IP Security Maintenance and Extensions
Internet-Draft
Intended status: Standards Track
Expires: 5 October 2025

A. Antony
S. Klassert
secunet

3 April 2025

Encrypted ESP Echo Protocol
draft-ietf-ipsecme-encrypted-esp-ping-00

Abstract

This document defines the Encrypted ESP Echo Function, a mechanism designed to assess the reachability of IP Security (IPsec) network paths using Encapsulating Security Payload (ESP) packets. The primary objective is to reliably and efficiently detect the status of end-to-end paths by exchanging only encrypted ESP packets between IPsec peers. The Encrypted Echo message can either use existing congestion control payloads from RFC9347 or a new message format defined here, with an option to specify a preferred return path when there is more than one pair of IPsec SAs between the same set of IPsec peers.

A peer MAY announce the support using a new IKEv2 Status Notifcation ENCRYPTED_PING_SUPPORTED.

Table of Contents

1. Introduction

In response to the operational need for a robust data-plane failure-detection mechanism for IP Security (IPsec) Encapsulating Security Payload (ESP) from [RFC4303], this document introduces Encrypted ESP Ping, including the Echo Request and Response. This protocol offers a solution for assessing network path reachability dynamically and can optionally specify a return path for echo Reply messages. The IPsec peer may announce its capability to support Encrypted ESP Ping using an IKEv2 Notification Status Type.

This document covers only Encrypted ESP Ping, typically used after an IKE negotiation, while [I-D.colitti-ipsecme-esp-ping] specifies an unauthenticated ESP Ping to be used before IKE negotation.

1.1. Terminology

This document uses the following terms defined in [RFC4301]: Encapsulating Security Payload (ESP), Security Association (SA), Security Policy Database (SPD).

This document uses the following terms defined in [RFC9347]: AGGFRAG tunnel.

This document uses the following terms defined in [RFC7110]: Return Path Specified LSP Ping

2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174]when, and only when, they appear in all capitals, as shown here.

3. Use cases

Diagnosing operational problems in IPsec can be challenging. The proposed Encrypted ESP Echo function aims to address some of these challenges by providing a reliable and efficient diagnostic protocol, enabling the development of effective tools; e.g. Encrypted ESP Ping.

3.1. ESP Blocked or Filtered

An IPsec session typically employs ESP, using IP or IPv6 packets. ESP parameters are negotiated using IKEv2, with default IKEv2 messages exchanged over UDP port 500. In scenarios where ESP packets are not encapsulated in UDP (i.e., using the ESP protocol), successful IKE negotiation may occur, but ESP packets might fail to reach the peer due to differences in the packet path or filtering policies compared to IKE packets (e.g., UDP is allowed while ESP is filtered, typically due to misconfiguration). Additionally, when using UDP encapsulation, ESP packets may encounter different filtering policies. This is typically due to broken packet filtering. Although this is less likely, it is still possible and can be difficult to diagnose. Operational experience suggests that networks and some home routers that drop ESP packets are common enough to cause problems for general- purpose VPN applications that require reliable performance on the Internet. Encrypted ESP Ping would greatly assist in diagnosing these scenarios.

3.2. Probing Multiple Paths

When there are multiple paths created using multiple Child SAs with identical Traffic Selectors as specified in [RFC7296]or more explicitly in [RFC9611], there is a need to probe each Child SA, including the network path, independently from an IPsec peer. Each SA may traverse different network paths and may have different policies. The Encrypted ESP Ping would specifically help determine the reachability of each path independently.

3.3. Probe Return Path

IPsec Security Associations (SAs) are negotiated as a pair, consisting of two unidirectional SAs in one exchange. IKEv2 [RFC7296] Section 2.9 allows installing multiple Child SAs with identical Traffic Selectors. When there are multiple paths, the Encrypted ESP Ping should support requesting an echo response via a specific return path IPsec SA. To request a return path, additional attributes are necessary. The initiator would propose a specific SPI as the preferred return path. A specific return path SPI is necessary when to probe a specific path among multiple possible SAs between same peer. Multiple paths can exist for various reasons, either [RFC9611] or a primary and secondary path scenario. For example over a satellite link and over fiber, the receiving peer may have a policy to respond via the fiber path even when the request arrives via the satellite link. If the initiator requests a return path, the responder SHOULD try to respond via that path, IPsec SA. However, the final decision is up to the responder. If the responder decides to send the response via a different path than the requested return path, the initiator SHOULD notice it and notify the initiator application. An example is Return Path Specified LSP ping specified in [RFC7110].

3.4. Manually Probing a Constant Rate on the AGGFRAG Tunnel

In IPsec setups, maintaining a constant traffic rate can help in disguising actual traffic patterns, providing enhanced security. The AGGFRAG tunnel enables constant rate probing to ensure consistent bandwidth usage, helping to mitigate the risk of traffic analysis by adversaries. This approach is particularly useful to discover possible bandwidth where maintaining a uniform traffic pattern is critical for security, using IP-TFS.

3.5. Why Not Use Existing IP Tools

Existing tools such as ICMP ping or traceroute assume IP connectivity. However, in IPsec gateway setups, the gateway itself may not have an IP address that matches the IPsec Security Policy Database (SPD). A peer MUST accept Encrypted ESP Ping messages even when it does not math a local SPD.

Additionally, in the case of multiple SAs as mentioned above, IP tools would find it hard, if not impossible, to generate IP traffic to explore multiple paths specifically

3.6. Also Track Incoming Traffic for liveness check

In addition to probing the outgoing paths, it is essential to monitor and account for the incoming traffic to ensure comprehensive network visibility of IPsec. Incoming SA traffic counters are unique to IPsec compared to other tunneling or native IP connections. In IPsec, the incoming counters reliably indicate a viable path. This should be taken into account when probing IPsec paths. For example, when the crypto subsystem is overloaded, the responder may miss out on Encrypted ESP Ping responses. However, tracking the incoming traffic after the ping probe is sent would help applications to recognize the IPsec path is still viable.

4. Protocol Specification

In a typical use case, after completing an IPsec SA negotiation, [RFC7296], an IPsec peer wishing to verify the viability of the current network path for ESP packets MAY initiate an ESP Echo Request. The ESP Echo Request packet must be encrypted. If the SPIs are negotiated it SHOULD utilize an SPI value previously negotiated, e.g. negotiated through IKEv2.

The initiator sets the ESP Next Header value to AGGFRAG_PAYLOAD which has the value 144, as specified in [RFC9347]. This can be followed by different echo request sub-type payloads with a well defined format and optional empty data blocks following it.

The receiving IPsec peer, having established ESP through IKE, MAY respond to an ESP Echo Response. When replying to an encrypted ESP Echo Request, the ESP Echo Response MUST be encrypted and utilize the corresponding SPI. The responder also sets the ESP Next Header value to AGGFRAG_PAYLOAD: 144, followed by the requested sub-type

AGGFRAG_PAYLOAD Payload starts from ESP Next Header value: 144 and followed one of the two Request payloads specified.

4.1. Using Congestion Control Payload

IP-TFS Congestion Control AGGFRAG_PAYLOAD Payload Format as specified in [RFC9347] Section 6.1.2 can be used for Echo Request and response. When using this payload for Echo Request and response, IPv4 or IPv6 Data Block MUST NOT be concatenated, especially when USE_AGGFRAG is not successfully negotiated. This this request does not support requesting a specific return path.

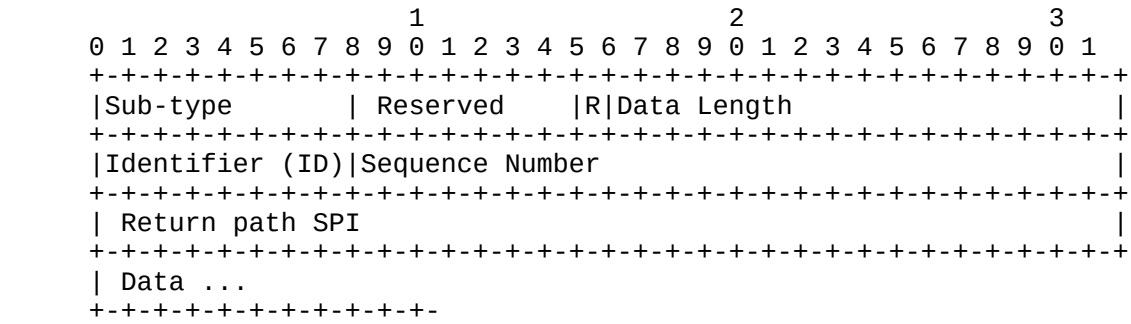
[AA when using USE_AGGFRAG tunnel is negotiated, responder may concatenate AGGFRAG_PAYLOAD Congestion control probe]

The Echo request and response payloads are not subject to IPsec Security Policy(SP), typically negotiated using IKEv2 a nd manually configured. End padding padding would be necessary of the the tunnel is always sending fixed size ESP payload or possibly detect path anomalies.

When probing do not take the lack of a response alone as an indication of the unreachability of the return path using ESP echo; also consider the received bytes on the return path. IPsec has a unique advantage over other tunneling protocols when the return path shows incoming bytes, indicating that the path is partially functional. This is especially useful when used as a liveness check on busy paths. When there is no response, instead of concluding that the path is not viable and taking action, such as tearing down the IPsec connection, read the incoming bytes. This would help avoid tearing down busy paths due to the missing ESP echo response.

4.2. Encrypted ESP Ping Payload Format

Control Payload Format



* Sub-Type: ESP-ECHO-REQUEST or ESP-ECHO-RESPONSE

* Reserved: 7 bits

* Return path: 1 bit flag, set when requesting a specific return path

* Data Length : number of data octets following, length 16 bits

* Identifier : A 16-bit request identifier. The identifier SHOULD be set to a unique value to distinguish between different ESP Request sessions. Response copy it from the request

* Sequence number: A 16-bit field that increments with each echo request sent.

* Return path: 32 bits, optional requested return path SPI, when R is set.

* Data : Optional data that follows the Echo request.

The responder SHOULD copy the request message and MUST change the Sub-type to ESP-ECHO-RESPONSE.

4.3. Return Path Validation

On the initiator, the return path SPI in the request MUST be in the local SADB with the same peer as the destination. The responder should also validate the requested return path SPI. When the SPI does not match the initiator in the SPD, the responder MUST NOT respond via the requested SPI. This is specifically to avoid amplification or DDoS. However,the responder MAY respond to the peer using its default Security Parameter Index (SPI).

5. IKEv2 Notification

The peer MAY announce support for Encrypted ESP Ping functionality using the Notification Status Type ‘ENCRYPTED_PING_SUPPORTED‘ during the IKEv2 negotiation, in the IKE_AUTH exchange. This announcement allows the initiator to determine if the peer supports Encrypted ESP Ping, enabling a reliable expectation of responses.

By advertising this support, peers enhance their ability to perform dynamic path reachability assessments for diagnostic purposes. However, this does not guarantee a response to every request a peer receives. Responding to each request remains a local policy decision, depending on the resources available at the time.

6. IANA Considerations

This document updates [RFC9347] to allow ESP Echo Request and ESP Echo Response without a successful negotiation of USE_AGGFRAG.

This document defines two new registrations for the IANA ESP [AGGFRAG] PAYLOAD Sub-Types.

Value	ESP AGGFRAG_PAYLOAD Sub-Type	Reference
2	ESP-ECHO-REQUEST	[this document]
3	ESP-ECHO-RESPONSE	[this document]

This document defines one new registration for the IANA "IKEv2 Notify Message Status Types" [STATUSNOTIFY].

Value	Notify Message Status Type	Reference
[TBD1]	ENCRYPTED_PING_SUPPORTED.	[this document]

7. Operational Considerations

When an explicit return path is requested and the ESP Echo responder SHOULD make best effort to respond via this path, however, if local policies do not allow this respond via another SA.

A typical implementation involves creating an ESP Echo socket, which allows setting an outgoing SPI during initialization,and matching source and destination address. Once socket is setup before sending any data, only write payload with optionally specifying return path.

8. Acknowledgments

ACKs TBD

9. Security Considerations

The security considerations are similar to other unconnected request-reply protocols such as ICMP or ICMPv6 echo. The proposed ESP echo and response does not constitute an amplification attack because the ESP Echo Reply is almost same size as the ESP Echo Request. Furthermore, this can be rate limited or filtered using ingress filtering per BCP 38 [RFC2827]

10. Normative References

[AGGFRAG] IANA, "ESP AGGFRAG_PAYLOAD Registry", <https://www.iana.org/assignments/esp-aggfrag-payload/esp-aggfrag-payload.xhtml>.

[I-D.colitti-ipsecme-esp-ping] Colitti, L., Linkova, J., and M. Richardson, "ESP Echo Protocol", Work in Progress, Internet-Draft, draft-

colitti-ipsecme-esp-ping-03, 7 November 2024, <https://datatracker.ietf.org/doc/html/draft-colitti-ipsecme-esp-ping-03>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC2827] Ferguson, P. and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", BCP 38, RFC 2827, DOI 10.17487/RFC2827, May 2000, <https://www.rfc-editor.org/info/rfc2827>.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, DOI 10.17487/RFC4301, December 2005, <https://www.rfc-editor.org/info/rfc4301>.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, DOI 10.17487/RFC4303, December 2005, <https://www.rfc-editor.org/info/rfc4303>.

[RFC7110] Chen, M., Cao, W., Ning, S., Jounay, F., and S. Delord, "Return Path Specified Label Switched Path (LSP) Ping", RFC 7110, DOI 10.17487/RFC7110, January 2014, <https://www.rfc-editor.org/info/rfc7110>.

[RFC7296] Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., and T. Kivinen, "Internet Key Exchange Protocol Version 2 (IKEv2)", STD 79, RFC 7296, DOI 10.17487/RFC7296, October 2014, <https://www.rfc-editor.org/info/rfc7296>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8194] Schoenwaelder, J. and V. Bajpai, "A YANG Data Model for LMAP Measurement Agents", RFC 8194, DOI 10.17487/RFC8194, August 2017, <https://www.rfc-editor.org/info/rfc8194>.

[RFC9347] Hopps, C., "Aggregation and Fragmentation Mode for Encapsulating Security Payload (ESP) and Its Use for IP Traffic Flow Security (IP-TFS)", RFC 9347, DOI 10.17487/RFC9347, January 2023, <https://www.rfc-editor.org/info/rfc9347>.

[RFC9611] Antony, A., Brunner, T., Klassert, S., and P. Wouters, "Internet Key Exchange Protocol Version 2 (IKEv2) Support for Per-Resource Child Security Associations (SAs)", RFC 9611, DOI 10.17487/RFC9611, July 2024, <https://www.rfc-editor.org/info/rfc9611>.

[STATUSNOTIFY] IANA, "IKEv2 Notify Message Status Types", <https://www.iana.org/assignments/ikev2-parameters/ikev2-parameters.xhtml#ikev2-parameters-16>.

Appendix A. Additional Stuff

TBD

Authors' Addresses

Antony Antony
secunet Security Networks AG
Email: antony.antony@secunet.com

Steffen Klassert
secunet Security Networks AG
Email: steffen.klassert@secunet.com