Solucionar error de CommPilot "SSL_ERROR_NO_CIPHER_OVERLAP"

Contenido

Introducción

Este documento describe cómo configurar y resolver problemas de BroadWorks para evitar el error "SSL_ERROR_NO_CIPHER_OVERLAP".

Prerequisites

Requirements

Cisco recomienda que conozca la plataforma BroadWorks.

Antecedentes

Configuración de BroadWorks

Para las versiones 22 y posteriores de Broadworks, los protocolos y los cifrados se pueden configurar a través de la CLI a través de los contextos vistos en diferentes niveles de configuración.

```
'Interface/Port specific - low level'
CLI/Interface/Http/HttpServer/SSLSettings/Protocols
```

```
CLI/Interface/Http/HttpServer/SSLSettings/Ciphers

'All interfaces - mid level'
CLI/Interface/Http/SSLCommonSettings/Protocols
CLI/Interface/Http/SSLCommonSettings/Ciphers

'Generic system level - high level'
CLI/System/SSLCommonSettings/JSSE/Protocols
CLI/System/SSLCommonSettings/JSSE/Ciphers
```

Un contexto denominado SSLCommonSettings hace referencia a un elemento menos específico de la jerarquía SSL y un contexto denominado SSLSettings hace referencia a un elemento más específico de la jerarquía.

Ejemplo de laboratorio funcional

Configuración

Configuración de bajo nivel vinculada a la interfaz y al puerto específicos sin cifrado definido:

```
CLI/Interface/Http/HttpServer/SSLSettings/Protocols> get 172.16.30.146 443
Protocol Name
===============
TLSv1.1
TLSv1.2
TLSv1

CLI/Interface/Http/HttpServer/SSLSettings/Ciphers> get 172.16.30.146 443
Cipher Name
=============

0 entry found.
```

Verificación

Verifique la configuración con el curl comando:

```
$ curl -v -k https://172.16.30.146
* About to connect() to 172.16.30.146 port 443 (#0)
* Trying 172.16.30.146...
* Connected to 172.16.30.146 (172.16.30.146) port 443 (#0)
* Initializing NSS with certpath: sql:/etc/pki/nssdb
* skipping SSL peer certificate verification
* SSL connection using TLS_RSA_WITH_AES_256_CBC_SHA256 <-----
* Server certificate:
* subject:
E=broadworks_tac@cisco.com,CN=*.calo.cisco.com,OU=BroadworksTAC,O=TestIssuer,ST=Veracruz,C=MX
* start date: Apr 04 20:39:56 2022 GMT
* expire date: Apr 04 20:39:56 2023 GMT
* common name: *.calo.cisco.com
* issuer: CN=Root CA test,OU=BroadworksTAC,O=TestIssuer,L=Tecolutla,ST=Veracruz,C=MX
>GET / HTTP/1.1
>User-Agent: curl/7.29.0
>Host: 172.16.30.146
>Accept: */*
>
<HTTP/1.1 302 Found
```

Aquí se ha conectado correctamente mediante TLSv1.2 con el cifrado

TLS_RSA_WITH_AES_256_CBC_SHA256.

Auditoría de conectividad

Para comprobar los protocolos y cifrados que se aceptan:

```
$ nmap -sV --script ssl-enum-ciphers -p 443 172.16.30.146

Starting Nmap 6.40 ( http://nmap.org ) at 2022-05-09 04:26 EDT
Nmap scan report for r23xsp01.calo.cisco.com (172.16.30.146)
Host is up (0.00013s latency).
PORT STATE SERVICE VERSION
443/tcp open ssl/https?
| ssl-enum-ciphers:
| TLSv1.0:
| ciphers:
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA - strong
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA - strong
| TLS_ECDHE_RSA_WITH_RC4_128_SHA - strong
| TLS_RSA_WITH_AES_128_CBC_SHA - strong
| TLS_RSA_WITH_AES_256_CBC_SHA - strong
| TLS_RSA_WITH_RC4_128_SHA - strong
| compressors:
| NULL
| TLSv1.1:
| ciphers:
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA - strong
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA - strong
| TLS_ECDHE_RSA_WITH_RC4_128_SHA - strong
| TLS_RSA_WITH_AES_128_CBC_SHA - strong
| TLS_RSA_WITH_AES_256_CBC_SHA - strong
| TLS_RSA_WITH_RC4_128_SHA - strong
| compressors:
| NULL
| TLSv1.2:
| ciphers:
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA - strong
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 - strong
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA - strong
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 - strong
| TLS_ECDHE_RSA_WITH_RC4_128_SHA - strong
| TLS_RSA_WITH_AES_128_CBC_SHA - strong
| TLS_RSA_WITH_AES_128_CBC_SHA256 - strong
| TLS_RSA_WITH_AES_256_CBC_SHA - strong
| TLS_RSA_WITH_AES_256_CBC_SHA256 - strong
| TLS_RSA_WITH_RC4_128_SHA - strong
| compressors:
| NULL
|_ least strength: strong
```

Ejemplo De Laboratorio Con Error

Problema

Error observado: "SSL_ERROR_NO_CIPHER_OVERLAP" a través del navegador.

```
# curl -v https://172.16.30.146
* About to connect() to 172.16.30.146 port 443 (#0)
```

```
* Trying 172.16.30.146...
* Connected to 172.16.30.146 (172.16.30.146) port 443 (#0)
* Initializing NSS with certpath: sql:/etc/pki/nssdb * CAfile: /etc/pki/tls/certs/ca-bundle.crt
CApath: none
* NSS error -12286 (SSL_ERROR_NO_CYPHER_OVERLAP)
* Cannot communicate securely with peer: no common encryption algorithm(s).
* Closing connection 0 curl: (35) Cannot communicate securely with peer: no common encryption
algorithm(s).
```

Configuración

Configuración de bajo nivel vinculada a la interfaz y el puerto específicos con el protocolo TLSv1.2 establecido con el cifrado TLSv1.0 TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 establecido:

```
CLI/Interface/Http/HttpServer/SSLSettings/Protocols> get 172.16.30.146 443
Protocol Name
===============
TLSv1.2

CLI/Interface/Http/SSLCommonSettings/Ciphers> get
Cipher Name
====================================
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
```

Verificación

Verifique la configuración con el curl comando:

```
$ curl -v -k https://172.16.30.146
* About to connect() to 172.16.30.146 port 443 (#0)
* Trying 172.16.30.146...
* Connected to 172.16.30.146 (172.16.30.146) port 443 (#0)
* Initializing NSS with certpath: sql:/etc/pki/nssdb
* NSS error -12286 (SSL_ERROR_NO_CYPHER_OVERLAP)
* Cannot communicate securely with peer: no common encryption algorithm(s).
* Closing connection 0
curl: (35) Cannot communicate securely with peer: no common encryption algorithm(s).
```

Auditoría de conectividad

Para comprobar los protocolos y cifrados que se aceptan:

```
$ nmap -sV --script ssl-enum-ciphers -p 443 172.16.30.146

Starting Nmap 6.40 ( http://nmap.org ) at 2022-05-09 05:31 EDT
Nmap scan report for r23xsp01.calo.cisco.com (172.16.30.146)
Host is up (0.000049s latency).
PORT STATE SERVICE VERSION
443/tcp open https?
| ssl-enum-ciphers:
|_ TLSv1.2: No supported ciphers found
```

De los resultados de la herramienta se observa que el protocolo TLSv1.2 está disponible pero no hay cifrados soportados.

Resolución

Elimine el cifrado de TLSv1.1 en **CLI/Interface/Http/SSLCommonSettings/Ciphers** y, a continuación, vuelva a abrir todos los cifrados de TLSv1.2 (o agregue un cifrado de TLSv1.2).

```
CLI/Interface/Http/HttpServer/SSLSettings/Protocols> get 172.16.30.146 443
Protocol Name
===============
TLSv1.2

CLI/Interface/Http/HttpServer/SSLSettings/Ciphers> get 172.16.30.146 443
Cipher Name
=============
0 entry found.

CLI/Interface/Http/SSLCommonSettings/Ciphers> get
Cipher Name
=============
0 entry found.
```

Verificación de resolución

```
$ curl -v -k https://172.16.30.146
* About to connect() to 172.16.30.146 port 443 (#0)
* Trying 172.16.30.146...
* Connected to 172.16.30.146 (172.16.30.146) port 443 (#0)
* Initializing NSS with certpath: sql:/etc/pki/nssdb
* skipping SSL peer certificate verification
* SSL connection using TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 <-----
* Server certificate:
* subject:
E=broadworks_tac@cisco.com,CN=*.calo.cisco.com,OU=BroadworksTAC,O=TestIssuer,ST=Veracruz,C=MX
* start date: Apr 04 20:39:56 2022 GMT
* expire date: Apr 04 20:39:56 2023 GMT
* common name: *.calo.cisco.com
* issuer: CN=Root CA test,OU=BroadworksTAC,O=TestIssuer,L=Tecolutla,ST=Veracruz,C=MX
>GET / HTTP/1.1
>User-Agent: curl/7.29.0
>Host: 172.16.30.146
>Accept: */*
>
<HTTP/1.1 302 Found

$ nmap -sV --script ssl-enum-ciphers -p 443 172.16.30.146

Starting Nmap 6.40 ( http://nmap.org ) at 2022-05-09 05:44 EDT
Nmap scan report for r23xsp01.calo.cisco.com (172.16.30.146)
Host is up (0.000063s latency).
PORT STATE SERVICE VERSION
443/tcp open https?
| ssl-enum-ciphers:
| TLSv1.2:
| ciphers:
| TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 - strong
| TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 - strong
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 - strong
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 - strong
```

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).