

IKEv2 IPv4 Downstream Fragmentation Notification Extension

Liu, Zhang. Migault

Problem Statement (Fragmentation)

Reassembling packets by a downstream security gateway:

- requires additional resources which under heavy load results in service degradations.
- the 16-bit IPv4 identification field that is not large enough to prevent duplication making fragmentation not sufficiently robust at high data rates.

The problem is only for IPv4

When the DF bit is set to 1, the security gateway is unlikely to receive the unencrypted ICMPv4 message Packet Too Big (PTB).

- this results in black holing

As a result DF is set to 0 and the security gateway does the reassembly operation.

We propose that the downstream security gateway advertises the other security gateway that fragmentation is ongoing with an indication of the acceptable MTU.

- similar to PTB and RFC8900 recommends each layer handles fragmentation at their layer and to reduce the reliance on IP fragmentation to the greatest degree possible

Initiator

Responder

HDR, SA, KEi, Ni -->

<-- HDR, SA, KEr, Nr

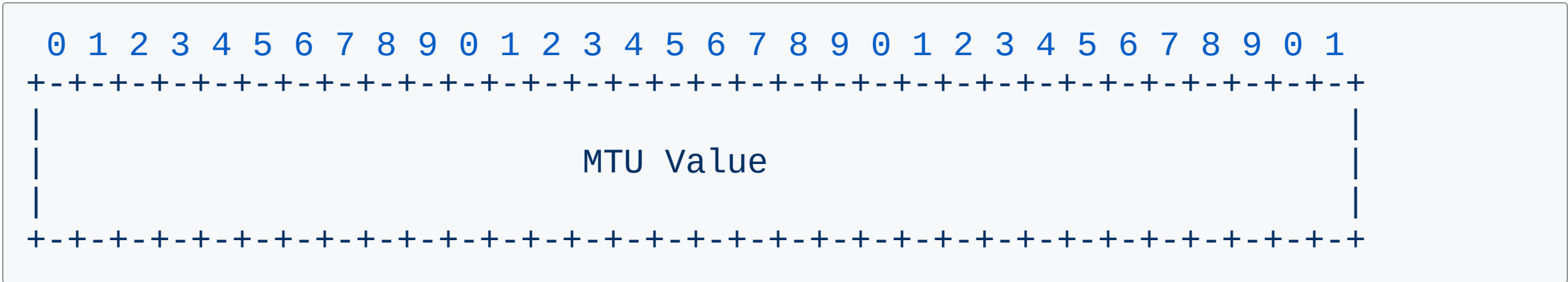
HDR, SK {IDi, AUTH,
SA, TSi, TSr,
N(IP4_DOWNSTREAM_FRAGMENTATION_SUPPORTED)} -->

<-- HDR, SK {IDr, AUTH,
SA, TSi, TSr,
N(IP4_DOWNSTREAM_FRAGMENTATION_SUPPORTED)}

Receiving Security Gateway

Sending Security Gateway

HDR SK { N(IP4_DOWNSTREAM_FRAGMENTATION)} -->



Upon receiving a IP4_DOWNSTREAM_FRAGMENTATION:

1. The sending security gateway SHOULD advertise sending nodes of the MTU expected for the inner packet and discard those that are larger.
2. If inner packet has its DF bit set to 0, the security gateway MAY perform inner fragmentation
3. The security gateway MAY perform outer fragmentation.
 - DF is then set to 1 and communication may be exposed to blackholing

Thanks!