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

eth0: 192.0.2.254/24 eth0: 192.0.1.126/25 eth1: 192.1.2.23/24 eth1: 192.0.1.252/25 pacifica sunset eth0 eth1 eth1 eth0 west east **ESP** eth1 **ESP** eth0 eth0: 192.0.1.254/25 eth0: 192.0.2.125/25 eth1: 192.1.1.45/24

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 -l 192.1.2.45 192.1.2.23

secunet

02/11/24

Example

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

espping -l 192.1.2.23 –spi 0xAABBCCDD 192.1.2.45

secunet

Packet format : Request

IP Header **ESP** Protocol 50 Next Header 144 AGGFRAG PAYLOAD Sub-type (2) ESP-ECHO-REQUEST R Flag Data Length Return Path SPI **Echo Payload Identifier** Sequence # **Optional Data** 9

02/11/24

secunet

Packet format : Response

IP Header **ESP** Protocol 50 Next Header 144 AGGFRAG PAYLOAD Sub-type (3) ESP-ECHO-RESPONSE R Flag Return Path SPI **Echo Payload** Data Length **Identifier** Sequence # **Optional Data**

10

securet 02/11/24