ESA에서 SSL/TLS와 함께 사용되는 방법 및 암호 변경

목차

소개

이 문서에서는 Cisco ESA(Email Security Appliance)에서 SSL(Secure Socket Layer) 또는 TLS(Transport Layer Security) 컨피그레이션과 함께 사용되는 방법 및 암호를 변경하는 방법에 대해 설명합니다.

SSL/TLS와 함께 사용되는 방법 및 암호 변경

> **참고:**회사의 특정 보안 정책 및 환경 설정에 따라 SSL/TLS 방법 및 암호를 설정해야 합니다. 암호와 관련된 서드파티 정보는 권장 서버 구성 및 자세한 정보를 보려면 보안/서버측 TLS Mozilla 문서를 참조하십시오.

관리자는 Cisco AsyncOS for Email Security를 사용하여 sslconfig 명령을 사용하여 GUI 통신에 사용되고, 인바운드 연결에 광고되고, 아웃바운드 연결에 대해 요청된 방법 및 암호에 대해 SSL 또는 TLS 프로토콜을 구성할 수 있습니다.

```
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.
[]>
```

SSL 컨피그레이션이 변경된 경우 모든 변경 사항을 **커밋해야** 합니다.

SSL 방법

AsyncOS for Email Security 버전 9.6 이상에서 ESA는 기본적으로 *TLS v1/TLS v1.2* 방법을 사용하도록 설정됩니다.이 경우 TLSv1.2는 전송 및 수신 당사자가 모두 사용하는 경우 통신에 대한 선례를 따릅니다.TLS 연결을 설정하려면 양쪽 모두에 일치하는 활성화된 방법이 하나 이상 있어야 하고 일치하는 활성화된 암호가 하나 이상 있어야 합니다.

> **참고:**AsyncOS for Email Security 버전 9.6 이전 버전에서는 기본값에는 두 가지 방법이 있습니다.*SSL v3* 및 *TLS v1*. 일부 관리자는 최근 취약성(SSL v3가 활성화된 경우)으로 인해 SSL v3을 비활성화할 수 있습니다.

SSL 암호

이전 예제에 나열된 기본 암호를 볼 때 두 개의 암호 다음에 *ALL*이라는 단어가 오는 이유를 이해하는 것이 중요합니다.*모두*에 앞에 오는 두 개의 암호가 포함되지만 암호 목록의 암호 순서에 따라 기본 설정이 결정됩니다.따라서 TLS 연결이 설정되면 클라이언트는 목록의 표시 순서에 따라 양쪽이 지원하는 첫 번째 암호를 선택합니다.

> **주**: RC4 암호는 ESA에서 기본적으로 활성화되어 있습니다. 이전 예에서 **MEDIUM:HIGH**는 ESA 및 SMA Cisco 문서에서 Null 또는 익명 암호를 위한 협상 방지를 기반으로 합니다 .RC4에 대한 자세한 내용은 Security/Server Side TLS Mozilla 문서 및 USENIX *Security Symposium 2013*에서 제공하는 TLS 및 WPA 문서의 RC4 보안을 참조하십시오.RC4 암호를 사용하지 않으려면 다음 예를 참조하십시오.

암호 목록을 조작하여 선택한 암호에 영향을 줄 수 있습니다.특정 암호 또는 암호 범위를 나열할 수 있으며, 다음과 같이 암호화 문자열에 **@STRENGTH** 옵션을 포함하여 강도를 기준으로 순서를 변경할 수도 있습니다.

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

ESA에서 사용 가능한 모든 암호와 범위를 검토해야 합니다.이를 보려면 sslconfig 명령을 입력하고 **verify** 하위 명령을 입력합니다.SSL 암호화 카테고리에 대한 옵션은 **LOW**, **MEDIUM**, **HIGH** 및 **ALL입니다**.

```
[]> 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
```

범위를 포함하기 위해 이러한 항목을 결합할 수도 있습니다.

```
[]> 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
```

구성하거나 사용할 수 없도록 하려는 SSL 암호는 특정 암호 앞에는 "**-**" 옵션을 사용하여 제거해야 합니다. 예를 들면 다음과 같습니다.

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

이 예제의 정보는 *NULL*, *EDH-RSA-DES-CBC3-SHA*, *EDH-DSS-DES-CBC3-SHA* 및 *DES-CBC3-SHA*를 광고하지 않고 SSL 통신에서 해당 사용을 금지합니다.

"**!**"을 포함하여 유사한 작업을 수행할 수도 있습니다. 사용할 수 없게 하려는 암호 그룹 또는 문자열 앞에 있는 문자:

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

이 예제의 정보는 모든 RC4 암호를 사용하지 않도록 제거합니다. 따라서 *RC4-SHA* 및 *RC4-MD5 암호는 부정되고* SSL 통신에서 광고되지 않습니다.

SSL 컨피그레이션이 변경된 경우 모든 변경 사항을 **커밋해야** 합니다.