

Network Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: April 29, 2010

G. Daley  
NetStar Networks  
S. Delord  
R. Key  
Telstra  
S. Krishnan  
Ericsson  
October 26, 2009

Guidelines for Multiprotocol Traffic Selector Bindings in IPsec  
draft-daley-mpsec-traffic-sel-ps-01.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/lid-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 29, 2010.

Copyright Notice

Copyright (c) 2009 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 in effect on the date of publication of this document (<http://trustee.ietf.org/license-info>). Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

## Internet-Draft Multiprotocol Traffic Selector Guidelines October 2009

## Abstract

In IPsec, secure connectivity is provided for network layer entities. Traffic Selectors which specify interesting traffic for security association encapsulation are identified only by network and transport layer addressing.

This document discusses extending traffic selectors to allow more generic definitions of interesting traffic.

## Table of Contents

<a href="#">1.</a>	Introduction . . . . .	<a href="#">3</a>
<a href="#">2.</a>	Description and Models . . . . .	<a href="#">3</a>
<a href="#">3.</a>	Related work . . . . .	<a href="#">5</a>
<a href="#">4.</a>	Applicability . . . . .	<a href="#">5</a>
<a href="#">5.</a>	Security Policy Database Considerations . . . . .	<a href="#">6</a>
<a href="#">6.</a>	IKEv2 Considerations . . . . .	<a href="#">6</a>
<a href="#">6.1.</a>	Selector Format Considerations . . . . .	<a href="#">7</a>
<a href="#">7.</a>	IPsec Mode Considerations . . . . .	<a href="#">7</a>
<a href="#">8.</a>	Backward Compatibility . . . . .	<a href="#">7</a>
<a href="#">9.</a>	Discussion of Initiator/Responder Mappings . . . . .	<a href="#">8</a>
<a href="#">10.</a>	External Interface Considerations . . . . .	<a href="#">9</a>
<a href="#">11.</a>	IANA Considerations . . . . .	<a href="#">10</a>
<a href="#">12.</a>	Security Considerations . . . . .	<a href="#">10</a>
<a href="#">13.</a>	Acknowledgments . . . . .	<a href="#">11</a>
<a href="#">14.</a>	References . . . . .	<a href="#">11</a>
<a href="#">14.1.</a>	Normative References . . . . .	<a href="#">11</a>
<a href="#">14.2.</a>	Informative References . . . . .	<a href="#">11</a>
	Authors' Addresses . . . . .	<a href="#">13</a>

---

Internet-Draft Multiprotocol Traffic Selector Guidelines October 2009

## 1. Introduction

IPsec is focused on providing tunnel and transport security for network layer IP traffic based on IP address and port selectors. In some circumstances, endpoints may wish to provide IPsec services based on other distinguishing information from the traffic stream [[RFC4301](#)].

This document discusses models, motivations, for multiprotocol bindings for IPsec Traffic Selectors, their use in the Security Policy Database (SPD) and their description within IKEv2 [[RFC4306](#)] [I-D.ietf-ipsecme-roadmap].

## 2. Description and Models

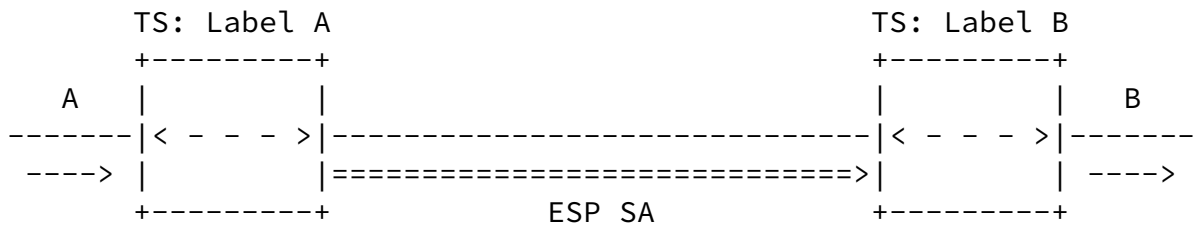
Devices which may prefer to choose extended traffic selector syntax may support non-IP protocols for packet delivery or may have non-Address and port information used in traffic selection for IP layer traffic.

### Example 1 MPLS Label

Where an MPLS label either arrives from an interface, or is used to encapsulate traffic, it may be useful to transport data carried within that label across the network.

At this stage, advice is sought on how encapsulation would occur, and whether the communications path connecting A and B would make use of an MPLS label inside the ESP label.

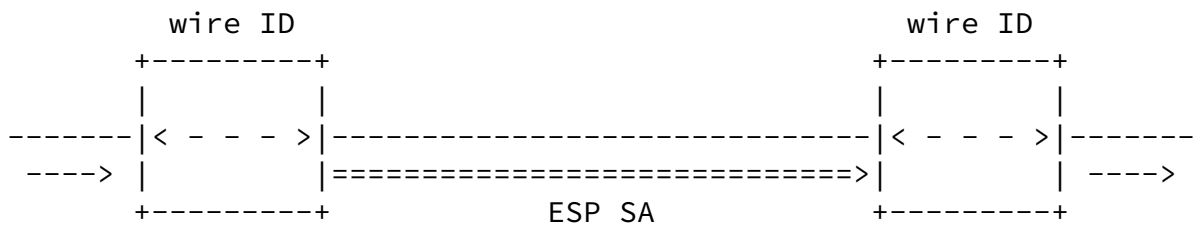
Similar to Diffserv in Example 1, the Traffic Class field of the MPLS label stack entry [[RFC5462](#)] may be used for traffic selectors.



## Example 2 Ethernet Pseudo Wire

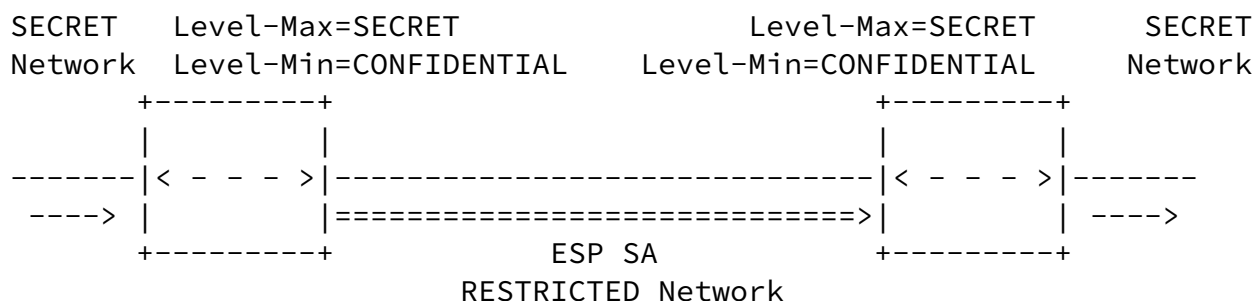
For systems which do not contain IP addresses on the traffic side (rather than the carriage side), there is currently no way to specify IPsec connectivity across to a remote device. This may be the case with Pseudo-wires which have shared identifiers, that are known at provisioning time.

Allowing data associated with a particular interface group to be encapsulated in protocols such as ESP, would provide a mechanism to deliver secured pseudo wires.



## Example 3 Security Classification Option

It is necessary under some security regimes to ensure that traffic of specific security classifications are encrypted before transportation over media of a lower protection value [[DSDISMu](#)]. Explicit marking the classifications packets is provided by IPSO in IPv4 [[RFC1108](#)] and CALIPSO in IPv6 [[RFC5570](#)].



### Use of classification levels in traffic selectors

The figure above shows the interconnection of two SECRET classified networks over a lower security medium, using a negotiated encrypted tunnel. It shows transmission of data classified in a range between CLASSIFIED and SECRET, as shown within the Classification Level field of the IPSO basic security option [[RFC1108](#)].

Use of the explicit labelling may provide a natural control point for

the encapsulation of data onto IPSec tunnels, or in filtering packets arriving from such a tunnel.

### 3. Related work

An Informational specification is available which shows how Fiberchannel Addressing can be used for traffic selectors in [[RFC4595](#)]. In [Section 4.4](#), it defines TS\_FC\_ADDR\_RANGE, which uses ranges of Fiberchannel addresses where other previously defined methods have used IP addresses.

[RFC 4595](#) also specifies transport of ESP (and AH) frames over Fiberchannel encapsulation. Within this document discussion of carriage of IKEv2, ESP and AH over non IP or IP/UDP transport is out-of-scope.

Descriptions of challenges and mechanisms for provisioning security on Pseudo-wires are available in [[PWESECREQ](#)][PWESEC]. This document takes a different approach to previous pseudo-wire security mechanisms in that it attempts to provide a more general key derivation mechanism for data other than pseudo-wires. Additionally,

this document doesn't seek to provide a non-IP carriage for ESP and ESP-like frames, as is the case in [[PWESEC](#)].

Ways of identifying security classifications within IKEv2 exchanges are described within [[I-D.jml-ipsec-ikev2-security-context](#)]. This mechanism proposes a Security Context Transform, which could instead be expressed within a Traffic-Selector type.

It is notable that there exist link-layer encryption mechanisms available via IEEE LAN/MAN 802.1 Working Group [[DOT1ae](#)][DOT1XREV]. This work doesn't seek to supplant existing link-layer security mechanisms, but does seek to allow for use of secured transports for non-IP data such as link-layer frames when used within the IPsec framework.

#### [4.](#) Applicability

This document aims at identifying practices for defining extended traffic selectors. It also explores alternative encoding mechanisms and their impact on policy expression in IKEv2.

This document does not define encapsulation of ESP or AH protocols over any new protocols, and only defines/discusses what may be encapsulated by them.

#### [5.](#) Security Policy Database Considerations

Security Policy Databases provide expressions of the encryption and authentication policy on IPsec hosts and gateways. SPDs are referenced as part of packet delivery processes in order to match packets either to a constructed SA, or to the key-deriving system (such as IKEv2), based on interesting traffic matches.

Databases therefore require an interface for packet processes when transmitting data [[USAGIXFRM](#)], configuration interfaces through which to construct policy [[RFC4807](#)][IPSECSPOL][[SETKEY](#)], and key derivation interfaces to ensure that policy is expressed through to the remote peer during the key exchange.

At this stage, specification of inter device communication operations

using IKEv2 is necessary if support for extended traffic selectors is to be provided.

## 6. IKEv2 Considerations

As a departure from IKE [[RFC2407](#)], IKEv2 specifies traffic selectors separate to identifiers [[RFC4306](#)], including for IPv4 and IPv6.

In order to provide more general mapping for traffic selectors to non-IP sources and destinations, Traffic Selector Type (TS Type) allocation needs to be made. The existing TS Type space is administered by IANA. As of April 2009 there are 230 allocatable values within the space.

Along with a selector type allocation the format within IKEv2 and interpretation of each traffic selector require specification. This either requires a specific Traffic Selector option format, or a general format which can express additional classes of information.

If a more expressive format were to be used, the syntax of this format could be used for the IPSO, MPLS Labels, or Pseudo-wire interchangeably. An endpoint which could understand the format, but could not support a particular selector could down select or reject the proposal.

[RFC4807](#) Specifies an SNMP MIB for IPsec Security Policies [[RFC4807](#)]. Within the specification is a mechanism to describe in ASN.1 encoding for IP Address and DSCP based traffic selectors [[RFC3289](#)]. Were the same encoding used for IKEv2 as the MIB, new object identifiers would need to be added, but the format would be predetermined.

Another alternative is to use an XML Schema, although the mechanism

would have to be able to present a single canonical syntax for a specific policy.

### 6.1. Selector Format Considerations

IKE Version 2 discusses security association rule ordering issues which arise when one traffic selection expression overlaps with another (selector correlation) [[RFC4306](#)]. The decorrelation

algorithm provides a means to identify non-overlapping subsets of the selected traffic.

Key to being able to express decorrelated selectors is that all fields which may be selected need to be expressed as ranges.

As such all selectable subfields within an MPLS Label would require expression as start and end-range values. Similarly, locally significant Pseudo-Wire Identifiers (PWids) make use of two integer based values, a fixed length Group ID and fixed length Pseudo Wire Identifier (PWid) [[RFC4447](#)].

Conversely encoded within the LDP formats for Generalized Pseudowire Identifiers have varying length bitstrings with data encoded within them. Similarly, IPSO and CALIPSO have bit fields which are a structured data representation within fixed fields.

These systems are not able to express these values easily as a range, which allows for easy decorrelation.

## 7. IPsec Mode Considerations

When constructing more elaborate traffic selectors for IKEv2, it is expected that the tunnel mode will be provided for traffic which doesn't travel within IP-layer packets.

Traffic selectors for data carried within IP packets may still be carried in Transport Mode, for example if DSCPs are used for selectors. This requires further investigation.

## 8. Backward Compatibility

One advantage of IPsec is that traffic descriptors for IPv4 and IPv6 are available across the majority of existing implementations. Introduction of multiple subsets of Traffic Selectors which are optional to implement may cause compatibility issues.

Security Policy Database entries for IPsec devices support IPv4 and



static Security Associations, or are defined in conjunction with IKEv2 policy [[RFC4301](#)][RFC4306].

Where keying and SA configuration are static, it is possible that traffic sent on an SA from a device supporting (and using) extended Traffic Selectors will be rejected upon reception at the far end SA. The reverse case (with legacy implementation ingress and general traffic selector egress) would have equivalent function, with only the intersection of the traffic selectors being allowed through to the remote site.

Without an IKEv2 control channel this is not easily remedied. Similar issues regarding persistent differences in configuration are described in [[RFC4306](#)]. In the case that IKEv2 is used for key negotiation, a system which supports only IPv4, IPv6 or Fiber Channel Traffic Selectors will not be able to choose a traffic selector from the extended mechanisms.

This may lead to Security Associations to fail completely, in conformance to the IKEv2 protocol [[RFC4306](#)].

## 9. Discussion of Initiator/Responder Mappings

Existing traffic selectors are for connectionless source and destinations. Assignment of multiple selectors to each of the initiator and responder is appropriate for such traffic. For systems which provide connection oriented point-to-point service, multiple sources and destinations are inappropriate. In such a case, there needs to be a one-to-one mapping between initiator and responder traffic selectors.

Expressed in existing IKEv2 syntax, it is not possible to describe within a single CHILD\_SA Security Association Initiator and Responder Traffic Selectors elements which are mutually exclusive.

For example, if:

TSi is the set [ 192.0.2.0/26, 192.0.2.128/26 ]  
and TSr set is [ 192.0.2.64/26, 192.0.2.192/26 ]

It is not possible to express in a single CHILD\_SA or IKEv2 which has the properties that only:

192.0.2.0/26 ==> 192.0.2.128/26 (A)  
and  
192.0.2.64/26 ==> 192.0.2.192/26 (B)  
  
while  
192.0.2.0/26 !=> 192.0.2.192/26  
and  
192.0.2.64/26 !=> 192.0.2.128/26

In order to allow only a single source and destination mapping within IKEv2's syntax, the only way to specify mappings (A) and (B) are via two separate SAs. For point-to-point circuit oriented connections such as pseudo-wires, given [RFC 4306](#) IKEv2 syntax, would require an SA per source, destination pair.

As described in [Section 4.4.1.2 of RFC4301](#), the structure of SPDs identified within that system allows for multiple Selector Sets which may be included into a single security association. As discussed within that document, in order to provision selector sets dynamically, changes need to be made within IKEv2.

At this stage, provisioning one circuit per SA is described, although it is worth identifying if selector sets are viable under revision of the specification.

## [10.](#) External Interface Considerations

Referral of packets to the security policy database is typically undertaken as a forwarding (routing) process in existing networks [[RFC4301](#)]. Defining Traffic Selectors with non-IP address components means that a different non-forwarding process may be invoked to refer to the SPD.

When the forwarding process accesses the SPD, there is a transform on a received packet which determines whether the traffic is interesting to send over IPsec. This will either invoke the IKEv2 key negotiation process, or assign the data to a security association (as described in [Section 2.9 of RFC 4306](#) [[RFC4306](#)]).

For forwarding and processes referring to the modified Security Policy Database, there needs to be a mechanism which allows the match new Traffic Selector attributes. This match process would then be used as above, to invoke IKEv2 or to assign data for transmission.

If individual mechanisms are defined through the process described

below, each Traffic Selector Definition will require specification not only of the type, and its expression within IKEv2, but also the

Internet-Draft Multiprotocol Traffic Selector Guidelines October 2009

filtering and operational processes required to achieve effective traffic protection [[RFC4306](#)].

Depending on the mechanisms defined for expressing extended traffic selectors, a general filtering mechanism may be defined which allows new selection filters to be applied to the SPD, and exchanged over IKEv2 using the Traffic Selector Payload [[RFC2819](#)]. The expressibility of the Traffic Selectors must then be matched by the filter mechanism, and map from the presented packet information to a PROTECT operation [[RFC4301](#)].

Existing interfaces between the Security Policy Database and the key management process make implicit assumptions that the Traffic Selectors are IP addresses [[RFC2367](#)]. Modifications to such mechanisms may need to occur before existing APIs may be used with new traffic selectors.

## [11.](#) IANA Considerations

No new formats or messages are defined in this document.

In order to allocate a new traffic selector class, it is necessary to receive a traffic selector type allocation from IANA [[RFC4306](#)][IANAIKEV2]. This requires Expert Review by an IANA identified resource, who would be able to understand the use case, and whether the allocation should occur.

## [12.](#) Security Considerations

Definition of new traffic selectors for non-IP traffic isn't a significant departure from IKEv2's security model. The identity associated with the communications, and the source and destination of the tunnel headers do not change. Only the traffic identified for transport changes.

Where non-IP datagrams are exchanged over ESP or AH tunnels, the behavior may be different to IP. When providing connectivity through

the IPsec tunnels for physical or link-layer technologies, the tunnel itself may establish alternative paths in the wider topology.

Where the tunneled lower layer traffic expands on an existing infrastructure, there is a chance of loop creation. Unless tunnel endpoints deploy mechanisms to prevent loops, data transfer through the tunnel could be used to trivially deny service to devices on the tunnel path, and the networks at either end.

Where more complex filter patterns are expressible within the Traffic Selector IKEv2 payload, they may require decoding by an external parser. Where an external parser for a language such as ASN.1 or XML is in use, there are additional interfaces to exploit, and a more complex structure to keep state about. The cost of this additional risk needs to be balanced against the value in expressing more complex policy.

### [13.](#) Acknowledgments

Thanks to Dave Thaler for his discussion of Traffic Selector tuples, and to Tero Kivinen and Stephen Kent for their contributions on expression of ranges in traffic selectors.

### [14.](#) References

#### [14.1.](#) Normative References

- [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.
- [RFC4807] Baer, M., Charlet, R., Hardaker, W., Story, R., and C. Wang, "IPsec Security Policy Database Configuration MIB", [RFC 4807](#), March 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.

#### [14.2](#). Informative References

[IANAIKEV2]

IANA, "<http://www.iana.org/assignments/ikev2-parameters>".

[IPSECSPOL]

"[http://developer.apple.com/documentation/Darwin/Reference/Manpages/man3/ipsec\\_set\\_policy.3.html](http://developer.apple.com/documentation/Darwin/Reference/Manpages/man3/ipsec_set_policy.3.html)".

[SETKEY]

"<http://linux.die.net/man/8/setkey>".

[USAGIXFRM]

Kanda, M., Miyazawa, K., and H. Esaki, "IPsec Security Policy Database Configuration MIB, USAGI IPv6 IPsec

Daley, et al.

Expires April 29, 2010

[Page 11]

---

Internet-Draft Multiprotocol Traffic Selector Guidelines October 2009

development for Linux. Applications and the Internet Workshops, 2004. SAINT 2004 Workshops".

[DOT1ae]

"<http://standards.ieee.org/getieee802/download/802.1AE-2006.pdf>".

[DOT1XREV]

"<http://www.ieee802.org/1/pages/802.1x-rev.html>".

[DSDISMu]

"Australian Government Information Security Manual (ISM)", Infosec policy The Australian Government Information and Communications Technology Security Manual, September 2009.

[I-D.ietf-ipsecme-roadmap]

Frankel, S. and S. Krishnan, "IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap", [draft-ietf-ipsecme-roadmap-01](#) (work in progress), March 2009.

[I-D.jml-ipsec-ikev2-security-context]

Latten, J., Wilson, G., Hallyn, S., and T. Jaeger, "Security Context Addendum to IPsec", [draft-jml-ipsec-ikev2-security-context-01](#) (work in progress), July 2009.

- [PWESEC] Stein, Y(J)., "Pseudowire Security (PWsec)", [draft-stein-pwe3-pwsec-00](#) (work in progress), October 2006.
- [PWESECREQ] Stein, Y(J)., "Requirements for PW Security", [draft-stein-pwe3-sec-req-01](#) (work in progress), February 2007.
- [RFC1108] Kent, S., "U.S", [RFC 1108](#), November 1991.
- [RFC2819] Waldbusser, S., "Remote Network Monitoring Management Information Base", STD 59, [RFC 2819](#), May 2000.
- [RFC2367] McDonald, D., Metz, C., and B. Phan, "PF\_KEY Key Management API, Version 2", [RFC 2367](#), July 1998.
- [RFC2407] Piper, D., "The Internet IP Security Domain of Interpretation for ISAKMP", [RFC 2407](#), November 1998.
- [RFC3289] Baker, F., Chan, K., and A. Smith, "Management Information Base for the Differentiated Services Architecture", [RFC 3289](#), May 2002.

Daley, et al.

Expires April 29, 2010

[Page 12]

---

Internet-Draft Multiprotocol Traffic Selector Guidelines October 2009

- [RFC4447] Martini, L., Rosen, E., El-Aawar, N., Smith, T., and G. Heron, "Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)", [RFC 4447](#), April 2006.
- [RFC4595] Maino, F. and D. Black, "Use of IKEv2 in the Fibre Channel Security Association Management Protocol", [RFC 4595](#), July 2006.
- [RFC5570] StJohns, M., Atkinson, R., and G. Thomas, "Common Architecture Label IPv6 Security Option (CALIPSO)", [RFC 5570](#), July 2009.

#### Authors' Addresses

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](mailto:gdaley@netstarnetworks.com)

Simon Delord  
Telstra  
242 Exhibition St  
Melbourne, VIC 3000  
Australia

Email: [simon.a.delord@team.telstra.com](mailto:simon.a.delord@team.telstra.com)

Raymond Key  
Telstra  
242 Exhibition St  
Melbourne, VIC 3000  
Australia

Email: [raymond.key@team.telstra.com](mailto:raymond.key@team.telstra.com)

Suresh Krishnan  
Ericsson  
8400 Decarie Blvd.  
Town of Mount Royal, QC  
Canada

Phone: +1 514 345 7900 x42871  
Email: [suresh.krishnan@ericsson.com](mailto:suresh.krishnan@ericsson.com)

