Измените методы и шифры, используемые с SSL/TLS на ESA

Содержание

Введение

Этот документ описывает, как изменить методы и шифры, которые используются с конфигурациями Протокола SSL или Transport Layer Security (TLS) на Cisco Email Security Appliance (ESA).

Измените методы и шифры, используемые с SSL/TLS

> **Примечание:** Методы SSL/TLS и шифры должны быть установлены на основе определенной политики безопасности и предпочтения вашей компании. Для получения информации о независимом поставщике в отношении шифров обратитесь к документу Mozilla TLS Безопасности/Стороны сервера для рекомендуемых конфигураций сервера и подробных сведений.

С Cisco AsyncOS для Безопасности электронной почты администратор может использовать **sslconfig** команду для настройки SSL или протоколов TLS для методов и шифров, которые используются для связи GUI, поместили объявление о входящих подключениях и запросили на исходящие соединения:

```
esa.local> sslconfig

sslconfig settings:
GUI HTTPS method: tlsv1/tlsv1.2
GUI HTTPS ciphers:
MEDIUM
HIGH
-SSLv2
-aNULL
!RC4
@STRENGTH
-EXPORT
Inbound SMTP method: tlsv1/tlsv1.2
Inbound SMTP ciphers:
```

```
MEDIUM
HIGH
-SSLv2
-aNULL
!RC4
@STRENGTH
-EXPORT
Outbound SMTP method: tlsv1/tlsv1.2
Outbound SMTP ciphers:
MEDIUM
HIGH
-SSLv2
-aNULL
!RC4
@STRENGTH
-EXPORT

Choose the operation you want to perform:
- GUI - Edit GUI HTTPS ssl settings.
- INBOUND - Edit Inbound SMTP ssl settings.
- OUTBOUND - Edit Outbound SMTP ssl settings.
- VERIFY - Verify and show ssl cipher list.
[]> inbound

Enter the inbound SMTP ssl method you want to use.
1. SSL v2
2. SSL v3
3. TLS v1/TLS v1.2
4. SSL v2 and v3
5. SSL v3 and TLS v1/TLS v1.2
6. SSL v2, v3 and TLS v1/TLS v1.2
[3]>

Enter the inbound SMTP ssl cipher you want to use.
[MEDIUM:HIGH:-SSLv2:-aNULL:!RC4:@STRENGTH:-EXPORT]>

sslconfig settings:
GUI HTTPS method: tlsv1/tlsv1.2
GUI HTTPS ciphers:
MEDIUM
HIGH
-SSLv2
-aNULL
!RC4
@STRENGTH
-EXPORT
Inbound SMTP method: tlsv1/tlsv1.2
Inbound SMTP ciphers:
MEDIUM
HIGH
-SSLv2
-aNULL
!RC4
@STRENGTH
-EXPORT
Outbound SMTP method: tlsv1/tlsv1.2
Outbound SMTP ciphers:
MEDIUM
HIGH
-SSLv2
-aNULL
!RC4
@STRENGTH
-EXPORT
```

```
Choose the operation you want to perform:
- GUI - Edit GUI HTTPS ssl settings.
- INBOUND - Edit Inbound SMTP ssl settings.
- OUTBOUND - Edit Outbound SMTP ssl settings.
- VERIFY - Verify and show ssl cipher list.
[]>
```

Если изменения внесены в конфигурацию SSL, гарантируют **фиксацию** любого и всех изменений.

Методы SSL

В AsyncOS для Версий Безопасности электронной почты 9.6 и позже, ESA собирается использовать метод *v1 2 v1/TLS TLS* по умолчанию. В этом случае TLSv1.2 берет прецедент для связи, если в использовании и передачей и принимающими сторонами. Для установления TLS подключение обе стороны должны иметь по крайней мере один включенный метод , который совпадает, и по крайней мере один включенный шифр, который совпадает.

> **Примечание:** В AsyncOS для версий Безопасности электронной почты до Версии 9.6 по умолчанию имеет два метода: *v3 SSL* и *v1 TLS*. Некоторые администраторы могли бы хотеть отключить v3 SSL из-за недавних уязвимостей (если v3 SSL включен).

Шифры SSL

Когда вы просматриваете шифр по умолчанию, который перечислен в предыдущем примере, важно понять причину, что это показывает два шифра, придерживавшиеся словом *ALL*. Несмотря на то, что *ALL* включает два шифра, которые предшествуют ему, заказ шифров в списке шифра определяет предпочтение. Таким образом, когда TLS подключение сделан, клиент выбирает первый шифр, который обе стороны поддерживают на основе заказа появления в списке.

> **Примечание:** Шифры RC4 включены по умолчанию на ESA. В предыдущем примере **MEDIUM:HIGH** основывается на Предотвратить Согласованиях относительно Пустых или Анонимных Шифров на Документе Cisco SMA и ESA. Для получения дополнительной информации в отношении RC4 в частности, обратитесь к документу Mozilla TLS Безопасности/Стороны сервера, и также На Безопасности RC4 в TLS и документе WPA, который представлен от *Symposium Безопасности USENIX 2013*. Для удаления шифров RC4 из использования обратитесь к примерам, которые придерживаются.

Посредством манипулирования списком шифра можно влиять на шифр, который выбран. Можно перечислить определенные шифры или диапазоны шифра, и также переупорядочить их силой с включением **@STRENGTH** опции в строке шифра, как показано здесь:

```
Enter the inbound SMTP ssl cipher you want to use.
[RC4-SHA:RC4-MD5:ALL]> MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH
```

Гарантируйте рассмотрение всех шифров и диапазонов, которые доступны на ESA. Для просмотра их введите **sslconfig** команду, придерживавшуюся **подкомандой verify** . Опции для категорий шифра SSL **НИЗКИ**, **MEDIUM**, **ВЫСОКИ**, и **ALL**:

```
[]> verify

Enter the ssl cipher you want to verify.
[]> MEDIUM

ADH-RC4-MD5 SSLv3 Kx=DH Au=None Enc=RC4(128) Mac=MD5
IDEA-CBC-SHA SSLv3 Kx=RSA Au=RSA Enc=IDEA(128) Mac=SHA1
RC4-SHA SSLv3 Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1
RC4-MD5 SSLv3 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
IDEA-CBC-MD5 SSLv2 Kx=RSA Au=RSA Enc=IDEA(128) Mac=MD5
RC2-CBC-MD5 SSLv2 Kx=RSA Au=RSA Enc=RC2(128) Mac=MD5
RC4-MD5 SSLv2 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
```

Можно также объединить их для включения диапазонов:

```
[]> verify

Enter the ssl cipher you want to verify.
[]> MEDIUM:HIGH

ADH-RC4-MD5 SSLv3 Kx=DH Au=None Enc=RC4(128) Mac=MD5
IDEA-CBC-SHA SSLv3 Kx=RSA Au=RSA Enc=IDEA(128) Mac=SHA1
RC4-SHA SSLv3 Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1
RC4-MD5 SSLv3 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
IDEA-CBC-MD5 SSLv2 Kx=RSA Au=RSA Enc=IDEA(128) Mac=MD5
RC2-CBC-MD5 SSLv2 Kx=RSA Au=RSA Enc=RC2(128) Mac=MD5
RC4-MD5 SSLv2 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
ADH-CAMELLIA256-SHA SSLv3 Kx=DH Au=None Enc=Camellia(256) Mac=SHA1
DHE-RSA-CAMELLIA256-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(256) Mac=SHA1
DHE-DSS-CAMELLIA256-SHA SSLv3 Kx=DH Au=DSS Enc=Camellia(256) Mac=SHA1
CAMELLIA256-SHA SSLv3 Kx=RSA Au=RSA Enc=Camellia(256) Mac=SHA1
ADH-CAMELLIA128-SHA SSLv3 Kx=DH Au=None Enc=Camellia(128) Mac=SHA1
DHE-RSA-CAMELLIA128-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(128) Mac=SHA1
DHE-DSS-CAMELLIA128-SHA SSLv3 Kx=DH Au=DSS Enc=Camellia(128) Mac=SHA1
CAMELLIA128-SHA SSLv3 Kx=RSA Au=RSA Enc=Camellia(128) Mac=SHA1
ADH-AES256-SHA SSLv3 Kx=DH Au=None Enc=AES(256) Mac=SHA1
DHE-RSA-AES256-SHA SSLv3 Kx=DH Au=RSA Enc=AES(256) Mac=SHA1
DHE-DSS-AES256-SHA SSLv3 Kx=DH Au=DSS Enc=AES(256) Mac=SHA1
AES256-SHA SSLv3 Kx=RSA Au=RSA Enc=AES(256) Mac=SHA1
ADH-AES128-SHA SSLv3 Kx=DH Au=None Enc=AES(128) Mac=SHA1
DHE-RSA-AES128-SHA SSLv3 Kx=DH Au=RSA Enc=AES(128) Mac=SHA1
DHE-DSS-AES128-SHA SSLv3 Kx=DH Au=DSS Enc=AES(128) Mac=SHA1
AES128-SHA SSLv3 Kx=RSA Au=RSA Enc=AES(128) Mac=SHA1
ADH-DES-CBC3-SHA SSLv3 Kx=DH Au=None Enc=3DES(168) Mac=SHA1
EDH-RSA-DES-CBC3-SHA SSLv3 Kx=DH Au=RSA Enc=3DES(168) Mac=SHA1
EDH-DSS-DES-CBC3-SHA SSLv3 Kx=DH Au=DSS Enc=3DES(168) Mac=SHA1
DES-CBC3-SHA SSLv3 Kx=RSA Au=RSA Enc=3DES(168) Mac=SHA1
DES-CBC3-MD5 SSLv2 Kx=RSA Au=RSA Enc=3DES(168) Mac=MD5
```

Любой из шифров SSL, которые вы не хотите настроенный и доступный, должен быть удален с **"-"** опция, которая предшествует определенным шифрам . Например:

```
[]> MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH:-EDH-RSA-DES-CBC3-SHA:
-EDH-DSS-DES-CBC3-SHA:-DES-CBC3-SHA
```

Информация в данном примере инвертировала бы *NULL*, *EDH-RSA-DES-CBC3-SHA*, *EDH-DSS-DES-CBC3-SHA*, и шифры *DES-CBC3-SHA* из рекламы и предотвратила бы их использование в связи SSL.

Можно также выполнить похожий с включением"**!**" символ перед группой шифра или строкой, что вы желаете стать недоступными:

```
[]> MEDIUM:HIGH:-SSLv2:-aNULL:!RC4:@STRENGTH
```

Информация в данном примере удалила бы все шифры RC4 от использования. Таким образом *SHA RC4* и шифры *MD5 RC4* отрицались бы и не объявлялись бы в связи SSL.

Если изменения внесены в конфигурацию SSL, гарантируют **фиксацию** любого и всех изменений.