更改ESA上与SSL/TLS一起使用的方法和密码

目录

简介

本文档介绍如何更改与思科邮件安全设备(ESA)上的安全套接字层(SSL)或传输层安全(TLS)配置一起使用的方法和密码。

更改与SSL/TLS一起使用的方法和密码

> **注意：**SSL/TLS方法和密码应根据您公司的特定安全策略和首选项进行设置。有关密码的第三方信息，请参阅安全/服务器端TLS Mozilla文档，以获取建议的服务器配置和详细信息。

使用Cisco AsyncOS for Email Security，管理员可以使用**sslconfig** 命令为用于GUI通信、为入站连接通告和为出站连接请求的方法和密码配置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.
[]>
```

如果对SSL配置进行了更改，请确保提**交所**有更改。

SSL方法

在邮件安全版本9.6及更高版本的AsyncOS中，默认情况下，ESA设置为*使用TLS v1/TLS v1.2*方法。在这种情况下，如果发送方和接收方都使用TLSv1.2,TLSv1.2将作为通信的先例。要建立TLS连接，两端必须至少有一个匹配的已启用方法，至少有一个匹配的已启用密码。

> **注意**：在9.6版之前的AsyncOS for E-mail Security版本中，默认有两种方法：*SSL v3*和*TLS v1*。由于最近的漏洞（如果启用了SSL v3），某些管理员可能想禁用SSL v3。

SSL密码

当您查看上一个示例中列出的默认密码时，了解其显示两个密码后跟单词ALL的原因非常重要。尽管*ALL*包含前面的两个密码，但密码列表中的密码顺序决定了首选项。因此，当建立TLS连接时，客户端根据列表中的外观顺序选择两端都支持的第一个密码。

> **注**:RC4密码在ESA上默认启用。在上一个示例中，**MEDIUM:HIGH**基于ESA和SMA Cisco文档上的Prevent Negotiations for Null或Anonymous Ciphers。有关RC4的详细信息，请参阅安全/服务器端TLS Mozilla文档，以及USENIX安全研讨会2013中提供的TLS和WPA文档中的*RC4安全性*。要删除RC4密码，请参阅以下示例。

通过处理密码列表，可以影响所选的密码。您可以列出特定密码或密码范围，也可以通过在密码字符串中包含**@STRENGTH**选项来按强度重新排序，如下所示：

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

请确保查看ESA上可用的所有密码和范围。要查看这些命令，请输入**sslconfig**命令，然后输入**verify**子命令。SSL密码类别的选项为**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
```

您还可以组合这些选项以包括范围：

```
[]> 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
```

您不希望配置和可用的任何SSL密码都应使用特定密码之前的“ **—** ”选项来删除。以下是一个示例：

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

本示例中的信息会否定*NULL*、*EDH-RSA-DES-CBC3-SHA*、*EDH-DSS-DES-CBC3-SHA*和*DES-CBC3-SHA*密码的通告和防止其使用在SSL通信中。

您还可以通过包含“！”来实现类似**的目**的 密码组或字符串前面的字符，您想要变为不可用：

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

本例中的信息将删除所有RC4密码。因此，*RC4-SHA*和*RC4-MD5*密码将被否定，并且不会在SSL通信中通告。

如果对SSL配置进行了更改，请确保提**交所**有更改。