IKE over TCP

Yoav Nir

IKE over TCP

- Draft -00 submited on August 28th.
  http://tools.ietf.org/html/draft-ietf-ipsecme-ike-tcp-00
- Little discussion since then.
- Still some open issues
  - Besides the obvious "what about IKEv1"…

Open Issues – TCP Port

- Do we fix the port at 500, or do we allow to specify another port.
  - Easier to get filters to recognize this if everyone uses the same port
  - Agility means you can use port forwarding on NATs.
- Related issue: Should the Initiator also send an IKE_TCP_SUPPORTED notification
  - Doesn’t using IKE over TCP pretty much guarantee you support it?

Open Issue – NAT (1)

- During IKE over TCP, we may find that there is NAT on path.
- Running IKE_AUTH over UDP port 4500 creates a mapping in the NAT device, which can later be used for returning ESP or IKE packets.
- Not so for IKE over TCP.
- ESP traffic would make this mapping, but we can't rely on it.

Open Issue – NAT (1)

- Valery Smylsov suggests the following text:

"If NAT is detected during IKE SA establishment and IKE_AUTH is done over TCP then the original initiator MUST initiate a Liveness Check over UDP 4500 immediately after the IKE_AUTH is complete."

Open Issue – NAT (2)

- The draft allows any request to be sent over any transport. Fair enough. Usually.
- Requests containing COOKIE will become useless if transmitted over a different transport from the original request. The cookie won't be valid.
- NAT Detection – these payloads change with ports.
- NO_NATS_ALLOWED – different transports may be routed differently.

Open Issue – NAT (2)

- Valery Smyslov suggests the following text:

"Messages containing COOKIE, NAT_DETETION_SOURCE_IP or NAT_DETECTION_DESTINATION_IP notifications MUST NOT be retransmitted over different transport. If MOBIKE is employed and the message contains a NO_NATS_ALLOWED notification, it MUST NOT be retransmitted over different transport."

Open Issue – NAT (3)

- Responders are required to open their own connections (or use UDP) if they have requests of their own.
- What if the peer is behind a NAT?
- Suggested text is to only open a new TCP connection if no NAT is detected.

Next Steps

- Discuss the four issues raised, plus any other one that comes up.
- Issue -01.
- WGLC & Ship it.