Modifiez les méthodes et les chiffrements utilisés avec SSL/TLS sur l'ESA

Contenu

Introduction

Ce document décrit comment modifier les méthodes et les chiffrements qui sont utilisés avec des configurations de Protocole SSL (Secure Socket Layer) ou de Transport Layer Security (TLS) sur l'appliance de sécurité du courrier électronique de Cisco (ESA).

Modifiez les méthodes et les chiffrements utilisés avec SSL/TLS

> **Note**: Les méthodes et des chiffrements SSL/TLS devraient être placés basés sur les stratégies de sécurité et les préférences spécifiques de votre société. Pour les tiers informations en vue de des chiffrements, document de Mozilla référez-vous de Sécurité/côté serveur à TLS pour des configurations du serveur et des informations détaillées recommandées.

Avec Cisco AsyncOS pour la sécurité du courrier électronique, un administrateur peut employer la commande de **sslconfig** afin de configurer les protocoles SSL ou de TLS pour les méthodes et les chiffrements qui sont utilisés pour la transmission GUI, annoncés pour des 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 que vous **commettez** l'intégralité de modifications.

Méthodes SSL

Dans AsyncOS pour des versions 9.6 et ultérieures de sécurité du courrier électronique, l'ESA est placé pour utiliser la méthode du *TLS v1/TLS v1.2* par défaut. Dans ce cas, TLSv1.2 prend le précédent pour la transmission, si en service par les interlocuteurs d'envoi et de réception. Afin d'établir une connexion de TLS, les deux côtés doivent avoir au moins une méthode activée qui s'assortit, et au moins un chiffrement activé qui s'assortit.

> **Note**: Dans AsyncOS pour des versions de sécurité du courrier électronique avant la version 9.6, le par défaut a deux méthodes : *SSL v3* et *TLS v1*. Quelques administrateurs pourraient vouloir désactiver SSL v3 dû aux vulnérabilités récentes (si SSL v3 est activé).

Chiffrements SSL

Quand vous visualisez le chiffrement par défaut qui est répertorié dans l'exemple précédent, il est important de comprendre la raison pour laquelle elle affiche deux chiffrements suivis *TOUT du* mot. Bien que *TOUT* inclue les deux chiffrements qui le précèdent, la commande des chiffrements dans la liste de chiffrement détermine la préférence. Ainsi, quand un rapport de TLS est établi, le client sélectionne le premier chiffrement que le support de les deux côtés a basé sur l'ordre de l'apparence dans la liste.

> **Note**: Les chiffrements RC4 sont activés par défaut sur l'ESA. Dans l'exemple précédent, le **SUPPORT : La HAUTE** est basée sur les négociations d'empêchement pour des chiffrements nuls ou anonymes sur le document Cisco ESA et SMA. Pour de plus amples informations en vue de le RC4 spécifiquement, document de Mozilla référez-vous de Sécurité/côté serveur à TLS, et également en fonction la Sécurité du RC4 dans le document de TLS et WPA qui est présenté du *colloque 2013 de Sécurité USENIX*. Afin de retirer les chiffrements RC4 de l'utilisation, référez-vous aux exemples qui suivent.

Par la manipulation de la liste de chiffrement, vous pouvez influencer le chiffrement qui est choisi. Vous pouvez répertorier des chiffrements ou des plages spécifiques de chiffrement, et les commandez à nouveau également par point fort avec l'intégration de l'option **@STRENGTH** dans la chaîne de chiffrement, comme affiché ici :

```
Enter the inbound SMTP ssl cipher you want to use.
```

```
[RC4-SHA:RC4-MD5:ALL]> MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH
```

Assurez-vous que vous passez en revue tous les chiffrements et plages qui sont disponibles sur l'ESA. Afin de visualiser ces derniers, sélectionnez la commande de **sslconfig**, suivie du commande secondaire de **vérifier**. Les options pour les catégories de chiffrement SSL sont **BAS**, **SUPPORT**, **HAUTE**, 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 combiner ces derniers 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
```

Des chiffrements SSL que vous ne voulez pas configuré et disponible l'uns des devraient être retirés 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 dans cet exemple réaliseraient une inversion les chiffrements de *NULL*, *EDH-RSA-DES-CBC3-SHA*, *EDH-DSS-DES-CBC3-SHA*, et *DES-CBC3-SHA de la* publicité et empêcheraient leur utilisation dans la transmission SSL.

Vous pouvez également accomplir semblable avec l'intégration du « **!** » caractère devant le groupe de chiffrement ou chaîne que vous désirez devenir indisponible :

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

Les informations dans cet exemple retireraient tous les chiffrements RC4 de l'utilisation. Ainsi, les chiffrements *RC4-SHA* et *RC4-MD5* seraient réalisés une inversion et pas annoncés dans la transmission SSL.

Si des modifications sont apportées à la configuration SSL, assurez-vous que vous commettez l'intégralité de modifications.