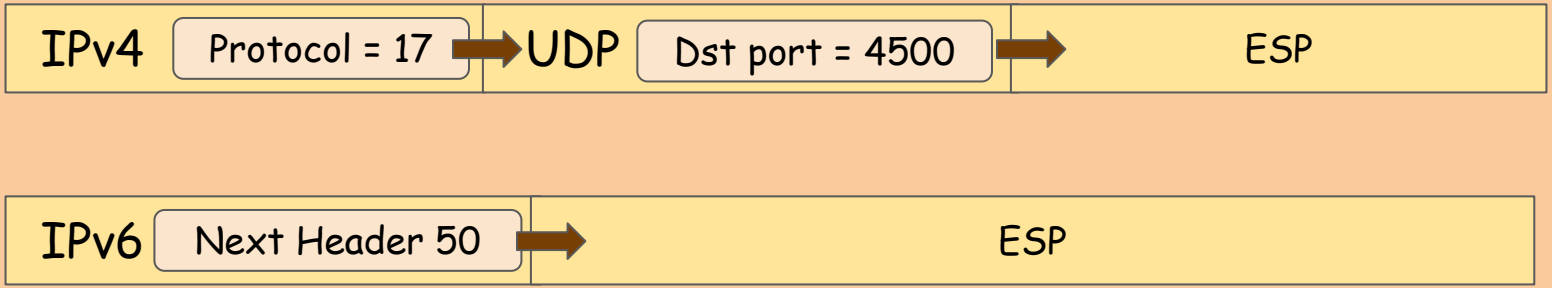
ESP Echo Protocol

draft-colitti-ipsecme-esp-ping-01

Lorenzo Colitti , Jen Linkova , Michael Richardson
IETF119, March 2024, Brisbane, AU

ESP, IPv4 and IPv6



Native ESP advantages:

- no keepalives needed (if ESP is statelessly allowed)
- fewer keepalives otherwise (ESP timeouts usually higher)

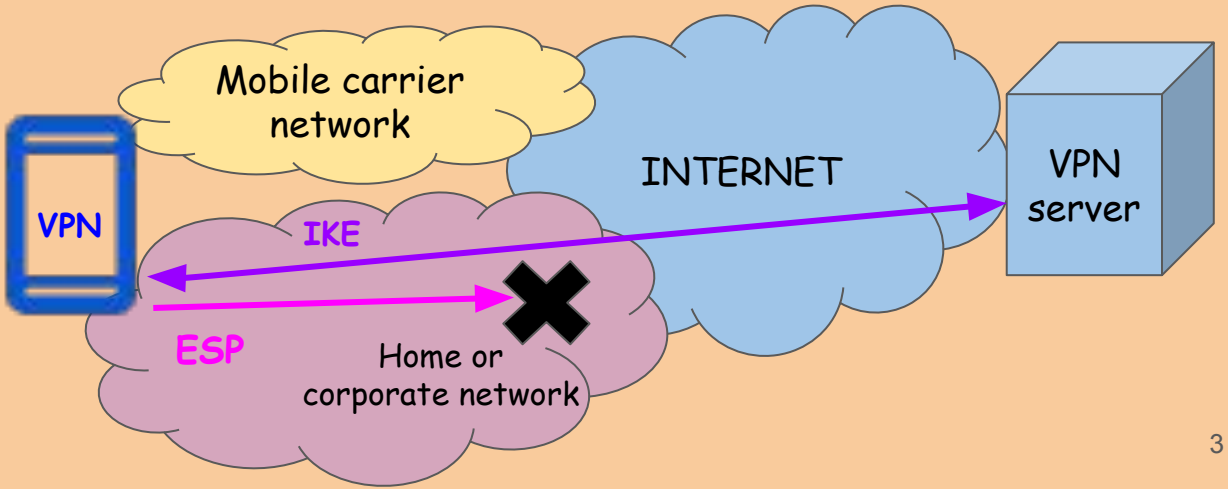
Problem Statement

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



Solution Overview

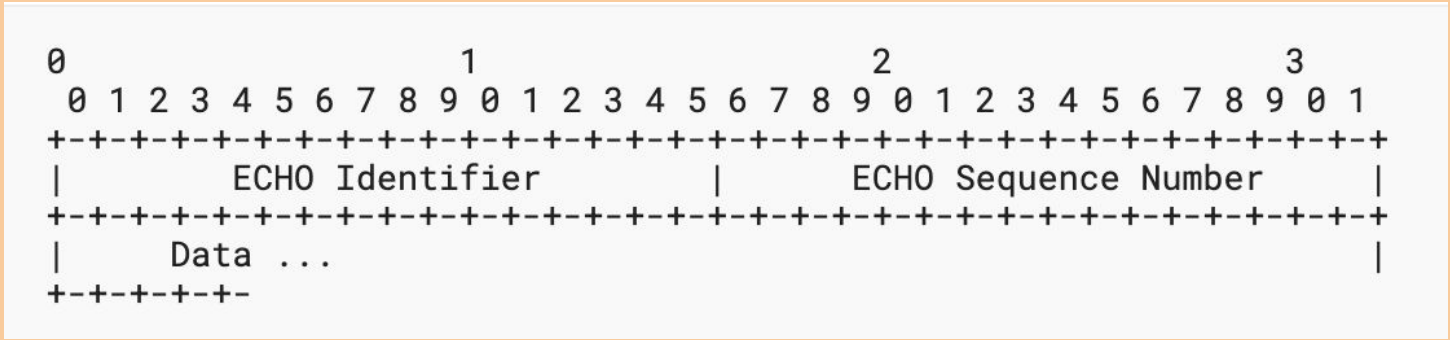
The node MAY send an IPv6 ESP Echo Request packet:

- SPI = 7, Next Header = 59

The peer SHOULD respond with an ESP Echo Reply packet:

- SPI = 8, Next Header = 59
- MUST copy the data from Echo Request up to the MTU

Payload Format (Based on Section 4 RFC4443)



Identifier: Specific to the ESP ping session. Expected to be randomized.

Sequence number: allows matching Echo Requests and Echo Response

Data: May or may not be zero.

Changes to RFC4303: Processing Next Header = 59

RFC4303 "Dummy" packets:

- used for padding
- ESP packets with next header == 59 (no next header)
- A transmitter MUST be capable of generating dummy packets
- a receiver MUST be prepared to discard such packets

Proposed changes:

If a packet with next header == 59 has SPI 7 or 8, then it's an ESP Echo packet and shall be processed as described in this document

Non-Reserved ("Production") SPIs

The proposed mechanism could be extended to "real" SPIs: how would that look?

- Specifically, a next-header of 59 would elicit a response in the paired IPsec SA?
- A Next-Header of ipv6-icmp (58) would elicit a response in the paired IPsec SA?

(do kernels even know what the associated paired IPsec SA is?)

Benefits:

- Preventing MitM attacks (replies are authenticated)
- Fate sharing with actual data flows

However, **such packets are indistinguishable from "dummy"** packets.

Security Considerations

The node MUST NOT fall back to unencrypted mode of communication in case of ESP Echo failure

Preventing a downgrade attack

ESP Echo Request can be used to discover IPsec speaker

….but so can be IKE INIT

Open Questions: Discovering ESP Echo Support

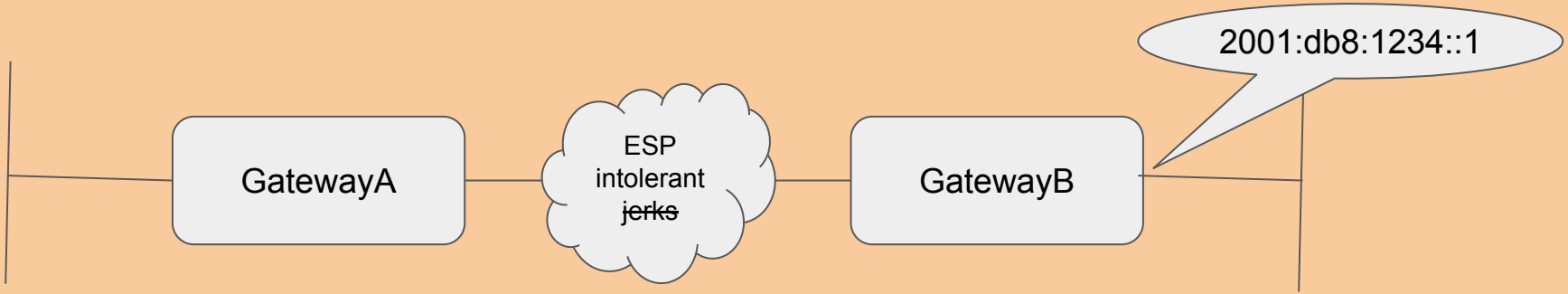
- Explicit (out-of-band) signal
  - E.g. a corporate VPN client is configured to use ESP Echo when connecting to the corporate servers
- **[not in the draft] Announcing ESP Echo support in IKEv2**
  - Is it needed?
  - Worth complexity?

Questions? Comments?

Adoption?

Open Questions: Ways to do ESP Ping within "production" SAs

- An IKEv2 Notify could be created that indicates that the sender is willing to accept ESP packets with {tunnel} mode ICMP(v6) messages.
  - The Notify would indicate an address to which an ICMPv6 message can be addressed that is willing to answer.



Do we need to also indicate a valid source address?