Configurazione di ESA per preferire PFS

Sommario

Introduzione

In questo documento viene descritto come configurare la preferenza per PFS (Perfect Forward Secrecy) nelle connessioni crittografate TLS (Transport Layer Security) su ESA (Email Security Appliance).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di SSL (Secure Sockets Layer)/TLS.

Componenti usati

Le informazioni di questo documento si basano su AsyncOS for Email versione 9.6 e successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

L'ESA offre il Forward Secrecy (PFS). Il segreto di inoltro significa che i dati vengono trasferiti tramite un canale che utilizza la crittografia simmetrica con segreti effimeri e, anche se la chiave privata (chiave a lungo termine) su uno o entrambi gli host è stata compromessa, non è possibile decrittografare una sessione registrata in precedenza.

Il segreto non viene trasferito tramite il canale, ma viene derivato da un problema matematico (problema di Diffie Hellman (DH). Il segreto non viene memorizzato in un punto diverso dalla RAM (Random Access Memory) dell'host durante la sessione stabilita o il timeout di rigenerazione della chiave.

L'ESA supporta DH per lo scambio di chiavi.

Configurazione

IN ENTRATA - ESA agisce come server TLS

Queste suite di cifratura sono disponibili sull'ESA per il traffico SMTP (Simple Mail Transfer Protocol) in entrata che fornisce il segreto di inoltro. In questo esempio, la selezione cifratura consente solo le suite di cifratura considerate HIGH o MEDIUM e l'utilizzo di Ephemeral Diffie Hellman (EDH) per Key Exchange e preferisce TLSv1.2. La sintassi di selezione cifratura segue la sintassi OpenSSL.

Crittografi con inoltro segreto su 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
```

La sezione Kx (= Scambio chiave) mostra che per derivare il segreto viene utilizzato DH.

L'ESA supporta questi cifrari con le impostazioni **sslconfig** predefinite (:ALL), ma non li preferisce. Se si preferiscono i cifrari che offrono PFS, *è* necessario modificare **sslconfig** e aggiungere EDH o una combinazione di **EDH+<nome del gruppo di cifratura>** alla selezione del cifrario.

Configurazione predefinita:

```
ESA> sslconfig

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

Nuova configurazione:

```
ESA> sslconfig
```

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

Nota: RC4 come cifratura e MD5 come MAC sono considerati deboli, legacy e al fine di evitare l'uso con SSL/TLS, soprattutto quando si tratta di un volume di dati maggiore senza rigenerazione della chiave.

Impostazioni sslconfig consigliate per INBOUND

Questa è un'opinione prevalente e permette solo cifrari generalmente considerati forti e sicuri.

Una configurazione consigliata per INBOUND che rimuove RC4 e MD5 oltre ad altre opzioni legacy e deboli, ovvero Export (EXP), Low (LOW), IDEA (IDEA), SEED (SEED), cifrari 3DES (3DES), certificati DSS (DSS), anonymous Key Exchange (aNULL), pre-shared Keys (PSK), SRP (SRP), disattiva Elliptic Curve Diffie Hellman (ECDH) per Key Exchange e Elliptic Curve Digital Signature Algorithm (ECDSA) sono gli esempi:

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

La stringa immessa in **sslconfig** restituisce il seguente elenco di cifrature supportate per 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
```

Nota: L'ESA che opera come server TLS (traffico IN ENTRATA) non supporta attualmente i certificati ECDHE (Elliptic Curve Diffie Hellman for Key Exchange) e ECDSA.

IN USCITA - ESA agisce come client TLS

Per il traffico SMTP in uscita, l'ESA oltre a INBOUND supporta i certificati ECDHE e ECDSA.

Nota: I certificati ECC (Elliptic Curve Cryptography) con l'ECDSA non sono molto diffusi.

Quando viene recapitato un messaggio e-mail in uscita, l'ESA è il client TLS. Un certificato client TLS è facoltativo. Se il server TLS non impone (richiede) all'ESA (come client TLS) di fornire un certificato client ECDSA, l'ESA può continuare con una sessione protetta ECDSA. Quando all'ESA come client TLS viene richiesto il suo certificato, fornisce il certificato RSA configurato per la direzione IN USCITA.

> **Attenzione:** L'archivio certificati CA attendibili (elenco sistemi) preinstallato nell'ESA non include i certificati radice ECC (ECDSA). Per rendere verificabile la catena di attendibilità ECC, potrebbe essere necessario aggiungere manualmente all'elenco personalizzato i certificati radice ECC ritenuti attendibili.

Per preferire i cifrari DHE/ECDHE che offrono il formato Forward Secrecy, è possibile modificare la selezione del cifrario **sslconfig** come indicato di seguito.

Aggiunge questo elemento alla selezione di cifratura corrente.

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

Impostazioni sslconfig consigliate per OUTBOUND

Questa è un'opinione prevalente e permette solo cifrari generalmente considerati forti e sicuri.

```
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
```

La stringa immessa in **sslconfig** restituisce il seguente elenco di cifrature supportate per 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
```

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- Apri cifrari SSL
- Cisco Next-Generation Encryption
- Documentazione e supporto tecnico – Cisco Systems