strongSwan - Issue #2319

gives up trying to bring up connection after DNS SERVFAIL

08.05.2017 12:05 - Daniel Pocock

Status:	Feedback		
Priority:	Normal		
Assignee:			
Category:			
Affected version:	5.3.3	**Resolution:**	

Description

I've got some of the following in a branch-office configuration on OpenWRT:

StrongSWAN version 5.3.3

```
conn mainoffice
left=%defaultroute
leftsubnet=192.168.1.0/24,my-ipv6-prefix::/64
leftcert=wrt1Cert.der
leftid=@wrt1.example.org
leftfirewall=yes
right=vpn.example.org
rightid=@vpn.example.org
rightsubnet=my-class-C/24,another-ipv6-prefix::/52
auto=start
dpdaction=restart
closeaction=restart
keyingtries=%forever
```

With this configuration (dpdaction, closeaction, keyingtries) I would expect the branch office to make every effort to reconnect and keep trying forever after any type of interruption.

I've observed that if the ISP link goes down (e.g. removing the fibre), if the ISP link is not ready when StrongSWAN starts up (e.g. after a router reboot) or if the VPN server is restart then the branch office fails to reconnect.

Looking at the logs (logread on OpenWRT) I notice an error about DNS failure for "vpn.example.org" and then it would give up.

I changed the line "right=vpn.example.org" to "right=A.B.C.D" and the problem went away. Now it really keeps retrying, so using the IP is a workaorund for this issue.

This was discussed on the mailing list
https://lists.strongswan.org/pipermail/users/2017-May/010984.html

and it was suggested that this is not a bug, that StrongSWAN should give up retrying after a permanent failure.

I feel that it should have a more fine-grained means of determining what type of failure is "permanent". For example:

- an expired certificate will always be an expired certificate, so this type of error is really permanent. However, if some script is updating the certificate for the user from time to time, will StrongSWAN notice when the new certificate file exists and immediately use it?

- a DNS NXDOMAIN response is also a strong suggestion that the DNS domain doesn't exist or hasn't been set up yet. However, if the sysadmin finishes the setup later in the day, should his VPN just start working automatically, or does he have to go and restart all the processes that received NXDOMAIN?

- a DNS SERVFAIL response can be a transient issue though (e.g. name server not under DDoS attack or ISP link gone down), it is a lot less "permanent" than the examples of an expired certificate or an NXDOMAIN response. A SERVFAIL situation may fix itself. Usually a SERVFAIL situation does not require the administrator to change anything in their ipsec.conf. In these cases I feel StrongSWAN should be able to retry without any intervention by the user or administrator to restart the process.

History

#1 - 08.05.2017 13:02 - Tobias Brunner

- Status changed from New to Feedback

As I already mentioned, there is a strongswan.conf option to avoid this particular failure: *charon.retry_initiate_interval*

#2 - 08.05.2017 15:27 - Daniel Pocock

What is the relationship (if any) between the ipsec.conf option *keyingtries* and the strongswan.conf option *charon.retry_initiate_interval*?

Maybe *charon.retry_initiate_interval* could be mentioned in the ipsec.conf man page, in the section about *keyingtries*?

How did you choose 0 as the default for *charon.retry_initiate_interval*?

#3 - 08.05.2017 15:36 - Tobias Brunner

> What is the relationship (if any) between the ipsec.conf option *keyingtries* and the strongswan.conf option *charon.retry_initiate_interval*?

They are independent. The latter only has an effect on DNS resolution (if it fails it will be retried in the configured number of seconds).

> How did you choose 0 as the default for *charon.retry_initiate_interval*?

If that wasn't the default you'd end up in an infinite loop if you configured e.g. an invalid host name. This way you get an error pretty much immediately. You are free to set that interval after you made sure your config is correct.

#4 - 08.05.2017 15:41 - Daniel Pocock

If you configure an invalid hostname then the DNS will return NXDOMAIN

Maybe there should be different retry interval for SERVFAIL with a default of 60 or 300 seconds?