pfSense - Bug #3894

OpenVPN client started multiple times when connecting to FQDN where connectivity to server is delayed

09/26/2014 05:48 AM - Dmitriy K

Status:	Resolved	**Start date:**	09/26/2014
Priority:	Normal	**Due date:**	
Assignee:	Chris Buechler	**% Done:**	100%
Category:	OpenVPN	**Estimated time:**	0.00 hour
Target version:	2.2		
Affected Version:	All	**Affected Architecture:**	

Description

Requirements:
1. WAN connection should not be Static/DHCP!

Steps to reproduce:
1. Create an ovpn client instance with DN as "server address" (for example: vpn.contoso.com).
2. Check "Server host name resolution" option.
3. Save and restart the router.

If WAN connection establishment delay was long enough our newly created ovpn instance will become "detached" from system.

Upon WAN iface goes up an ovpn client daemon will resolve a DN and establish connection to the server. Good! But you will not be able to control that ovpn instance anymore. That means you wont be able to stop, start, restart, disable/enable it! Ovpn iface will be up and working 4ver.

Associated revisions

Revision d882658e - 11/19/2014 02:32 AM - Ermal Luçi

Fixes #3894, --resolv-retry is infinite by default. To avoid the issues of locking the persistnet tun device by this just retry two times by default. People can enable resolv-retry infinite themselves for previous behaviour

Revision 93ead355 - 11/22/2014 12:42 PM - Chris Buechler

In some circumstances, OpenVPN doesn't exit on SIGTERM. SIGKILL it when that happens. Ticket #3894

Revision 02a2bffa - 11/22/2014 12:57 PM - Chris Buechler

add a usleep here to prevent killing twice. Ticket #3894

Revision 30640018 - 12/03/2014 11:05 AM - Chris Buechler

Change our default resolv-retry back to OpenVPN's default. Changing this
didn't help the ticket where it was intended to help, which was later
fixed differently. This change in defaults is problematic in a lot of
scenarios, go back to the way things were before. Ticket #3894

History

#1 - 10/06/2014 05:29 AM - Ermal Luçi

- Priority changed from High to Normal

Normally openvpn instances are restarted on interface up event!

Can you back this claim with proper information as pid/ps -axwwvv etc... info?

#2 - 10/06/2014 03:47 PM - Dmitriy K

Here is a video http://rghost.net/private/58388261/44e5fb12a48d08550c2bb5cd6c676bd3

Bug is 100% reproducible. My guess is Bind server is being restarted right after ovpn is done restarting so resolving is not available at the time when ovpn trying to resolve DN. When Bind is up on iface ovpn successfully resolves DN and connects to the server being detached from GUI.

Maybe i'm wrong, maybe not ...

#3 - 10/09/2014 08:07 AM - Dmitriy K

After some research I've found out that system can't connect to "detached" ovpn instance socket.

I've added some logging to **openvpn_get_client_status()** of **openvpn.inc** and here is the output:
/index.php: openvpn_get_client_status(Array, unix:///var/etc/openvpn/client3.sock) = 61;

File (unix:///var/etc/openvpn/client3.sock) itself is exists but not accessible;

#4 - 10/09/2014 08:35 AM - Dmitriy K

Error code 61 means "Connection refused".

#5 - 10/10/2014 05:00 AM - Dmitriy K

- File openvpn.log added

- File openvpn_client3.pid added

Here are logs from clean start with only one ovpn instance enabled. Obviously, "2nd" instance is being detached, because the very 1st launched by system has exited.

#6 - 10/15/2014 02:41 PM - Ermal Luçi

From the logs seems you have already an running instance hence you cannot start a second one!
Can you post your system logs?

#7 - 10/16/2014 01:49 AM - Dmitriy K

- File system.log added

Yeah, obviously I can't run 2 times same instance but bug in logic can. So, here is system log.

Looks like opvn is being ran 2 times: at bootup and newwanip. Bug is located, I suppose.

#8 - 10/16/2014 01:50 AM - Dmitriy K

Look for "openvpn_restart" event in the system log to speedup things. Just forgot to mention it in the post above.

#9 - 10/16/2014 04:10 AM - Dmitriy K

Also, in **rc.newwanipv6** instances are started twice ...

#10 - 10/17/2014 11:27 AM - Ermal Luçi

I am sorry but you need to read better the source!

#11 - 10/29/2014 10:43 PM - Chris Buechler

- Subject changed from System looses control over specifically configured ovpn client instance after reboot to OpenVPN client started multiple times when connecting to FQDN where connectivity to server is delayed

- Assignee set to Chris Buechler

- Affected Documentation 0 added

The specific issue here is OpenVPN client is launched multiple times when connecting to FQDN with "resolv-retry infinite", where there is a delay in the Internet coming up, or network connectivity to the VPN server and/or DNS is unavailable. I have a good test case for this, will look into it further.

#12 - 11/18/2014 03:03 PM - Michael Schefczyk

On a server with two OpenVPN Clients in Peer to Peer (SSL/TLS) mode, I have the same issue, while "Infinitely resolve server" is NOT being checked. The issue occurs after every reboot. It can be cured by determining the OpenVPN clients' PIDs and then killing and restarting the processes. Usually, only one of the two clients is affected. Of course, I would very much welcome if the server could reboot to full functionality without manual intervention.

The setting is: 2.1.5-RELEASE (amd64), Intel(R) Atom(TM) CPU C2758 @ 2.40GHz 8 CPUs: 1 package(s) x 8 core(s), two WAN gateways, two OpenVPN Client in Peer to Peer (SSL/TLS) mode, Quagga OPSF package, Unbound package.

#13 - 11/18/2014 04:52 PM - Chris Buechler

- Status changed from New to Confirmed

#14 - 11/19/2014 02:27 AM - Ermal Luçi

- Status changed from Confirmed to Feedback

The issue here is that resolve-retry infinite is on by default.
I pushed a fix to do only 2 retries by default which should fix the issue at hand.
Previous behaviour people can just enable resolv-retry infinite if they want.

#15 - 11/19/2014 02:50 AM - Ermal Luçi

- % Done changed from 0 to 100

Applied in changeset d882658e826ca1c9e41c0832b3d0f433756ed903.

#16 - 11/22/2014 12:43 PM - Chris Buechler

- Status changed from Feedback to Resolved

Ermal's change is good, but doesn't help this circumstance. The root cause here is OpenVPN doesn't exit when sent a SIGTERM in this circumstance, and then we start it again while it's still running. Changed to send a SIGKILL if it doesn't exit after SIGTERM. Confirmed this resolves the circumstance described here.

#17 - 12/02/2014 10:01 AM - Phillip Davis

I have systems where the internet somewhere goes away quite regularly. The actual pfSense WAN interface to the upstream device (ISP, whatever) is fine, so there is no link down/link up event for pfSense to see in that sense.
OpenVPN site-to-clients time out after a bit, and then try to find their server end again. For this they try to resolve the FQDN of the server again. However the ISP issue lasts more than a few minutes, the DNS resolution fails, and with the now-default "resolv-retry 2", the OpenVPN client simply gives up and exits.
Then there is nothing in the system to try and start it again, either when ISP internet is better, or every so often. The clients stay down.
I have noticed this happen quite a few times recently and now realise the "resolv-retry 2" change is the reason for the new behavior. It seems odd to have a config that will simply exit in a reasonably-expected situation (DNS resolution has gone away for a few minutes) and that the client process

just exits and is never restarted.
I can select "Infinitely resolve server" and that will put things back the way they were. But it will be a hassle for lots of users to find this out after upgrading to 2.2
But with Chris' comment above about the SIGKILL/SIGTERM stuff - if that really resolves the underlying issue, then would it be best to revert the commit of the "resolv-retry 2" stuff?

#18 - 12/02/2014 10:30 AM - Ermal Luçi

You have an option resolve-retry-inifinite on the openvpn settings.
Use that to have it behave as before.

#19 - 12/02/2014 10:46 AM - Phillip Davis

I understand that, and I will now go to all my site-to-site clients on 2.1.5 and turn on that setting so it carries over into 2.2.
At the moment in 2.1.5, no resolv-retry goes in the config by default. And thus the OpenVPN default is in effect:

"By default, --resolv-retry infinite is enabled."

I am thinking that there might be quite a few people who experience this after upgrading to 2.2. Or is my situation an unusual edge case? Just thought I would raise the issue so others can think and comment.

#20 - 12/03/2014 11:02 AM - Chris Buechler

Since the circumstance Phil noted is pretty common, and the change that caused a problem there had no benefit on the original bug in this ticket, I changed our resolv-retry default back to OpenVPN's default of infinite. It'd break too much otherwise.

#21 - 12/03/2014 12:48 PM - Dmitriy K

Does that mean that the issue remains intact? Or SIGKILL will do in my case?

#22 - 12/03/2014 10:53 PM - Chris Buechler

The last update has nothing to do with your issue Dmitriy, the fix I put in a couple weeks ago is fine for that. Ermal's other change in this ticket is what broke Phil's setup and would end up breaking a lot of others, which was undone today. Everything related here is all good.

Files

openvpn.log	500 KB	10/10/2014	Dmitriy K
openvpn_client3.pid	6 Bytes	10/10/2014	Dmitriy K
system.log	27.1 KB	10/16/2014	Dmitriy K