strongSwan - Issue #3600

Strongswan and Fortigate IPv6 over IPv4 Ref. Issue #3432

16.10.2020 16:15 - Daniel Sugondo

Status:	Closed		
Priority:	Normal		
Assignee:			
Category:	configuration		
Affected version:	5.7.2	**Resolution:**	No change required

Description

Hi all,

Ref. to Issue #3432https://wiki.strongswan.org/issues/3432

After a very long time, to solve this problem, I'd to change the authmethod on the Fortigate from
set authmethod psk to set authmethod signature
because the Fortinet guys means, the Strongswan rejects the key from IPSec responder.
12[IKE] no shared key found for...
To get signature authentication I've to set a certificate, please refer to
https://kb.fortinet.com/kb/viewContent.do?externalId=FD38854&sliceId=1
It's necessary too, to configure on Fortigate
set peertype any
first to try the functionality. You can change it later, if you want.

On the attachment, you can find some hints for the configuration.

History

#1 - 16.10.2020 16:18 - Noel Kuntze

- Category set to swanctl

- Status changed from New to Feedback

Hi,

I don't see a secrets section in your swanctl.conf.
Did you configure your secrets?

#2 - 16.10.2020 16:29 - Daniel Sugondo

Hi Noel,

the secret is configured, I just removed it from the configuration.

I only want to give a feedback to my old ticket, which has been closed, that the problem is solved now.

#3 - 16.10.2020 16:33 - Noel Kuntze

I see. So no further issues?

#4 - 16.10.2020 16:33 - Noel Kuntze

- Category changed from swanctl to configuration

#5 - 16.10.2020 16:39 - Daniel Sugondo

At this time, it's working like a charm.

Maybe one thing, it's possible to separate the configuration file between the connection and the secret section?

#6 - 16.10.2020 16:40 - Noel Kuntze

Yes, just use the "include" directive. You can split it into, AFAIK, an unlimited number of files.

#7 - 16.10.2020 16:46 - Daniel Sugondo

OK, I'll give it a try next week. But now, it's weekend.

Have a nice weekend!

Kind regards,

Daniel.

#8 - 19.10.2020 16:19 - Daniel Sugondo

Hi Noel,

just a short feedback, the include directive works for my secret section properly. Thank you for the hint.

Just cut the whole secret section from swanctl.conf and replace it on swanctl.conf with
include conf.d/eap_myuser.conf
and paste the secret section into conf.d/eap_myuser.conf

One another point, my StrongSwan is delivered from my distribution, Debian Buster, it has systemd.
I've tried to verbose the log messages, because I had to debug the connection, why it didn't work.

```
charon-systemd {
journal {
default = 4
ike = 4
knl = 3
}
}
```

but it doesn't show any effects. The standard log file /var/log/strongswan.log doesn't show more output from StrongSwan.

During the remote session with Fortinet guys, I got the information about SK_ei, SK_er, SK_ai, and SK_ar from Fortigate, if we want to debug and decrypt IKEv2 on Wireshark, is there any option or if it's possible to get these informations on StrongSwan too?

Thank you!

#9 - 19.10.2020 17:22 - Tobias Brunner

> but it doesn't show any effects.

That only works if you are actually using charon-systemd and not the regular charon daemon (Debian has separate packages for these). And you'll have to use *journalctl* to access the log.

> The standard log file /var/log/strongswan.log doesn't show more output from StrongSwan.

There is no such "standard" log file (by default, the daemon logs to syslog). If you want to log to that file, configure it appropriately (by the way, loggers configured in the *charon* section also apply to *charon-systemd* should you eventually use it).

> During the remote session with Fortinet guys, I got the information about SK_ei, SK_er, SK_ai, and SK_ar from Fortigate, if we want to debug and decrypt IKEv2 on Wireshark, is there any option or if it's possible to get these informations on StrongSwan too?

If you already have the keys from them, you obviously don't need them again (they are the same on both ends after all). But log level 4 in the *ike* subsystem will log the IKE keys (there is also the *save-keys* plugin, but Debian does not ship it).

#10 - 19.10.2020 18:45 - Daniel Sugondo

Hi Tobias,

> That only works if you are actually using charon-systemd and not the regular charon daemon (Debian has separate packages for these). And you'll have to use *journalctl* to access the log.

OK, I'll take a look for it.

> There is no such "standard" log file (by default, the daemon logs to syslog). If you want to log to that file, configure it appropriately (by the way, loggers configured in the *charon* section also apply to *charon-systemd* should you eventually use it).

Yes, you're right, I created a filter on syslog for StrongSwan long time ago and I forget about this filter. Sorry.

> If you already have the keys from them, you obviously don't need them again (they are the same on both ends after all). But log level 4 in the *ike* subsystem will log the IKE keys (there is also the *save-keys* plugin, but Debian does not ship it).

The purpose is to get all the decrypt information from StrongSwan directly. It's not really my favorit, to have 2 machines running at home, the first one to get the debug info from Fortigate and the second one to try the initiator to connect to the responder.

#11 - 24.03.2021 17:58 - Daniel Sugondo

Forgot to give a reply, my problem with logging is solved.
The issue with Fortigate is still open, because there is an another dependency with other parts, which has to be resolved too.
I think this case can be closed now, because it's not affect strongSwan.

#12 - 03.05.2021 11:26 - Tobias Brunner

- Status changed from Feedback to Closed

- Resolution changed from Fixed to No change required

Files

20201016_fortigate.cfg	1.79 KB	16.10.2020	Daniel Sugondo
20201016_swanctl.conf	704 Bytes	16.10.2020	Daniel Sugondo
20201016_log.txt	1.21 KB	16.10.2020	Daniel Sugondo