Настройте ESA для предпочтения безопасной пересылки (Perfect Forward Secrecy, PFS)

Содержание

[Введение](#)
[Предварительные условия](#)
[Требования](#)
[Используемые компоненты](#)
[Общие сведения](#)
[Настройка](#)
[ВХОДЯЩИЙ - ESA, действующий как сервер TLS](#)
[Рекомендуемые sslconfig параметры настройки для ВХОДЯЩЕГО](#)
[ИСХОДЯЩИЙ - ESA, действующий как клиент TLS](#)
[Рекомендуемые sslconfig параметры настройки для ИСХОДЯЩЕГО](#)
[Дополнительные сведения](#)

Введение

Этот документ описывает, как настроить предпочтение безопасной пересылке (Perfect Forward Secrecy, PFS) в Transport Layer Security (TLS) encrpyted соединения на Email Security Appliance (ESA).

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- SSL/TLS

Используемые компоненты

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

- AsyncOS для Почтовой версии 9.6 и выше

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

ESA действительно предлагает Прямую секретность (Непосредственный контроль секретности (Perfect Forward Secrecy)). Прямая секретность означает, что данные переданы через канал, который использует симметричное шифрование с эфемерными тайнами, и даже если секретный ключ (долгосрочный ключ) на одном или обоих из хостов поставился под угрозу, не возможно дешифровать ранее зарегистрированный сеанс.

Тайна не передана через канал, вместо этого общий секретный ключ получен с помощью *математической проблемы (проблема Диффи-Хеллмана).* Тайна не сохранена больше нигде, чем оперативное запоминающее устройство (RAM) хостов во время установленного сеанса (или ключевой таймаут регенерации).

ESA поддерживает **Диффи-Хеллман (DH) для Обмена ключами**.

Настройка

ВХОДЯЩИЙ - ESA, действующий как сервер TLS

Ниже наборов шифров доступны на ESA для входящего трафика SMTP, которые предоставляют Прямую секретность. Ниже *примера* выбор шифра позволяет только наборы шифров, которые рассматривают *ВЫСОКИМИ* или *MEDIUM*, и используйте эфемерный DH для Обмена ключами, и предпочитает TLSv1.2. Синтаксис выбора шифра придерживается синтаксиса OpenSSL.

Шифры с прямой секретностью на AsyncOS 9.6 +

```
"EDH+TLSv1.2:EDH+HIGH:EDH+MEDIUM:!LOW:!EXP:!aNULL:!RC4:!DSS:!SEED:!IDEA:!MD5:!PSK:!3DES:!SRP"

List:  DHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(256) Mac=AEAD
DHE-RSA-AES256-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(256) Mac=SHA256
DHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(128) Mac=AEAD
DHE-RSA-AES128-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(128) Mac=SHA256
DHE-RSA-AES256-SHA SSLv3 Kx=DH Au=RSA Enc=AES(256) Mac=SHA1
DHE-RSA-CAMELLIA256-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(256) Mac=SHA1
DHE-RSA-AES128-SHA SSLv3 Kx=DH Au=RSA Enc=AES(128) Mac=SHA1
DHE-RSA-CAMELLIA128-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(128) Mac=SHA1
```

Kx (= Обмен ключами) раздел показывает, что Диффи-Хеллман используется для получения тайны.

ESA поддерживает эти шифры с по умолчанию sslconfig параметры настройки (: ALL), но не предпочитает его. Если вы хотите предпочесть шифры, которые предлагают безопасную пересылку (PFS), необходимо было бы изменить **sslconfig** и добавить *Эфемерный Диффи-Хеллман (EDH)* или комбинацию "*EDH + <шифр или имя группы шифра>*" к выбору шифра.

Конфигурация по умолчанию:

```
"EDH+TLSv1.2:EDH+HIGH:EDH+MEDIUM:!LOW:!EXP:!aNULL:!RC4:!DSS:!SEED:!IDEA:!MD5:!PSK:!3DES:!SRP"

List:  DHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(256) Mac=AEAD
DHE-RSA-AES256-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(256) Mac=SHA256
DHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(128) Mac=AEAD
DHE-RSA-AES128-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(128) Mac=SHA256
```

```
DHE-RSA-AES256-SHA SSLv3 Kx=DH Au=RSA Enc=AES(256) Mac=SHA1
DHE-RSA-CAMELLIA256-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(256) Mac=SHA1
DHE-RSA-AES128-SHA SSLv3 Kx=DH Au=RSA Enc=AES(128) Mac=SHA1
DHE-RSA-CAMELLIA128-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(128) Mac=SHA1
```

Новая конфигурация:

```
"EDH+TLSv1.2:EDH+HIGH:EDH+MEDIUM:!LOW:!EXP:!aNULL:!RC4:!DSS:!SEED:!IDEA:!MD5:!PSK:!3DES:!SRP"

List:  DHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(256) Mac=AEAD
DHE-RSA-AES256-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(256) Mac=SHA256
DHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(128) Mac=AEAD
DHE-RSA-AES128-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(128) Mac=SHA256
DHE-RSA-AES256-SHA SSLv3 Kx=DH Au=RSA Enc=AES(256) Mac=SHA1
DHE-RSA-CAMELLIA256-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(256) Mac=SHA1
DHE-RSA-AES128-SHA SSLv3 Kx=DH Au=RSA Enc=AES(128) Mac=SHA1
DHE-RSA-CAMELLIA128-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(128) Mac=SHA1
```

Примечание: RC4 как шифр и MD5 как MAC считают слабым, устаревшим и избегать для использования с SSL/TLS, особенно когда дело доходит до более высокого объема данных без ключевой регенерации.

Рекомендуемые sslconfig параметры настройки для ВХОДЯЩЕГО

Ниже приводится преобладая мнение и только позволять шифры, которые обычно считают сильными и безопасными

Рекомендуемая конфигурация для ВХОДЯЩЕГО, который удаляет RC4 и MD5, а также другие устаревшие и слабые опции, а именно, Экспорт (EXP), Низко (НИЗКИЙ), IDEA (IDEA), ПРОТОТИП (ПРОТОТИП), 3DES (3DES) шифры, сертификаты DSS (DSS) и анонимный Обмен ключами (aNULL) и предварительные общие ключи (PSK) и протокол SRP (SRP), и отключает ECDH и ECDSA, была бы, например:

```
"EDH+TLSv1.2:EDH+HIGH:EDH+MEDIUM:!LOW:!EXP:!aNULL:!RC4:!DSS:!SEED:!IDEA:!MD5:!PSK:!3DES:!SRP"

List:  DHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(256) Mac=AEAD
DHE-RSA-AES256-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(256) Mac=SHA256
DHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(128) Mac=AEAD
DHE-RSA-AES128-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(128) Mac=SHA256
DHE-RSA-AES256-SHA SSLv3 Kx=DH Au=RSA Enc=AES(256) Mac=SHA1
DHE-RSA-CAMELLIA256-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(256) Mac=SHA1
DHE-RSA-AES128-SHA SSLv3 Kx=DH Au=RSA Enc=AES(128) Mac=SHA1
DHE-RSA-CAMELLIA128-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(128) Mac=SHA1
```

Строка выше введенного в **sslconfig** приводит к этому списку поддерживаемых шифров для ВХОДЯЩЕГО:

```
"EDH+TLSv1.2:EDH+HIGH:EDH+MEDIUM:!LOW:!EXP:!aNULL:!RC4:!DSS:!SEED:!IDEA:!MD5:!PSK:!3DES:!SRP"

List:  DHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(256) Mac=AEAD
DHE-RSA-AES256-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(256) Mac=SHA256
DHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(128) Mac=AEAD
DHE-RSA-AES128-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(128) Mac=SHA256
DHE-RSA-AES256-SHA SSLv3 Kx=DH Au=RSA Enc=AES(256) Mac=SHA1
DHE-RSA-CAMELLIA256-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(256) Mac=SHA1
```

```
DHE-RSA-AES128-SHA SSLv3 Kx=DH Au=RSA Enc=AES(128) Mac=SHA1
DHE-RSA-CAMELLIA128-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(128) Mac=SHA1
```

> **Примечание:** ESA, действующий как сервер TLS (входящий трафик) в настоящее время, не поддерживает Диффи-Хеллман Эллиптической кривой для Обмена ключами Сертификатов *Алгоритма цифровой подписи эллиптической кривой (ECDSA)* и *(ECDHE)*.

ИСХОДЯЩИЙ - ESA, действующий как клиент TLS

Для исходящего трафика SMTP ESA **в дополнение к ВХОДЯЩЕМУ** Обмену ключами *Эфемерного Диффи-Хеллмана эллиптической кривой (ECDHE)* поддержек и Сертификатам *Алгоритма цифровой подписи эллиптической кривой (ECDSA)*.

> **Примечание:** Сертификаты Шифрования в эллиптических кривых (ECC) с Эллиптической кривой Алгоритм сигнатуры Digitial, (ECDSA) широко не приняты.

При отправке (исходящей) электронной почты ESA является клиентом TLS. Сертификат клиента TLS является дополнительным. Если Сервер TLS не вызывает (требуют), чтобы ESA (как клиент TLS) предоставил сертификат клиента ECDSA, ESA может продолжить ECDSA защищенный сеанс. Когда ESA как Клиент TLS просят относительно его сертификата, он предоставляет настроенный сертификат ***RSA*** для Исходящего направления.

> **Внимание. :** Предварительно установленное *Доверяемое Хранилище Сертификата CA* (*Системный Список*) на ESA не включает ECC (ECDSA) Корневые сертификаты! Это может потребоваться, чтобы вручную добавлять Корневые сертификаты ECC (которому вы доверяете) к *Пользовательскому Списку* для создания Цепочки ECC Доверия поддающейся проверке.

Для предпочтения шифров DHE/ECDHE, которые предлагают Прямую секретность можно модифицировать **sslconfig** выбор шифра следующим образом.

Добавьте ниже к вашему существующему выбору шифра.

```
"EDH+TLSv1.2:EDH+HIGH:EDH+MEDIUM:!LOW:!EXP:!aNULL:!RC4:!DSS:!SEED:!IDEA:!MD5:!PSK:!3DES:!SRP"

List:  DHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(256) Mac=AEAD
DHE-RSA-AES256-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(256) Mac=SHA256
DHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(128) Mac=AEAD
DHE-RSA-AES128-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(128) Mac=SHA256
DHE-RSA-AES256-SHA SSLv3 Kx=DH Au=RSA Enc=AES(256) Mac=SHA1
DHE-RSA-CAMELLIA256-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(256) Mac=SHA1
DHE-RSA-AES128-SHA SSLv3 Kx=DH Au=RSA Enc=AES(128) Mac=SHA1
DHE-RSA-CAMELLIA128-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(128) Mac=SHA1
```

Рекомендуемые sslconfig параметры настройки для ИСХОДЯЩЕГО

Ниже приводится преобладая мнение и только позволять шифры, которые обычно считают сильными и безопасными

```
"EDH+TLSv1.2:EDH+HIGH:EDH+MEDIUM:!LOW:!EXP:!aNULL:!RC4:!DSS:!SEED:!IDEA:!MD5:!PSK:!3DES:!SRP"
```

```
List:  DHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(256) Mac=AEAD
DHE-RSA-AES256-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(256) Mac=SHA256
DHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(128) Mac=AEAD
DHE-RSA-AES128-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(128) Mac=SHA256
DHE-RSA-AES256-SHA SSLv3 Kx=DH Au=RSA Enc=AES(256) Mac=SHA1
DHE-RSA-CAMELLIA256-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(256) Mac=SHA1
DHE-RSA-AES128-SHA SSLv3 Kx=DH Au=RSA Enc=AES(128) Mac=SHA1
DHE-RSA-CAMELLIA128-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(128) Mac=SHA1
```

Строка выше введенного в **sslconfig** приводит к этому списку поддерживаемых шифров для ИСХОДЯЩЕГО:

```
"EDH+TLSv1.2:EDH+HIGH:EDH+MEDIUM:!LOW:!EXP:!aNULL:!RC4:!DSS:!SEED:!IDEA:!MD5:!PSK:!3DES:!SRP"

List:  DHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(256) Mac=AEAD
DHE-RSA-AES256-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(256) Mac=SHA256
DHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(128) Mac=AEAD
DHE-RSA-AES128-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(128) Mac=SHA256
DHE-RSA-AES256-SHA SSLv3 Kx=DH Au=RSA Enc=AES(256) Mac=SHA1
DHE-RSA-CAMELLIA256-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(256) Mac=SHA1
DHE-RSA-AES128-SHA SSLv3 Kx=DH Au=RSA Enc=AES(128) Mac=SHA1
DHE-RSA-CAMELLIA128-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(128) Mac=SHA1
```

Дополнительные сведения

- Открытые шифры SSL
- Шифрование следующего поколения Cisco