Securing draft-ietf-v6ops-mech-v2 tunnels using IPsec

("the scenarios and how to set it up")

draft-tschofenig-v6ops-secure-tunnels-03.txt

Tschofenig, Savola, Parthasarathy, Graveman

Background

- Revising draft-ietf-v6ops-mech-v2 about a year ago..
  - RFC 2893 said just, "use IPsec"
  - That’s now insufficient, we needed to spell out *how*
  - We decided to put it to a separate document (this one)
- At the IESG review there was a comment for mech-v2
  - Then-security AD Bellovin blocked mech-v2 until this ready
  - Mech-v2 has been stalled for 6+ months now..
  - No matter what, it seems the IPsec/IKE details must be somewhere
    - And security area does not specify how to use IPsec with other areas’ protocols
    - We have do deal with this on our own, though they can help

Current status

- At -03 already
  - Has had significant amount of review from IPsec people
  - Still some nits to address
  - But seems to be "almost ready" for Informational
  - Presented 2 IETF’s ago, no objections then
- Comments so far for -03
  - Need to clean it up a bit further (thanks Elwyn, et al)
- Fundamental issues -- Comments?
  - Should we encrypt everything, or just the link-local control traffic?
- What next?
  - Adoption for WG item, then WG last call before Paris IETF?
  - We need people to read and comment on it