

ESA および SMA でのヌルまたは匿名の暗号化のネゴシエーションの防止

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[ヌルか匿名暗号のためのネゴシエーションを防いで下さい](#)

[E メール セキュリティ バージョン 9.5 または それ 以降のための AsyncOS を実行する ESA](#)

[E メール セキュリティ バージョン 9.1 のための AsyncOS をまたはより古い実行する ESA](#)

[コンテンツ セキュリティ マネジメント 9.6 のための AsyncOS をまたはより新しい実行する](#)

[SMA](#)

[コンテンツ セキュリティ マネジメント 9.5 またはそれ以降のための AsyncOS を実行する SMA](#)

[関連情報](#)

概要

この資料にヌルか匿名暗号のためのネゴシエーションを防ぐために Cisco E メール セキュリティ アプライアンス (ESA) および Cisco セキュリティ 管理 アプライアンス (SMA) 暗号設定を変える方法を記述されています。この資料はハードウェア基づいたおよびバーチャルによって基づくアプライアンスに適用します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco ESA
- Cisco SMA

使用するコンポーネント

この文書に記載されている情報は Cisco ESA および Cisco SMA のすべてのバージョンに基づいています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

ヌルか匿名暗号のためのネゴシエーションを防いで下さい

このセクションは E メール セキュリティ バージョン 9.1 および それ 以降のための AsyncOS を実行するとまた Cisco SMA のヌルか匿名暗号のためのネゴシエーションを記述します Cisco ESA 防ぐ方法を。

E メール セキュリティ バージョン 9.5 または それ 以降のための AsyncOS を実行する ESA

E メール セキュリティ バージョン 9.5 のための AsyncOS の概要によって、TLS v1.2 は現在サポートされます。前のセクションにまだ説明があるコマンドは動作します;ただし、出力に含まれていた TLS v1.2 については更新が表示されます。

CLI からの出力例はここにあります:

```
> 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]>
```

GUI からこれらの設定に、ナビゲート システム 管理 > SSL 設定 > Edit 設定に達するため...

Edit SSL Configuration

SSL Configuration	
GUI HTTPS:	Methods: <input checked="" type="checkbox"/> TLS v1/TLS v1.2 <input type="checkbox"/> SSL v3 <input type="checkbox"/> SSL v2
	SSL Cipher(s) to use: MEDIUM:HIGH:-SSLv2:-aNULL:@STRE
Inbound SMTP:	Methods: <input checked="" type="checkbox"/> TLS v1/TLS v1.2 <input type="checkbox"/> SSL v3 <input type="checkbox"/> SSL v2
	SSL Cipher(s) to use: MEDIUM:HIGH:-SSLv2:-aNULL:@STRE
Outbound SMTP:	Methods: <input checked="" type="checkbox"/> TLS v1/TLS v1.2 <input type="checkbox"/> SSL v3 <input type="checkbox"/> SSL v2
	SSL Cipher(s) to use: MEDIUM:HIGH:-SSLv2:-aNULL:@STRE

Note: SSLv2 and TLSv1 cannot be enabled simultaneously, but both can be enabled for use with SSLv3.

ヒント：完全情報に関しては、バージョン 9.5 または それ 以降のための適切な ESA [イン
ドユーザ ガイド](#)を参照して下さい。

E メール セキュリティ バージョン 9.1 のための AsyncOS をまたはより古い実行する ESA

sslconfig コマンドで ESA で使用する暗号を修正できます。ヌルか匿名暗号のための ESA ネゴシエーションを防ぐために、sslconfig コマンドを ESA CLI に入力し、これらの設定を加えて下さい：

- 受信 Simple Mail Transfer Protocol (SMTP) 方式: **sslv3tlsv1**
- 受信 SMTP 暗号: **MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH**
- 送信 SMTP 方式: **sslv3tlsv1**
- 送信 SMTP 暗号: **MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH**

受信暗号のための設定例はここにあります：

```
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

注: GUI、および発信を各暗号のために必要に応じて受信 設定 して下さい。

Eメールセキュリティバージョン 8.5 のための AsyncOS 現在で、**sslconfig** コマンドは GUI によってまた利用できます。GUI からこれらの設定に、ナビゲートシステム管理 > SSL コンフィギュレーション > Edit 設定に達するため:

SSL Configuration			
GUI HTTPS:	Methods:	TLS v1	
	SSL Cipher(s) to use:	MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH:!EXPORT	
Inbound SMTP:	Methods:	TLS v1	
	SSL Cipher(s) to use:	MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH:!EXPORT	
Outbound SMTP:	Methods:	TLS v1	
	SSL Cipher(s) to use:	MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH:!EXPORT	

[Edit Settings...](#)

ヒント : ソケットを保護して下さい Layer (SSL) バージョン 3.0 ([RFC-6101](#)) が廃止および不安定なプロトコルである。Cisco バグ ID [CSCur27131](#) によってトラッキングされる *Downgraded* レガシー 暗号化 (プードル) 攻撃の Oracle のパッチングとして知られている SSLv3 [CVE-2014-3566](#) に脆弱性があります。Cisco は暗号を、使用し Transport Layer Security (TLS だけ) を、『Option』を選択する 3 つを変更する間、SSLv3 をディセーブルにすることを推奨します (TLS v1)。完全な詳細については Cisco バグ ID [CSCur27131](#) を参照して下さい。

コンテンツ セキュリティ マネジメント 9.6 のための AsyncOS をまたはより新しい実行する SMA

ESA に類似した、CLI の **sslconfig** コマンドを実行して下さい。

コンテンツ セキュリティ マネジメント 9.5 またはそれ以降のための AsyncOS を実行する SMA

sslconfig コマンドは SMA の古いバージョンに利用できません。

注: SMA のための AsyncOS のより古いバージョンは TLS v1 だけをサポートしました。9.6 にまたは最新 SSL 管理のための SMA でより新しいアップグレードして下さい。

SSL 暗号を修正するために SMA CLI からのこれらのステップを完了して下さい:

1. ローカル コンピュータに SMA コンフィギュレーション ファイルを保存して下さい。

2. XML ファイルを開いて下さい。

3. XML の <ssl/> セクションを捜して下さい:

```
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
```

4. 暗号を望まれるように修正し、XML を保存して下さい:

```
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
```

5. SMA に新しいコンフィギュレーション ファイルをロードして下さい。

6. すべての変更を入れ、保存して下さい。

関連情報

- [Cisco ESA -リリース ノート](#)
- [Cisco ESA -ユーザガイド](#)
- [Cisco SMA -リリース ノート](#)
- [Cisco SMA -ユーザガイド](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)