LABELED IPSEC

IPsec, IETF 106
November, 2019

Sahana Prasad, Red Hat

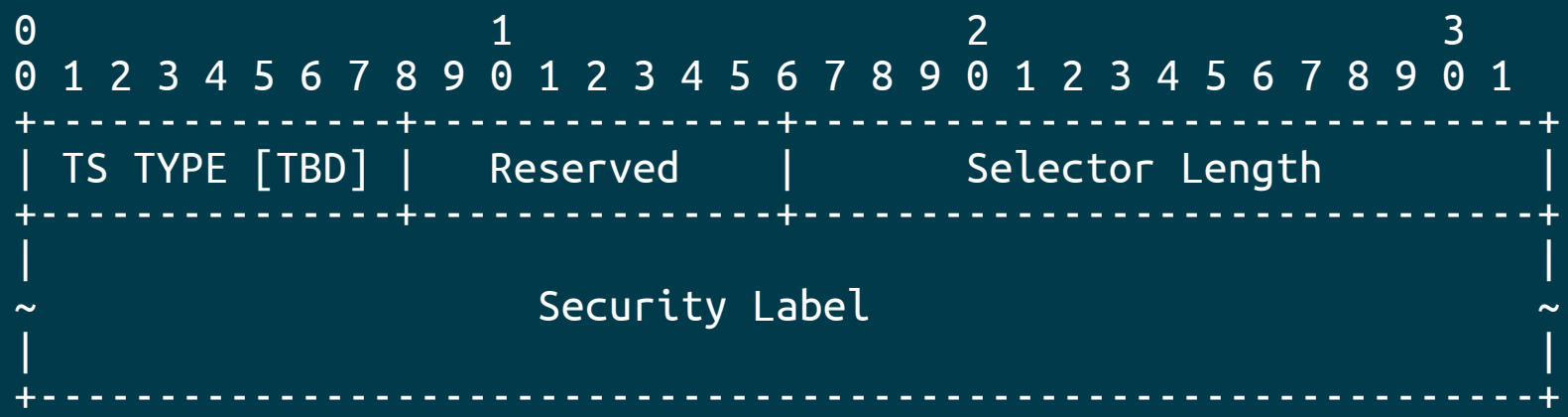
Paul Wouters, Red Hat

Example SPD Linux kernel

```
# ip xfrm pol
src 192.0.1.0/24 dst 192.0.2.0/24
        security context system_u:object_r:test_spd_t:s0
        dir out priority 4294964199 ptype main
        tmpl src 192.1.2.45 dst 192.1.2.23
                proto esp reqid 16389 mode tunnel
src 192.0.2.0/24 dst 192.0.1.0/24
        security context system_u:object_r:test_spd_t:s0
        dir fwd priority 4294964199 ptype main
        tmpl src 192.1.2.23 dst 192.1.2.45
                proto esp reqid 16389 mode tunnel
src 192.0.2.0/24 dst 192.0.1.0/24
        security context system_u:object_r:test_spd_t:s0
        dir in priority 4294964199 ptype main
        tmpl src 192.1.2.23 dst 192.1.2.45
                proto esp reqid 16389 mode tunnel
```

draft-sprasad-ipsecme-labeled-ipsec-00

Add a new IKEv2 traffic selector type:

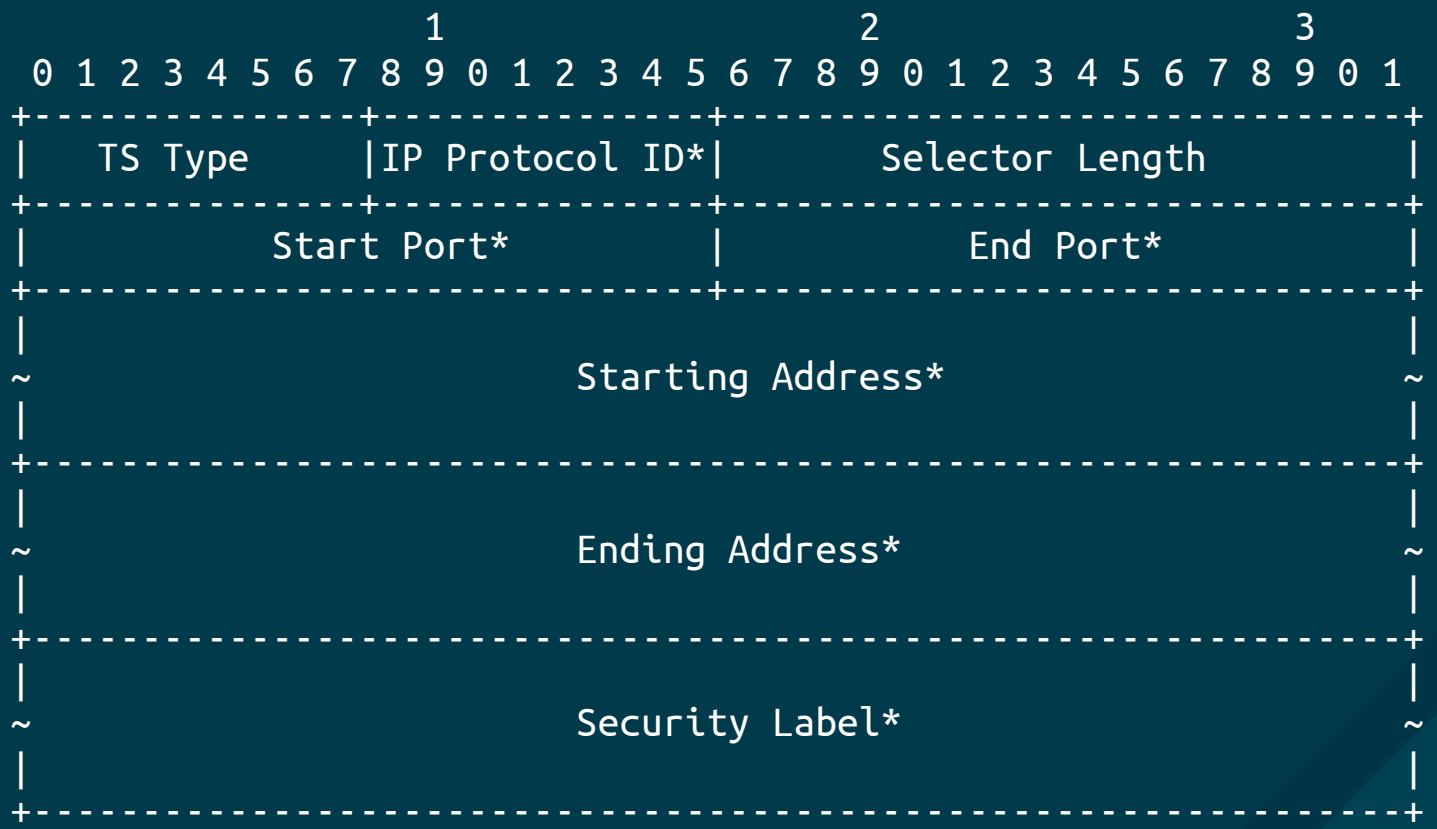


- TS TYPE (one octet) - Specifies the type of Traffic Selector.
- Selector Length (2 octets, network byte order) - Specifies the length of Security Label including the header.
- Security Label - This field contains the opaque payload.

draft-ietf-ipsecme-labeled-ipsec-00

Add two new IKEv2 traffic selector types:

- TS_IPV4_ADDR_RANGE_SECLABEL
- TS_IPV6_ADDR_RANGE_SECLABEL



redhat. | libreswan

RFC 7296 TS negotiation

- Initiator MUST send one or more TS_IPV4_ADDR_RANGE or TS_IPV6_ADDR_RANGE per TSi/TSr
- Initiator MAY additionally send other TS TYPEs (one or more of each TS TYPE)
- Responder MUST pick one or more TS per TSi/TSr TS_IPV4_ADDR_RANGE and/or TS_IPV6_ADDR_RANGE
- Responder drops (narrows) any TS TYPE it does not support
- Should this be interpreted as OR or as AND

RFC 7296 TS negotiation

- Initiator MUST send one or more TS_IPV4_ADDR_RANGE or TS_IPV6_ADDR_RANGE per TSi/TSr
- Initiator MAY additionally send other TS TYPEs (one or more of each TS TYPE)
- Responder MUST pick one or more TS per TSi/TSr TS_IPV4_ADDR_RANGE and/or TS_IPV6_ADDR_RANGE
- Responder drops (narrows) any TS TYPE it does not support
- Should this be interpreted as OR or as AND

Please pick one

- A new notify payload with SECLABEL
  - Was not in any draft
- A new TS TYPE with modified RFC 7296 TS negotiation
  - draft-ietf-ipsecme-labeled-ipsec-02
- A new V4+SECLABEL / V6+SECLABEL type
  - draft-sprasad-ipsecme-labeled-ipsec-00