

Network  
Internet-Draft  
Updates: [7296](#) (if approved)  
Intended status: Standards Track  
Expires: September 5, 2018

S. Prasad  
Technical University of Munich  
P. Wouters  
Red Hat  
March 4, 2018

**Labeled IPsec Traffic Selector support for IKEv2**  
**draft-sprasad-ipsecme-labeled-ipsec-00**

Abstract

Some IPsec implementations support Security Labels otherwise known as Security Contexts, to be configured as a selector within the Security Policy Database (SPD) for IPsec SAs. This document adds support to IKEv2 to negotiate these Security Labels or Contexts using a new Traffic Selector (TS) Type TS\_SECLABEL. The approach is named "Labeled IPsec". It assumes that the SPD processing of [RFC 4303](#) is already extended to support Security Labels. This document only adds the ability for IKE to negotiate the Security Labels used with the SPD.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

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."

This Internet-Draft will expire on September 5, 2018.

Copyright Notice

Copyright (c) 2018 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents

carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

<a href="#">1.</a>	Introduction . . . . .	<a href="#">2</a>
<a href="#">1.1.</a>	Requirements Language . . . . .	<a href="#">3</a>
<a href="#">2.</a>	Labeled IPsec Traffic Selector . . . . .	<a href="#">3</a>
<a href="#">2.1.</a>	Narrowing of Labeled IPsec Traffic Selector . . . . .	<a href="#">4</a>
<a href="#">3.</a>	Security Considerations . . . . .	<a href="#">4</a>
<a href="#">4.</a>	IANA Considerations . . . . .	<a href="#">5</a>
<a href="#">5.</a>	References . . . . .	<a href="#">5</a>
<a href="#">5.1.</a>	Normative References . . . . .	<a href="#">5</a>
<a href="#">5.2.</a>	Informative References . . . . .	<a href="#">5</a>
	Authors' Addresses . . . . .	<a href="#">5</a>

## [1.](#) Introduction

A Security Context or Security Label is a mechanism used to classify resources. It allows the enforcement of rules on how or by whom these resources are accessible. This document introduces a mechanism to negotiate these values using IKE. This negotiation is done via a new Traffic Selector (TS) Type in the TSi/TSr Payloads of the IKE\_AUTH Exchange.

Traffic Selector (TS) payloads allow endpoints to communicate some of the information from their SPD to their peers. [Section 2.9](#) in the Internet Key Exchange protocol version 2 [[RFC7296](#)] illustrates the Traffic selector negotiation procedure.

Two or more TS payloads appear in each of the messages in the exchange that creates a Child SA pair. Each TS payload contains one or more Traffic Selectors. The Traffic Selector types TS\_IPV4\_ADDR\_RANGE and TS\_IPV6\_ADDR\_RANGE consists of an address range, a port range, and an IP protocol ID. [[RFC4595](#)] defines Traffic Selector type TS\_FC\_ADDR\_RANGE to denote a list of Fibre Channel (FC) addresses and protocol ranges. This document extends the above set by adding a new TS Type that allows endpoints to agree on assigning a Security Label or Context to the IPsec SA.

Negotiating and applying the Security Label or Context in the new TS Type will act as an additional selector criterium that has to match along with any other existing Traffic Selectors.

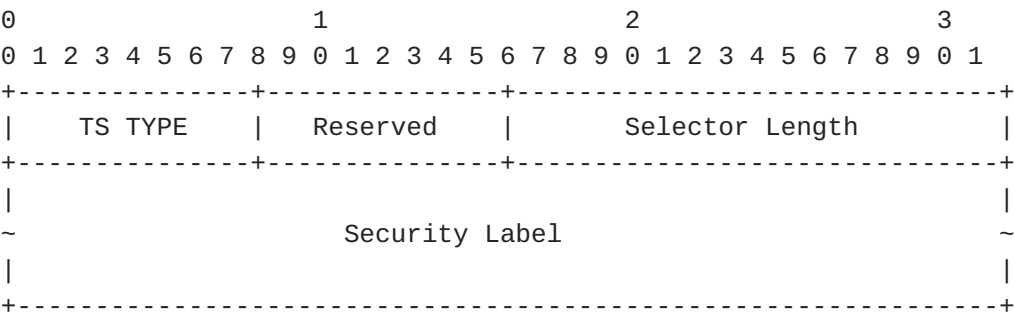


1.1. Requirements Language

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. Labeled IPsec Traffic Selector

Labeled IPsec Traffic Selectors allow endpoints to negotiate the Security Label using the Selector Type TS\_SECLABEL. In addition to the regular processing of Traffic Selectors as described in [Section 3.13.1 of \[RFC7296\]](#), the context or label of an IP packet now also has to match the Security Label Traffic Selector.



- o TS TYPE (one octet) - Specifies the type of Traffic Selector.
- o Selector Length (2 octets, network byte order) - Specifies the length of Security Label including the header.
- o Security Label - This field contains the opaque payload.

The following table lists the assigned value for the Labeled IPsec Traffic Selector Type field:

TS Type	Value
-----	-----
TS_SECLABEL	[TBD]

To indicate support and a requirement for agreeing on a specific security context, the initiator MUST include the security context or label via TS\_SECLABEL in the TSi (Traffic Selector-initiator) and TSr (Traffic Selector-responder) Payloads. On reception of TS\_SECLABEL, the responder MUST find a matching Security Policy Database (SPD) entry that contains a Security Label and match the proposed label. Assuming that this proposal was acceptable to the responder, it would send the same or narrowed TS payloads in the IKE\_AUTH reply. If the



Security Label was not found in the SPD by the responder, it MUST respond with a TS\_UNACCEPTABLE Notify message.

As per [section 2.9.2 in \[RFC7296\]](#), TS sets MUST BE kept identical during rekey. If a Security Label needs to change, the IPsec SA must be torn down and a new one must be negotiated with the updated TS\_SECLABEL values.

### **2.1. Narrowing of Labeled IPsec Traffic Selector**

The IKE daemon might or might not be able to interpret the Security Label beyond an exact match. It might be possible for the IKE daemon to apply narrowing to the Security Labels. For example, a Security Label "Top Secret" could mean that this IPsec SA may also transport traffic with label "Secret". An initiator requesting "Top Secret" might be willing to be narrowed down to a "Secret" security context. Or a security context of "\*" might mean "any security context". If the daemon does not interpret the Security Label, then it can only support an exact match of the raw data of the TS.

The rules of responder narrowing as explained in [section 2.9 in \[RFC7296\]](#) are applicable to TS\_SECLABEL.

The TS\_SECLABEL Traffic Selector Type if present MUST be mutually agreed upon. If one side includes a TS\_SECLABEL and the other side does not, the IPsec SA negotiation MUST fail with TS\_UNAVAILABLE. If a responder insists on a TS\_SECLABEL security context and receives a TSi/TSr set that does not contain a TS\_SECLABEL Traffic Selector, it MUST fail the negotiation with TS\_UNAVAILABLE.

DISCUSS: Should a TS\_SECLABEL of length 0 be allowed? If so, should it mean "any label" ?

### **3. Security Considerations**

While matching the Security Label on the endpoints, an assumption that the Security label will contain only ASCII text MUST NOT be made. If the Security Label is handed off to a helper routine for interpretation, it MUST be assumed that the content can be malicious. While Security Labels might look like text, there is no guarantee this text is null terminated.

Any errors in handling the SPD entry, such as failing to add the SPD entry with the negotiated Security Label, MUST be able as any other failure of SPD processing as defined in [\[RFC4303\]](#).



#### **4. IANA Considerations**

This document defines one new Traffic Selector Type in the IKEv2 Traffic Selector Types Registry namespace.

TS Type	Value
-----	-----
TS_SECLABEL	[TBD]

Figure 1

#### **5. References**

##### **5.1. Normative References**

- [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>>.
- [RFC4595] Maino, F. and D. Black, "Use of IKEv2 in the Fibre Channel Security Association Management Protocol", [RFC 4595](#), DOI 10.17487/RFC4595, July 2006, <<https://www.rfc-editor.org/info/rfc4595>>.
- [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>>.

##### **5.2. Informative References**

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

#### **Authors' Addresses**

Sahana Prasad  
Technical University of Munich

Email: [sahana.prasad07@gmail.com](mailto:sahana.prasad07@gmail.com)





Paul Wouters  
Red Hat

Email: [pwouters@redhat.com](mailto:pwouters@redhat.com)