Encrypted ESP Ping

draft-antony-ipsecme-encrypted-esp-ping

Antony Antony <antony.antony@secunet.com>
IPsec Background

- IKE is control plane (UDP 500 or UDP 4500)
- ESP is Data plane (ESP or ESP-in-UDP 4500)
Problem Statement

- Diagnose after IKE is established
- ESP packets do not share fate with IKE
- IKE might succeed but ESP packets are dropped
- Hard to detect and recover
- Data traffic is blackholed
- Why Not Use Existing IP Tools?
Why not ping over IPsec?

- xfrm policy 192.0.2.125/25 <-> 192.0.2.125/25
- Xfrm state 192.1.2.23 <-> 192.1.2.23
- espping -l 192.1.2.45 192.1.2.34 <data>

eth0: 192.0.2.125/25
eth1: 192.0.2.126/25
eth0: 192.0.2.252/25
eth1: 192.0.2.254/25
eth0: 192.1.2.23/24
eth1: 192.1.2.45/24

pacific

eth0

espping -l 192.1.2.45 192.1.2.34 <data>
Use cases

- Diagnose ESP Blocked or Filtered
- Probing Multiple ESP Paths to same end point
- Probe Return Path
  - ESP is two unidirectional Security Associations
Example

- espping -s <size> -I <src ip> [--spi <spi>] <dst ip>

- espping -I 192.1.2.23 –spi 0xAABBCCDD 192.1.2.45
Packet format: Request

IP Header
- Protocol 50

ESP
- Next Header 144

AGGFRAG_PAYLOAD
- Sub-type (3) ESP-ECHO-REQUEST

Echo Payload
- R Flag
- Data Length
- Return Path SPI
- Identifier
- Sequence #
- Optional Data
Packet format: Response

**IP Header**
- Protocol 50

**ESP**
- Next Header 144

**AGGFRAG_PAYLOAD**
- Sub-type (4) ESP-ECHO-RESPONSE

**Echo Payload**
- R Flag
- Data Length
- Return Path SPI
- Identifier
- Sequence #
- Optional Data
## RFC 9347 CC Payloads

<table>
<thead>
<tr>
<th>Sub-type (1)</th>
<th>Reserved</th>
<th>BlockOffset</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>LossEventRate</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RTT(22)</td>
<td>Echo Delay(21)</td>
</tr>
<tr>
<td></td>
<td>Transmit Delay (21)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TVal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TEcho</td>
<td></td>
</tr>
<tr>
<td>DataBlocks ...</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
IP-TFC Congestion Control Payload

• CC payload helps to discover path properties:
  - One way delays,
  - loss rate.
  - estimate bandwidth

• Useful to probe manually even when IP-TFS is not negotiated
IKEv2 Notify to announce support?

Add IKEv2 Notification in -03 I.D.
ENCRYPTED_PING_SUPPORTED
SADB Implementation on receiver

• How to validate Return Path requested?
  – SADB is unidirectional
  – Especially when there are multiple SAs
  – Only IKEd knows the return path in its peer DB
Questions / Feedback?

Adoption?
Similar ideas

- MPLS LSP ping with return path: RFC 7110
- Bidirectional Forwarding Detection (BFD)
  - IP only (Not suitable for Encrypted ESP Ping)
  - [https://www.rfc-editor.org/rfc/rfc8562](https://www.rfc-editor.org/rfc/rfc8562)
ESP Message

- Security Parameters Index (SPI)
- Anti-Replay Sequence Number
- Initialization Vector IV, (8/16 bytes)
- Payload Data (variable)
- Padding (0-255 bytes)
- Authentication Data (variable)

Authenticated

Encrypted