Split DNS
Configuration for IKEv2

draft-pauly-ipsecme-split-dns-02

Tommy Pauly (tpauly@apple.com)

IPSECME
IETF 97, November 2016, Seoul
New in split-dns-02

- Clarification of DNSSEC payload types
  - Changed INTERNAL_DNSSEC_TA from presentation to wire format
  - Explained how to associate DNSSEC values with specific domains
  - Incorporated textual changes from three reviewers
Next Steps

• Charter targets IETF last call for February 2017

• Get formal working group adoption. Is there any outstanding feedback?

• More interoperability (Apple-Libreswan tested)

• IANA assignment
TCP Encapsulation of IKE and IPsec Packets

draft-ietf-ipsecme-tcp-encaps-03

Tommy Pauly (tpauly@apple.com)

IPSECMEME
IETF 97, November 2016, Seoul
Fallback from UDP to TCP

- Clarification and guidance requested during charter review

- Added following recommendation to -03:
  - Always attempt UDP first
  - Wait for some fraction of the configuration’s retransmission of IKE_SA_INIT
Fallback from UDP to TCP

• Previously have proposed having a separate informational draft with more recommendations for how TCP encapsulation will be used for scenarios like Wi-Fi Calling (ePDG/IWLAN)

• Do we think this work would be useful?

• Are there other recommendations that should be part of the current proposed standard draft?
Not Just TCP

- The encapsulation headers to send IKE and ESP in a stream can work over any stream
- TCP, TLS, or something else in the future
- Added clarification in response to charter discussion. Do we want more emphasis on this point?
Multiple TCP x Multiple IKE/Child

• Areas of confusion around use of multiple TCP flows for a single IKE SA, or multiple IKE SAs for a single TCP flow

• New version clarifies that all combinations are supported; however, generally one-to-one is advised

• This is based on the premise that the IKE associations should be independent from TCP connections
Next Steps

• Continue interoperability testing (Apple-Cisco tests validated). If you have an implementation, please let us know!

• Charter targets IETF last call for December 2016

• Let’s wrap it up!