

## strongSwan - Feature #700

### Tunnel got established even after deleting cacert

12.09.2014 08:14 - Hari Alavandar

<b>Status:</b>	Closed	<b>Start date:</b>	12.09.2014
<b>Priority:</b>	Normal	<b>Due date:</b>	
<b>Assignee:</b>	Martin Willi	<b>Estimated time:</b>	0.00 hour
<b>Category:</b>	libcharon		
<b>Target version:</b>	5.3.0		
<b>Resolution:</b>	Fixed		

#### Description

Hi,

I have done below listed steps and founded that the IpSec tunnels are got established despite removal of CA certificate.

1. Loaded same CA certificate and BTS certificate at both ends: Tunnel got established
2. Deleted CA certificate at one: Tunnel got established
3. Removed BTS certificate @ /usr/local/etc/config/keystore/certs : Tunnel NOT established
4. Loaded only BTS certificate (CA certificate not installed) : Tunnel got established

My requirement is that when CA certificate the tunnel shouldn't have established.

Here is the ipsec.conf that is used

```
config setup
    plutostart=yes
    plutodebug=none
    nat_traversal=no
    uniqueids=no
    charonstart=yes
    charondebug="dmn 1, mgr 1, ike 0, chd 1, job 0, cfg 0, knl 0, net 0, enc -1, lib -1"

ca rootca0
    cacert=rootCaCert_0.pem

conn %default
    auto=start
    pfs=no
    forceencaps=no
    keyingtries=%forever
    mobike=no

conn conn1
    type=tunnel
    leftsubnet=20.0.0.1/24
    rightsubnet=20.0.0.2/24
    left=20.0.0.1
    right=20.0.0.2
    keyexchange=ikev2
    reauth=no
    ike=aes128-sha1-modp1024,3des-sha1-modp1024!
    ikelifetime=83376s
    esp=aes128-sha1,3des-sha1!
    authby=pubkey
    rightid=%any
    keylife=86400s
    dpdaction=restart
    dpddelay=10s
    dpdtimeout=120s
    leftcert=/etc/ipsec.d/certs/btsCert.pem
    rekeyfuzz=50%
    rekeymargin=180s
```

---

## Associated revisions

---

### Revision 1fd70254 - 03.03.2015 13:52 - Martin Willi

Merge branch 'stroke-purge-on-reread'

Remove all previously loaded certificates during "ipsec reread", finally allowing the removal of CA certificates from a running daemon.

Fixes #842, #700, #305.

## History

---

### #1 - 17.09.2014 13:24 - Tobias Brunner

- Description updated
- Status changed from New to Feedback
- Priority changed from High to Normal

1. Loaded same CA certificate and BTS certificate at both ends: Tunnel got established
2. Deleted CA certificate at one: Tunnel got established
3. Removed BTS certificate @ /usr/local/etc/config/keystore/certs : Tunnel NOT established
4. Loaded only BTS certificate (CA certificate not installed) : Tunnel got established

My requirement is that when CA certificate the tunnel shouldn't have established.

I don't understand what you mean. Are you referring to case 4 above (i.e. did you mean "...when **no** CA certificate...")?

What commands did you execute after deleting/adding certificate files? Did you run ipsec restart? Or any of the ipsec reread... or ipsec purge... commands (see [ipsec](#) for details)?

Was the config the same for all the scenarios? Or did you e.g. set *rightcert* at some point?

### #2 - 03.03.2015 14:30 - Martin Willi

- Tracker changed from Issue to Feature
- Category set to libcharon
- Status changed from Feedback to Closed
- Assignee changed from Tobias Brunner to Martin Willi
- Target version set to 5.3.0
- Resolution set to Fixed

With the referenced merge, "ipsec reread" removes any previously loaded CA certificates before reloading them from disk. I assume this fixes your issue you have seen, let us know if not.

Regards  
Martin