Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 22, 2010

G. Daley
NetStar Networks

October 19, 2009

MPLS Label Traffic Selectors for Internet Key Exchange Version 2
draft-daley-mpsec-label-ts-00.txt

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

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.

This Internet-Draft will expire on April 22, 2010.

Copyright Notice

Abstract

Existing mechanisms for encapsulating MPLS labels in ESP or AH payloads lack the ability to specify which Labels are to be transported.

This document provides new traffic selector format for IKEv2 in which MPLS label fields and parameters can be selected.

Table of Contents

1. Introduction

Carrying MPLS Label payloads in IPsec requires a mapping between the ingress interface and Label carriage which is typically determined by a label distribution protocol. While this is the case, it is important to specify the label to IPSec Security Association mappings especially where data encapsulated by one label requires different protection to that encapsulated by another.

One IETF Standards Track RFC currently specifies carriage of MPLS Labels in ESP or AH payloads [RFC4023]. The specification for "Encapsulating MPLS in IP or GRE" [RFC4023] identifies that labels are to be carried in Transport Mode by specifiying the source and destination addresses as well as the protocol field being set to 137 with IKEv1 or IKEv2 [RFC2409][RFC4306]. It does not specify which labels receive protection by an SA.

At this stage, additional specification of label header fields is not feasible with IKEv1, but IKEv2 allows specification of new traffic selector types. This document specifies a new format for traffic selectors in IKEv2, to be used in conjunction with existing uses of MPLS and IPSec.

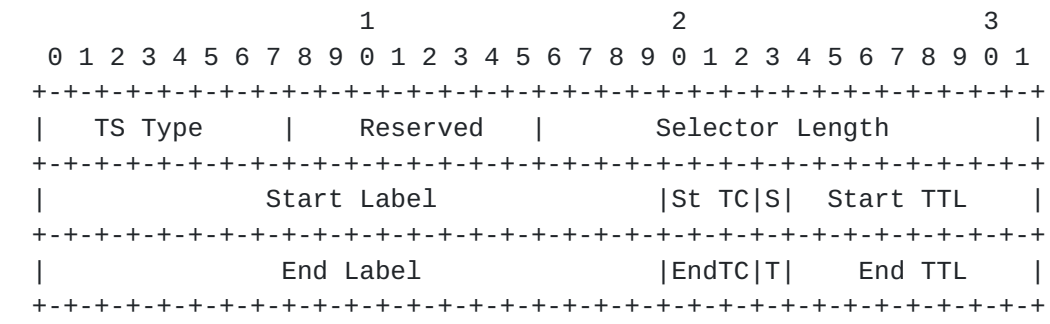
The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2. Traffic Selector Format

In order to allow for efficient expression of decorrelated selectors, each element from the MPLS Label are expressed in the traffic selector as ranges [RFC3032][RFC5462].

Each of these values parameters may be expressed as a single value, a range, or the symbolic values ANY or OPAQUE, as specified in [RFC4301].

The traffic selector format follows the IKE version 2 specification, and is presented below:



Label Traffic Selector

The TS Type for this traffic selector is TBD. The Selector Length is 12. TS Type specific fields are detailed below.

Start Label, End Label: The selected Label range is specified by the Start and End Label fields.

Size : 20 bits

MINIMUM: 0

MAXIMUM: 1048575

ANY : Start Label=0, End Label=1048575

OPAQUE : Start Label=1048575, End Label=0

St TC, EndTC: The selected Quality of Service Traffic class is specified by the St TC (Start Traffic Class) and EndTC (End Traffic Class) fields.

Size : 3 bits

MINIMUM: 0

MAXIMUM: 7

ANY : St TC=0, EndTC=7

OPAQUE : St TC=7, End TC=0

S, T: The selected Top of Stack identified is specified by the 'S' (Start Top of Stack) and 'T' (End Top of Stack) fields.

Size : 1 bit

MINIMUM: 0

MAXIMUM: 1

ANY : S=0, T=1

OPAQUE : S=1, T=0

Start TTL, End TTL: The selected Time-To-Live values for the next MPLS Label are specifies in the Start TTL and End TTL fields.

Size : 8 bits

MINIMUM: 0

MAXIMUM: 255

ANY : Start TTL=0, End TTL=255

OPAQUE : Start TTL=255, End TTL=0

Behaviour of the ANY and OPAQUE Values as specified here operate as specified in [RFC4301]. When specifying a traffic selector, all sub fields (except Reserved) must be specifically set. For fields where the value doesn't matter, the pair of fields should be set to specify ANY.

Where a packet is to be transmitted or recived upon an SA derived from traffic selection using this TS Type, the encapsulated Label's fields MUST match the accepted policy as specified in the IKEv2 negotiation. Packets which do not match specification MUST be discarded in accordance with [RFC4301].

Where multiple fields (for example Label Value and Traffic Class), are set as specified ranges, the recipient MUST check that both constraints are met by incoming labels.

3. Security Policy Database Considerations

In order to express the Label which is required for protection, it may be necessary to augment Security Policy Database elements. This would allow initiation of negotiation of an SA upon reception of an interesting packet, or upon reception of a Label signalling message that specified a label matching the policy.

4. IANA Considerations

This document describes a new traffic selector payload for IKEv2 and its use.

Traffic selectors are defined by IANA Expert Review. This document will be submitted for expert review and selector allocation upon a subsequent draft submission.

Until submission implementations should use one of the Private Use selectors. The suggested value is 250. Please note that implementations would have to update to a new value when allocated under IANA.

5. Security Considerations

The traffic selector format defined in this document omits the source and destination IP addresses, which are used within ingress packet checks within IPSec. This is less expressive than in traditional IPSec.

This is probably acceptable for the following reasons:

- Source and Destination IP addresses may be inferred from the Key Exchange conversation itself.

- Label exchanges are typically performed by another protocol which itself presents the endpoint IP addresses.

As previously described [RFC4023], external MPLS Label exchange mechanisms MUST use authentication mechanisms. For targetted Label Distribution Protocol, it is suggested that SAs are established using IKE to protect the LDP signalling (on TCP and UDP port 646) [RFC5036].

6. Acknowledgments

Simon De Lord and Raymond Key contributed to the development of the Traffic Selection problem statement which motivated this specification. Thanks to Tero Kivinen who provided initial input on the format of the field ranges.

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3032] Rosen, E., Tappan, D., Fedorkow, G., Rekhter, Y., Farinacci, D., Li, T., and A. Conta, "MPLS Label Stack Encoding", RFC 3032, January 2001.

[RFC4023] Worster, T., Rekhter, Y., and E. Rosen, "Encapsulating MPLS in IP or Generic Routing Encapsulation (GRE)", RFC 4023, March 2005.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[RFC4306] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.

[RFC5036] Andersson, L., Minei, I., and B. Thomas, "LDP Specification", RFC 5036, October 2007.

[RFC5462] Andersson, L. and R. Asati, "Multiprotocol Label Switching (MPLS) Label Stack Entry: "EXP" Field Renamed to "Traffic Class" Field", RFC 5462, February 2009.

7.2. Informative References

[RFC2409] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

Author's Address

Greg Daley
NetStar Australia Pty Ltd
Lvl 9/636 St Kilda Rd
Melbourne, Victoria 3004
Australia

Phone: +61 401 772 770
Email: gdaley@netstarnetworks.com