Labeled IPSEC

IPsec, IETF 104
March, 2019

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
• use secctx-attr-type=32001 (or 10 for backwards compatibility)
• No method to negotiate security context using IKEv2

• There was a previous attempt to standardize this: draft-jml-ipsec-ikev2-security-label

• First draft: https://tools.ietf.org/html/draft-sprasad-ipsecme-labeled-ipsec
• Second draft: https://tools.ietf.org/html/draft-ietf-ipsecme-labeled-ipsec
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:

| 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. |
Add two new IKEv2 traffic selector types:
- TS_IPV4_ADDR_RANGE_SECLABEL
- TS_IPV6_ADDR_RANGE_SECLABEL

<table>
<thead>
<tr>
<th>TS Type</th>
<th>IP Protocol ID*</th>
<th>Selector Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Port*</td>
<td>End Port*</td>
<td></td>
</tr>
<tr>
<td>Starting Address*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ending Address*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Label*</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Is this really the best way?

We will need other selectors too.

- VXLANID / VNI
- Queue Pair (QP) for Infiniband

We don’t want combinatory explosion of TS TYPES? what if in the future we need a TS to cover:

10.0.1.2 port 4789 to 10.0.1.3 port 4789 with VNI 13 using seclabel “foo”?
Change TS negotiation?

• Initiator MUST send one or more TS_IPV4_ADDR_RANGE or TS_IPV6_ADDR_RANGE

• Initiator MAY additionally send other TS TYPEs (one or more of each TS TYPE)

• Responder MUST pick one TS_IPV4_ADDR_RANGE or TS_IPV6_ADDR_RANGE

• Responder MUST pick one of each other TS TYPE (which may or may not support narrowing). If unknown TS TYPE, it MUST return TS_UNAVAILABLE.

• Then SECLABEL can be its own TS TYPE as we had originally
CLAP please