配置ESA以首選PFS

目錄

簡介

本文描述如何在郵件安全裝置(ESA)上配置傳輸層安全(TLS)加密連線中的完全轉發保密(PFS)首選項。

必要條件

需求

思科建議您瞭解安全套接字層(SSL)/TLS。

採用元件

本文檔中的資訊基於AsyncOS for Email 9.6及更高版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

ESA提供前向保密(PFS)。 前向保密意味著資料將通過使用對稱加密的通道傳輸，該通道具有臨時機密，且即使一台主機或兩台主機上的私密金鑰（長期金鑰）被破壞，也無法將先前記錄的作業階段解密。

金鑰不通過通道傳輸，而是通過數學問題匯出共用金鑰(Diffie Hellman(DH)問題)。*在建立的會話或金鑰重新生成超時*期間，金鑰不會儲存在除主機隨機訪問儲存器(RAM)以外的任何位置。

ESA支援金鑰交換的DH。

設定

入站 — ESA充當TLS伺服器

ESA上提供這些密碼套件，用於提供轉發保密的入站簡單郵件傳輸協定(SMTP)流量。在本例中，密碼選擇僅允許被視為HIGH或MEDIUM的密碼套件，並對金鑰交換使用短暫Diffie Hellman(EDH)，並且優先使用TLSv1.2。密碼選擇語法遵循OpenSSL語法。

在AsyncOS 9.6+上使用前向保密的密碼：

```
"EDH+TLSv1.2:EDH+HIGH:EDH+MEDIUM:!LOW:!EXP:!aNULL:!RC4:!DSS:!SEED:!IDEA:!MD5:!PSK:!3DES:!SRP"

List:  DHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(256) Mac=AEAD
DHE-RSA-AES256-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(256) Mac=SHA256
DHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(128) Mac=AEAD
DHE-RSA-AES128-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(128) Mac=SHA256
DHE-RSA-AES256-SHA SSLv3 Kx=DH Au=RSA Enc=AES(256) Mac=SHA1
DHE-RSA-CAMELLIA256-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(256) Mac=SHA1
DHE-RSA-AES128-SHA SSLv3 Kx=DH Au=RSA Enc=AES(128) Mac=SHA1
DHE-RSA-CAMELLIA128-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(128) Mac=SHA1
```

Kx（=金鑰交換）部分顯示DH用於派生金鑰。

ESA使用預設的**sslconfig**設定(:ALL)支援這些密碼，但並不偏好使用。如果要優先使用提供PFS*的密碼，則需要更改***sslconfig**，並將EDH或組合**EDH+<cipher or cipher group name>**新增到您的密碼選擇中。

預設配置：

```
ESA> sslconfig

sslconfig settings:
 Inbound SMTP method:  tlsv1/tlsv1.2
 Inbound SMTP ciphers:
       RC4-SHA
       RC4-MD5
       ALL
```

新配置：

```
ESA> sslconfig

Inbound SMTP method:  tlsv1/tlsv1.2
 Inbound SMTP ciphers:
       EDH+TLSv1.2
       EDH+HIGH
       EDH+MEDIUM
       RC4-SHA
       RC4-MD5
       ALL
```

附註：RC4作為密碼，MD5作為MAC被認為是弱舊的，為了避免使用SSL/TLS，特別是在沒有金鑰重新生成的較高資料量時。

建議的INBOUND的sslconfig設定

這是一種普遍的觀點，只允許一般認為強大且安全的密碼。

可建議的INBOUND配置，刪除RC4和MD5以及其他遺留和弱選項，即Export(EXP)、Low(LOW)、IDEA(IDEA)、SEED(SEED)、3DES(3DES)密碼、DSS證書(DSS)、匿名金鑰交換(aNULL)、預共用金鑰(PSK)、SRP協定(SRP)，對金鑰交換和橢圓曲線數位簽章禁用橢圓曲線Diffie Hellman(ECDH)演算法(ECDSA)是範例：

```
EDH+TLSv1.2:EDH+HIGH:EDH+MEDIUM:HIGH:MEDIUM:!ECDH:!ECDSA:!LOW:!EXP:!aNULL:!RC4:!DSS:!SEED:!IDEA:
!MD5:!PSK:!3DES:!SRP
```

在**sslconfig**中輸入的字串導致此受支援的INBOUND密碼清單：

```
DHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(256) Mac=AEAD
DHE-RSA-AES256-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(256) Mac=SHA256
DHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(128) Mac=AEAD
DHE-RSA-AES128-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(128) Mac=SHA256
DHE-RSA-AES256-SHA SSLv3 Kx=DH Au=RSA Enc=AES(256) Mac=SHA1
DHE-RSA-CAMELLIA256-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(256) Mac=SHA1
DHE-RSA-AES128-SHA SSLv3 Kx=DH Au=RSA Enc=AES(128) Mac=SHA1
DHE-RSA-CAMELLIA128-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(128) Mac=SHA1
AES256-GCM-SHA384 TLSv1.2 Kx=RSA Au=RSA Enc=AESGCM(256) Mac=AEAD
AES256-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AES(256) Mac=SHA256
AES256-SHA SSLv3 Kx=RSA Au=RSA Enc=AES(256) Mac=SHA1
CAMELLIA256-SHA SSLv3 Kx=RSA Au=RSA Enc=Camellia(256) Mac=SHA1
AES128-GCM-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AESGCM(128) Mac=AEAD
AES128-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AES(128) Mac=SHA256
AES128-SHA SSLv3 Kx=RSA Au=RSA Enc=AES(128) Mac=SHA1
CAMELLIA128-SHA SSLv3 Kx=RSA Au=RSA Enc=Camellia(128) Mac=SHA1
```

附註：充當TLS伺服器（入站流量）的ESA當前不支援用於金鑰交換(ECDHE)和ECDSA證書的橢圓曲線Diffie Hellman。

出站 — ESA充當TLS客戶端

對於出站SMTP流量，除入站外，ESA還支援ECDHE和ECDSA證書。

附註：採用ECDSA的橢圓曲線加密(ECC)證書並未被廣泛採用。

傳送出站電子郵件時，ESA是TLS客戶端。TLS客戶端證書是可選的。如果TLS-Server不強制（需要）ESA（作為TLS客戶端）以提供ECDSA客戶端證書，則ESA可以繼續ECDSA安全會話。當作為TLS-Client的ESA請求其證書時，它為OUTBOUND方向提供配置的RSA證書。

注意：ESA上預安裝的受信任CA證書儲存（系統清單）不包括ECC(ECDSA)根證書！您可能需要手動將ECC根證書（您信任的）新增到自定義清單，以使ECC信任鏈可驗證。

若要優先使用提供正向保密的DHE/ECDHE密碼，您可以按如下方式修改sslconfig密碼選擇。

將此項新增到當前的密碼選擇中。

```
"EDH+TLSv1.2:ECDH+TLSv1.2:EDH+HIGH:EDH+MEDIUM:ECDH+HIGH:ECDH+MEDIUM"
```

建議的OUTBOUND的sslconfig設定

這是一種普遍的觀點，只允許一般認為強大且安全的密碼。

```
EDH+TLSv1.2:ECDH+TLSv1.2:EDH+HIGH:EDH+MEDIUM:ECDH+HIGH:ECDH+MEDIUM:HIGH:MEDIUM:!LOW:!EXP:!aNULL:
!RC4:!DSS:!SEED:!IDEA:!MD5:!PSK:!3DES:!SRP
```

在sslconfig中輸入的字串導致此受支援的OUTBOUND密碼清單：

```
DHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(256) Mac=AEAD
DHE-RSA-AES256-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(256) Mac=SHA256
DHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(128) Mac=AEAD
DHE-RSA-AES128-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(128) Mac=SHA256
ECDHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH Au=RSA Enc=AESGCM(256) Mac=AEAD
ECDHE-ECDSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AESGCM(256) Mac=AEAD
ECDHE-RSA-AES256-SHA384 TLSv1.2 Kx=ECDH Au=RSA Enc=AES(256) Mac=SHA384
ECDHE-ECDSA-AES256-SHA384 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AES(256) Mac=SHA384
ECDHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH Au=RSA Enc=AESGCM(128) Mac=AEAD
ECDHE-ECDSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AESGCM(128) Mac=AEAD
ECDHE-RSA-AES128-SHA256 TLSv1.2 Kx=ECDH Au=RSA Enc=AES(128) Mac=SHA256
ECDHE-ECDSA-AES128-SHA256 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AES(128) Mac=SHA256
DHE-RSA-AES256-SHA SSLv3 Kx=DH Au=RSA Enc=AES(256) Mac=SHA1
DHE-RSA-CAMELLIA256-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(256) Mac=SHA1
DHE-RSA-AES128-SHA SSLv3 Kx=DH Au=RSA Enc=AES(128) Mac=SHA1
DHE-RSA-CAMELLIA128-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(128) Mac=SHA1
ECDHE-RSA-AES256-SHA SSLv3 Kx=ECDH Au=RSA Enc=AES(256) Mac=SHA1
ECDHE-ECDSA-AES256-SHA SSLv3 Kx=ECDH Au=ECDSA Enc=AES(256) Mac=SHA1
ECDHE-RSA-AES128-SHA SSLv3 Kx=ECDH Au=RSA Enc=AES(128) Mac=SHA1
ECDHE-ECDSA-AES128-SHA SSLv3 Kx=ECDH Au=ECDSA Enc=AES(128) Mac=SHA1
AES256-GCM-SHA384 TLSv1.2 Kx=RSA Au=RSA Enc=AESGCM(256) Mac=AEAD
AES256-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AES(256) Mac=SHA256
AES256-SHA SSLv3 Kx=RSA Au=RSA Enc=AES(256) Mac=SHA1
CAMELLIA256-SHA SSLv3 Kx=RSA Au=RSA Enc=Camellia(256) Mac=SHA1
AES128-GCM-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AESGCM(128) Mac=AEAD
AES128-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AES(128) Mac=SHA256
AES128-SHA SSLv3 Kx=RSA Au=RSA Enc=AES(128) Mac=SHA1
CAMELLIA128-SHA SSLv3 Kx=RSA Au=RSA Enc=Camellia(128) Mac=SHA1
```

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- 開放式SSL密碼
- 思科下一代加密
- 技術支援與文件 - Cisco Systems