Konfigurieren der ESA zum Bevorzugen von PFS

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie die Präferenz für Perfect Forward Secrecy (PFS) in TLS-verschlüsselten Verbindungen (Transport Layer Security) auf der E-Mail Security Appliance (ESA) konfigurieren.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in Bezug auf SSL (Secure Sockets Layer)/TLS zu verfügen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf AsyncOS für E-Mail Version 9.6 und höher.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Die ESA bietet Forward Secrecy (PFS) an. Weiterleitungsgeheimnis bedeutet, dass die Daten über einen Kanal übertragen werden, der symmetrische Verschlüsselung mit flüchtigen

Geheimnissen verwendet. Selbst wenn der private Schlüssel (Langzeitschlüssel) auf einem oder beiden Hosts kompromittiert wurde, ist es nicht möglich, eine zuvor aufgezeichnete Sitzung zu entschlüsseln.

Das Geheimnis wird nicht über den Kanal übertragen, sondern das gemeinsam verwendete Geheimnis wird mit einem mathematischen Problem (Diffie Hellman (DH) Problem) *abgeleitet.* Der geheime Speicher wird während der festgelegten Sitzung oder während der Zeitüberschreitung bei der Schlüsselwiederherstellung nirgendwo anders als der Arbeitsspeicher des Hosts mit wahlfreiem Zugriff (Random Access Memory, RAM) gespeichert.

Die ESA unterstützt DH für Key Exchange.

Konfigurieren

EINGEHEND - ESA fungiert als TLS-Server.

Diese Verschlüsselungssuiten sind auf der ESA für INBOUND Simple Mail Transfer Protocol (SMTP)-Datenverkehr verfügbar, der Weiterleitungsgeheimnisse bietet. In diesem Beispiel lässt die Verschlüsselungsauswahl nur Verschlüsselungssuiten zu, die als HIGH oder MEDIUM gelten, und verwendet Ephemeral Diffie Hellman (EDH) für Key Exchange und bevorzugt TLSv1.2. Die Verschlüsselungsauswahlsyntax folgt der OpenSSL-Syntax.

Ciphers mit Forward Secrecy auf AsyncOS 9.6+:

```
"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
```

Der Abschnitt Kx (= Key Exchange) zeigt, dass DH verwendet wird, um den geheimen Schlüssel abzuleiten.

Die ESA unterstützt diese Chiffren mit den Standard-**SSL**-Konfigurationseinstellungen (:ALL), zieht sie jedoch nicht vor. Wenn Sie Chiffren bevorzugen möchten, die PFS anbieten, müssen Sie Ihre **sslconfig** ändern und EDH oder eine Kombination **von EDH+<cipher oder cipher group name>** Ihrer Chiffrierauswahl hinzufügen.

Standardkonfiguration:

```
ESA> sslconfig

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

```
       ALL
```

Neue Konfiguration:

```
ESA> sslconfig

Inbound SMTP method:  tlsv1/tlsv1.2
 Inbound SMTP ciphers:
       EDH+TLSv1.2
       EDH+HIGH
       EDH+MEDIUM
       RC4-SHA
       RC4-MD5
       ALL
```

Hinweis: RC4 als Verschlüsselung und MD5 als MAC wird als schwach, veraltet und um die Verwendung mit SSL/TLS zu vermeiden, besonders wenn es um ein höheres Datenvolumen ohne wichtige Regeneration geht.

Empfohlene SSL-Konfigurationseinstellungen für INBOUND

Dies ist eine vorherrschende Meinung und nur, um Chiffren zuzulassen, die allgemein als stark und sicher gelten.

Eine empfehlenswerte Konfiguration für INBOUND, die RC4 und MD5 sowie weitere ältere und schwache Optionen entfernt, nämlich Export (EXP), Niedrig (LOW), IDEA (IDEA), SEED (SEED), 3DES (3DES)-Verschlüsselung, DSS-Zertifikate (DSS), Anonymous Key Exchange (aNULL), Pre-Shared Keys (PSK), SRP-Protokoll (SRP) deaktiviert Elliptic Curve Diffie Hellman (ECDH) für Key Exchange und Elliptic Curve Digital Signature Algorithm (ECDSA) sind die folgenden Beispiele:

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

Die in **sslconfig** eingegebene Zeichenfolge führt zu dieser Liste unterstützter Chiffren für INBOUND:

```
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
```

Hinweis: Die ESA, die als TLS-Server (INBOUND-Datenverkehr) fungiert, unterstützt derzeit

keine Elliptic Curve Diffie Hellman for Key Exchange (ECDHE)- und ECDSA-Zertifikate.

AUSGEHEND - ESA fungiert als TLS-Client

Für den OUTBOUND-SMTP-Verkehr unterstützt die ESA zusätzlich zum INBOUND ECDHE- und ECDSA-Zertifikate.

> **Hinweis**: Elliptic Curve Cryptography (ECC)-Zertifikate mit der ECDSA werden nicht häufig verwendet.

Wenn eine OUTBOUND-E-Mail zugestellt wird, ist die ESA der TLS-Client. Ein TLS-Client-Zertifikat ist optional. Wenn der TLS-Server die ESA (als TLS-Client) nicht erzwingt (erfordert), um ein ECDSA-Client-Zertifikat bereitzustellen, kann die ESA mit einer ECDSA-gesicherten Sitzung fortfahren. Wenn die ESA als TLS-Client nach dem Zertifikat gefragt wird, stellt sie das konfigurierte RSA-Zertifikat für die OUTBOUND-Richtung bereit.

> **Vorsicht**: Der vorinstallierte Trusted CA Certificate Store (Systemliste) auf der ESA enthält keine ECC (ECDSA)-Root-Zertifikate! Möglicherweise müssen Sie der Benutzerdefinierten Liste ECC-Stammzertifikate manuell hinzufügen (denen Sie vertrauen), um die ECC-Vertrauenskette verifizierbar zu machen.

Um DHE/ECDHE-Verschlüsselungen vorzuziehen, die die Rufumleitung bieten, können Sie die Auswahl der **SSLconfig-**Verschlüsselung wie folgt ändern.

Fügen Sie diese der aktuellen Verschlüsselungsauswahl hinzu.

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

Empfohlene SSL-Konfigurationseinstellungen für OUTBOUND

Dies ist eine vorherrschende Meinung und nur, um Chiffren zuzulassen, die allgemein als stark und sicher gelten.

```
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
```

Die in **sslconfig** eingegebene Zeichenfolge führt zu dieser Liste unterstützter Chiffren für OUTBOUND:

```
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
```

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- Open SSL-Chiffren
- Cisco Verschlüsselungstechnologie der nächsten Generation
- Technischer Support und Dokumentation - Cisco Systems