École Nationale Supérieure
des Télécommunications de Bretagne

ENST Bretagne

IKEv2 peer address management

draft-dupont-ikev2-addrmgmt-05.txt

IETF60-Mobike

www.enst-bretagne.fr

Groupe des écoles
des télécommunications

Summary

- Peer address set
  - peer addresses = addresses IKE runs over = outer addresses of tunnel mode IPsec SAs
  - a primary peer address, some alternate peer addresses (per peer)
  - add/delete/set-primary operations
  - later: how to trust/verify a peer address
- Peer address update
  - doesn’t deal with transport mode IPsec SAs
  - IPsec/IKE SA list
  - “all SAs” flag

Changes from previous drafts

- Return routability check: recommend a nonce payload in order to make probes unpredictable

- (Planned) More details about how to perform an update with return routability check (window of one issue)

- (Planned) Clone the NAT_DETECTION_* notifications into NAT_PREVENTION_* notifications (Pasi's idea)

- (Planned) Fork the statement about transport mode into a dedicated document using only an address list assumption

Differences from other proposals

- No NAT traversal interoperability
- Support for SCTP (both the protocol itself and its model of multi-homing)
- Flexible trusting/verification of peer addresses (move the issue from the protocol to the policy: next slide)
- Per SA update

How to trust/verify peer addresses

- Recognized as the main issue!
- First way: configured as trusted
- Common traditional IKE way: authenticated/authorized by certificates (present in an alternate subject name)
- Road-warrior way: verified by the implicit return routability check of IKE exchanges (note: needs a protection of the peer addresses: NAT_PREVENTION_* notifications, cookie)
- MIPv6 routing optimization way: explicit return routability check
- MIPv6 mobile node - home agent way: topologically plausibleness by ingress filtering and trust in the peer