

PFS を好む設定 ESA

目次

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[受信-ESA は TLS サーバとして機能します](#)

[受信の推奨される sslconfig 設定](#)

[送信-ESA は TLS クライアントとして機能します](#)

[送信の推奨される sslconfig 設定](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

概要

この資料に E メール セキュリティ アプライアンス (ESA) の Transport Layer Security (TLS) 暗号化接続の完全な前方機密性 (PFS) のためのプリファレンスを設定する方法を記述されています。

前提条件

要件

Cisco は Secure Sockets Layer (SSL) /TLS のナレッジがあることを推奨します。

使用するコンポーネント

この資料に記載されている情報はメール バージョン 9.6 および それ 以上のための AsyncOS に基づいています。

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

背景説明

ESA は前方機密性 (PFS) を提供します。前方機密性はホストの 1 つまたは両方の秘密キー (長期キー) は妥協されてもデータがチャネルによって転送されることを意味しはかないシークレットと対称暗号化を使用する、記録された セッションを以前に復号化することはできません。

シークレットはチャネルによって転送されません、その代り共用シークレットは数学問題 (Diffie Hellman (DH) 問題) と得られます。シークレットはホスト ランダムアクセスメモリ (RAM) より設定されたセッションがキー再生成タイムアウトの間に他の場所保存されません。

キー交換のための DH (Diffie-Hellman) ESA サポート。

設定

受信- ESA は TLS サーバとして機能します

前方機密性を提供するこれらの暗号スイートは受信 Simple Mail Transfer Protocol (SMTP) トラフィックに ESA で利用できます。この例では、選択割り当て暗号スイートだけ考慮し、高/中キー交換のために使用し、はかない Diffie Hellman (EDH) を好みます TLSv1.2 を暗号化して下さい。暗号選択構文は OpenSSL 構文に続きます。

AsyncOS 9.6+ の前方機密性の暗号:

```
"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 (= キー交換) セクションは示しますシークレットを得るために DH (Diffie-Hellman) 使用される。

ESA はデフォルト `sslconfig` 設定とのこれらの暗号をサポートします (: すべては)、しかしそれを好みません。PFS を提供する暗号を好みたいと思えば、`sslconfig` を変更し、暗号選択に EDH が組み合わせ `EDH+<cipher または暗号グループ name>` 追加する必要があります。

デフォルト 設定:

```
"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
```

新しい設定:

```
"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
```

注: MAC として暗号および MD5 として RC4 は弱い、レガシーとおよび SSL/TLS の使用を、特にキー再生成なしでより高いデータ量に関しては避けるためにみなされます。

受信の推奨される sslconfig 設定

これは勝つ意見一般に強く、セキュアと考慮される暗号しか許可しないためにであり。

受信 RC4 のための recommendable 設定はおよび MD5、また他のレガシーおよび弱いオプション、即ちエクスポート (EXP)、低く (LOW)、IDEA (IDEA)、シードする (シードする)、トリプル DES (トリプル DES) 暗号、DSS 証明書 (DSS)、匿名キー Exchange (aNULL)、事前共有キー (PSK)、SRP プロトコル (SRP)、ディセーブル キー Exchange のための楕円カーブ Diffie Hellman (ECDH) および楕円曲線デジタル署名アルゴリズム (取除く ECDSA) 例です:

```
"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
```

sslconfig で入力されるストリングは受信のためのサポートされた暗号のこのリストという結果に終わります:

```
"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
```

注: TLS サーバ (受信 トラフィック) として現在機能する ESA はキー Exchange (ECDHE) および ECDSA 証明書のための楕円カーブ Diffie Hellman をサポートしません。

送信- ESA は TLS クライアントとして機能します

受信サポート ECDHE に加える送信 SMTP トラフィック、ESA および ECDSA 証明書に関しては。

注: ECDSA の楕円カーブ暗号解読法 (ECC) 証明書は大幅に取り入れられません。

送信メールが渡されるとき、ESA は TLS クライアントです。TLS クライアント証明書はオプションです。ECDSA クライアント 認証を提供するために TLS サーバが (必要となるため) ESA を (TLS クライアントとして) 強制しない場合 ESA は ECDSA によって保護されるセッションと続くことができます。TLS クライアントとして ESA はそれをである証明書頼まれるとき、送信方向に設定された RSA 証明書を提供します。

注意: ESA のプレインストールされた信頼された CA 認証 ストア (システム リスト) は ECC (ECDSA) ルート証明が含まれていません! 信頼のします ECC チェーンを証明できるように手動で (信頼) orderto のカスタム リストに ECC ルート証明追加する必要があるかもしれません。

前方機密性を提供する DHE/ECDHE 暗号を好むために、**sslconfig** 暗号選択を次の通り修正できます。

現在の暗号選択にこれを追加して下さい。

```
"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
```

送信の推奨される **sslconfig** 設定

これは勝つ意見一般に強く、セキュアと考慮される暗号しか許可しないためにであり。

```
"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
```

sslconfig で入力されるストリングは送信のためのサポートされた暗号のこのリストという結果に終わります:

```
"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

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- [SSL 暗号を開いて下さい](#)
- [Cisco 次世代暗号化](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)