Modifier les méthodes et les chiffrements utilisés avec SSL/TLS sur le ESA

Contenu

Introduction

Ce document décrit comment modifier les méthodes et les chiffrements utilisés avec les configurations SSL (Secure Socket Layer) ou TLS (Transport Layer Security) sur le dispositif de sécurité de la messagerie électronique Cisco (ESA).

Modifier les méthodes et les chiffrement utilisés avec SSL/TLS

> **Note**: Les méthodes et les chiffrements SSL/TLS doivent être définis en fonction des stratégies et des préférences de sécurité spécifiques de votre entreprise. Pour obtenir des informations tierces sur les chiffrements, reportez-vous au document Mozilla Security/Server Side TLS pour obtenir des configurations de serveur recommandées et des informations détaillées.

Avec Cisco AsyncOS pour la sécurité de la messagerie, un administrateur peut utiliser la commande **sslconfig** afin de configurer les protocoles SSL ou TLS pour les méthodes et les chiffrement utilisés pour la communication de l'interface utilisateur graphique, annoncés pour les connexions entrantes et demandés pour les connexions sortantes :

```
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.
[]>
```

Si des modifications sont apportées à la configuration SSL, assurez-vous de **valider** toutes les modifications.

Méthodes SSL

Dans AsyncOS pour les versions 9.6 et ultérieures de la sécurité de la messagerie, l'ESA est configuré pour utiliser la méthode *TLS v1/TLS v1.2* par défaut. Dans ce cas, TLSv1.2 crée un précédent pour la communication, si elle est utilisée à la fois par les parties émettrice et réceptrice. Pour établir une connexion TLS, les deux côtés doivent avoir au moins une méthode activée qui correspond et au moins un chiffrement activé qui correspond.

> **Note**: Dans AsyncOS pour les versions de sécurité de la messagerie antérieures à la version 9.6, la valeur par défaut est de deux méthodes : *SSL v3* et *TLS v1*. Certains administrateurs peuvent vouloir désactiver SSL v3 en raison de vulnérabilités récentes (si SSL v3 est activé).

Chiffres SSL

Lorsque vous affichez le chiffre par défaut qui est indiqué dans l'exemple précédent, il est important de comprendre la raison pour laquelle il affiche deux chiffres suivis du mot *ALL*. Bien que *ALL* comprenne les deux chiffres qui l'précèdent, l'ordre des chiffres dans la liste de chiffres détermine la préférence. Ainsi, lorsqu'une connexion TLS est établie, le client choisit le premier chiffre que les deux côtés prennent en charge en fonction de l'ordre d'apparition dans la liste.

> **Remarque** : les chiffrements RC4 sont activés par défaut sur l'ESA. Dans l'exemple précédent, **MEDIUM : HIGH** est basé sur le document Prevent Negotiations for Null or Anonymous Ciphers sur le document ESA et SMA Cisco. Pour plus d'informations concernant spécifiquement RC4, consultez le document Mozilla Security/Server Side TLS, ainsi que le document On the Security of RC4 in TLS and WPA présenté lors du *colloque sur la sécurité de l'USENIX 2013*. Afin de supprimer les chiffrement RC4 de l'utilisation, reportez-vous aux exemples suivants.

En manipulant la liste de chiffrement, vous pouvez influencer le chiffre choisi. Vous pouvez répertorier des plages de chiffrement ou de chiffrement spécifiques, et également les réorganiser par force avec l'inclusion de l'option **@STRENGTH** dans la chaîne de chiffrement, comme indiqué ici :

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

Assurez-vous de consulter tous les algorithmes de chiffrement et les plages disponibles sur l'ESA. Afin de les afficher, entrez la commande **sslconfig**, suivie de la sous-commande **verify**. Les options pour les catégories de chiffrement SSL sont **FAIBLE**, **MOYEN**, **ÉLEVÉ** et **TOUTES** :

```
[]> 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
```

Vous pouvez également les combiner afin d'inclure des plages :

```
[]> 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
```

Tous les chiffrements SSL que vous ne voulez pas configurer et disponibles doivent être supprimés avec l'option "**-**" qui précède les chiffrements spécifiques. Voici un exemple :

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

Les informations de cet exemple annuleraient les chiffres *NULL*, *EDH-RSA-DES-CBC3-SHA*,

EDH-DSS-DES-CBC3-SHA et *DES-CBC3-SHA* de la publicité et empêcheraient leur utilisation dans la communication SSL.

Vous pouvez également effectuer la même chose avec l'inclusion de " **!**" caractère devant le groupe ou la chaîne de chiffrement que vous souhaitez rendre indisponible :

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

Les informations de cet exemple supprimeraient l'utilisation de tous les chiffrement RC4. Ainsi, les chiffres *RC4-SHA* et *RC4-MD5* seraient annulés et non annoncés dans la communication SSL.

Si des modifications sont apportées à la configuration SSL, assurez-vous de **valider** toutes les modifications.