strongSwan - Issue #775

Thread handle under high load, is this a bug?

24.11.2014 08:14 - richard hu

Status:	Closed			
Priority:	Normal			
Assignee:				
Category:	charon			
Affected version:	5.2.1		**Resolution:**	No feedback

Description

We think this is a bug when strongswan handling thread.
attached screen shot for monitor system for our production system.
we have 12 vpn online and total end user number do not change too much and equally use these vpn servers.
when after a vpn restarted, the worker thread is keep at a lower level.
after it runs for more than 1 days, the worker thread suddenly jump to a very higher level. see attached pic.
and in the same time connecting number also suddenly increase and medium job quene increase.
all above monitor data was collected from ipsec status all.

History

#1 - 25.11.2014 11:23 - richard hu

```
charon {

    i_dont_care_about_security_and_use_aggressive_mode_psk = no
    install_routes = yes
    install_virtual_ip = yes
    duplicheck.enable = no
    dns1 = x.x.x.x
    #dns1=8.8.8.8
    #dns2=8.8.4.4
    #nbns1=8.8.8.8
    #nbns2=8.8.4.4
    port = 500
    port_nat_t = 4500
    threads = 64
    keep_alive=0

    #inactivity_close_ike = yes

    load_modular=yes

    plugins {
        include strongswan.d/charon/*.conf
    }

    plugins {
        eap-radius {
            accounting=yes
            servers {
                primary {
                    nas_identifier=primary
                    address=127.0.0.1
                    #port=1812
                    auth_port=1812
                    acct_port=1813
                    secret=xxx
                    sockets=200
                    #preference=99
                }

            }

            dae {
                enable = yes
                listen = x.x.x.x
                port = 3799
                secret =xxx
```

```
                }

        }

        xauth-eap {
            backend = radius
            fixedsecret = xxx
        }

    }
    include strongswan.d/charon-logging.conf

}

config setup
    strictcrlpolicy=no
    uniqueids=never

conn %default
    aggressive=no
    compress=yes
    dpdaction=clear
    dpddelay=30s
    dpdtimeout=150s
    esp=aes128-sha1!
    fragmentation=yes
    ike=aes128-sha1-sha1-modp1024!
    ikelifetime=10h
    keyingtries=3
    keylife=3h
    mobike=yes
    rekeymargin=9m
    type=tunnel
    left=%defaultroute
    leftsubnet=0.0.0.0/0
    right=%any

#For IOS and OSX Cisco IPSec, android IPSec RSA mode
conn XauthRSA
    keyexchange=ikev1
    leftauth=pubkey
    leftcert=server.crt
    rightsourceip=x.x.x.x/20
    rightauth=pubkey
    rightauth2=xauth-eap
    auto=add

#For strongswan android client cert mode
#IKE2 can not support wildcard certificate
conn android_client_IKEv2
    keyexchange=ikev2
    leftauth=pubkey
    leftcert=server.crt
    rightsourceip=x.x.x.x/20
    rightauth=pubkey
    rightauth2=eap-radius
    auto=add
    dpddelay=30m
```

#2 - 28.11.2014 01:59 - richard hu

By checking the log on problem server, I found there are too many IKE_SA half open time out.
And seems this result in reconnect and high connecting and worker thread number.
By read the log steps of half open time out, it's because vpn server did not get client send message.
After "sending packet:..." no received and after 30s it time out.
But I did not found the NIC has packets drop number, is there any chance that strongswan did not handle message send and receive correctly under high load.

#3 - 19.12.2014 14:13 - Martin Willi

- Assignee deleted (Martin Willi)

- Priority changed from Urgent to Normal

#4 - 07.07.2015 16:14 - Tobias Brunner

- Tracker changed from Bug to Issue

- Status changed from New to Closed

- Resolution set to No feedback

Closing some old tickets. Please open a new ticket if the issue persists.

Files

vpn-connecting.jpg	1.54 MB	24.11.2014	richard hu
vpn-workerthread.jpg	1.7 MB	24.11.2014	richard hu
vpn-jobquene.jpg	1.67 MB	24.11.2014	richard hu