ESA の SSL/TLS で使用される方式と暗号の変更

目次

概要

このドキュメントでは、Cisco E メール セキュリティ アプライアンス（ESA）のセキュア ソケット レイヤ（SSL）または Transport Layer Security（TLS）設定で使用される方式と暗号の変更方法について説明します。

SSL/TLS で使用される方式と暗号の変更

> **注:** SSL/TLS の方式と暗号は、企業のセキュリティ ポリシーと環境設定に基づいて設定する必要があります。 暗号に関するサードパーティの情報については、推奨されるサーバ設定と詳細情報が記載された Mozilla のドキュメント「Security/Server Side TLS」を参照してください。

Cisco AsyncOS for Email Security では、管理者が **sslconfig** コマンドを使用して SSL または TLS プロトコルの方式と暗号を設定できます。これらの方式と暗号は、GUI の通信に使用され、着信接続に対してアドバタイズされ、発信接続に対して要求されます。

```
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.
[]>
```

SSL の設定を変更した場合は、すべての変更を**コミット**するようにしてください。

SSL 方式

AsyncOS for Email Security バージョン 9.6 以降では、デフォルトで *TLS v1/TLS v1.2* 方式を使用するように ESA が設定されます。 この場合、送信側と受信側の両方で使用されていれば、TLSv1.2 の方が優先して通信に使用されます。 TLS 接続を確立するには、両側で一致する方式が少なくとも 1 つは有効になっており、一致する暗号が少なくとも 1 つは有効になっている必要があります。

> **注:** バージョン 9.6 よりも前の AsyncOS for Email Security には、デフォルトとして *SSL v3* と *TLS v1* の 2 つの方法があります。 管理者は、最近脆弱性が見つかった SSL V3 を無効にすることもできます（SSL V3 が有効になっている場合）。

SSL 暗号

前の例に示したデフォルトの暗号を参照するときは、2 つの暗号の後に *ALL* という単語が表示されている理由を理解することが重要です。 *ALL* はその前からある 2 つの暗号を含んでいますが、暗号リスト内の暗号の順序によって環境設定が決定されます。 したがって、TLS 接続を行うと、クライアントはこのリストの出現順序に基づいて、両側でサポートされる最初の暗号を選択します。

> **注:** ESA では、RC4 暗号がデフォルトで有効になっています。 前の例で、**MEDIUM: HIGH** はシスコのドキュメント「ESA および SMA で NULL 暗号または匿名暗号のネゴシエーションを防止する」に基づいています。 特に RC4 の詳細については、Mozilla のドキュメント「Security/Server Side TLS」および *USENIX Security Symposium 2013* で公開された「On the Security of RC4 in TLS and WPA」を参照してください。 RC4 暗号を削除して使用できないようにするには、次の例を参照してください。

暗号リストを操作することで、選択される暗号に影響を与えることができます。 次に示すように、暗号ストリングに **@STRENGTH** オプションを含めることによって、特定の暗号や暗号範囲を列挙し、それらを強度で並べ替えることもできます。

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

ESA で使用できるすべての暗号と範囲を確認するようにしてください。 これらを表示するには、**sslconfig** コマンドの後に **verify** サブコマンドを入力します。 SSL 暗号のカテゴリを示すオプションは、**LOW**、**MEDIUM**、**HIGH**、**ALL** です。

```
[]> 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
```

これらを組み合わせて範囲を含めることもできます。

```
[]> 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
```

設定する必要がないのに使用可能になっている SSL 暗号は、該当する暗号の前に「**-**」オプションを付けて削除してください。 次に例を示します。

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

この例の情報によって、*NULL*、*EDH-RSA-DES-CBC3-SHA*、*EDH-DSS-DES-CBC3-SHA*、*DES-CBC3-SHA* 暗号がアドバタイズメントから除外され、SSL 通信に使用されなくなります。

また、使用不可能にする暗号グループまたはストリングの前に「**!**」 文字を含めることで、同じことを実現できます。

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

この例の情報によって、すべての RC4 暗号が削除され、使用できなくなります。 つまり、*RC4-SHA* および *RC4-MD5* 暗号が除外され、SSL 通信でアドバタイズされなくなります。

SSL の設定を変更した場合は、すべての変更を**コミット**するようにしてください。