修改方法和密码器与在ESA的SSL/TLS一起使用

目录

简介

本文描述如何修改方法，并且使用与在思科的安全套接字层SSL或传输层安全的密码器(TLS)配置给安全工具(ESA)发电子邮件。

修改方法和密码器与SSL/TLS一起使用

> **注意**：应该设置SSL/TLS方法和密码器根据您的公司特定安全策略和首选。 关于密码器的第三方信息，参考安全/服务器端TLS Mozilla文档推荐的服务器配置和详细信息。

使用电子邮件安全的思科AsyncOS，管理员能使用**sslconfig**命令为了配置使用GUI通信，为Inbound连接通告，并且为出站连接请求的方法和密码器的SSL或TLS协议：

```
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.
[]>
```

如果变动做对SSL配置，请保证您**确认**任意更改。

SSL方法

默认情况下在电子邮件安全版本9.6和以上的AsyncOS， ESA设置使用*TLS v1/TLS v1.2*方法。在这种情况下， TLSv1.2由发送和接收方采取通信的先例，如果在使用中。为了建立TLS连接，两边必须有配比至少的一个启用的方法和配比至少的一启用的密码器。

> **注意**：在电子邮件安全版本的AsyncOS在版本9.6之前，默认有两个方法：*SSL v3*和*TLS v1*。(如果SSL v3启用)，一些管理员也许要禁用SSL v3由于最近的漏洞。

SSL密码器

当您查看在前一个示例列出的默认密码器时，了解原因是重要的显示词跟随的两密码器*全部*。虽然*所有*包括先于它的两密码器，密码器的定货在密码器列表的确定首选。因此，当TLS联系被建立时，客户端选择两边支持根据大约在列表的外观的第一密码器。

> **注意**： 默认情况下RC4密码器在ESA启用。 在前一个示例中，**介质：海伊**根据空或匿名密码器的防止协商在ESA和SMA Cisco文档。欲知详情关于特定RC4，参考安全/服务器端TLS Mozilla文档，并且RC4安全在从*USENIX安全Symposium 2013*被提交的TLS和WPA文档的。为了从使用删除RC4密码器，参考跟随的示例。

通过密码器列表的处理，您能影响选择的密码器。您能列出特定密码器或密码器范围，并且由与**@STRENGTH**选项的包括的优点重拨他们在密码器字符串的，如显示此处：

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

保证是可用的在ESA的您查看所有密码器和范围。为了查看这些，输入**sslconfig**命令，遵从被**验证**子命令。SSL密码器类别的选项是**LOW**、**介质**，**海伊**和**全部**：

```
[]> 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
```

您能也结合这些为了包括范围：

```
[]> 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
```

您不想要已配置的和可用的其中任一SSL密码器应该删除与先于特定密码器的“**-**”选项。 示例如下：

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

在本例中的信息将否定从广告的*NULL*、*EDH-RSA-DES-CBC3-SHA*、*EDH-DSS-DES-CBC3-SHA*和*DES-CBC3-SHA*密码器并且防止他们的在SSL通信的使用。

您能也完成类似与包括“**!**”您希望变得不可用在密码器组前面的字符或字符串：

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

在本例中的信息从使用将删除所有RC4密码器。 因此， *RC4-SHA*和*RC4-MD5*密码器在SSL通信将否定和未通告。

如果变动做对SSL配置，请保证您**确认**任意更改。