

Algoritmos de encriptación fuerte del permiso CS para la comunicación SSL

Contenido

[Problema](#)

[Solución](#)

Problema

Por abandono, el Cisco Security Manager (CS) presenta las cifras siguientes para la comunicación HTTPS:

```
%ASA-7-725011: Cipher[1] : AES128-SHA
%ASA-7-725011: Cipher[2] : DHE-RSA-AES128-SHA
%ASA-7-725011: Cipher[3] : DHE-DSS-AES128-SHA
%ASA-7-725011: Cipher[4] : DES-CBC3-SHA
%ASA-7-725011: Cipher[5] : EDH-RSA-DES-CBC3-SHA
%ASA-7-725011: Cipher[6] : EDH-DSS-DES-CBC3-SHA
%ASA-7-725011: Cipher[7] : DES-CBC-SHA
%ASA-7-725011: Cipher[8] : EDH-RSA-DES-CBC-SHA
%ASA-7-725011: Cipher[9] : EDH-DSS-DES-CBC-SHA
%ASA-7-725011: Cipher[10] : EXP-DES-CBC-SHA
%ASA-7-725011: Cipher[11] : EXP-EDH-RSA-DES-CBC-SHA
%ASA-7-725011: Cipher[12] : EXP-EDH-DSS-DES-CBC-SHA
%ASA-7-725011: Cipher[13] : ECDHE-ECDSA-AES128-SHA256
%ASA-7-725011: Cipher[14] : ECDHE-RSA-AES128-SHA256
%ASA-7-725011: Cipher[15] : AES128-SHA256
%ASA-7-725011: Cipher[16] : DHE-RSA-AES128-SHA256
%ASA-7-725011: Cipher[17] : DHE-DSS-AES128-SHA256
%ASA-7-725011: Cipher[18] : ECDHE-ECDSA-AES128-SHA
%ASA-7-725011: Cipher[19] : ECDHE-RSA-AES128-SHA
%ASA-7-725011: Cipher[20] : AES128-SHA
%ASA-7-725011: Cipher[21] : DHE-RSA-AES128-SHA
%ASA-7-725011: Cipher[22] : DHE-DSS-AES128-SHA
%ASA-7-725011: Cipher[23] : ECDHE-ECDSA-DES-CBC3-SHA
%ASA-7-725011: Cipher[24] : ECDHE-RSA-DES-CBC3-SHA
%ASA-7-725011: Cipher[25] : DES-CBC3-SHA
%ASA-7-725011: Cipher[26] : EDH-RSA-DES-CBC3-SHA
%ASA-7-725011: Cipher[27] : EDH-DSS-DES-CBC3-SHA
%ASA-7-725011: Cipher[28] : ADH-AES128-SHA256
%ASA-7-725011: Cipher[29] : ADH-AES128-SHA
%ASA-7-725011: Cipher[30] : ADH-DES-CBC3-SHA
%ASA-7-725011: Cipher[31] : DES-CBC-SHA
%ASA-7-725011: Cipher[32] : EDH-RSA-DES-CBC-SHA
%ASA-7-725011: Cipher[33] : EDH-DSS-DES-CBC-SHA
%ASA-7-725011: Cipher[34] : ADH-DES-CBC-SHA
%ASA-7-725011: Cipher[35] : EXP-DES-CBC-SHA
%ASA-7-725011: Cipher[36] : EXP-EDH-RSA-DES-CBC-SHA
%ASA-7-725011: Cipher[37] : EXP-EDH-DSS-DES-CBC-SHA
%ASA-7-725011: Cipher[38] : EXP-ADH-DES-CBC-SHA
%ASA-7-725011: Cipher[39] : NULL-SHA256
%ASA-7-725011: Cipher[40] : ECDHE-ECDSA-NULL-SHA
%ASA-7-725011: Cipher[41] : ECDHE-RSA-NULL-SHA
%ASA-7-725011: Cipher[42] : NULL-SHA
```

```
%ASA-7-725011: Cipher[43] : NULL-MD5
```

Sin embargo si configuramos el ASA para soportar solamente un algoritmo fuerte del encryptuon (como AES256-SHA):

La comunicación fallará y veremos el SYSLOG siguiente en el ASA:

```
%ASA-7-725014: SSL lib error. Function: ssl3_get_client_hello Reason: no shared cipher
```

Y el inicio siguiente el CS:

```
"Unable to communicate with the Device"
```

```
The Security Manager Server and the device could not negotiate the security level"
```

Solución

Debido importar las regulaciones en algunos países la implementación del Oracle proporciona un archivo de políticas criptográfico predeterminado de la jurisdicción que limite la fuerza de los algoritmos criptográficos. Si algoritmos más fuertes necesitan ser configurados o se configuran ya en el dispositivo (por ejemplo, AES con las claves del 256-bit, el grupo DH con 5,14,24), siga los siguientes pasos:

1. Descargue las Javas 7 archivos ilimitados de la criptografía policy.jar de la fuerza de <http://www.oracle.com>. [Cisco](#) recomienda buscar para el siguiente en el sitio web del Oracle: Javas ilimitadas 7 de los archivos de políticas de la jurisdicción de la fuerza de la extensión de la criptografía de las Javas (JCE)

<http://www.oracle.com/technetwork/java/javase/downloads/jce-7-download-432124.html>

2. Reemplace local_policy.jar y US_export_policy.jar en su servidor del administrador de seguridad en el CSCOPx \ MDC \ vms \ jre \ liberación \ Seguridad de la carpeta.
3. Recomience su servidor del administrador de seguridad.

Ahora el CS presentará las cifras siguientes:

```
%ASA-7-725011: Cipher[1] : AES128-SHA
%ASA-7-725011: Cipher[2] : DHE-RSA-AES128-SHA
%ASA-7-725011: Cipher[3] : DHE-DSS-AES128-SHA
%ASA-7-725011: Cipher[4] : DES-CBC3-SHA
%ASA-7-725011: Cipher[5] : EDH-RSA-DES-CBC3-SHA
%ASA-7-725011: Cipher[6] : EDH-DSS-DES-CBC3-SHA
%ASA-7-725011: Cipher[7] : DES-CBC-SHA
%ASA-7-725011: Cipher[8] : EDH-RSA-DES-CBC-SHA
%ASA-7-725011: Cipher[9] : EDH-DSS-DES-CBC-SHA
%ASA-7-725011: Cipher[10] : EXP-DES-CBC-SHA
%ASA-7-725011: Cipher[11] : EXP-EDH-RSA-DES-CBC-SHA
%ASA-7-725011: Cipher[12] : EXP-EDH-DSS-DES-CBC-SHA
%ASA-7-725011: Cipher[13] : ECDHE-ECDSA-AES256-SHA384
%ASA-7-725011: Cipher[14] : ECDHE-RSA-AES256-SHA384
%ASA-7-725011: Cipher[15] : AES256-SHA256
%ASA-7-725011: Cipher[16] : DHE-RSA-AES256-SHA256
%ASA-7-725011: Cipher[17] : DHE-DSS-AES256-SHA256
%ASA-7-725011: Cipher[18] : ECDHE-ECDSA-AES256-SHA
```

%ASA-7-725011: Cipher[19] : ECDHE-RSA-AES256-SHA
%ASA-7-725011: Cipher[20] : AES256-SHA
%ASA-7-725011: Cipher[21] : DHE-RSA-AES256-SHA
%ASA-7-725011: Cipher[22] : DHE-DSS-AES256-SHA
%ASA-7-725011: Cipher[23] : ECDHE-ECDSA-AES128-SHA256
%ASA-7-725011: Cipher[24] : ECDHE-RSA-AES128-SHA256
%ASA-7-725011: Cipher[25] : AES128-SHA256
%ASA-7-725011: Cipher[26] : DHE-RSA-AES128-SHA256
%ASA-7-725011: Cipher[27] : DHE-DSS-AES128-SHA256
%ASA-7-725011: Cipher[28] : ECDHE-ECDSA-AES128-SHA
%ASA-7-725011: Cipher[29] : ECDHE-RSA-AES128-SHA
%ASA-7-725011: Cipher[30] : AES128-SHA
%ASA-7-725011: Cipher[31] : DHE-RSA-AES128-SHA
%ASA-7-725011: Cipher[32] : DHE-DSS-AES128-SHA
%ASA-7-725011: Cipher[33] : ECDHE-ECDSA-DES-CBC3-SHA
%ASA-7-725011: Cipher[34] : ECDHE-RSA-DES-CBC3-SHA
%ASA-7-725011: Cipher[35] : DES-CBC3-SHA
%ASA-7-725011: Cipher[36] : EDH-RSA-DES-CBC3-SHA
%ASA-7-725011: Cipher[37] : EDH-DSS-DES-CBC3-SHA
%ASA-7-725011: Cipher[38] : ADH-AES256-SHA256
%ASA-7-725011: Cipher[39] : ADH-AES256-SHA
%ASA-7-725011: Cipher[40] : ADH-AES128-SHA256
%ASA-7-725011: Cipher[41] : ADH-AES128-SHA
%ASA-7-725011: Cipher[42] : ADH-DES-CBC3-SHA
%ASA-7-725011: Cipher[43] : DES-CBC-SHA
%ASA-7-725011: Cipher[44] : EDH-RSA-DES-CBC-SHA
%ASA-7-725011: Cipher[45] : EDH-DSS-DES-CBC-SHA
%ASA-7-725011: Cipher[46] : ADH-DES-CBC-SHA
%ASA-7-725011: Cipher[47] : EXP-DES-CBC-SHA
%ASA-7-725011: Cipher[48] : EXP-EDH-RSA-DES-CBC-SHA
%ASA-7-725011: Cipher[49] : EXP-EDH-DSS-DES-CBC-SHA
%ASA-7-725011: Cipher[50] : EXP-ADH-DES-CBC-SHA
%ASA-7-725011: Cipher[51] : NULL-SHA256
%ASA-7-725011: Cipher[52] : ECDHE-ECDSA-NULL-SHA
%ASA-7-725011: Cipher[53] : ECDHE-RSA-NULL-SHA
%ASA-7-725011: Cipher[54] : NULL-SHA
%ASA-7-725011: Cipher[55] : NULL-MD5

Y la conexión será acertada ahora:

%ASA-7-725012: Device chooses cipher AES256-SHA for the SSL session with client
asa:10.88.243.57/49949 to 10.122.160.233/443