strongSwan - Bug #3139

load-test error

08.08.2019 14:29 - Krishnamurthy Daulatabad

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	testing		
Target version:	5.8.1		
Affected version:	5.7.2	**Resolution:**	Fixed

Description

Hi
I am trying to run the ike load-tests using the load-test plugin. I am using strongswan version 5.7.2 and certificate had expired in load_tester_creds.c and I pulled the latest key and cert from master on github. With this I am seeing the below error on the initiator which is "rejecting certificate without digitalSignature or nonRepudiation keyUsage flags". Am I missing anything here? Please let me know if you need any other information.

```
2019-08-08T17:48:48.0+0530 07[NET] <load-test|8> received packet: from 20.0.0.1[500] to 20.0.0.2[5
00] (481 bytes)
2019-08-08T17:48:48.0+0530 07[ENC] <load-test|8> parsed IKE_SA_INIT response 0 [ SA KE No N(NATD_S
_IP) N(NATD_D_IP) CERTREQ N(HASH_ALG) N(MULT_AUTH) ]
2019-08-08T17:48:48.0+0530 07[CFG] <load-test|8> selected proposal: IKE:AES_CBC_128/HMAC_SHA1_96/P
RF_HMAC_SHA1/MODP_2048
2019-08-08T17:48:48.0+0530 07[IKE] <load-test|8> received cert request for "CN=srv, OU=load-test,
O=strongSwan"
2019-08-08T17:48:48.0+0530 07[IKE] <load-test|8> sending cert request for "CN=srv, OU=load-test, O
=strongSwan"
2019-08-08T17:48:48.0+0530 07[IKE] <load-test|8> authentication of 'CN=c8-r1, OU=load-test, O=stro
ngSwan' (myself) with RSA_EMSA_PKCS1_SHA2_256 successful
2019-08-08T17:48:48.0+0530 07[IKE] <load-test|8> sending end entity cert "CN=c8-r1, OU=load-test,
O=strongSwan"
2019-08-08T17:48:48.0+0530 07[IKE] <load-test|8> establishing CHILD_SA load-test{10}
2019-08-08T17:48:48.0+0530 07[ENC] <load-test|8> generating IKE_AUTH request 1 [ IDi CERT N(INIT_C
ONTACT) CERTREQ IDr AUTH N(ESP_TFC_PAD_N) SA TSi TSr N(MULT_AUTH) N(EAP_ONLY) N(MSG_ID_SYN_SUP) ]
2019-08-08T17:48:48.0+0530 07[NET] <load-test|8> sending packet: from 20.0.0.2[4500] to 20.0.0.1[4
500] (1036 bytes)
2019-08-08T17:48:48.0+0530 15[NET] <load-test|8> received packet: from 20.0.0.1[4500] to 20.0.0.2[
4500] (396 bytes)
2019-08-08T17:48:48.0+0530 15[ENC] <load-test|8> parsed IKE_AUTH response 1 [ IDr AUTH N(ESP_TFC_P
AD_N) SA TSi TSr N(AUTH_LFT) ]
2019-08-08T17:48:48.0+0530 15[CFG] <load-test|8>   using trusted certificate "CN=srv, OU=load-test
, O=strongSwan"
**2019-08-08T17:48:48.0+0530 15[IKE] <load-test|8> rejecting certificate without digitalSignature
or nonRepudiation keyUsage flags
2019-08-08T17:48:48.0+0530 15[IKE] <load-test|8> signature validation failed, looking for another
key
**2019-08-08T17:48:48.0+0530 15[ENC] <load-test|8> generating INFORMATIONAL request 2 [ N(AUTH_FAI
LED) ]
2019-08-08T17:48:48.0+0530 15[NET] <load-test|8> sending packet: from 20.0.0.2[4500] to 20.0.0.1[4
500] (76 bytes)
```

Associated revisions

Revision a1295ff9 - 22.08.2019 15:33 - Tobias Brunner

load-tester: Add digitalSignature keyUsage flag to test certificate

This allows using the certificate, which is technically a CA cert, as
end-entity certificate again after the RFC4945-related changes added
with 5.6.3.

Fixes #3139.

History

#1 - 09.08.2019 09:06 - Krishnamurthy Daulatabad

I am using strongswan version 5.7.1

#2 - 12.08.2019 18:16 - Tobias Brunner

- Tracker changed from Issue to Bug

- Description updated

- Category set to testing

- Status changed from New to Feedback

- Priority changed from Urgent to Normal

- Target version set to 5.8.1

The problem is that the pre-defined certificate is technically a CA certificate, but in the load-tester's default configuration (i.e. if no custom configuration and server certificate is used, which can do to workaround the issue) also serves as end-entity certificate for the responder. This won't work anymore due to the changes added with 5.6.3 (compliance with RFC 4945).

I guess the simplest fix is to just add the *digitalSignature* keyUsage bit for this test certificate. I did so in the *3139-load-test-cert* branch.

#3 - 13.08.2019 08:13 - Krishnamurthy Daulatabad

Thanks for the fix. Followup question: How can this *digitalsignature* flag be set with the pki tool while generating the CA certificate?

#4 - 13.08.2019 10:22 - Tobias Brunner

- File ca-cert-digitalsignature.patch added

> How can this *digitalsignature* flag be set with the pki tool while generating the CA certificate?

Requires a code change (see attachment).

#5 - 22.08.2019 15:35 - Tobias Brunner

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Resolution set to Fixed

Files

ca-cert-digitalsignature.patch	603 Bytes	13.08.2019	Tobias Brunner