Modifica dei metodi e dei cifrari utilizzati con SSL/TLS sull'ESA

Sommario

Introduzione

In questo documento viene descritto come modificare i metodi e i cifrari utilizzati con le configurazioni Secure Sockets Layer (SSL) o Transport Layer Security (TLS) su Cisco Email Security Appliance (ESA).

Modifica dei metodi e delle cifrature utilizzati con SSL/TLS

> **Nota:** I metodi e le cifrature SSL/TLS devono essere impostati in base ai criteri e alle preferenze di sicurezza specifici della società. Per informazioni di terze parti relative alle cifrature, consultare il documento Security/Server Side TLS Mozilla per le configurazioni server consigliate e informazioni dettagliate.

Con Cisco AsyncOS for Email Security, un amministratore può utilizzare il comando **sslconfig** per configurare i protocolli SSL o TLS per i metodi e le cifrature utilizzati per la comunicazione GUI, annunciati per le connessioni in entrata e richiesti per le connessioni in uscita:

```
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.
[]>
```

Se vengono apportate modifiche alla configurazione SSL, accertarsi di eseguire il **commit su** qualsiasi modifica.

Metodi SSL

In AsyncOS for Email Security versione 9.6 e successive, l'ESA è impostata per utilizzare il metodo *TLS v1/TLS v1.2* per impostazione predefinita. In questo caso, TLSv1.2 ha la precedenza nella comunicazione, se utilizzata sia dalla parte mittente che da quella ricevente. Per stabilire una connessione TLS, entrambi i lati devono avere almeno un metodo abilitato corrispondente e almeno una cifratura abilitata corrispondente.

> **Nota:** Nelle versioni di AsyncOS for Email Security precedenti alla versione 9.6, l'impostazione predefinita prevede due metodi: *SSL v3* e *TLS v1*. Alcuni amministratori potrebbero voler disabilitare SSL v3 a causa di vulnerabilità recenti (se SSL v3 è abilitato).

Cifre SSL

Quando si visualizza la cifratura predefinita elencata nell'esempio precedente, è importante comprendere il motivo per cui vengono visualizzati due cifrari seguiti dalla parola *ALL*. Sebbene *ALL* includa i due cifrari precedenti, l'ordine dei cifrari nell'elenco determina la preferenza. Pertanto, quando viene stabilita una connessione TLS, il client sceglie la prima cifratura supportata da entrambi i lati in base all'ordine di visualizzazione nell'elenco.

> **Nota**: i cifrari RC4 sono abilitati per impostazione predefinita sull'ESA. Nell'esempio precedente, il valore **MEDIUM:HIGH** si basa sul documento Cisco dell'ESA e dell'SMA che impedisce le negoziazioni per i cifrari nulli o anonimi. Per ulteriori informazioni in particolare su RC4, fare riferimento al documento Security/Server Side TLS Mozilla e anche al documento On the Security of RC4 in TLS and WPA che è presentato dal *Simposio USENIX Security 2013*. Per rimuovere i cifrari RC4, fare riferimento agli esempi seguenti.

La modifica dell'elenco di cifratura consente di influenzare la cifratura scelta. È possibile elencare cifrari o intervalli di cifratura specifici e riordinarli in base alla forza includendo l'opzione **@STRENGTH** nella stringa di cifratura, come mostrato di seguito:

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

Assicurarsi di esaminare tutti i cifrari e gli intervalli disponibili sull'ESA. Per visualizzarli, immettere il comando **sslconfig**, seguito dal sottocomando **verify**. Le opzioni per le categorie di cifratura SSL sono **LOW**, **MEDIUM**, **HIGH** e **ALL**:

```
[]> 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
```

Èinoltre possibile combinare questi elementi per includere intervalli:

```
[]> 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
```

Qualsiasi cifratura SSL che non si desidera configurare e rendere disponibile deve essere rimossa con l'opzione "**-**" che precede la cifratura specifica. Di seguito è riportato un esempio:

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

Le informazioni contenute in questo esempio impediscono l'utilizzo dei cifrari *NULL*, *EDH-RSA-DES-CBC3-SHA*, *EDH-DSS-DES-CBC3-SHA* e *DES-CBC3-SHA* nella comunicazione SSL.

La stessa operazione può essere eseguita anche includendo il simbolo "**!**" carattere davanti al gruppo di cifratura o alla stringa che si desidera rendere non disponibile:

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

Le informazioni contenute in questo esempio impedirebbero l'utilizzo di tutti i cifrari RC4. Di conseguenza, i cifrari *RC4-SHA* e *RC4-MD5* verrebbero negati e non pubblicizzati nella comunicazione SSL.

Se vengono apportate modifiche alla configurazione SSL, accertarsi di eseguire il commit su qualsiasi modifica.