Configurez l'ESA pour préférer le PFS

Contenu

Introduction

Ce document décrit comment configurer la préférence pour le perfect forward secrecy (PFS) dans des connexions cryptées de Transport Layer Security (TLS) sur l'appliance de sécurité du courrier électronique (ESA).

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance de Secure Sockets Layer (SSL) /TLS.

Composants utilisés

Les informations dans ce document sont basées sur AsyncOS pour la version 9.6 et ultérieures d'email.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

L'ESA offre le forward secrecy (PFS). Le forward secrecy signifie que les données sont transférées par l'intermédiaire d'un canal qui utilise le cryptage symétrique avec des secrets éphémères, et même si la clé privée (clé à long terme) sur un ou chacun des deux hôtes a été

compromise, il n'est pas possible de déchiffrer une session précédemment enregistrée.

Le secret n'est pas transféré par le canal, au lieu de cela le secret partagé est dérivé avec un problème mathématique problème (de Diffie Hellman (CAD)). Le secret n'est pas enregistré n'importe où ailleurs que la mémoire à accès aléatoire d'hôtes (RAM) pendant le délai d'attente établi de régénération de session ou de clé.

L'ESA prend en charge le CAD pour le Key Exchange.

Configurez

D'ARRIVÉE - L'ESA agit en tant que serveur de TLS

Ces suites de chiffrement sont disponibles sur l'ESA pour le trafic D'ARRIVÉE de Protocole SMTP (Simple Mail Transfer Protocol) qui fournissent le forward secrecy. Dans cet exemple, la sélection de chiffrement permet seulement des suites de chiffrement considérées HAUTE ou SUPPORT et utilisation Diffie éphémère Hellman (EDH) pour le Key Exchange et préfère TLSv1.2. La syntaxe de sélection de chiffrement suit la syntaxe d'OpenSSL.

Chiffrements avec le forward secrecy sur AsyncOS 9.6+ :

```
"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
```

La section KX (= Key Exchange) prouve que le CAD est utilisé afin de dériver le secret.

L'ESA prend en charge ces chiffrements avec les configurations par défaut de **sslconfig** (: TOUT), mais ne le préfère pas. Si vous voulez préférer des chiffrements qui offrent le PFS, vous devez changer votre **sslconfig** et ajouter EDH ou une combinaison **EDH+<cipher ou chiffrer le name> de groupe à** votre sélection de chiffrement.

Configuration par défaut :

```
"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
```

Nouvelle configuration :

```
"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
```

Note: Le RC4 en tant qu'un chiffrement et MD5 comme MAC est considéré faible, legs et afin d'éviter l'utilisation avec SSL/TLS, particulièrement quand il s'agit de volume données plus élevé sans régénération principale.

Configurations recommandées de sslconfig pour D'ARRIVÉE

C'est une opinion actuelle et pour permettre seulement les chiffrements qui sont généralement considérés forts et sécurisés.

Une configuration recommandable pour qui retire le RC4 D'ARRIVÉE et le MD5 aussi bien que d'autres options existantes et faibles, à savoir exportation (EXP), bas (BAS), IDÉE (IDÉE), GRAINE (GRAINE), chiffrements 3DES (3DES), Certificats de DSS (DSS), Key Exchange anonyme (aNULL), clés pré-partagées (PSK), protocole SRP (SRP), curve elliptique de débronchements Diffie Hellman (ECDH) pour le Key Exchange et algorithme elliptique de signature numérique de curve (ECDSA) sont les exemples :

```
"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
```

La chaîne est entrée dans des résultats de **sslconfig** dans cette liste de chiffrements pris en charge pour D'ARRIVÉE :

```
"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
```

Note: L'ESA qui agit en tant que serveur de TLS (le trafic D'ARRIVÉE) actuellement ne prend en charge pas la curve elliptique Diffie Hellman pour le Key Exchange (ECDHE) et les Certificats ECDSA.

SORTANT - L'ESA agit en tant que client de TLS

Pour le trafic SORTANT de SMTP, l'ESA en plus des supports D'ARRIVÉE ECDHE et des Certificats ECDSA.

> **Note**: Des Certificats elliptiques du chiffrement de curve (ECC) avec l'ECDSA ne sont pas largement adoptés.

Quand un email SORTANT est fourni, l'ESA est le client de TLS. Un certificat de Tls-client est facultatif. Si le Tls-serveur ne forcent pas (exiger) l'ESA (en tant que Tls-client) afin de fournir un certificat client ECDSA, l'ESA peut continuer une session sécurisée par ECDSA. Quand l'ESA en tant que Tls-client est demandé lui est certificat, il fournit le certificat configuré RSA pour la direction sortante.

> **Attention** : La mémoire de confiance préinstallée de certificat de CA (liste de système) sur l'ESA n'inclut pas des certificats racine ECC (ECDSA) ! Vous pourriez devoir ajouter manuellement les certificats racine ECC (qui vous confiance) à la liste faite sur commande dans l'orderto rendez la chaîne ECC de la confiance vérifiable.

Afin de préférer des chiffrements DHE/ECDHE qui offrent le forward secrecy, vous pouvez modifier la sélection de chiffrement de **sslconfig** comme suit.

Ajoutez ceci à votre sélection en cours de chiffrement.

```
"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
```

Configurations recommandées de sslconfig pour SORTANT

C'est une opinion actuelle et pour permettre seulement les chiffrements qui sont généralement considérés forts et sécurisés.

```
"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
```

La chaîne est entrée dans des résultats de **sslconfig** dans cette liste de chiffrements pris en charge pour SORTANT :

```
"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
```

Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Ouvrez les chiffrements SSL
- Cryptage de nouvelle génération de Cisco
- **Support et documentation techniques - Cisco Systems**