strongSwan - Feature #92
IPv6 and %defaultroute
24.09.2009 05:16 - Grigory Ivanov

<table>
<thead>
<tr>
<th>Status:</th>
<th>Closed</th>
<th>Start date:</th>
<th>24.09.2009</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
<td>Due date:</td>
<td></td>
</tr>
<tr>
<td>Assignee:</td>
<td></td>
<td>Estimated time:</td>
<td>0.00 hour</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td>5.0.0</td>
<td>Resolution:</td>
<td>Fixed</td>
</tr>
</tbody>
</table>

Description

In a mixed IPv4+IPv6 dynamic address environment IPSEC/IPv6 is not usable. Configurations like:

```
conn my
  left=%defaultroute
  leftcert=mycert.pem
  right=%any
  type=transport
  auto=add
```

will match only IPv4 left address. «right=%any6» will break configuration completely with error «address family inconsistency in connection».

So there should be magic value like %defaultroute6 to automatically match IPv6 local address.

But sometimes (I could not figure why) %defaultroute matches IPv6 address. So, to safeguard configuration from suddenly stop working, there should be value like «%defaultroute4» which will only match IPv4 addresses. Or, more better, some option like «addressfamily» should be invited to unambiguously clarify for which address family this connection definition would match.

Related issues:

- Related to Feature #196: Add support for right=%any (for auto=route) - Closed 18.06.2012

History

#1 - 24.09.2009 10:29 - Andreas Steffen

If you have the option, try the more advanced IKEv2 charon daemon with the configuration which should automatically find a matching network interface (IPv4 or IPv6) depending on the route to the destination.

```
conn my
  left=%any
  leftcert=mycert.pem
  right=%any
  type=transport
  keyexchange=ikev2
  auto=add
```

#2 - 24.09.2009 16:34 - Grigory Ivanov

Unfortunately, some of my peers uses only IKEv1 (racoon).

#3 - 26.09.2009 13:28 - Grigory Ivanov

I have tried to use IKEv2/IPv6 between two strongswans on identical debian systems.

```
# ipsec version
Linux strongSwan U4.3.2/K2.6.30-1-686
Institute for Internet Technologies and Applications
University of Applied Sciences Rapperswil, Switzerland
See 'ipsec --copyright' for copyright information.
```

ipsec.conf:
config setup
  nat_traversal=no
  charonstart=yes
  plutostart=no
  charondebug="dnm 2, mgr 2, ike 2, chd 2, job 2, cfg 2, knl 2, net 2, lib 2"

conn my
  left=%any6
  leftcert=mycert.pem
  right=%any6
  type=transport
  keyexchange=ikev2
  auto=add

ipsec-tools.conf:

  flush;
  spdflush;
  spdadd -6 ::/0 2000::/3 any -P out ipsec
    esp/transport//use;
  spdadd -6 ::/0 ::/0 any -P in ipsec
    esp/transport//use;

Then I ping one machine from another. Ping goes normally, but ping initiator gets following errors in syslog:

charon: 03[KNL] received a XFRM_MSG_ACQUIRE
charon: 03[KNL] XFRMA_TMP
charon: 10[CFG] trap not found, unable to acquire reqid 0

Ping receiver logs is silent. No IPSEC SA is made:

ping initiator:

```
# setkey -D
  esp mode=transport spi=0x00000000 reqid=0x00000000
  seq=0x00000000 replay=0 flags=0x00000000 state=larval
diff: 17(s) hard: 30(s) soft: 0(s)
last: hard: 0(s) soft: 0(s)
current: 0(bytes) hard: 0(bytes) soft: 0(bytes)
allocated: 0 hard: 0 soft: 0
sadb_seq=0 pid=1340 refcnt=0
```

ping receiver:

```
# setkey -D
No SAD entries.
```

The only thing about «traps» I found in documentation, is
«auto = ignore | add | route | start […] route loads a connection and installs kernel traps.»

I tried to use «auto = route» and got following on initiator side:

charon: 03[KNL] received a XFRM_MSG_ACQUIRE
charon: 03[KNL] XFRMA_TMP
charon: 16[MGR] created IKE_SA
charon: 16[IKE] unable to initiate to %any
charon: 16[MGR] checkin and destroy IKE_SA
charon: 16[MGR] check-in and destroy of IKE_SA successful

No ping replies, no packets really sent to network.
Nor this works with explicitly assigned left addresses. The only configuration which works is in examples — explicitly assigned both right/left addresses and both certificates (otherwise there will be AUTHENTICATION_FAILED error).

Is charon really works with dynamic addresses?

#4 - 14.06.2012 16:04 - Pavel Šimerda
I'd like to ask if this is still the case.

#5 - 15.06.2012 10:59 - Tobias Brunner
What do you mean? The initial question about %defaultroute vs. IPv6, or that strongSwan can't initiate to %any? The former is the case for IKEv1 with versions before 5.0.0, for IKEv2 %any/%any6 can be used and with 5.0.0 %defaultroute is actually an alias for %any. The latter is still the case as we currently don't consider the addresses in the acquire generated by the kernel. Releases since 4.4.1 (i.e. newer than what was used here) actually won't allow you to install trap policies with right=%any.

#6 - 18.06.2012 10:16 - Pavel Šimerda
I am trying to monitor IPv6-related bugs in various software packages we have in Fedora. This issue has apparently been open for years, so I'm curious about the current status. As I'll be upgrading to 5.0.0 soon, I'm more curious about bugs that get into 5.0.0.

#7 - 18.06.2012 10:26 - Grigory Ivanov
Since strongswan was unusable in dynamic ipv6 environment, and developers seems to not interested in resolving such issues, I had begun using "racoon". Which works perfectly with IPv6. I do not know whether this problem is relevant to this day. Its too difficult to set up testing environment, just to confirm abandoned ticket.

#8 - 18.06.2012 11:11 - Pavel Šimerda
Racoon is a no-go for us because of lack of IKEv2 and overly difficult setup of more than just simple transport/tunnel. Strongswan is tested with IPv6. See http://data.pavlix.net/devconf/2012/

#9 - 18.06.2012 11:23 - Grigory Ivanov
Racoon worked, strongswan not. Support of IKEv2 is irrelevant at such angle.

Yes, it is unfortunate that Racoon does not support IKEv2. But at least it works. Racoon2 supports IKEv2, but I have not tried it yet.

#10 - 18.06.2012 11:26 - Tobias Brunner
- Status changed from New to Closed
- Target version set to 5.0.0
- Resolution set to Fixed

The problem is not IPv6 support per se but the support or right=%any (or %any6 for that matter). This is due to the long abandoned support for opportunistic encryption and something like groups (FreeS/WAN supported the configuration of IP ranges, or at least subnets, to which a tunnel was to be established based on traffic). Due to the fact that prior to 5.0.0 strongSwan used two IKE daemons this was not that easy to implement as the kernel's SPD and SAD were not exclusively managed by any one daemon. But guess we could add a similar feature in the future.

I added a new ticket #196 which addresses this and will close this ticket now as the problem with %defaultroute is fixed with 5.0.0.

#11 - 18.06.2012 11:42 - Pavel Šimerda
I'm sorry for misusing this report for a discussion, we'll keep it short or move off.

Racoon worked, strongswan not. Support of IKEv2 is irrelevant at such angle.

I recommend retrying with Strongswan. I did it half a year ago and it is superior to Openswan and Racoon in every way for things that I tested.

Yes, it is unfortunate that Racoon does not support IKEv2. But at least it works. Racoon2 supports IKEv2, but I have not tried it yet.

Racoon2 supports many things and looks very interesting. I've packaged it for Fedora roughly the same time I did with Strongswan. But, Racoon2 is not Racoon. It's a different project and it is also finished. It is not abandoned but it recieves only little updates. It may be in some ways superior to Strongswan. See my slides if you wish so.