Reliable Transport for IKEv2

draft-smyslov-ipsecme-ikev2-reliable-transport

Valery Smyslov
svan@elvis.ru

IETF 117
IKE Transport

- IKE originally used only UDP as a transport protocol
  - depending on the presence of NATs ESP either run over IP or were UDP encapsulated
- RFC 9329 extends IKEv2 to use TCP when UDP is unavailable
  - in this case ESP is always TCP encapsulated
Problem

• When post-quantum algorithms are employed (e.g. as defined in RFC 9370) size of IKE messages increases
  – use of IKE fragmentation eliminates problems with IP fragmentation, but doesn’t address issues with possible congestion
  – simple retransmission mechanism of IKEv2 always resends the whole message even if only one fragment lost

• Using TCP solves the problem with transmission of large IKE messages, but
  – as ESP in this case also uses TCP, performance suffers (see Section 9 of RFC 9329)
Proposed Solution

• De-couple IKE and ESP transports (first proposed in draft-tjhai-ikev2-beyond-64k-limit)
  – use reliable transport (TCP) for IKE
  – use unreliable transport (IP, UDP) for ESP
Negotiation

• IKE-SA_INIT is initiated on UDP:4500 (to verify that UDP packets are routable)

<table>
<thead>
<tr>
<th>Initiator</th>
<th>Responder</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IKE_SA_INIT</strong> HDR,SAIL,KEi,Ni, [N(NAT_DETECTION_SOURCE_IP), N(NAT_DETECTION_DESTINATION_IP)], N(RELIABLE_IKE_TRANSPORT)</td>
<td>UDP</td>
</tr>
<tr>
<td>UDP</td>
<td><strong>IKE_SA_INIT</strong> HDR,SAR1,KEr,Nr, [N(NAT_DETECTION_SOURCE_IP), N(NAT_DETECTION_DESTINATION_IP)], N(RELIABLE_IKE_TRANSPORT)</td>
</tr>
</tbody>
</table>
Use

- Once extension is negotiated, peers switch to TCP in the next exchange (IKE_INTERMEDIATE or IKE_AUTH) and continue to use TCP for all subsequent exchanges, including those of rekeyed IKE SAs.

```
Initiator  Responder

HDR, SK{...}  TCP  HDR, SK{...}
TCP
TCP
```

- ESP SAs are being created over IP or with UDP encapsulation.
Some Details

• NAT keep-alive packets must still be sent over UDP if NAT is present

• Peers should not try to switch IKE SA to UDP if IP addresses changed and MOBIKE is in use
  – issue: no return routability check for UDP packets if IP addresses changed; perhaps INFORMATIONAL over UDP may be performed in this case

• Perhaps make reliable IKE transport negotiable (e.g. QUIC)?
Thank you!

- Comments?
- Questions?
- Any interest in this work?