ESA 및 SMA에서 Null 또는 익명 암호에 대한 협상 방지

목차

소개

이 문서에서는 null 또는 익명 암호화에 대한 협상을 방지하기 위해 Cisco ESA(Email Security Appliance) 및 Cisco SMA(Security Management Appliance) 암호 설정을 변경하는 방법에 대해 설명합니다.이 문서는 하드웨어 기반 및 가상 기반 어플라이언스에 모두 적용됩니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco ESA
- Cisco SMA

사용되는 구성 요소

이 문서의 정보는 Cisco ESA 및 Cisco SMA의 모든 버전을 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

Null 또는 익명 암호에 대한 협상 방지

이 섹션에서는 AsyncOS for Email Security 버전 9.1 이상 및 Cisco SMA에서 실행되는 Cisco ESA에서 null 또는 익명 암호화에 대한 협상을 방지하는 방법에 대해 설명합니다.

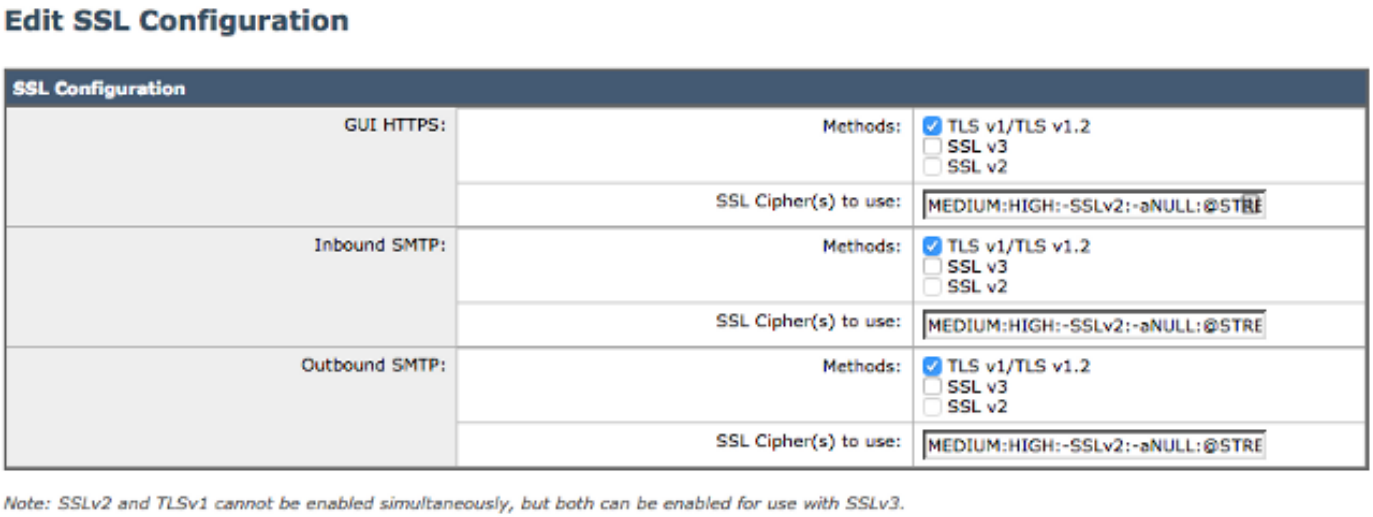
AsyncOS for Email Security 버전 9.5 이상을 실행하는 ESA

AsyncOS for Email Security 버전 9.5가 도입됨에 따라 TLS v1.2가 지원됩니다. 이전 섹션에서 설명한 명령은 여전히 작동합니다.그러나 출력에 포함된 TLS v1.2의 업데이트가 표시됩니다.

다음은 CLI의 출력 예입니다.

```
> 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]>
```

GUI에서 이러한 설정에 액세스하려면 **System Administration(시스템 관리) > SSL Configuration(SSL 컨피그레이션) > Edit Settings(설정 편집)..**:



팁:자세한 내용은 버전 9.5 이상의 해당 ESA 최종 사용자 설명서를 참조하십시오.

AsyncOS for Email Security 버전 9.1 이상을 실행하는 ESA

sslconfig 명령을 사용하여 ESA에서 사용되는 암호를 수정할 수 **있습니다**.null 또는 익명 암호화에 대한 ESA 협상을 방지하려면 ESA CLI에 sslconfig 명령**을** 입력하고 다음 설정을 적용합니다.

- 인바운드 SMTP(Simple Mail Transfer Protocol) 방법:**sslv3tlsv1**
- 인바운드 SMTP 암호:**보통:높음:-SSLv2:-aNULL:@STRENGTH**
- 아웃바운드 SMTP 방법:**sslv3tlsv1**
- 아웃바운드 SMTP 암호:**보통:높음:-SSLv2:-aNULL:@STRENGTH**

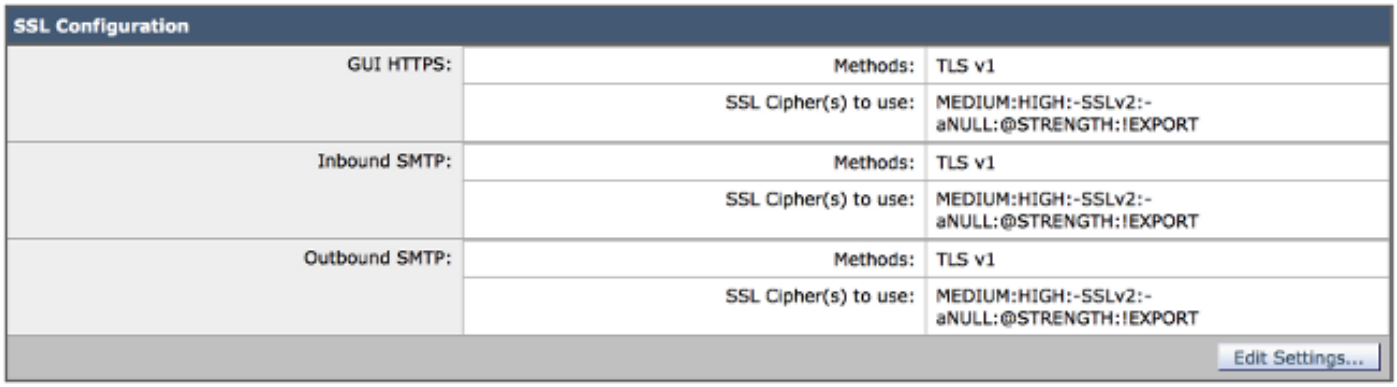
인바운드 암호화에 대한 컨피그레이션의 예는 다음과 같습니다.

```
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
```

참고:각 암호에 필요한 **GUI**, **INBOUND** 및 **OUTBOUND**를 설정합니다.

AsyncOS for Email Security 버전 8.5부터 sslconfig 명령**은** GUI를 통해서도 사용할 수 있습니다 .GUI에서 이러한 설정에 액세스하려면 System Administration(시스템 관리) **> SSL Configurations(SSL 컨피그레이션) > Edit Settings(설정 편집)로** 이동합니다.



팁:SSL(Secure Sockets Repress) 버전 3.0(RFC-6101)은 오래되고 안전하지 않은 프로토콜 입니다.SSLv3 CVE-2014-3566의 취약성이 있습니다. 이는 Cisco 버그 ID CSCur27131에 의해 추적되는 *POODD(Downgraded Legacy Encryption) 공격*으로 알려져 있습니다. 암호를 변경하고 SSL 보안 레이어(Transport Layer)를 사용하는 동안 SSL를 비활성화하는 것이 좋습니다. (만)을 선택하고 *옵션 3*(TLS v1)을 선택합니다. 자세한 내용은 Cisco 버그 ID CSCur27131을 참조하십시오.

Content Security Management 9.6 이상용 AsycnOS를 실행하는 SMA

ESA와 마찬가지로 CLI에서 sslconfig 명령을 실행합니다.

AsyncOS for Content Security Management 9.5 이상을 실행하는 SMA

sslconfig 명령은 이전 버전의 SMA에 사용할 수 없습니다.

참고:이전 버전의 AsyncOS for SMA는 TLS v1만 지원합니다. 최신 SSL 관리를 위해 SMA에서 9.6 이상으로 업그레이드하십시오.

SSL 암호를 수정하려면 SMA CLI에서 다음 단계를 완료해야 합니다.

1. SMA 구성 파일을 로컬 컴퓨터에 저장합니다.
2. XML 파일을 엽니다.
3. XML에서 *<ssl>* 섹션을 검색합니다.

```
<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. 원하는 대로 암호를 수정하고 XML을 저장합니다.

```
<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. SMA에 새 컨피그레이션 파일을 로드합니다.

6. 모든 변경 사항을 **제출하고** 커밋합니다.

관련 정보

- Cisco ESA - 릴리스 정보
- Cisco ESA - 사용 설명서
- Cisco SMA - 릴리스 정보
- Cisco SMA - 사용 설명서
- 기술 지원 및 문서 – Cisco Systems