Encrypted ESP Ping

draft-antony-ipsecme-encrypted-esp-ping-04

IETF 121, Dublin, November 2024

Antony Antony <antony.antony@secunet.com>

Problem Statement

- Diagnose ESP 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

Use cases

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

Since IETF 120

- -04 new version of the I.D.
  - fix IP-TFS subtype
  - IKEv2 Notify: **ENCRYPTED_PING_SUPPORTED**
  - Re-phrasing ot text.
- From hallway chats: there is interest in this work

Next Steps

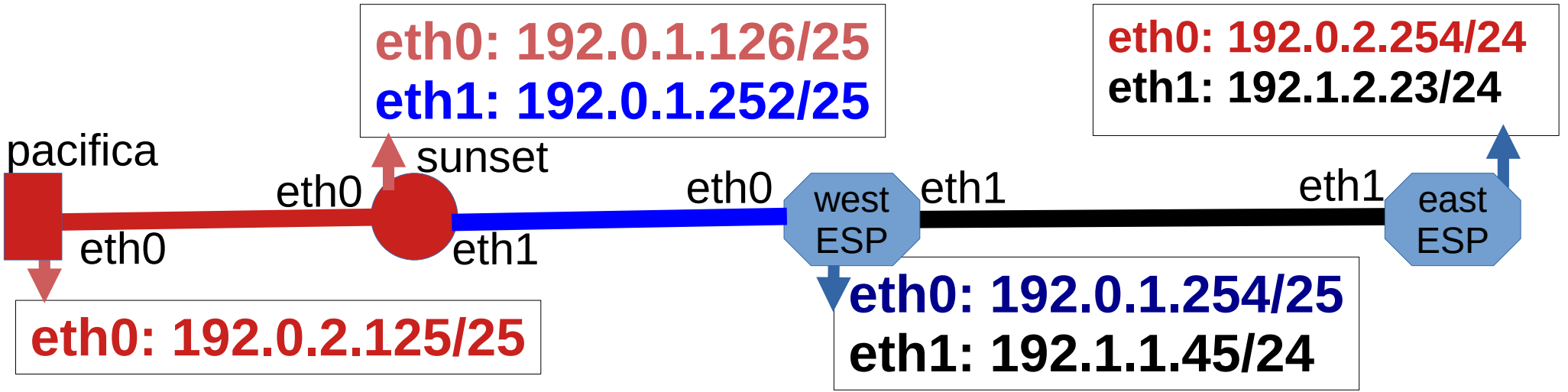
Questions/Feedback?

Call for WG Adoption

Extra Slides
Backup

Why not ping over IPsec?

IPsec gateways has no IP from policy



xfrm policy 192.0.2.125/25 <-> 192.0.2.0/24

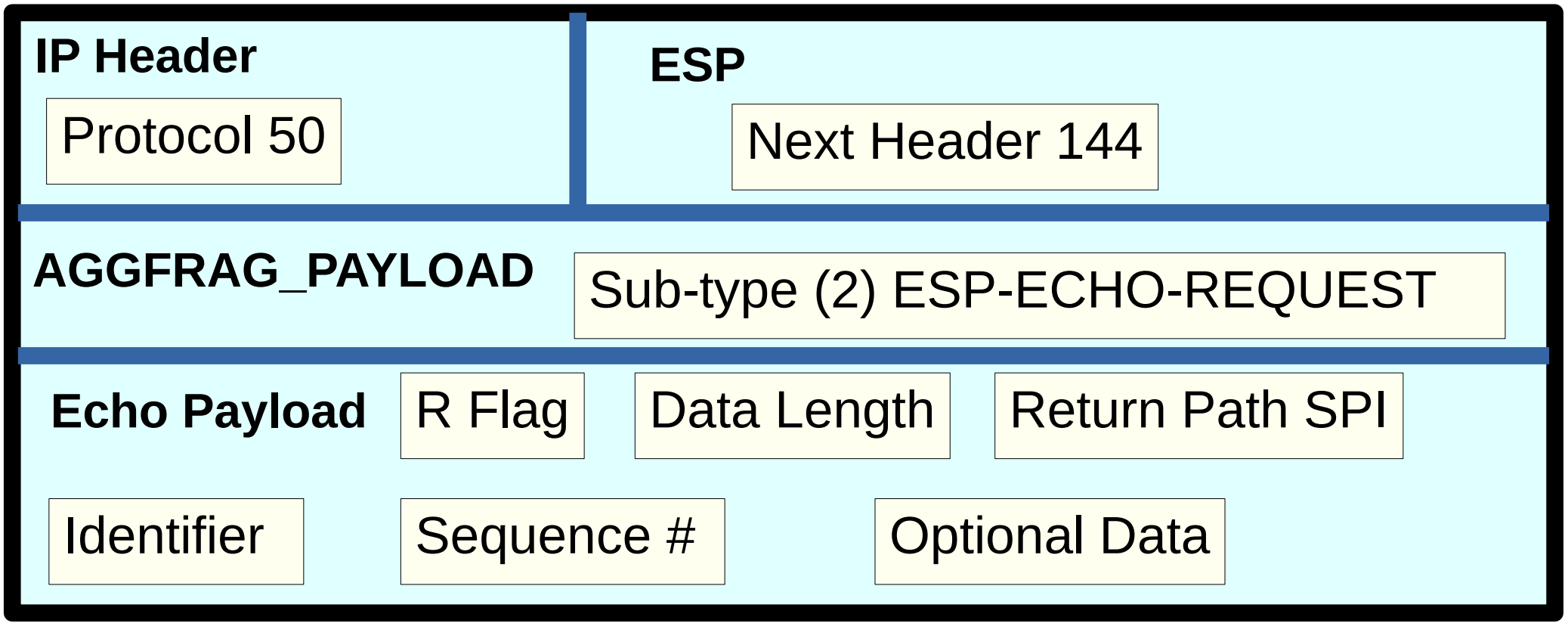
xfrm state 192.1.2.23 <=> 192.1.2.45 SPI 0xAABBCCDD

espping -s 0xAABBCCDD -I 192.1.2.45 192.1.2.23

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



Packet format : Response