IPsec BEET Mode

draft-antony-ipsecme-beet-mode

IETF 118, November 2023

Antony Antony, Steffen Klassert

secunet

Goal

- Standardize IPsec BEET Mode with IKEv2
  - This has been in use for over 10 years
  - Overlooked RFC 7402 Appendix : BEET defined

History 2003 – 2009

- IETF draft-nikander-esp-beet-mode-09 expired!
  - Then HIP working group (not in IPsecME)
- Code was accepted to Linux Kernel

  Usage increased over time.

2010 - 2015

- RFC 7402 defined BEET mode in Appendix B
  - Without IKEv2

Current Use cases

- For End-to-end tunnels BEET saves bytes.
  - About 20 bytes for IPv4 (without IPv4 options)
  - 40 bytes for IPv6
- HIP RFC 7402, RFC 5202
  - Note HIP use without IKE?
- Minimal IPsec RFC 9333
- Are there more use cases that should be covered?

Software support

- Linux initial commit 2006
  - Linux kernel sees several related fixes
- strongSwan supports using private IKE Notify
- iproute2 command line tool to setup SA
  - (ip xfrm)

Next steps

- Update ID with RFC 7402 focusing on IKEv2
  - Mobile IP use cases : keep or remove?
  - NAT Use cases : keep or remove?

Questions?

- Are there any other use cases of BEET mode?
- Any other BEET mode issue to address at IETF?

BEET Pseudo-Header(PH)
esp → nextheader =94?

- Only used for IPv4 with Options or fragments.

- Linux Heders: include/uapi/linux/in.h

IPPROTO_BEETPH = **94** /* IP option pseudo header for BEET */

IPPROTO_IPIP = 4 /* IPIP tunnels (older KA9Q tunnels use 94). */

- IANA Protocol Numbers

94 IPIP IP-within-IP Encapsulation Protocol

4 IPv4 IPv4 encapsulation [RFC2003]

Backup : transport mode fragments

RFC 4301 Section 4.1

“Note: AH and ESP cannot be applied using transport mode

to IPv4 packets that are fragments. Only tunnel mode can be employed in such cases. For IPv6, it would be feasible to carry a plaintext fragment on a transport mode SA; however, for simplicity, this restriction also applies to IPv6 packets.”

Backup : IANA : 94

https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml

Decimal, Keyword,Protocol,IPv6 Extension Header, Reference

94, IPIP,IP-within-IP Encapsulation Protocol, “[John_Ioannidis]”
4,IPv4 IPv4 encapsulation, [RFC2003],

[John_Ioannidis] John Ioannidis mailto:ji&tla.org 2015-01-06