strongSwan - Bug #440

charon logs incorrect host name if it can't resolve remote address

11.11.2013 09:43 - Noel Kuntze

Status:	Closed	**Start date:**	11.11.2013
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	charon		
Target version:	5.1.2		
Affected version:	5.1.1	**Resolution:**	Fixed

Description

Sometimes charon can't "up" a connection, because it thinks it isn't there, but "ipsec statusall" clearly shows it.
It mostly happens after I restarted strongSwan.

```
# ipsec statusall
Status of IKE charon daemon (strongSwan 5.1.1, Linux 3.11.6-1-ARCH, x86_64):
  uptime: 11 seconds, since Nov 11 09:36:05 2013
  malloc: sbrk 2420736, mmap 0, used 391808, free 2028928
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 0
  loaded plugins: charon test-vectors curl random nonce x509 revocation constraints pubkey pkcs1 p
em openssl af-alg gmp xcbc cmac hmac ccm attr kernel-netlink socket-default farp stroke updown eap
-identity eap-gtc eap-mschapv2 eap-radius xauth-generic xauth-eap unity resolve
Listening IP addresses:
  141.79.50.88
Connections:
        home:  %any...cdgsthermi.no-ip.org  IKEv2, dpddelay=10s
        home:   local:  [C=DE, ST=Baden-W??rttemberg, O=ThermiCorp, OU=Users, CN=Thermi Thinkpad,
E=Thermi_Thinkpad@cdgsthermi.no-ip.org] uses public key authentication
        home:    cert:  "C=DE, ST=Baden-W??rttemberg, O=ThermiCorp, OU=Users, CN=Thermi Thinkpad,
E=Thermi_Thinkpad@cdgsthermi.no-ip.org"
        home:   remote: [cdgsthermi.no-ip.org] uses public key authentication
        home:   child:  dynamic === 192.168.178.0/24 TUNNEL, dpdaction=restart
      tunnel:   child:  dynamic === 0.0.0.0/0 TUNNEL, dpdaction=restart
      server:  %any...192.168.178.48  IKEv2, dpddelay=10s
      server:   local:  [C=DE, ST=Baden-W??rttemberg, O=ThermiCorp, OU=Users, CN=Thermi Thinkpad,
E=Thermi_Thinkpad@cdgsthermi.no-ip.org] uses public key authentication
      server:    cert:  "C=DE, ST=Baden-W??rttemberg, O=ThermiCorp, OU=Users, CN=Thermi Thinkpad,
E=Thermi_Thinkpad@cdgsthermi.no-ip.org"
      server:   remote: [cdgsthermi.no-ip.org] uses public key authentication
      server:   child:  dynamic === 192.168.178.48/32 141.79.0.0/16 TUNNEL, dpdaction=restart
Security Associations (0 up, 0 connecting):
  none

[root@thermi-thinkpad thermi]# ipsec up home
unable to resolve %any, initiate aborted
tried to check-in and delete nonexisting IKE_SA
establishing connection 'home' failed
```

Associated revisions

Revision be8af56e - 23.01.2014 10:03 - Tobias Brunner

ike: Use proper hostname(s) when name resolution failed

Was wrong since 0edce687675df8f10f4026fa12a8fc3b3dd003f5.

Fixes #440.

Revision 53d2164c - 23.01.2014 10:04 - Tobias Brunner

ike: Simplify error handling if name resolution failed

This avoids a second name resolution attempt just to determine if %any
etc. was configured.

Fixes #440.

History

#1 - 11.11.2013 09:43 - Noel Kuntze

Sorry, accidently hit "Enter" when I was editing the title.
It was supposed to mean "charon doesn't acknowledge existence of config".

#2 - 11.11.2013 16:39 - Tobias Brunner

- Tracker changed from Issue to Bug

- Subject changed from charon doesn to charon logs incorrect host name if it can't resolve remote address

- Description updated

- Status changed from New to Feedback

- Assignee set to Tobias Brunner

```
unable to resolve %any, initiate aborted
```

It looks like the host name *cdgsthermi.no-ip.org* couldn't get resolved (not that the config was not found). But that error message is wrong since 0edce687 (get_other_addr() should get called on line 1169 to display *right*). And since it is now possible to configure multiple addresses for *right*, the code there got a bit strange. After a failure to resolve the address(es) the code attempts another name resolution right before logging the error message, just to determine if *%any* (or a variant of it) was configured. In your case the name resolution actually seems to have succeeded the second time around (otherwise the error message would be different). I pushed a couple of commits to the *init-resolve* branch of our repository to fix this.

Anyway, if the address can't be resolved charon can't do much about it, other than retry, which happens if you configure *charon.retry_initiate_interval* in strongswan.conf. If it is set charon will retry initiation (irrespective of the *keyingtries* setting) until it is able to resolve the host name and can continue, or the initiation is canceled manually.

#3 - 11.11.2013 19:02 - Noel Kuntze

I edited resolv.conf prior to trying to "up" the connection, so it contained a valid nameserver. What do you think is the issue then? Was the change to resolv.conf I made not written to the disk yet?

#4 - 12.11.2013 10:08 - Tobias Brunner

> I edited resolv.conf prior to trying to "up" the connection, so it contained a valid nameserver. What do you think is the issue then? Was the change to resolv.conf I made not written to the disk yet?

Perhaps it *was* an issue with the resolver, but without knowing whether there was a DNS query or not, and to which server (old or new), and if that query was successful, it's hard to tell what exactly happened.

Can you reproduce this? If so, you should try to capture some traffic.

#5 - 23.01.2014 10:05 - Tobias Brunner

- Status changed from Feedback to Closed

- Target version set to 5.1.2

- Resolution set to Fixed

Files

ipsec.conf	861 Bytes	11.11.2013	Noel Kuntze