ESP-NULL Heuristics

An Update

Tero Kivinen
Dan McDonald

Hello! Anyone out there?

- This draft became a WG document on April 16.
- Nobody has responded since then.

Draft Highlights

- Even without WESP, middleboxes performing deep-packet-inspection need to handle older end-nodes.
- Start with an upper bound of 3.8% chance of misclassifying an encrypted packet as an ESP-NULL packet with no work beyond inspecting last-pad-byte/pad-length pairs.
- Techniques in the draft reduce this probability to near-zero.
- Example pseudocode in Appendix A.

Questions and TBDs

- How much do people care about SCTP?
  - I hadn't consulted my SCTP wizard about chunk-specific processing, but can.
- How readable and usable is the Appendix A pseudocode?