< draft-ietf-pce-pceps-15-old.txt

draft-ietf-pce-pceps-15.txt >

PCE Working Group D. Lopez
Internet-Draft O. Gonzalez de Dios
Updates: 5440 (if approved) Telefonica I+D
Intended status: Standards Track Q. Wu
Expires: January 29, 2018 D. Dhody
Huawei
July 28, 2017

PCE Working Group D. Lopez
Internet-Draft O. Gonzalez de Dios
Updates: 5440 (if approved) Telefonica I+D
Intended status: Standards Track Q. Wu
Expires: February 1, 2018 D. Dhody
Huawei
July 31, 2017

Secure Transport for PCEP
draft-ietf-pce-pceps-15

Abstract

The Path Computation Element Communication Protocol (PCEP) defines the mechanisms for the communication between a Path Computation Client (PCC) and a Path Computation Element (PCE), or among PCEs. This document describe the usage of Transport Layer Security (TLS) to

skipping to change at *page 1, line 43*

This Internet-Draft will expire on January 29, 2018.

This Internet-Draft will expire on February 1, 2018.

skipping to change at *page 2, line 34*

Table of Contents

1. Introduction

The Path Computation Element Communication Protocol (PCEP) [RFC5440] defines the mechanisms for the communication between a Path Computation Client (PCC) and a Path Computation Element (PCE), or between two PCEs. These interactions include requests and replies that can be critical for a sustainable network operation and adequate resource allocation, and therefore appropriate security becomes a key element in the PCE infrastructure. As the applications of the PCE

skipping to change at *page 4, line 51*

3.2. Initiating the TLS Procedures

Since PCEP can operate either with or without TLS, it is necessary for the PCEP speaker to indicate whether it wants to set up a TLS connection or not. For this purpose, this document specifies a new PCEP message called StartTLS. Thus the PCEP session is secured via TLS from the start before exchange of any other PCEP message (that includes the Open message). This document thus updates [RFC5440], which required the Open message to be the first PCEP message. In the case of a PCEP session using TLS the StartTLS message will be sent first.

Since PCEP can operate either with or without TLS, it is necessary for the PCEP speaker to indicate whether it wants to set up a TLS connection or not. For this purpose, this document specifies a new PCEP message called StartTLS. Thus the PCEP session is secured via TLS from the start before exchange of any other PCEP message (that includes the Open message). This document thus updates [RFC5440], which required the Open message to be the first PCEP message. In the case of a PCEP session using TLS the StartTLS message will be sent first. Also a PCEP speaker that supports PCEPS MUST NOT start the

OpenWait timer after the TCP establishment, instead it starts a StartTLSWait timer as described in Section 3.3.

The PCEP speaker MAY discover that the PCEP peer supports PCEPS or can be preconfigured to use PCEPS for a given peer (see Section 4 for more details). Securing via TLS of an existing PCEP session is not permitted, the session MUST be closed and re-established with TLS as per the procedure described in this document.

The StartTLS message is a PCEP message sent by a PCC to a PCE and by a PCE to a PCC in order to initiate the TLS procedure for PCEP. The Message-Type field of the PCEP common header for the StartTLS message

skipping to change at *page 5, line 40*

skipping to change at *page 5, line 42*

(PCEP StartTLS failure) and Error-value set to 2 (reception of any other message apart from StartTLS, Open, or PCErr message), and MUST close the TCP connection.

If the PCEP speaker that does not support PCEPS, receives a StartTLS message, it will behave according to the existing error mechanism described in section 6.2 of [RFC5440] (in case message is received prior to an Open message) or section 6.9 of [RFC5440] (for the case of reception of unknown message). See Section 5 for more details.

If the PCEP speaker that only supports PCEPS connection (as a local policy), receives an Open message, it MUST treat it as an unexpected message and reply with a PCErr message with Error-Type set to 1 (PCEP session establishment failure) and Error-value set to 1 (reception of an invalid Open message or a non Open message), and MUST close the TCP connection.

If a PCC that supports PCEPS connection as well as allow non-PCEPS connection (as a local policy), it MUST first try to establish PCEPS, by sending StartTLS message and in case it receives an PCErr from the PCE, it MAY retry to establish connection without PCEPS by sending an Open message. If a PCE that supports PCEPS connection as well as allow non-PCEPS connection (as a local policy), it MUST wait to respond after TCP establishment, based on the message received from the PCC. In case of StartTLS message, PCE responds with sending StartTLS message and moving to TLS establishment procedures as described in this document. In case of Open message, PCE responds with Open message and move to PCEP session establishment procedure as per [RFC5440].

After the exchange of StartTLS messages, if a PCEP speaker cannot establish a TLS connection for some reason (e.g. the required mechanisms for certificate revocation checking are not available), it MUST return a PCErr message (in clear) with Error-Type set to [TBA2 by IANA] (PCEP StartTLS failure) and Error-value set to:

o 3 (not without TLS) if it is not willing to exchange PCEP messages without the solicited TLS connection, and it MUST close the TCP session.

skipping to change at *page 7, line 10*

skipping to change at *page 7, line 29*

exchange of Open messages MUST be applied by the PCEP peers during the exchange of StartTLS messages.

The format of a StartTLS message is as follows:

<StartTLS Message>::= <Common Header>

The StartTLS message MUST contain only the PCEP common header with Message-Type field set to [TBA1 by IANA].

Once the TCP connection has been successfully established and the StartTLS message sent, the sender MUST start a timer called StartTLSWait timer, after the expiration of which, if no StartTLS message has been received (and in case of failure, a PCErr or Open message is not received), it MUST send a PCErr message with Error-Type set to [TBA2 by IANA] and Error-value set to 5 (no StartTLS (nor PCErr/Open) message received before the expiration of the StartTLSWait timer) and it MUST release the TCP connection . A RECOMMENDED value for StartTLSWait timer is 60 seconds.

Once the TCP connection has been successfully established, the PCEP speaker MUST start a timer called StartTLSWait timer, after the expiration of which, if neither StartTLS message has been received, nor a PCErr/Open (in case of failure and PCEPS not supported by the peer respectively), it MUST send a PCErr message with Error-Type set to [TBA2 by IANA] and Error-value set to 5 (no StartTLS (nor PCErr/Open) message received before the expiration of the StartTLSWait timer) and it MUST release the TCP connection . A RECOMMENDED value for StartTLSWait timer is 60 seconds. The value of StartTLSWait timer MUST NOT be less than OpenWait timer.

skipping to change at *page 7, line 42*

skipping to change at *page 8, line 27*

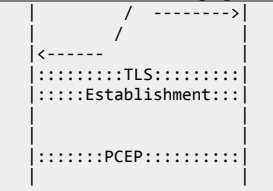

Figure 1: Both PCEP Speaker supports PCEPS

Figure 1: Both PCEP Speaker supports PCEPS (strict)

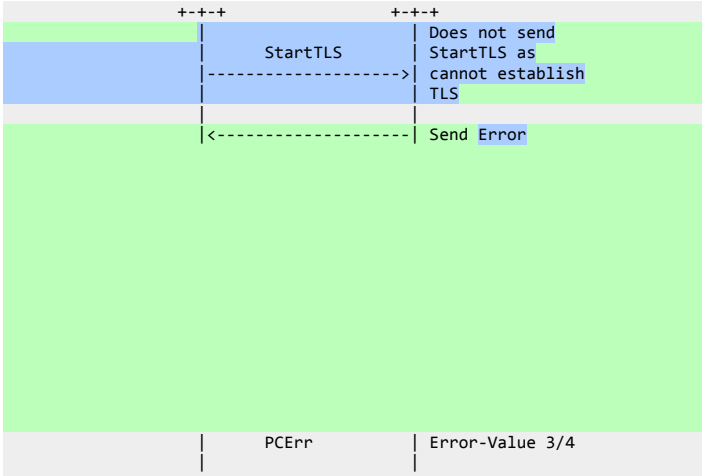

Figure 2: Both PCEP Speaker supports PCEPS, But cannot establish TLS

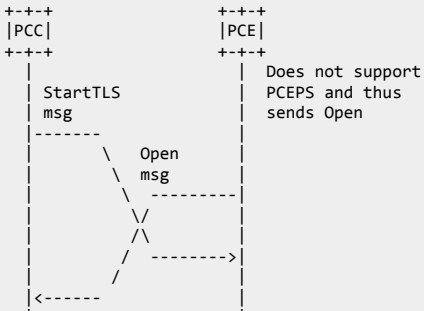

Figure 3: One PCEP Speaker does not support PCEPS

3.4. TLS Connection Establishment

Once the establishment of TLS has been agreed by the PCEP peers, the

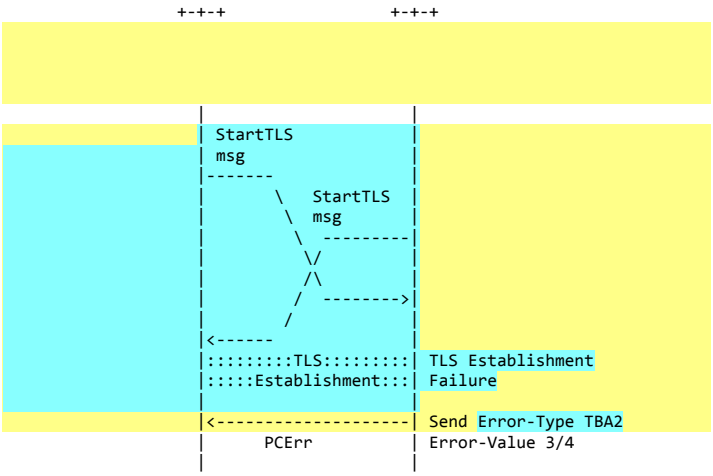

Figure 2: Both PCEP Speaker supports PCEPS (strict), but cannot establish TLS

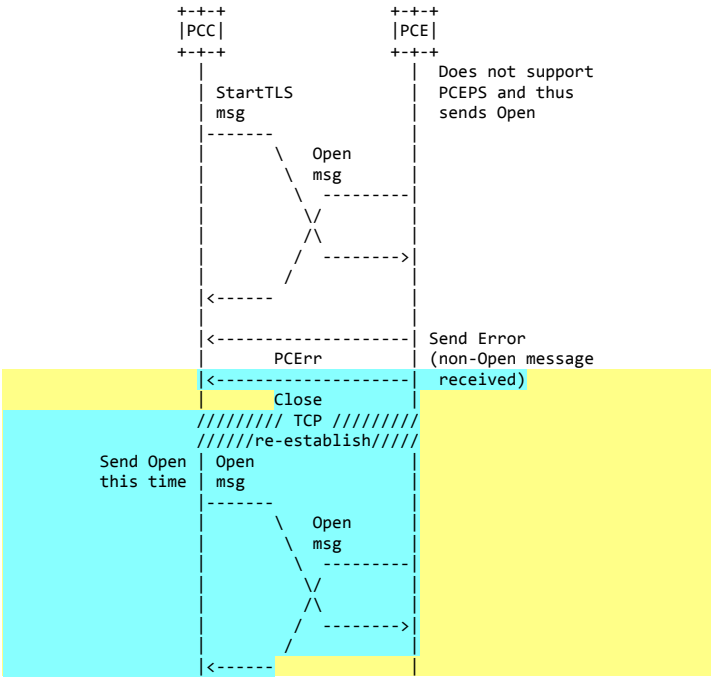

Figure 3: One PCEP Speaker (PCE) does not support PCEPS, while PCC supports both with or without PCEPS

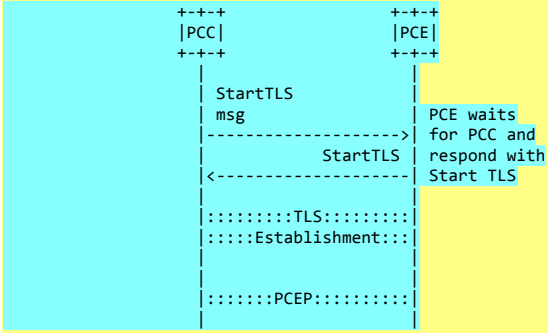

Figure 4: Both PCEP Speaker supports PCEPS as well as without PCEPS

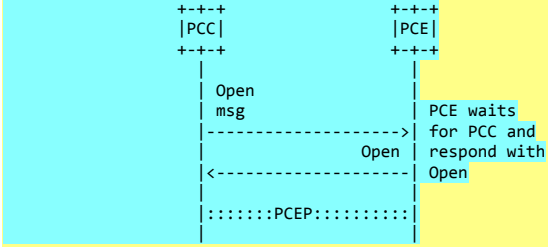

Figure 5: PCE supports PCEPS as well as without PCEPS, while PCC does not support PCEPS

3.4. TLS Connection Establishment

Once the establishment of TLS has been agreed by the PCEP peers, the

```
   connection establishment SHALL follow the following steps:

   1.  Immediately negotiate a TLS session according to [RFC5246].  The
       following restrictions apply:

       *  Support for TLS v1.2 [RFC5246] or later is REQUIRED.
```

skipping to change at *page 10, line 26*

```
       *  TLS with X.509 certificates using certificate fingerprints:
          Implementations MUST allow the configuration of a list of
          trusted certificates, identified via fingerprint of the
          Distinguished Encoding Rules (DER) encoded certificate octets.
          Implementations MUST support SHA-256 as defined by [SHS] as
          the hash algorithm for the fingerprint.

   3.  Start exchanging PCEP messages.
```

```
   To support TLS re-negotiation both peers MUST support the mechanism
   described in [RFC5746].  Any attempt to initiate a TLS handshake to
   establish new cryptographic parameters not aligned with [RFC5746]
   SHALL be considered a TLS negotiation failure.

3.5.  Peer Identity

   Depending on the peer authentication method in use, PCEPS supports
   different operation modes to establish peer's identity and whether it
   is entitled to perform requests or can be considered authoritative in
```

End of changes. 14 change blocks.

45 lines changed or deleted

```
   connection establishment SHALL follow the following steps:

   1.  Immediately negotiate a TLS session according to [RFC5246].  The
       following restrictions apply:

       *  Support for TLS v1.2 [RFC5246] or later is REQUIRED.
```

skipping to change at *page 13, line 22*

```
       *  TLS with X.509 certificates using certificate fingerprints:
          Implementations MUST allow the configuration of a list of
          trusted certificates, identified via fingerprint of the
          Distinguished Encoding Rules (DER) encoded certificate octets.
          Implementations MUST support SHA-256 as defined by [SHS] as
          the hash algorithm for the fingerprint.

   3.  Start exchanging PCEP messages.

       *  Once the TLS connection has been successfully established, the
          PCEP speaker MUST start the OpenWait timer [RFC5440], after
          the expiration of which, if no Open message has been received,
          it sends a PCErr message and releases the TCP/TLS connection.
```

```
   To support TLS re-negotiation both peers MUST support the mechanism
   described in [RFC5746].  Any attempt to initiate a TLS handshake to
   establish new cryptographic parameters not aligned with [RFC5746]
   SHALL be considered a TLS negotiation failure.

3.5.  Peer Identity

   Depending on the peer authentication method in use, PCEPS supports
   different operation modes to establish peer's identity and whether it
   is entitled to perform requests or can be considered authoritative in
```

End of changes. 14 change blocks.

134 lines changed or added