Contenu

Introduction

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

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- SSL/TLS

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- 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 (perfect forward secrecy). 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 utilisant un *problème mathématique (problème de Diffie Hellman).* Le secret n'est pas enregistré n'importe où ailleurs que la mémoire à accès aléatoire d'hôtes (RAM) pendant la session établie (ou le délai d'attente de régénération de clé).

L'ESA prend en charge **Diffie Hellman (CAD) pour le Key Exchange**.

Configurez

D'ARRIVÉE - ESA agissant en tant que serveur de TLS

Au-dessous du chiffrement les suites sont disponibles sur l'ESA pour le trafic d'arrivée de SMTP qui fournissent le forward secrecy. La sélection ci-dessous de chiffrement d'*exemple* permet seulement des suites de chiffrement considérées CAD éphémère de *HAUTE* ou de *SUPPORT* et d'utilisation 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=AEADDHE-RSA-AES256-
SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(256) Mac=SHA256DHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=DH
Au=RSA Enc=AESGCM(128) Mac=AEADDHE-RSA-AES128-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(128)
Mac=SHA256DHE-RSA-AES256-SHA SSLv3 Kx=DH Au=RSA Enc=AES(256) Mac=SHA1DHE-RSA-CAMELLIA256-SHA
SSLv3 Kx=DH Au=RSA Enc=Camellia(256) Mac=SHA1DHE-RSA-AES128-SHA SSLv3 Kx=DH Au=RSA Enc=AES(128)
Mac=SHA1DHE-RSA-CAMELLIA128-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(128) Mac=SHA1
```

La section **KX** (= Key Exchange) prouve que Diffie Hellman est utilisé pour 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 devriez changer votre **sslconfig** et ajouter Diffie éphémère Hellman (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=AEADDHE-RSA-AES256-
SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(256) Mac=SHA256DHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=DH
Au=RSA Enc=AESGCM(128) Mac=AEADDHE-RSA-AES128-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(128)
Mac=SHA256DHE-RSA-AES256-SHA SSLv3 Kx=DH Au=RSA Enc=AES(256) Mac=SHA1DHE-RSA-CAMELLIA256-SHA
SSLv3 Kx=DH Au=RSA Enc=Camellia(256) Mac=SHA1DHE-RSA-AES128-SHA SSLv3 Kx=DH Au=RSA Enc=AES(128)
Mac=SHA1DHE-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=AEADDHE-RSA-AES256-
SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(256) Mac=SHA256DHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=DH
Au=RSA Enc=AESGCM(128) Mac=AEADDHE-RSA-AES128-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(128)
Mac=SHA256DHE-RSA-AES256-SHA SSLv3 Kx=DH Au=RSA Enc=AES(256) Mac=SHA1DHE-RSA-CAMELLIA256-SHA
SSLv3 Kx=DH Au=RSA Enc=Camellia(256) Mac=SHA1DHE-RSA-AES128-SHA SSLv3 Kx=DH Au=RSA Enc=AES(128)
Mac=SHA1DHE-RSA-CAMELLIA128-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(128) Mac=SHA1
```

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

Configurations recommandées de sslconfig pour D'ARRIVÉE

Ce qui suit est opinion actuelle et pour permettre seulement les chiffrements qui sont généralement considérés forts et sécurisés

Une configuration recommandable pour D'ARRIVÉE qui retire le RC4 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) et Key Exchange anonyme (aNULL) et clés pré-partagées (PSK) et protocole SRP (SRP) et désactive ECDH et ECDSA serait par exemple :

```
"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=AEADDHE-RSA-AES256-
SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(256) Mac=SHA256DHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=DH
Au=RSA Enc=AESGCM(128) Mac=AEADDHE-RSA-AES128-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(128)
Mac=SHA256DHE-RSA-AES256-SHA SSLv3 Kx=DH Au=RSA Enc=AES(256) Mac=SHA1DHE-RSA-CAMELLIA256-SHA
SSLv3 Kx=DH Au=RSA Enc=Camellia(256) Mac=SHA1DHE-RSA-AES128-SHA SSLv3 Kx=DH Au=RSA Enc=AES(128)
Mac=SHA1DHE-RSA-CAMELLIA128-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(128) Mac=SHA1
```

Ce qui précède de chaîne présenté dans le **sslconfig** a comme conséquence 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=AEADDHE-RSA-AES256-
SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(256) Mac=SHA256DHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=DH
Au=RSA Enc=AESGCM(128) Mac=AEADDHE-RSA-AES128-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(128)
Mac=SHA256DHE-RSA-AES256-SHA SSLv3 Kx=DH Au=RSA Enc=AES(256) Mac=SHA1DHE-RSA-CAMELLIA256-SHA
SSLv3 Kx=DH Au=RSA Enc=Camellia(256) Mac=SHA1DHE-RSA-AES128-SHA SSLv3 Kx=DH Au=RSA Enc=AES(128)
Mac=SHA1DHE-RSA-CAMELLIA128-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(128) Mac=SHA1
```

Remarque: L'ESA agissant 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 elliptiques de l'algorithme de signature numérique de curve (*ECDSA*).

SORTANT - ESA agissant en tant que client de TLS

Pour le trafic sortant de SMTP l'ESA **en plus du** Key Exchange éphémère elliptique de Diffie Hellman de curve de supports **D'ARRIVÉE** (*ECDHE*) et des Certificats elliptiques de l'algorithme de signature numérique de curve (*ECDSA*).

Remarque: Des Certificats elliptiques du chiffrement de curve (ECC) avec l'algorithme elliptique de signature de Digitial de curve, (ECDSA) ne sont pas largement adoptés.

En fournissant l'email (sortant), l'ESA est le client de TLS. Un certificat de Tls-client est facultatif. Si le Tls-serveur ne force pas (exiger) l'ESA (en tant que Tls-client) pour fournir un certificat client ECDSA, l'ESA peut continuer une session sécurisée par ECDSA. Quand l'ESA en tant que Tls-client est demandé son 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) ! Il peut exiger pour ajouter manuellement les certificats racine ECC (qui vous confiance) à la *liste faite sur commande* pour rendre la chaîne ECC de la confiance vérifiable.

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

Ajoutez le ci-dessous à votre sélection existante 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=AEADDHE-RSA-AES256-
SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(256) Mac=SHA256DHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=DH
Au=RSA Enc=AESGCM(128) Mac=AEADDHE-RSA-AES128-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(128)
Mac=SHA256DHE-RSA-AES256-SHA SSLv3 Kx=DH Au=RSA Enc=AES(256) Mac=SHA1DHE-RSA-CAMELLIA256-SHA
SSLv3 Kx=DH Au=RSA Enc=Camellia(256) Mac=SHA1DHE-RSA-AES128-SHA SSLv3 Kx=DH Au=RSA Enc=AES(128)
Mac=SHA1DHE-RSA-CAMELLIA128-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(128) Mac=SHA1
```

Configurations recommandées de sslconfig pour SORTANT

Ce qui suit est 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=AEADDHE-RSA-AES256-
SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(256) Mac=SHA256DHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=DH
Au=RSA Enc=AESGCM(128) Mac=AEADDHE-RSA-AES128-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(128)
Mac=SHA256DHE-RSA-AES256-SHA SSLv3 Kx=DH Au=RSA Enc=AES(256) Mac=SHA1DHE-RSA-CAMELLIA256-SHA
SSLv3 Kx=DH Au=RSA Enc=Camellia(256) Mac=SHA1DHE-RSA-AES128-SHA SSLv3 Kx=DH Au=RSA Enc=AES(128)
Mac=SHA1DHE-RSA-CAMELLIA128-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(128) Mac=SHA1
```

Ce qui précède de chaîne présenté dans le **sslconfig** a comme conséquence 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=AEADDHE-RSA-AES256-
SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(256) Mac=SHA256DHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=DH
Au=RSA Enc=AESGCM(128) Mac=AEADDHE-RSA-AES128-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(128)
Mac=SHA256DHE-RSA-AES256-SHA SSLv3 Kx=DH Au=RSA Enc=AES(256) Mac=SHA1DHE-RSA-CAMELLIA256-SHA
SSLv3 Kx=DH Au=RSA Enc=Camellia(256) Mac=SHA1DHE-RSA-AES128-SHA SSLv3 Kx=DH Au=RSA Enc=AES(128)
Mac=SHA1DHE-RSA-CAMELLIA128-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(128) Mac=SHA1
```

Informations connexes

- Ouvrez les chiffrements SSL
- Cryptage de nouvelle génération de Cisco