PFS를 선호하도록 ESA 구성

목차

소개

이 문서에서는 ESA(Email Security Appliance)에서 TLS(Transport Layer Security) 암호화 연결의 PFS(Perfect Forward Secrecy) 환경 설정을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 SSL(Secure Sockets Layer)/TLS에 대해 알고 있는 것이 좋습니다.

사용되는 구성 요소

이 문서의 정보는 AsyncOS for Email 버전 9.6 이상을 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.

배경 정보

ESA는 PFS(Forward Secrecy)를 제공합니다. Forward secrecy는 데이터가 임시 비밀과 대칭 암호화를 사용하는 채널을 통해 전송되며, 호스트 중 하나 또는 둘 모두의 개인 키(장기 키)가 손상된 경우에도 이전에 기록된 세션의 암호를 해독할 수 없음을 의미합니다.

암호는 채널을 통해 전송되지 않고 수학 문제(DH(Diffie Hellman) 문제)로 파생됩니다. 설정된 세션 또는 키 재생성 시간 초과 동안 비밀번호는 호스트 RAM(Random Access Memory)보다 다른 곳에

저장되지 않습니다.

ESA는 키 교환을 위해 DH를 지원합니다.

구성

인바운드 - ESA가 TLS 서버로 작동

이러한 암호 그룹은 ESA에서 Forward Secrecy를 제공하는 SMTP(INBOUND Simple Mail Transfer Protocol) 트래픽에 사용할 수 있습니다.이 예에서 암호 선택은 HIGH 또는 MEDIUM으로 간주되는 암호 그룹만 허용하고 키 교환에 EDH(Ephemeral Diffie Hellman)를 사용하고 TLSv1.2를 선호합니다. 암호 선택 구문은 OpenSSL 구문을 따릅니다.

AsyncOS 9.6 이상에서 Forward Secrecy가 있는 암호:

```
"EDH+TLSv1.2:EDH+HIGH:EDH+MEDIUM:!LOW:!EXP:!aNULL:!RC4:!DSS:!SEED:!IDEA:!MD5:!PSK:!3DES:!SRP"

List:  DHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(256) Mac=AEAD
DHE-RSA-AES256-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(256) Mac=SHA256
DHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(128) Mac=AEAD
DHE-RSA-AES128-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(128) Mac=SHA256
DHE-RSA-AES256-SHA SSLv3 Kx=DH Au=RSA Enc=AES(256) Mac=SHA1
DHE-RSA-CAMELLIA256-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(256) Mac=SHA1
DHE-RSA-AES128-SHA SSLv3 Kx=DH Au=RSA Enc=AES(128) Mac=SHA1
DHE-RSA-CAMELLIA128-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(128) Mac=SHA1
```

Kx (= Key Exchange) 섹션에서는 암호를 파생하기 위해 DH가 사용됨을 보여줍니다.

ESA는 기본 sslconfig 설정(:**ALL**)을 사용하여 이러한 암호를 지원하지만 선호하지는 않습니다 .PFS를 제공하는 암호를 선호하려면 sslconfig를 변경하고 **EDH** 또는 EDH**+<암호 또는 암호 그룹 이름>** 조합을 암호 선택에 추가해야 합니다.

기본 구성:

```
ESA> sslconfig

sslconfig settings:
 Inbound SMTP method:  tlsv1/tlsv1.2
 Inbound SMTP ciphers:
       RC4-SHA
       RC4-MD5
       ALL
```

새 구성:

```
ESA> sslconfig

Inbound SMTP method:  tlsv1/tlsv1.2
 Inbound SMTP ciphers:
       EDH+TLSv1.2
       EDH+HIGH
       EDH+MEDIUM
```

```
RC4-SHA
RC4-MD5
ALL
```

참고:RC4는 MAC의 암호이고 MD5는 약하며, SSL/TLS의 사용을 피하기 위해, 특히 키 재생성 없이 더 높은 데이터 볼륨에 대해서는 RC4를 사용합니다.

인바운드 SSLCONFIG 권장 설정

이것은 일반적인 견해이며 일반적으로 강하고 안전한 것으로 간주되는 암호만을 허용하는 것입니다.

RC4 및 MD5와 기타 레거시 및 취약점 옵션(Export(EXP), Low(LOW), IDEA(IDEA), SEED(SEED), 3DES(3DES) 암호, DSS(Anonymous Key Exchange), PSK(Pre-shared Keys), SRP(SRP) 프로토콜)을 제거하는 INBOUND의 권장 구성), Key Exchange에 대한 ECDH(Elliptic Curve Diffie Hellman)를 비활성화하고 ECDSA(Elliptic Curve Digital Signature Algorithm)가 그 예입니다.

```
EDH+TLSv1.2:EDH+HIGH:EDH+MEDIUM:HIGH:MEDIUM:!ECDH:!ECDSA:!LOW:!EXP:!aNULL:!RC4:!DSS:!SEED:!IDEA:
!MD5:!PSK:!3DES:!SRP
```

sslconfig에 입력한 문자열**은** INBOUND에 대해 지원되는 암호 목록에 표시됩니다.

```
DHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(256) Mac=AEAD
DHE-RSA-AES256-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(256) Mac=SHA256
DHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(128) Mac=AEAD
DHE-RSA-AES128-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(128) Mac=SHA256
DHE-RSA-AES256-SHA SSLv3 Kx=DH Au=RSA Enc=AES(256) Mac=SHA1
DHE-RSA-CAMELLIA256-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(256) Mac=SHA1
DHE-RSA-AES128-SHA SSLv3 Kx=DH Au=RSA Enc=AES(128) Mac=SHA1
DHE-RSA-CAMELLIA128-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(128) Mac=SHA1
AES256-GCM-SHA384 TLSv1.2 Kx=RSA Au=RSA Enc=AESGCM(256) Mac=AEAD
AES256-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AES(256) Mac=SHA256
AES256-SHA SSLv3 Kx=RSA Au=RSA Enc=AES(256) Mac=SHA1
CAMELLIA256-SHA SSLv3 Kx=RSA Au=RSA Enc=Camellia(256) Mac=SHA1
AES128-GCM-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AESGCM(128) Mac=AEAD
AES128-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AES(128) Mac=SHA256
AES128-SHA SSLv3 Kx=RSA Au=RSA Enc=AES(128) Mac=SHA1
CAMELLIA128-SHA SSLv3 Kx=RSA Au=RSA Enc=Camellia(128) Mac=SHA1
```

참고:현재 TLS 서버(인바운드 트래픽)로 작동하는 ESA는 ECDHE(Elliptic Curve Diffie Hellman for Key Exchange) 및 ECDSA 인증서를 지원하지 않습니다.

아웃바운드 - ESA가 TLS 클라이언트로 작동

아웃바운드 SMTP 트래픽의 경우 INBOUND 외에 ESA는 ECDHE 및 ECDSA 인증서를 지원합니다.

참고:ECDSA를 사용하는 ECC(Elliptic Curve Cryptography) 인증서는 널리 채택되지 않습니다.

아웃바운드 이메일이 전달되면 ESA는 TLS 클라이언트입니다. TLS 클라이언트 인증서는 선택 사항입니다.TLS-Server가 ECDSA 클라이언트 인증서를 제공하기 위해 ESA(TLS-클라이언트로)를

강제(필요)하지 않을 경우 ESA는 ECDSA 보안 세션을 계속할 수 있습니다.TLS-Client로 ESA에 인증서를 요청하는 경우 아웃바운드 방향에 대해 구성된 RSA 인증서를 제공합니다.

> **주의:**ESA에 사전 설치된 Trusted CA Certificate Store(시스템 목록)에는 ECC(ECDSA) 루트 인증서가 포함되지 않습니다!ECC 신뢰 체인을 확인할 수 있도록 하려면 신뢰 할 수 있는 ECC 루트 인증서를 사용자 지정 목록에 수동으로 추가해야 할 수도 있습니다.

Forward Secrecy를 제공하는 DHE/ECDHE 암호화를 선호하려면 다음과 같이 sslconfig 암호 선택을 수정할 수 있습니다.

현재 암호 선택 항목에 추가합니다.

```
"EDH+TLSv1.2:ECDH+TLSv1.2:EDH+HIGH:EDH+MEDIUM:ECDH+HIGH:ECDH+MEDIUM"
```

OUTBOUND에 대한 권장 sslconfig 설정

이것은 일반적인 견해이며 일반적으로 강하고 안전한 것으로 간주되는 암호만을 허용하는 것입니다.

```
EDH+TLSv1.2:ECDH+TLSv1.2:EDH+HIGH:EDH+MEDIUM:ECDH+HIGH:ECDH+MEDIUM:HIGH:MEDIUM:!LOW:!EXP:!aNULL:
!RC4:!DSS:!SEED:!IDEA:!MD5:!PSK:!3DES:!SRP
```

sslconfig에 입력한 문자열은 OUTBOUND에 대해 지원되는 암호 목록에 표시됩니다.

```
DHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(256) Mac=AEAD
DHE-RSA-AES256-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(256) Mac=SHA256
DHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(128) Mac=AEAD
DHE-RSA-AES128-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(128) Mac=SHA256
ECDHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH Au=RSA Enc=AESGCM(256) Mac=AEAD
ECDHE-ECDSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AESGCM(256) Mac=AEAD
ECDHE-RSA-AES256-SHA384 TLSv1.2 Kx=ECDH Au=RSA Enc=AES(256) Mac=SHA384
ECDHE-ECDSA-AES256-SHA384 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AES(256) Mac=SHA384
ECDHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH Au=RSA Enc=AESGCM(128) Mac=AEAD
ECDHE-ECDSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AESGCM(128) Mac=AEAD
ECDHE-RSA-AES128-SHA256 TLSv1.2 Kx=ECDH Au=RSA Enc=AES(128) Mac=SHA256
ECDHE-ECDSA-AES128-SHA256 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AES(128) Mac=SHA256
DHE-RSA-AES256-SHA SSLv3 Kx=DH Au=RSA Enc=AES(256) Mac=SHA1
DHE-RSA-CAMELLIA256-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(256) Mac=SHA1
DHE-RSA-AES128-SHA SSLv3 Kx=DH Au=RSA Enc=AES(128) Mac=SHA1
DHE-RSA-CAMELLIA128-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(128) Mac=SHA1
ECDHE-RSA-AES256-SHA SSLv3 Kx=ECDH Au=RSA Enc=AES(256) Mac=SHA1
ECDHE-ECDSA-AES256-SHA SSLv3 Kx=ECDH Au=ECDSA Enc=AES(256) Mac=SHA1
ECDHE-RSA-AES128-SHA SSLv3 Kx=ECDH Au=RSA Enc=AES(128) Mac=SHA1
ECDHE-ECDSA-AES128-SHA SSLv3 Kx=ECDH Au=ECDSA Enc=AES(128) Mac=SHA1
AES256-GCM-SHA384 TLSv1.2 Kx=RSA Au=RSA Enc=AESGCM(256) Mac=AEAD
AES256-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AES(256) Mac=SHA256
AES256-SHA SSLv3 Kx=RSA Au=RSA Enc=AES(256) Mac=SHA1
CAMELLIA256-SHA SSLv3 Kx=RSA Au=RSA Enc=Camellia(256) Mac=SHA1
AES128-GCM-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AESGCM(128) Mac=AEAD
AES128-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AES(128) Mac=SHA256
AES128-SHA SSLv3 Kx=RSA Au=RSA Enc=AES(128) Mac=SHA1
CAMELLIA128-SHA SSLv3 Kx=RSA Au=RSA Enc=Camellia(128) Mac=SHA1
```

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- SSL 암호 열기
- Cisco 차세대 암호화
- 기술 지원 및 문서 – Cisco Systems