Impedisci negoziazioni per cifrari nulli o anonimi sull'ESA e l'SMA

Sommario

Introduzione

In questo documento viene descritto come modificare le impostazioni della cifratura Cisco Email Security Appliance (ESA) e Cisco Security Management Appliance (SMA) per impedire negoziazioni per cifrari nulli o anonimi. Questo documento si applica sia agli accessori basati su hardware che a quelli basati su virtuali.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco ESA
- Cisco SMA

Componenti usati

Le informazioni di questo documento si basano su tutte le versioni di Cisco ESA e Cisco SMA.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Impedisci negoziazioni per cifrari nulli o anonimi

In questa sezione viene descritto come impedire le negoziazioni per i cifrari nulli o anonimi

sull'ESA Cisco con AsyncOS for Email Security versione 9.1 e successive e anche sull'SMA Cisco.

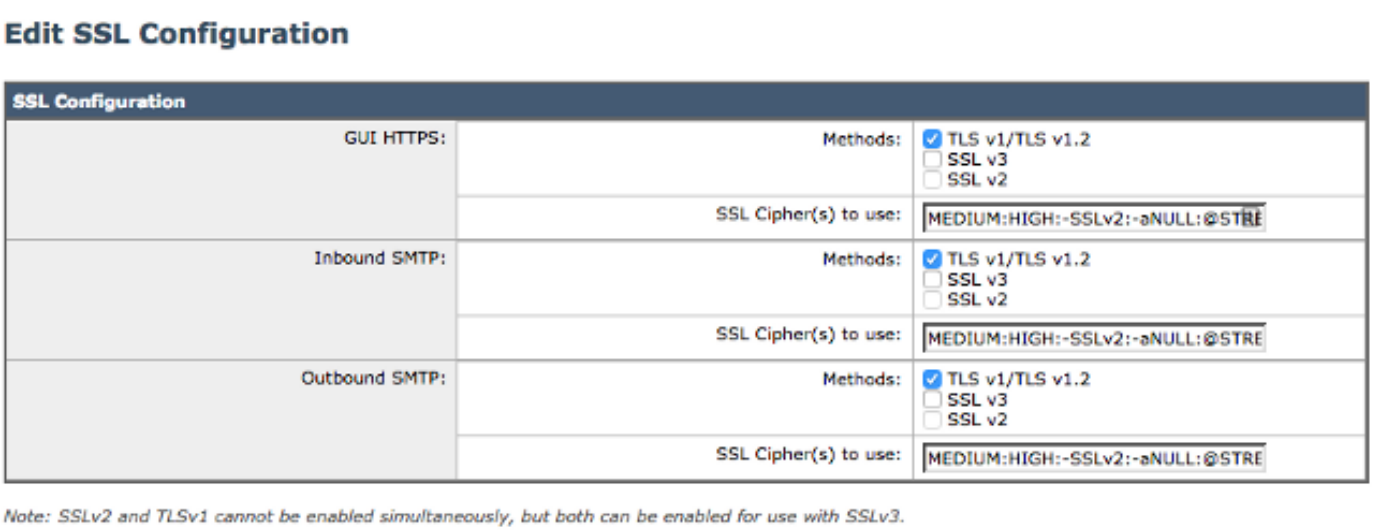
ESA con AsyncOS per Email Security versione 9.5 o successive

Con l'introduzione di AsyncOS for Email Security versione 9.5, è ora supportato TLS v1.2. I comandi descritti nella sezione precedente funzionano ancora; tuttavia, gli aggiornamenti per TLS v1.2 saranno inclusi negli output.

Di seguito è riportato un esempio di output dalla CLI:

```
> sslconfig

sslconfig settings:
GUI HTTPS method: tlsv1/tlsv1.2
GUI HTTPS ciphers:
MEDIUM
HIGH
-SSLv2
-aNULL
@STRENGTH
Inbound SMTP method: tlsv1/tlsv1.2
Inbound SMTP ciphers:
MEDIUM
HIGH
-SSLv2
-aNULL
@STRENGTH
Outbound SMTP method: tlsv1/tlsv1.2
Outbound SMTP ciphers:
MEDIUM
HIGH
-SSLv2
-aNULL
@STRENGTH

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]>
```

Per raggiungere queste impostazioni dalla GUI, selezionare **System Administration > SSL Configuration > Edit Settings...** (Amministrazione sistema > Configurazione SSL > Modifica impostazioni...):



Suggerimento: Per informazioni complete, fare riferimento alla Guida dell'utente finale ESA per la versione 9.5 o successive.

ESA con AsyncOS per Email Security versione 9.1 o precedenti

Per modificare i cifrari usati sull'ESA, usare il comando **sslconfig**. Per impedire le negoziazioni ESA per i cifrari nulli o anonimi, immettere il comando **sslconfig** nella CLI ESA e applicare queste impostazioni:

- Metodo SMTP (Simple Mail Transfer Protocol) in entrata: **sslv3tlsv1**
- Cifre SMTP in ingresso: **MEDIO:ALTO:-SSLv2:-aNULL:@FORZA**
- Metodo SMTP in uscita: **sslv3tlsv1**
- Cifre SMTP in uscita: **MEDIO:ALTO:-SSLv2:-aNULL:@FORZA**

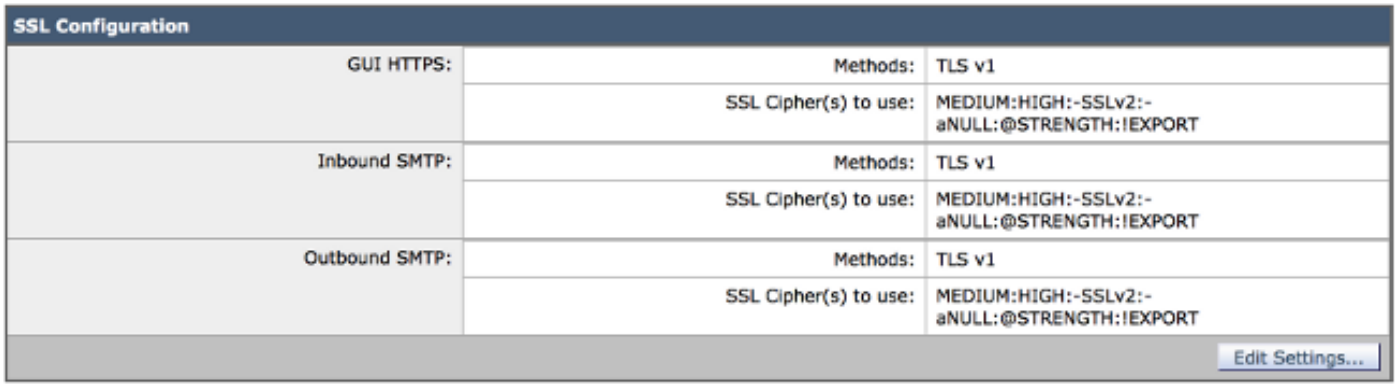
Di seguito è riportato un esempio di configurazione per i cifrari in entrata:

```
CLI: > sslconfig

sslconfig settings:
  GUI HTTPS method:  sslv3tlsv1
  GUI HTTPS ciphers: RC4-SHA:RC4-MD5:ALL
  Inbound SMTP method:  sslv3tlsv1
  Inbound SMTP ciphers: RC4-SHA:RC4-MD5:ALL
  Outbound SMTP method:  sslv3tlsv1
  Outbound SMTP ciphers: RC4-SHA:RC4-MD5:ALL

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
4. SSL v2 and v3
5. SSL v3 and TLS v1
6. SSL v2, v3 and TLS v1
[5]> 3

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

Nota: Impostare **GUI**, **INBOUND** e **OUTBOUND** in base alle esigenze per ciascuna cifratura.

a partire dalla versione 8.5 di AsyncOS for Email Security, il comando **sslconfig** è disponibile anche dalla GUI. Per raggiungere queste impostazioni dalla GUI, selezionare **System Administration > SSL Configurations > Edit Settings** (Amministrazione sistema > Configurazioni SSL > Modifica impostazioni):



Suggerimento: SSL (Secure Sockets Laver) versione 3.0 (RFC-6101) è un protocollo obsoleto e non sicuro. Esiste una vulnerabilità nell'*attacco* SSLv3 CVE-2014-3566 noto come *Padding Oracle On Downgrade Legacy Encryption (POODLE)*, rilevato dall'ID bug Cisco CSCur27131. Cisco consiglia di disabilitare SSLv3 mentre si modificano le cifrature, utilizzare solo Transport Layer Security (TLS) e selezionare l'*opzione 3* (TLS v1). Per ulteriori informazioni, fare riferimento all'ID bug Cisco CSCur27131.

SMA con AsyncOS for Content Security Management 9.6 o versioni successive

Analogamente all'ESA, eseguire il comando **sslconfig** sulla CLI.

SMA con AsyncOS per Content Security Management versione 9.5 o successive

il comando **sslconfig** non è disponibile per le versioni precedenti di SMA.

Nota: Le versioni precedenti di AsyncOS per SMA supportano solo TLS v1. Eseguire l'aggiornamento alla versione 9.6 o successive sull'SMA per una gestione SSL aggiornata.

Per modificare le cifrature SSL, è necessario completare i seguenti passaggi dalla CLI di SMA:

1. Salvare il file di configurazione SMA nel computer locale.
2. Aprire il file XML.

3. Cercare la sezione *<ssl>* nel file XML:

```
<ssl>
   <ssl_inbound_method>sslv3tlsv1</ssl_inbound_method>
   <ssl_inbound_ciphers>RC4-SHA:RC4-MD5:ALL</ssl_inbound_ciphers>
   <ssl_outbound_method>sslv3tlsv1</ssl_outbound_method>
   <ssl_outbound_ciphers>RC4-SHA:RC4-MD5:ALL</ssl_outbound_ciphers>
   <ssl_gui_method>sslv3tlsv1</ssl_gui_method>
   <ssl_gui_ciphers>RC4-SHA:RC4-MD5:ALL</ssl_gui_ciphers>
 </ssl>
```

4. Modificare i cifrari come desiderato e salvare il file XML:

```
<ssl>
<ssl_inbound_method>tlsv1</ssl_inbound_method>
<ssl_inbound_ciphers>MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH</ssl_inbound_ciphers>
<ssl_outbound_method>tlsv1</ssl_outbound_method>
<ssl_outbound_ciphers>MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH</ssl_outbound_ciphers>
<ssl_gui_method>tlsv1</ssl_gui_method>
<ssl_gui_ciphers>MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH</ssl_gui_ciphers>
</ssl>
```

5. Caricare il nuovo file di configurazione nello SMA.

6. **Invia** ed **esegue** il **commit di** tutte le modifiche.

Informazioni correlate

- Cisco ESA - Note release
- Cisco ESA - Guide per l'utente
- Cisco SMA - Note sulla release
- Cisco SMA - Guide per l'utente
- Documentazione e supporto tecnico – Cisco Systems