更改在ESA上與SSL/TLS一起使用的方法和密碼

目錄

簡介

本檔案介紹如何變更與思科電子郵件安全裝置(ESA)上的安全通訊端層(SSL)或傳輸層安全(TLS)設定搭配使用的方法和密碼。

更改與SSL/TLS一起使用的方法和密碼

> **附註**：SSL/TLS方法和密碼應根據您公司的特定安全策略和首選項設定。有關密碼的第三方資訊，請參閱安全/伺服器端TLS Mozilla文檔，以瞭解建議的伺服器配置和詳細資訊。

使用適用於郵件安全的Cisco AsyncOS，管理員可以使用**sslconfig**命令為用於GUI通訊、通告入站連線以及請求出站連線的方法和密碼配置SSL或TLS協定：

```
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.
[]>
```

如果對SSL配置進行了更改，請確保**提交**所有更改。

SSL方法

在AsyncOS for Email Security Versions 9.6及更高版本中，ESA被設定為預設使用*TLS v1/TLS v1*.2方法。在這種情況下，如果傳送方和接收方都使用TLSv1.2進行通訊，則會優先使用它。為了建立TLS連線，兩端必須至少有一個匹配的已啟用方法，以及至少一個匹配的已啟用密碼。

> **附註**：在AsyncOS for Email Security 9.6之前的版本中，預設方法有兩種：*SSL v3*和*TLS v1*。某些管理員可能由於最近的漏洞（如果已啟用SSL v3）而希望禁用SSL v3。

SSL密碼

當您檢視上例中列出的預設密碼時，請務必瞭解它顯示兩個密碼的原因，後跟單詞*ALL*。雖然*ALL*包括前面兩個密碼，但密碼清單中密碼的順序決定了優先順序。因此，當建立TLS連線時，客戶端根據清單中的出現順序選擇雙方都支援的第一個密碼。

> **註**:RC4密碼預設情況下在ESA上啟用。在上一個示例中，**MEDIUM:HIGH**基於Prevent Negotiations for Null or Anonymous Ciphers on the ESA and SMA Cisco文檔。如需更多有關RC4的資訊，請參閱安全/伺服器端TLS Mozilla文檔，以及USENIX安全研討會2013提供的TLS和WPA中RC4的安全性文件。為了不再使用RC4密碼，請參閱以下示例。

通過操縱密碼清單，您可以影響所選密碼。您可以列出特定密碼或密碼範圍，也可以通過在密碼字串中包含**@STRENGTH**選項來按強度重新排列它們，如下所示：

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

確保複查ESA上可用的所有密碼和範圍。若要檢視這些專案，請輸入**sslconfig**指令，然後輸入**verify**子指令。SSL密碼類別的選項為**LOW**、**MEDIUM**、**HIGH**和**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
```

您也可以將這些組合起來以包含範圍：

```
[]> 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
```

應使用特定密碼前面的「**-**」選項刪除不想要配置且可用的任何SSL密碼。以下是一個示例：

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

本示例中的資訊會使*NULL*、*EDH-RSA-DES-CBC3-SHA*、*EDH-DSS-DES-CBC3-SHA*和*DES-CBC3-SHA*的密碼無法進行通告，並阻止在SSL通訊中使用這些密碼。

您還可以通過包含「！」完成類似的**工作** 要不可用的密碼組或字串前面的字元：

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

此示例中的資訊將刪除所有RC4密碼的使用。因此，*RC4-SHA*和*RC4-MD5*密碼將為SSL通訊中的否定且不通告。

如果對SSL配置進行了更改，請確保**提交**所有更改。