Labeled IPSEC

IPsec, IETF 101
March 23, 2018

Sahana Prasad, Technical University of Munich
Paul Wouters, RHEL Security
History of Labeled IPsec

- Available as selector option in the SPD in Linux since 2.6.x
- Available in IKEv1 using libreswan in RHEL7, RHEL6 and with openswan in RHEL5
- Squatted on IANA “IPSEC Security Association Attributes” with value 10
- Value 10 was assigned to ECN Tunnel
- Moved to private use number 32001
- use secctx-attr-type=32001 (or 10 for backwards compatibility)
- No method to negotiate security context using IKEv2
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
Add a new IKEv2 traffic selector type:

<table>
<thead>
<tr>
<th>TS TYPE [TBD]</th>
<th>Reserved</th>
<th>Selector Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Label</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- 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.
Open issues

• Should we allow sub-types for Label kind?
• MUST label be identical for inbound/outbound?
• Should we allow a NULL label (length=0) ?
  • What would that mean?
• Should we allow label narrowing if the IKE daemon understands the label blob ?
  • narrow “system_u” to “system_u:object_r:bin_t:s0” ?