IPsec

Here documents known IPsec corner cases which need to be keep in mind when deploy various IPsec configuration in real world production environment.

1. IPcomp:

   Small IP packet won't get compressed at sender, and failed on policy check on receiver.

Quote from RFC3173:

```
2.2. Non-Expansion Policy

 If the total size of a compressed payload and the IPComp header, as
 defined in section 3, is not smaller than the size of the original
 payload, the IP datagram MUST be sent in the original non-compressed
 form.  To clarify: If an IP datagram is sent non-compressed, no

 IPComp header is added to the datagram.  This policy ensures saving
 the decompression processing cycles and avoiding incurring IP
 datagram fragmentation when the expanded datagram is larger than the
 MTU.

 Small IP datagrams are likely to expand as a result of compression.
 Therefore, a numeric threshold should be applied before compression,
 where IP datagrams of size smaller than the threshold are sent in the
 original form without attempting compression.  The numeric threshold
 is implementation dependent.
```

Current IPComp implementation is indeed by the book, while as in practice when sending non-compressed packet to the peer (whether or not packet len is smaller than the threshold or the compressed len is larger than original packet len), the packet is dropped when checking the policy as this packet matches the selector but not coming from any XFRM layer, i.e., with no security path. Such naked packet will not eventually make it to upper layer. The result is much more wired to the user when ping peer with different payload length.

One workaround is try to set "level use" for each policy if user observed above scenario. The consequence of doing so is small packet(uncompressed) will skip policy checking on receiver side.