K15475: Troubleshooting SSL/TLS renegotiation

Diagnostic

Original Publication Date: Aug 28, 2014
Update Date: Jun 22, 2018

Issue

You should consider using these procedures under the following condition:

- A virtual server processing Secure Socket Layer (SSL)/Transport Layer Security (TLS) connection is experiencing handshake/renegotiation failures.

Note: The remainder of this article uses SSL to indicate the SSL/TLS protocols.

Symptoms

As a result of SSL handshake/renegotiation failures, you may encounter the following symptoms:

- The renegotiation process fails for a virtual server that processes SSL connections.
- The BIG-IP system logs error messages related to SSL handshake/renegotiation failures.
- SSL profile statistics indicate that the virtual server rejected renegotiation attempts.

Recommended Actions

SSL handshake overview

SSL communication consists of a series of messages exchanged between two parties (client and server). The messages determine the parameters of the encrypted communication channel that the two parties will use; the client and server must agree on the message details, such as the protocol version, cipher suites, secure renegotiation or client certificate requests—otherwise the handshake will fail.

The SSL handshake has the following messaging components:

ClientHello

When a client first attempts to connect to an SSL server, it initiates the session by sending a ClientHello message to the server. The ClientHello message starts the SSL communication between the two systems and includes attributes such as the session identifier (session ID) and others.

ServerHello

If the server is able to find an acceptable set of algorithms, it responds to the ClientHello message with a ServerHello message. The ServerHello message contains some of the same components as the ClientHello, including the session ID.
Certificate

The server sends its Certificate message containing the server’s certificate or list of (chain) certificates, depending on the selected cipher suite.

ServerKeyExchange

The ServerKeyExchange is sent by the server only when the server Certificate message (if sent) doesn’t have enough data to allow the client to exchange a premaster secret, such as when DHE_DSS, DHE_RSA, DH_anon, or Elliptic Curve Cryptography (ECDHE/EDCH) is used.

ServerHelloDone

After sending its certificate, the server sends a ServerHelloDone message, indicating it is done with handshake negotiation.

ClientKeyExchange

The client sends the ClientKeyExchange message containing the PreMasterSecret. The PreMasterSecret is sent encrypted using the public key of the server.

ChangeCipherSpec

The ChangeCipherSpec message is sent by both the client and server after the security parameters have been determined. The ChangeCipherSpec message activates the negotiated SSL options to be used for the session. From this point forward, all messages are authenticated and encrypted. This stage is significant as it indicates that subsequent records will be protected under the newly negotiated CipherSpec and keys.

Finished

Each party sends a Finished message under the new algorithm, keys, and secrets. The Finished message indicates that the handshake is complete, and the parties may begin to exchange application layer data.

Renegotiated SSL sessions

The SSL protocol allows either party in the SSL transaction to renegotiate the SSL handshake using new cryptographic parameters. Renegotiation is useful when an SSL session is established and one of the parties in the transaction needs to change the parameters of the SSL connection. For example, a user establishes an SSL session and anonymously browses an online shopping site. When the user later decides to log in (authenticate) and make a purchase on the site, the client and server will need to renegotiate the SSL handshake using new cryptographic parameters.

**Note:** SSL renegotiation and resumption differ in that renegotiation is a process by which the full SSL handshake process takes place over an existing SSL connection. SSL resumption is a process by which the client uses the session ID to re-establish a previously negotiated SSL session, skipping the public key operation.

Renegotiation settings
The SSL profiles contain the following options related to SSL renegotiation:

- **Renegotiation**: Specifies how the virtual server processes SSL renegotiation requests. When disabled, the system terminates the connection, or ignores the request, depending on system configuration. The default is enabled.
- **Renegotiation period**: Specifies whether the virtual server renegotiates the SSL session after a specified amount of time has passed. The default is Indefinite.
- **Renegotiate Size**: Specifies whether the virtual server renegotiates the SSL session after a specified amount of data has been exchanged. The default is Indefinite.
- **Renegotiate Max Record Delay**: Specifies the number of delayed records the system allows during SSL renegotiation. The default is Indefinite.
- **Secure renegotiation**: The BIG-IP SSL profiles support the TLS Renegotiation Indication Extension (RFC 5746) which improves security by cryptographically binding renegotiations to the initial connections with which they are associated. The Secure Renegotiation profile setting allows the user to specify the method of secure renegotiation for SSL connections. If you are experiencing SSL handshake failures related to SSL renegotiation, you may need to change the SSL profile’s Secure Renegotiation setting. The values for the Secure Renegotiation setting are as follows:
  - **Request**
    - **clientssl**: Specifies that the system requests secure renegotiation of SSL connections.
    - **serverssl**: Specifies that the system requests secure renegotiation of SSL connections.
  - **Require**
    - **clientssl (default)**: Specifies that the system requires secure renegotiation of SSL connections. In this mode, the system permits initial SSL handshakes from clients, but terminates renegotiations from unpatched clients.
    - **serverssl**: Specifies that the system requires secure renegotiation of SSL connections. In this mode, SSL connections initiated from the BIG-IP LTM system to an unpatched server fail when renegotiation is enabled.
  - **Require Strict**
    - **clientssl**: Specifies that the system requires strict secure renegotiation of SSL connections. In this mode, the system does not accept new SSL connections from unpatched clients.
    - **serverssl (default)**: Specifies that the system requires strict, secure renegotiation of SSL connections. In this mode, SSL connections initiated from the BIG-IP LTM system to an unpatched server fail when renegotiation is enabled.

**Procedures**

When experiencing SSL handshake/renegotiation issues, you can use the following troubleshooting steps to determine the root cause:

- **Identifying renegotiation failures**
Enabling SSL debug logging

Testing SSL renegotiations (using s_client)

Reviewing log messages related to SSL renegotiation failures

Packet tracing using the ssldump utility

Adjusting the Secure Renegotiation profile setting

Identifying renegotiation failures

To identify SSL renegotiation attempts and renegotiation failures, review the statistics for the SSL profile associated with the virtual server. To do so, perform the following steps:

**Impact of procedure:** Performing the following procedure should not have a negative impact on your system.

1. Log in to the Traffic Management Shell (tmsh) by typing the following command:
   
   tmsh

2. To view the SSL profile statistics, use the following command syntax:

   ```
   show /ltm profile <client-ssl/server-ssl> <profile_name>
   ```

   For example, the following command displays the SSL renegotiation statistics for the client SSL profile named `client-ssl-renegotiation`:

   ```
   show /ltm profile client-ssl client-ssl-renegotiation | grep -i 'secure handshakes\|renegotiations'
   ```

   Secure Handshakes 1956
   Insecure Handshakes Accepted 0
   Insecure Handshakes Rejected 73
   Insecure Renegotiations Rejected 34

   This output indicates unpatched clients attempted to renegotiate SSL sessions 34 times and were rejected by the virtual server.

Enabling SSL debug logging

You can obtain more information about the renegotiation failures by enabling SSL debug logging on the BIG-IP system. You can then test SSL renegotiation for the virtual server using a web browser or the OpenSSL client, and then review the debug log files. Doing so will provide more useful logging information when troubleshooting SSL renegotiation issues, and help identify any unpatched clients responsible for the renegotiation failures.

**Note:** Beginning in 12.0.0, the BIG-IP system automatically logs SSL errors through standard logging; the use of debug logging for SSL errors is not required.

For example, with debug logging enabled, the system logs error messages to the `/var/log/ltm` file that appear similar to the following example:

- The SSL handshake failed for client 10.12.23.27 when connecting to virtual server 10.12.23.242:443:
The client renegotiation attempt failed:

deb tmm[11005]: 01260009:7: Connection error: ssl_hs_rxhello:3840: insecure renegotiation disallowed (40)

The client initiates a connection to a virtual server configured with a Server SSL profile, and the back-end SSL server lacks support for the TLS Renegotiation Indication Extension (**RFC 5746**): 

tmm warning tmm[7213]: 01260017:4: Connection attempt to insecure SSL server (see RFC5746) aborted: 10.12.23.28:443

To enable SSL debug logging, perform the following procedure:

**Impact of procedure:** *F5 recommends that you return the SSL log level to the default value after you complete the troubleshooting steps. Leaving debug logging enabled when the system is in normal production mode may generate excessive logging and cause poor performance.*

1. Log in to **tmsh** by typing the following command:
   
   tmsh

2. Enable SSL debug logging by typing the following command:
   
   modify /sys db log.ssl.level value Debug

**Important:** After you test SSL connections for the virtual server using a web browser or OpenSSL client, you should disable SSL debug logging by typing the following command:

modify /sys db log.ssl.level value Warning

**Testing SSL renegotiations (using s_client)**

After you enable SSL debug logging on the BIG-IP system, you should test SSL renegotiations for the virtual server using a web browser or other utility, such as the OpenSSL utility, **s_client**, or **cURL**. Using the **s_client** utility may provide additional debugging information that you can use to troubleshoot the issue. After making renegotiation requests to the virtual server, you can review and analyze the debug log files on the BIG-IP system.

To test SSL renegotiations using the **s_client**, perform the following procedure:

**Impact of procedure:** *Performing the following procedure should not have a negative impact on your system.*

1. Log in to the command line of a Linux host (with a current version of OpenSSL) that can access the SSL virtual server.
2. Test SSL connections for the virtual server using the following command syntax:
openssl s_client -connect <virtual_server>:<port>

For example:

openssl s_client -connect 10.12.23.115:443

3. At the prompt, type an upper-case R, and press enter.

For example, if the renegotiation is successful, you should see output similar to the following example:

R <enter>

RENEGOTIATING
depth=0 C = US, ST = WA, L = Seattle, O = MyCompany, OU = IT, CN = localhost.localdomain,
emailAddress = root@localhost.localdomain verify error:num=18:self signed certificate
verify return:1
depth=0 C = US, ST = WA, L = Seattle, O = MyCompany, OU = IT, CN = localhost.localdomain,
emailAddress = root@localhost.localdomain
verify return:1

If the renegotiation fails, you should see output similar to the following example:

R <enter>

RENEGOTIATING
12377:error:14094410:SSL routines:SSL3_READ_BYTES:sslv3 alert handshake failure:s3_pkt.c:1052:SSL alert number 40
12377:error:1409E0E5:SSL routines:SSL3_WRITE_BYTES:ssl handshake failure:s3_pkt.c:529:

Reviewing log messages related to SSL renegotiation failures

After you test SSL renegotiations using a web browser or OpenSSL client, you should review the BIG-IP log files for debug error messages related to the SSL handshake. To do so, perform the following procedure:

**Impact of procedure:** Performing the following procedure should not have a negative impact on your system.

1. Log in to the BIG-IP command line.
2. Use a Linux text utility, such as less or tail, to review the /var/log/ltm file.

   For example:

   tail -f /var/log/ltm

   **Note:** To filter the log information for SSL errors only, use the grep command.

   For example:

   cat /var/log/ltm |grep -i 'ssl'

3. Review the debug logs for SSL renegotiation errors, SSL handshake failures, or SSL alert codes.
Packet tracing using the ssldump utility

The **ssldump** utility is a protocol analyzer for SSL/TLS that identifies TCP connections from a chosen packet trace or network interface and attempts to interpret the packets as SSL/TLS traffic. You can use the **ssldump** utility to examine, decrypt, and decode SSL-encrypted packet streams that are processed by the BIG-IP system. For information about using **ssldump** to troubleshoot SSL handshake failures, refer to **K10209: Overview of packet tracing with the ssldump utility**.

Adjusting the Secure Renegotiation profile setting

If you want to further test SSL renegotiation, you can temporarily change the **Secure Renegotiation** setting to **Request** in the SSL profile and then re-test SSL renegotiations using **s_client** or a web browser. To change the **Secure Renegotiation** setting to **Request** in the SSL profile, perform the following procedure:

**Impact of procedure**: The virtual server will request secure renegotiation of SSL connections and will accept SSL connections from unpatched clients / servers.

1. Log in to **tmsh** by typing the following command:

   `tmsh`

2. To change the **Secure Renegotiation** setting to **Request** in the SSL profile, use the following command syntax:

   `modify /ltm profile client-ssl <profile-name> secure-renegotiation request`

   For example:

   `modify /ltm profile client-ssl my-SSL-profile secure-renegotiation request`

3. Save the changes by typing the following command:

   `save /sys config`

Supplemental Information

- **K15292**: Troubleshooting SSL/TLS handshake failures
- **K75464225**: Configuring the BIG-IP to match SSL/TLS protocol versions in renegotiated sessions
- **K27445283**: Server SSL virtual servers may fail to complete SSL/TLS renegotiation handshakes
- **K14783**: Overview of the Client SSL profile (11.x - 12.x)
- **K14806**: Overview of the Server SSL profile (11.x - 12.x)
- **K13860**: Error Message: Connection attempt to insecure SSL server (see RFC5746) aborted:
- **K13512**: The BIG-IP SSL profiles now require secure renegotiation of SSL connections
- **K6767**: Overview of the BIG-IP SSL session cache profile settings
- **IANA Assigned Cipher Suites Hex Values -- RFC5289**
- **K09322055**: The BIG-IP system now logs debug SSL errors through standard logging

Applies to:
**Product:** BIG-IP, BIG-IP AAM, BIG-IP AFM, BIG-IP APM, BIG-IP ASM, BIG-IP Edge Gateway, BIG-IP LTM, BIG-IP PEM, BIG-IP PSM, BIG-IP WebAccelerator, BIG-IP WOM

12.1.2, 12.1.1, 12.1.0, 12.0.0, 11.6.1, 11.6.0, 11.5.4, 11.5.3, 11.5.2, 11.5.1, 11.5.0, 11.4.1, 11.4.0, 11.3.0, 11.2.1, 11.2.0, 11.1.0, 11.0.0