Hello to all!

In our environment I detected an IPSEC channel drop after ISAKMP rekeying phase between StrongSwan and Cisco.

Initially, the IPSEC tunnel between StrongSwan and Cisco is installed correctly and everything works.

After the first IPSEC rekey also all work.

Then the ISAKMP rekey happens and everything also works.

But, then, when the second IPSEC rekey is happened, then a new IPSEC is installed on Cisco, but the StrongSwan cannot read the IPSEC proposals in the payload from Cisco (with the 'no acceptable traffic selectors found' message). As a result, on Cisco we see ISAKMP and IPSEC, and on StrongSwan only ISAKMP.

As a result, the IPSEC stops working between StrongSwan and Cisco.

This problem is observed with on Apline Linux 3.11, strongswan-5.8.1-r1 and Cisco 2811,3825,2911.

Did anyone have the same problem?

Are there any solutions?

---

**History**

#1 - 06.04.2020 13:02 - Tobias Brunner

- Status changed from New to Feedback

Do you use ipsec reload a lot? If so, see e.g. #1338-3 (it discusses ipsec update, which behaves like ipsec reload only for changed configs and is otherwise a better choice).

#2 - 07.04.2020 07:43 - Stanislav Vasilevskiy

We do not use starter. We have charon/swanctl/vici configuration.

#3 - 07.04.2020 09:35 - Tobias Brunner

- Category set to ikev1

  We do not use starter. We have charon/swanctl/vici configuration.

Then it's probably the Cisco boxing doing something incorrectly (or it's just because it's IKEV1). Since you provided no logs we can't help you any further (see HelpRequests).

#4 - 07.04.2020 20:13 - Stanislav Vasilevskiy

- File info.7z added

  The necessary files are in the attached archive.
  There are 2 events in charon.log.err "no acceptable traffic selectors found"
  They happened at Apr  4 14:53:54 and Apr  4 15:07:50
  From that time you can see what was on Cisco.
  StrongSwan is used with DMVPN combination.

#5 - 08.04.2020 16:53 - Tobias Brunner

  There are 2 events in charon.log.err "no acceptable traffic selectors found".
Seems strange, because when handling the initial Quick Mode request, traffic selectors were successfully selected:

```
Apr  4 15:07:50 06[ENC] <dmvpn|2> parsed QUICK_MODE request 2290461800 [ HASH SA No KE ID ]
Apr  4 15:07:50 06[CFG] <dmvpn|2> looking for a child config for 212.116.120.61/32[gre] => 78.25.123.26/32[gre]
Apr  4 15:07:50 06[CFG] <dmvpn|2> proposing traffic selectors for us:
Apr  4 15:07:50 06[CFG] <dmvpn|2> 212.116.120.61/32[gre]
Apr  4 15:07:50 06[CFG] <dmvpn|2> proposing traffic selectors for other:
Apr  4 15:07:50 06[CFG] <dmvpn|2> 78.25.123.26/32[gre]
Apr  4 15:07:50 06[CFG] <dmvpn|2> candidate "dmvpn" with prio 5+5
Apr  4 15:07:50 06[CFG] <dmvpn|2> found matching child config "dmvpn" with prio 10
Apr  4 15:07:50 06[CFG] <dmvpn|2> selecting traffic selectors for other:
Apr  4 15:07:50 06[CFG] <dmvpn|2> selecting traffic selectors for us:
Apr  4 15:07:50 06[CFG] <dmvpn|2> config: 212.116.120.61/32[gre], received: 212.116.120.61/32[gre] => match: 212.116.120.61/32[gre]
```

Then later we see that error:

```
Apr  4 15:07:50 07[ENC] <dmvpn|2> parsed QUICK_MODE request 2290461800 [ HASH ]
Apr  4 15:07:50 07[CHD] <dmvpn|2> CHILD_SA dmvpn{5} state change: CREATED => INSTALLING
Apr  4 15:07:50 07[IKE] <dmvpn|2> no acceptable traffic selectors found
```

This might be caused by the unity plugin, which is really only useful in roadwarrior scenarios.

```
rekey_time = 150s
life_time = 150s
```

This makes no sense (you can't start a rekeying when the SA already expired).

---

#6 - 08.04.2020 17:29 - Stanislav Vasilevskiy

Yes, the situation with "no acceptable traffic selectors found" comes up only after IKE is re-keyed. But let me arrange, step by step, to align with the process:

1. IKE SA set up and IPSEC SA set up (IPSEC SA signedhashed with IKE SA)
2. During IKE SA lifetime IPSEC SA can be re-keyed as many times as it likes
3. IKE SA is re-keyed (on Cisco side, for instance, there's no way to disable such re-keying)
4. This way existing IPSEC SA should be resigned/rehashed to match with the new IKE SA
5. The following re-keying for IPSEC SA should be normal and signed correctly

But in our situation, it seems that IPSEC SA is hashed with an old IPSEC SA and can't be processed by charon (i.e. decrypted during installing traffic selectors). As you can see in log file re-key procedure is happened twice until IKE SA is re-keyed, and this procedure succeeded.

What about unity plugin - it's disabled due to default value in charon. I didn't enable it specially. Why do you point that this might be caused by it?

And at last, rekey_time and life_time - agreed, no sense, but it can't be the matter of my problem, right?

---

#7 - 08.04.2020 18:30 - Tobias Brunner

4. This way existing IPSEC SA should be resigned/rehashed to match with the new IKE SA
5. The following re-keying for IPSEC SA should be normal and signed correctly

But in our situation, it seems that IPSEC SA is hashed with an old IPSEC SA and can't be processed by charon (i.e. decrypted during installing traffic selectors).

Again, no idea what exactly you are referring to. I don't see any packages getting dropped because they are not encryptedsigned with the correct keys.

As you can see in log file re-key procedure is happened twice until IKE SA is re-keyed, and this procedure succeeded.
True, see below for the explanation.

What about unity plugin - it's disabled due to default value in charon. I didn't enable it specially. Why do you point that this might be caused by it?

It's not disabled, it's loaded according to the log. And it modifies the traffic selectors during Quick Mode in some situations. In particular in the NARROW_RESPONDER_POST hook, which comes right before the error message (it allows plugins to change the negotiated traffic selectors before they are installed in the kernel).

Typically the plugin would only narrow the traffic selectors as Quick Mode responder if the initiator proposed 0.0.0.0/0. The problem here is that the roles are reversed after the IKE_SA reauthentication (the original IKE_SA was initiated by the peer, so strongSwan was responder for both IKE_SA and Quick Mode request, the new one by strongSwan). In roadwarrior scenarios only the client can usually reauthenticate the IKE_SA, so the roles generally stay the same. However, as initiator of the IKE_SA, the behavior in the plugin as Quick Mode responder is reversed. So the remote traffic selectors are always narrowed to the Unity attributes received. Of course there aren't any, so the plugin tries to narrow to the configured traffic selectors. But since you configured dynamic and the plugin does not pass any IP addresses when deriving them, this results in an empty list and this error message.

So to fix it disable the unity plugin.

#8 - 10.04.2020 19:39 - Stanislav Vasilevskiy
Dear Tobias,
Great job, everything works now.
Many thanks for the help!

#9 - 14.04.2020 11:01 - Tobias Brunner
- Status changed from Feedback to Closed
- Assignee set to Tobias Brunner
- Resolution set to No change required

Files
info.7z 39.7 KB 07.04.2020 Stanislav Vasilevskiy