Internet Engineering Task Force
INTERNET DRAFT
Expires in August 2001

Francis Dupont
ENST Bretagne
February 22. 2001

Mobility-aware IPsec ESP tunnels

<draft-dupont-movesptun-00.txt>

Status of this Memo

This document is an Internet Draft and is in full conformance with all provisions of Section 10 of RFC 2026.

This document is an Internet-Draft. Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

Distribution of this memo is unlimited.

Abstract

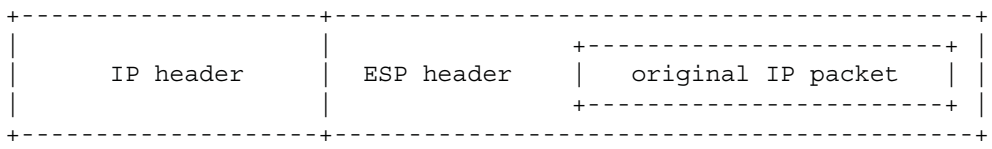
A common usage of IPsec is bidirectional ESP tunnels (secure Virtual Private Networks): the original packet is encapsulated in a new IP header and protected (ESP can provide confidentiality, authentication, integrity and anti-replay) by IPsec ESP (in tunnel mode).

This conflicts with all mobility devices [ID1, ID2] which are based on addresses for no good reasons when some of these mobility devices should be able to use the four addresses in the two headers.

This document tries to solve this conflict in order to make secure and mobile supports colaborating, ie. to pay for the two features only once.

1. Introduction

IPsec [RFC 2401] defines Encapsulation Security Payload (ESP) [RFC 2406] tunnel mode as an encapsulation of an original/inner IP packet in an outer IP packet:



Address based mobility protocols use two addresses for a mobile node:
- the home address which is static but virtual
- a care-of address which is temporary but denotes the current position of the mobile node.

These protocols can use options (source routing header and home address destination option) for the optimized version or a tunnel for the unoptimized version. Both versions apply the same rules:
- the mobile node should send packets with a care-of address as the outer source and the home address as the inner source.
- a correspondent node should send packets with a care-of address as the outer destination and the home address as the inner destination.

If an ESP tunnel is already used we want to add no option or new encapsulation. If security and mobility protocols can colaborate we shall get mobility support without overhead. This document describes how this colaboration can be archieved: packets are transported as for ESP tunnels, IPsec and mobility signaling control together outer addresses.

2. IPsec issues

IPsec specifications [RFC 2401] do not mandate any check of the outer source address in incoming processing but many implementations do this kind of check. They are (still) compliant but they cannot interoperate if the source address can change, ie. with an address based mobility device or a Network Address Translator.

There is no real issue with Internet Key Exchange [RFC 2409]
but the phase one is done with a care-of address then:
- the lifetime of ISAKMP Security Association built by the
  phase one should be in the same order than the lifetime of
  the care-of address.
- the care-of address should not be used in an Identity payload
  (ie. user_FQDN Identity payload is recommended for phase one).
- in some case the care-of address of the peer is not known then
  the initiator should be the mobile node.

In phase two the home-address should be used in the Identity payload,
the policy should tie the phase one identity with the home-address in
order to authorize the setup and update of proper IPsec SAs.

The PF_KEY API [RFC 2367] defines identities and addresses (three
kind of addresses, source, destination and proxy) for SAs.
For a mobile node the care-of address is the source and
the home address the proxy according to section 5.2 example.
The current specifications need to be updated in order to
provide a way to update the source or the destination address.

There is not yet a PF_POLICY document but the requirements are
exactly the same than for PF_KEY: the source or the destination
address of the outer headers must be updatable.

3. Signaling

Address based mobility protocols manage a care-of/home address
pair on both ends of a mobility session. In the case covered
by the document this pair is the outer/inner source address pair
on the mobile node, the outer/inner destination address pair
on the correspondent node.

The signaling function provides a way to update the care-of address
in this pair on correspondent nodes when the mobile node has moved,
ie. has acquired a new care-of address.

If the signaling is done inline, ie. signaling protocol elements
are transported through the ESP tunnel from the mobile node to
a correspondent, then ESP must provide authentication, integrity
check and anti-replay protection.

The signaling responder on correspondents MUST interoperate with
IPsec management, for instance using standard extended APIs like
PF_KEY as decribed before.

4. Extensions

Most of this document was written with bidirectional tunnels in mind but it can be applied in the unidirectional case where previous issues are less critical but still exist.

AH in tunnel mode is not commonly used but this document applies to it too. The only difference is that AH protects the whole outer header, including the outer source address.

5. Security Considerations

Signaling devices have some security requirements which can be provided by ESP.

The correspondent policy have to authorize both the setup of SAs negociated by an initiator using a (a priori random) care-of address and the update of the mobile node outer address in these SAs.

6. Acknowledgements

I would like to thank Richard Draves (Microsoft Research) to point to that the interaction between mobile IPv6 and IPsec is near a complete disaster and something must be done.

7. References

[ID1] D. Johnson, C. Perkins, "Mobility Support in IPv6", draft-ietf-mobileip-ipv6-13.tx, work in progress, November 2000.

[ID2] F. Dupont, "IPv6 over IPv4 tunnels for home to Internet access", draft-ietf-ngtrans-hometun-01.txt, work in progress, November 2000.

[RFC 2401] S. Kent, R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[RFC 2406] S. Kent, R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, November 1998.

[RFC 2409] D. Harkins, D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[RFC 2367] D. McDonald, C. Metz, B. Phan, "PF_KEY Key Management API, Version 2", RFC 2367, July 1998.

8. Author's Address

Francis Dupont
ENST Bretagne
Campus de Rennes
2 rue de la Chataigneraie
BP 78
35512 Cesson-Sevigne Cedex
FRANCE
Fax: +33 2 99 12 70 30
EMail: Francis.Dupont@enst-bretagne.fr

Expire in 6 months (August 22, 2001)