:08:49 2005 Info: New SMTP ICID 282204971 interface Management
(10.2.3.4) address 10.3.4.5 reverse dns host unknown verified no
Tue Jun 28 19:08:49 2005 Info: ICID 282204971 ACCEPT SG None match SBRS None
Tue Jun 28 19:08:49 2005 Info: ICID 282204971 TLS failed
Tue Jun 28 19:08:49 2005 Info: ICID 282204971 lost
Tue Jun 28 19:08:49 2005 Info: ICID 282204971 TLS was required but remote host did
not initiate it
Tue Jun 28 19:08:49 2005 Info: ICID 282204971 close
```

Вот пример успешного TLS подключение к удаленному хосту (доставка):

```
Tue Jun 28 19:28:31 2005 Info: New SMTP DCID 834 interface 10.10.10.100 address
192.168.1.25 port 25
Tue Jun 28 19:28:31 2005 Info: DCID 834 TLS success protocol TLSv1 cipher
DHE-RSA-AES256-SHA
Tue Jun 28 19:28:31 2005 Info: Delivery start DCID 834 MID 1074 to RID [0]
```

Вот пример отказавшего TLS подключение к удаленному хосту (доставка):

```
Fri Jul 22 22:00:05 2005 Info: DCID 2386070 IP 10.3.4.5 TLS failed: STARTTLS
unexpected response
```

Дополнительные сведения

- Устройство безопасности электронной почты Cisco - руководства пользователя
- Устройство менеджмента безопасности содержания Cisco - руководства пользователя
- Cisco Systems – техническая поддержка и документация