TCP Encapsulation of IKE and IPSec Packets

Tommy Pauly (tpauly@apple.com)
Samy Touati (samy.touati@ericsson.com)
Ravi Mantha (ramantha@cisco.com)

IPSECME
IETF 96, July 2016, Berlin

Document Status

- New revision on July 7: draft-ietf-ipsecme-tcp-encaps-01
- Moved TLS support to an informational appendix
- Added a Stream Prefix to help responders identify TCP Encapsulated IKE streams

Configuration

- Use TCP Encapsulation as a fallback from failed UDP-based negotiations; try UDP again first when doing MOBIKE

- No fixed port number specified. May use 4500, which is allocated for IKE NAT Traversal. Often will use 443 in practice.

- TLS mentioned only in appendix, with examples of how exchanges will work. Generally will use port 443.

Stream Prefix

4. TCP-Encapsulated Stream Prefix

```
 0      1      2      3      4      5
+------+------+------+------+------+------+
| 0x49 | 0x4b | 0x45 | 0x54 | 0x43 | 0x50 |
+------+------+------+------+------+------+
   I      K      E      T      C      P
```

- Helps Responder identify TCP-encapsulated IPSec traffic
- Precedes Initiator’s stream of IKE and ESP messages in any new connection
- If using TLS, the prefix should be within the encrypted stream

Minor Changes

- Replaced references to “IKEv2” with “IKE” to apply to future versions of IKE if needed
- Modified length field from 32 bits to 16 bits to align with specs from 3GPP

Interoperability Testing

- Cisco and Apple working on implementation interoperability
- If other implementations would like to add support, please test with us!
- Options for adding TCP support to IKE clients:
  - Do TCP/TLS in kernel alongside UDP encapsulation
  - Divert ESP packets to userspace using a tun-type interface, and send out over TCP/TLS
  - Divert inner traffic to userspace using a tun-type interface and do ESP and TCP/TLS together

Next steps

- Please review latest revision and provide feedback
- Participate in interoperability testing
- When should we target WGLC?