Troubleshoot CommPilot Error "SSL_ERROR_NO_CYPHER_OVERLAP"

Contents

Introduction

This document describes how to Configure and Troubleshoot BroadWorks to avoid the "SSL_ERROR_NO_CYPHER_OVERLAP" error.

Prerequisites

Requirements

Cisco recommends that you have knowledge of the BroadWorks platform.

Background Information

BroadWorks Configuration

For Broadworks Releases 22 and later, the protocols and ciphers are configurable via the CLI via the contexts seen at different configuration levels.

```
'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
```

A context named SSLCommonSettings refers to a less specific item from the SSL hierarchy and a context named SSLSettings refers to a more specific item from the hierarchy.

Functional Lab Example

Configuration

Low-level configuration tied to the specific interface & port with no ciphers defined:

```
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.
```

Verification

Verify the configuration with the curl command:

```
$ 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
```

Here it has successfully connected via TLSv1.2 with cipher TLS_RSA_WITH_AES_256_CBC_SHA256.

Connectivity Audit

To verify the Protocols and Ciphers that are accepted:

```
$ 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
```

Lab Example With Error

Problem

Error observed – "SSL_ERROR_NO_CYPHER_OVERLAP" via the browser.

```
# 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).
```

Configuration

Low-level configuration tied to the specific interface & port with the TLSv1.2 Protocol set with the TLSv1.0 Cipher TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 set:

```
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
```

Verification

Verify the configuration with the curl command:

```
$ 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).
```

Connectivity Audit

To verify the Protocols and Ciphers that are accepted:

```
$ 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
```

From the results of the tool it is observed that the TLSv1.2 protocol is available but there are no supported ciphers.

Resolution

Delete the TLSv1.1 cipher under **CLI/Interface/Http/SSLCommonSettings/Ciphers** , and then open all TLSv1.2 ciphers again (or add a TLSv1.2 cipher).

```
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.
```

Resolution Verification

```
$ 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
```