pfSense - Bug #1116

IPsec error, racoon won't start with more than one phase 2

12/18/2010 10:46 PM - David Szpunar

Status:	Resolved	**Start date:**	12/18/2010
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	100%
Category:	IPsec	**Estimated time:**	0.00 hour
Target version:	2.0		
Affected Version:	2.0	**Affected Architecture:**	

Description

Mobile IPsec connection with more than one Phase 2 connections create an invalid /var/etc/racoon.conf file that prevents the racoon service from starting. May apply to other Phase 1's other than Mobile, but I didn't test. Dec. 18th (current) builds for i386 (not confirmed on other architectures) and past few days to a week or so (unsure exactly when it started, could be a bit longer) have the problem at least. Logs, racoon.conf, and <ipsec> tag from config.xml examples from machine with error are all at http://forum.pfsense.org/index.php/topic,31255.0.html.

Confirmed that deleting all but one Phase 2 tunnel allows racoon to start and VPN works normally. However the multiple-phase-2 version of the config was working fine in the past; upgrading to a newer snapshot broke it, without any additional configuration changes (to the IPsec area) being made.

Associated revisions

Revision 8f5c3d8d - 12/28/2010 04:23 PM - Pierre POMES

Ticket #1116: anonymous sainfo may be used only for single phase2 ipsec VPN's

History

#1 - 12/19/2010 07:55 PM - Pierre POMES

Note : the bug seems to be in /etc/inc/vpn.inc, line 640:

```
    640                                                         if (($localid_type == "none") ||
    641                                                                 (($ph1ent['authentication_method'] == "xauth_p
sk_server") ||
    642                                                                 ($ph1ent['authentication_method'] == "pre_shar
ed_key"))
    643                                                                 && isset($ph1ent['mobile']))
    644                                                                 $localid_spec = " ";
```

This is causing several "sainfo" section without any local specification ==> duplicate sainfo when more then one phase2.

#2 - 12/19/2010 08:13 PM - Jim Pingle

Will probably need some more logic in there then, because several types of mobile configurations will break without just 'sainfo anonymous'

#3 - 12/22/2010 03:09 PM - Pierre POMES

I check the code a little, we can have "sainfo anonymous" when setting the phase2 to "transport". So for such mobiles, it could be a documented issue in the wiki (only use one phase II in transport mode for such devices), and we could remove the condition (on isset($ph1ent['mobile']) in the code at line 643.

Otherwise, we could:
- add a checkbox "anonymous phase2" in the phase1 screen.
- when checked, only one "transport" phase2 can be added.

What do you think ?

#4 - 12/22/2010 03:59 PM - Jim Pingle

Sounds OK, though we also had reports that the Cisco VPN client would only connect with sainfo anonymous even without transport mode.

So what it might need is some more logic, if it's a single p2, use sainfo anonymous, if it's multiple p2, use the other method. A checkbox would work but may not be the best way.

#5 - 12/22/2010 05:41 PM - Pierre POMES

Ok, so:
- for multi p2, use complete sainfo.
- for mobile single p2, for pure-psk or psk/xauth, generate anonymous sainfo.

This should satisfy all cases.

#6 - 12/22/2010 05:46 PM - Jim Pingle

I think that sounds right, it should do the right thing automatically then.

Not sure if we should prevent someone from adding a second p2 to an xauth tunnel or not. Probably needs testing to see if the Cisco client and/or Shrew client work with that kind of setup.

#7 - 12/22/2010 11:47 PM - David Szpunar

If you're asking if multiple P2 networks should be supported then YES! I was using this regularly from Shrew and my iPhone until earlier this month when it broke and I finally reported this bug when it didn't start working again for more than a week. iPhone requires this setup (if you don't want to set up certs) including Xauth, and the iPhone IPsec client *is* a Cisco-branded client. I was using that and Shrew both to access multiple networks behind pfSense (several VLAN interfaces) for remote administration. I'm not familiar enough with IPsec and the source code to see why things changed, but it was working perfectly before, and I would very much like to see it continue working. The only hitch before now was that the newest upgrade to the Shrew client necessitated the fix I located at http://forum.pfsense.org/index.php/topic,30188.0.html

#8 - 12/22/2010 11:51 PM - Jim Pingle

Well of course they should, but whether or not both Cisco and Shrew will work with the same config is the question. :-) If it works, great, if it doesn't, we may need that checkbox to force a certain behavior, or a warning that multiple P2s don't work with Cisco if that is the case (which is may not be, it just needs tested to verify).

#9 - 12/28/2010 04:26 PM - Pierre POMES

Hi !

Jim: I just commited what we concluded a few days ago. If we need more logic, I suppose we could open a new ticket.
David: can you try again ? This should work now ;-)

Thanks,
Pierre

#10 - 12/28/2010 09:50 PM - Pierre POMES

- Status changed from New to Feedback

- % Done changed from 0 to 100

#11 - 12/30/2010 01:47 PM - Michel Samovojski

working for me :)

#12 - 12/30/2010 01:49 PM - Michel Samovojski

but i can see in syslog

php: /status_services.php: The command '/usr/local/sbin/setkey -f /var/etc/spd.conf' returned exit code '1', the output was 'setkey: fopen: No such file or directory'

#13 - 12/30/2010 09:20 PM - Pierre POMES

Hi Michel,

Can you copy/paste me (with anonymous IP's and keys) your ipsec section from /cf/conf/config.xml ?

Thanks,
Pierre

#14 - 01/03/2011 01:56 AM - David Szpunar

OK I added a second subnet (phase 2) entry after upgrading my firewall VM to the most recent beta (Jan 1 i386) to my Mobile IPsec tunnel, the only IPsec tunnel on this system. I was getting some System log entries like:

```
Jan 3 01:37:52    php: /vpn_ipsec.php: Could not determine VPN endpoint for 'Mobile IPsec'
```

in addition to:

```
Jan 3 01:37:52    php: /vpn_ipsec.php: The command '/usr/local/sbin/racoonctl -s /var/db/racoon/racoon.sock reload-config' returned exit code '1', the output was ''
```

and I couldn't connect, but I rechecked all tunnel configs (since I'd changed a lot in troubleshooting this earlier) and on my client and now the first VPN endpoint message seems to have gone away, but the second one about "exit code '1'" still shows up at least when I save/apply the IPsec settings.

However, racoon IS running now and the client (Shew) DOES connect, and I CAN talk to both subnets at the end of both phase2 tunnels! I don't know if the log entries are worth chasing down if it's working but if you need any additional information, I'll try to help. I just tried a third phase2 entry as well and it also works.

I also verified that I could access two of the phase2 tunnels through the iPhone using an iPhone 4 with latest firmware and the built-in IPsec client, however the LAN network didn't seem to be available when I tried pinging hosts while connected to the VPN, using the "Net Utility" iPhone app to ping. It pinged hosts in the other two subnets just fine. While connected via Shrew I was able to ping hosts in all three subnets, however. Not sure if this is a fluke or what's happening but it "mostly" works :-)

#15 - 01/03/2011 11:04 AM - Pierre POMES

Thanks for the feedback.

partial answer: for the error "The command '/usr/local/sbin/racoonctl -s /var/db/racoon/racoon.sock reload-config' returned exit code '1', the output was "", I am afraid it is a racoon problem. raconctl seems to return 1 in any case.

This is not the expected behavior according to the man page... (racoonctl should return 0 on success, and 1 on failure)

Pierre

#16 - 01/04/2011 12:11 PM - David Szpunar

Excellent, the iPhone access is not my priority right now though it is odd I could only get to two of the three subnets (when I did just two, they both worked). However with Shrew it all seems to be working great, regardless of the error you are saying is not expected (I can ignore it, just wanted to make sure it wasn't relevant).

#17 - 01/04/2011 08:35 PM - Pierre POMES

Hi David,

I am curious on the third subnet problem with your iPhone. In your pfSense IPSEC logs, do you have entries like "failed to pre-process packet", "failed to get sainfo" or something else ?

I would propose that you start racoon in debug mode from a ssh terminal:

```
kill <pid of racoon>
racoon -F -d -v -f /var/etc/racoon.conf
```

(this will start racoon in foreground, and you will have logs in your ssh terminal).

Then connect with your iPhone, and generate traffic a few seconds for the problematic subnet only.

Once done, ctrl+c on racoon (and start it again normally from the services menu).

If you find any relevant information in logs, let us know !

Pierre

#18 - 02/06/2011 01:47 AM - Chris Buechler

- Status changed from Feedback to Resolved

the original bug is fixed, and the later issue with non-0 exit status on racoonctl is fixed in ipsec-tools 0.8.0.