Network
Internet-Draft
Intended status: Standards Track
Expires: September 11, 2019

P. Wouters
Red Hat
S. Prasad
Technical University of Munich
March 10, 2019

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

Abstract

This document defines two new Traffic Selector (TS) Types for Internet Key Exchange version 2 to add support for Mandatory Access Control (MAC) security labels, also known as "Labeled IPsec". The two new TS Types are TS_IPV4_ADDR_RANGE_SECLABEL and TS_IPV6_ADDR_RANGE_SECLABEL, which are identical to their non-seclabel namesakes except for the addition of a variable length opaque field specifying the security label. These new Traffic Selector Types facilitate negotiating security labels as an additional selector of the Security Policy Database to further restrict the type of traffic allowed to be send and received over the IPsec SA.

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 http://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 11, 2019.

Copyright Notice

Table of Contents

1. Introduction 2
1.1. Requirements Language 3
2. Traffic Selector negotiation 3
3. SECLABEL Traffic Selector 3
4. Traffic Selector matching 5
5. Security Considerations 6
6. IANA Considerations 6
7. Acknowledgements 6
8. References 6
8.1. Normative References 6
8.2. Informative References 7
Authors' Addresses 7

1. Introduction

In computer security, Mandatory Access Control usually refers to systems in which all subjects and objects are assigned a security label. A security label is comprised of a set of security attributes. The security labels along with a system authorization policy determine access. Rules within the system authorization policy determine whether the access will be granted based on the security attributes of the subject and object.

Traditionally, security labels used by Multilevel Systems (MLS) are comprised of a sensitivity level (or classification) field and a compartment (or category) field, as defined in [FIPS188] and [RFC5570]. As MAC systems evolved, other MAC models gained in popularity. For example, SELinux, a Flux Advanced Security Kernel (FLASK) implementation, has security labels represented as colon-separated ASCII strings composed of values for identity, role, and type. The security labels are often referred to as security contexts.

This document specifies two new Traffic Selector Types for IKEv2 that can be used to negotiate security labels as additional selectors for the Security Policy Database (SPD) to further restrict the type of traffic allowed to be send and received over the IPsec SA.

Traffic Selector (TS) payloads allow endpoints to communicate some of the information from their SPD to their peers. These must be communicated to IKE from the SPD. TS payloads specify the selection criteria for packets that will be forwarded over the newly set up SA. Section 2.9 in the Internet Key Exchange protocol version 2 [RFC7296] illustrates the Traffic Selector negotiation procedure.

Two 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. Currently, each Traffic Selector consists of an address range (IPv4 or IPv6), a port range, and an IP protocol ID. However, a security context or a label is missing. Therefore this document extends the section 2.9 in the Internet Key Exchange protocol version 2 [RFC7296] to add support for a new traffic selector type which would be used to negotiate the security label or context.

Negotiating and verifying the security context or label in the new TS types will act as an additional criteria that has to match along with the previously mentioned 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. Traffic Selector negotiation

The negotiation of Traffic Selectors is specified in Section 2.9 of [RFC7296]. The initiating IKE peer sends a Traffic Selector payload for the initiator side (TSi) and a Traffic Selector payload for the responder side (TSr). The TSi and TSr payloads contain a list of one or more Traffic Selectors (TS). The responder picks one TS from the TSi list and one TS from the TSr list and returns these in their own TSi/TSr payloads to the initiator in the IKE response as confirmation of the chosen traffic selectors. [RFC7296] defines two TS Types, TS_IPV4_ADDR_RANGE and TS_IPV6_ADDR_RANGE. These TS payloads contain the TS Type, IP protocol ID, Selector Length, Start and End Port and Start and End Address.

3. SECLABEL Traffic Selector

This document defines two new TS Types, TS_IPV4_ADDR_RANGE_SECLABEL and TS_IPV6_ADDR_RANGE_SECLABEL. In addition to the above mentioned selectors, it contains a single new opaque Security Label selector.

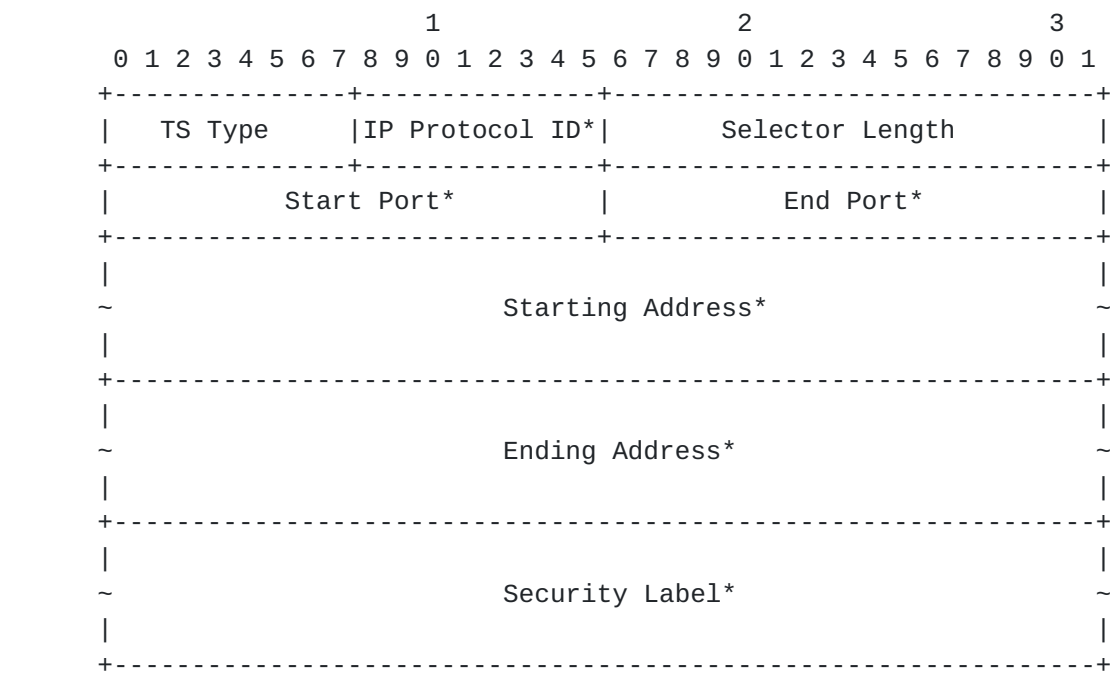

Figure 1: Labeled IPsec Traffic Selector

*Note: All fields other than TS Type and Selector Length depend on the TS Type. The fields shown are for TS Types [TBD] and [TBD], the two values this document defines.

- TS Type (one octet) - Specifies the type of Traffic Selector.

- IP protocol ID (1 octet) - Value specifying an associated IP protocol ID (such as UDP, TCP, and ICMP). A value of zero means that the protocol ID is not relevant to this Traffic Selector -- the SA can carry all protocols.

- Selector Length (2 octets, unsigned integer) - Specifies the length of this Traffic Selector substructure including the header.

- Start Port (2 octets, unsigned integer) - Value specifying the smallest port number allowed by this Traffic Selector. For protocols for which port is undefined (including protocol 0), or if all ports are allowed, this field MUST be zero. ICMP and ICMPv6 Type and Code values, as well as Mobile IP version 6 (MIPv6) mobility header (MH) Type values, are represented in this field as specified in Section 4.4.1.1 of [RFC4301]. ICMP Type and Code values are treated as a single 16-bit integer port number, with Type in the most significant eight bits and Code in the least significant eight bits. MIPv6 MH Type values are treated as a single 16-bit integer port number, with Type in the most

significant eight bits and the least significant eight bits set to zero.

- End Port (2 octets, unsigned integer) - Value specifying the largest port number allowed by this Traffic Selector. For protocols for which port is undefined (including protocol 0), or if all ports are allowed, this field MUST be 65535. ICMP and ICMPv6 Type and Code values, as well as MIPv6 MH Type values, are represented in this field as specified in Section 4.4.1.1 of [RFC4301]. ICMP Type and Code values are treated as a single 16-bit integer port number, with Type in the most significant eight bits and Code in the least significant eight bits. MIPv6 MH Type values are treated as a single 16-bit integer port number, with Type in the most significant eight bits and the least significant eight bits set to zero.

- Starting Address - The smallest address included in this Traffic Selector (length determined by TS Type).

- Ending Address - The largest address included in this Traffic Selector (length determined by TS Type).

- Security Label - An opaque byte stream of at least one octet.

4. Traffic Selector matching

Matching of the IP protocol, start and end address, and start and end port is performed the same way as for the TS_IPV4_ADDR_RANGE and TS_IPV6_ADDR_RANGE TS types. Additionally, the Security Label is compared for an exact match as well. Label matching is done by comparing the opaque bytestream.

The Security Label in the TSi and TSr MUST be identical. If the responder's policy does not allow it to accept any part of the proposed Traffic Selector including the Security Label, it MUST ignore the TS and look for another matching TS in the list. If no list entry matches, a TS_UNACCEPTABLE Notify message is returned.

A zero length Security Label MUST NOT be sent. If the SPD policy contains no Security Label selectors, the TS Types TS_IPV4_ADDR_RANGE_SECLABEL and TS_IPV6_ADDR_RANGE_SECLABEL should not be used and TS_IPV4_ADDR_RANGE and TS_IPV6_ADDR_RANGE should be used instead. Any received Traffic Selector with a zero length Security Label MUST be ignored, and if no valid TS can be selected, an TS_UNACCEPTABLE Error Notify message is returned. A zero length Security Label MUST NOT be interpreted as a wildcard security label.

If multiple Security Labels are allowed for a given IP protocol, start and end address/port match, multiple TS_IPV4_ADDR_RANGE_SECLABEL or TS_IPV6_ADDR_RANGE_SECLABEL Traffic Selectors must be included that only differ in the Security Label.

Narrowing of Traffic Selectors applies to TS_IPV4_ADDR_RANGE_SECLABEL and TS_IPV6_ADDR_RANGE_SECLABEL as well, but the Security Label itself is not interpreted and cannot itself be narrowed. It MUST be matched exactly. Rekey of an IPsec SA MUST only use identical Traffic Selectors, which means the same TS Type and selectors MUST be used. This guarantees that a Security Label once negotiated, remains part of the IPsec SA after a rekey.

5. Security Considerations

It is assumed that the Security Label can be matched by the IKE implementation to its own configured value, even if the IKE implemention itself cannot interpret the Security Label value.

6. IANA Considerations

This document defines two new entries in the IKEv2 Traffic Selector Types registry:

Value	TS Type	Reference
TBD	TS_IPV4_ADDR_RANGE_SECLABEL	[this document]
TBD	TS_IPV6_ADDR_RANGE_SECLABEL	[this document]

Figure 2

7. Acknowledgements

A large part of the introduction text was taken verbatim from [draft-jml-ipsec-ikev2-security-label] whose authors are J Latten, D. Quigley and J. Lu. Part of the Traffic Selector description is reproduced from [RFC7296].

8. References

8.1. 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>.

[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>.

8.2. Informative References

[draft-jml-ipsec-ikev2-security-label] Latten, J., Quigley, D., and J. Lu, "Security Label Extension to IKE", draft-wouters-edns-tcp-keeaplive (work in progress), January 2011.

[FIPS188] NIST, "National Institute of Standards and Technology, "Standard Security Label for Information Transfer"", Federal Information Processing Standard (FIPS) Publication 188, September 1994.

[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>.

[RFC5570] StJohns, M., Atkinson, R., and G. Thomas, "Common Architecture Label IPv6 Security Option (CALIPSO)", RFC 5570, DOI 10.17487/RFC5570, July 2009, <https://www.rfc-editor.org/info/rfc5570>.

Authors' Addresses

Paul Wouters
Red Hat

Email: pwouters@redhat.com

Sahana Prasad
Technical University of Munich

Email: sahana.prasad07@gmail.com