strongSwan - Issue #2405

Android client not caching CRL response

17.08.2017 12:42 - Sam Leung

Status:	Closed		
Priority:	Normal		
Assignee:	Tobias Brunner		
Category:	android		
Affected version:	5.6.0	**Resolution:**	Fixed

Description

Hello,

I found that the Android client always fetch the CRL online and not caching it.

Here is the log of the first connection.

```
Aug 17 18:12:46 00[DMN] Starting IKE charon daemon (strongSwan 5.5.3, Android 6.0.1 - MXB48T/2017-
06-01, LG-K220 - lge/mk6pn_global_com/LGE, Linux 3.18.19+, armv7l)
Aug 17 18:12:46 00[LIB] loaded plugins: androidbridge charon android-log openssl fips-prf random n
once pubkey chapoly curve25519 pkcs1 pkcs8 pem xcbc hmac socket-default revocation eap-identity ea
p-mschapv2 eap-md5 eap-gtc eap-tls
Aug 17 18:12:46 00[JOB] spawning 16 worker threads
Aug 17 18:12:47 15[IKE] initiating IKE_SA android[1] to 103.254.155.147
Aug 17 18:12:47 15[ENC] generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FR
AG_SUP) N(HASH_ALG) N(REDIR_SUP) ]
Aug 17 18:12:47 15[NET] sending packet: from 10.49.103.180[55365] to 103.254.155.147[500] (746 byt
es)
Aug 17 18:12:47 09[NET] received packet: from 103.254.155.147[500] to 10.49.103.180[55365] (38 byt
es)
Aug 17 18:12:47 09[ENC] parsed IKE_SA_INIT response 0 [ N(INVAL_KE) ]
Aug 17 18:12:47 09[IKE] peer didn't accept DH group ECP_256, it requested ECP_521
Aug 17 18:12:47 09[IKE] initiating IKE_SA android[1] to 103.254.155.147
Aug 17 18:12:47 09[ENC] generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FR
AG_SUP) N(HASH_ALG) N(REDIR_SUP) ]
Aug 17 18:12:47 09[NET] sending packet: from 10.49.103.180[55365] to 103.254.155.147[500] (814 byt
es)
Aug 17 18:12:47 10[NET] received packet: from 103.254.155.147[500] to 10.49.103.180[55365] (385 by
tes)
Aug 17 18:12:47 10[ENC] parsed IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) CERTREQ
 N(FRAG_SUP) N(HASH_ALG) N(MULT_AUTH) ]
Aug 17 18:12:47 10[IKE] local host is behind NAT, sending keep alives
Aug 17 18:12:47 10[IKE] received cert request for "C=US, O=DigiCert Inc, OU=www.digicert.com, CN=D
igiCert Global Root CA"
Aug 17 18:12:47 10[IKE] received 1 cert requests for an unknown ca
Aug 17 18:12:47 10[IKE] sending cert request for "C=US, O=DigiCert Inc, OU=www.digicert.com, CN=Di
giCert Global Root CA"
Aug 17 18:12:47 10[IKE] establishing CHILD_SA android
Aug 17 18:12:47 10[ENC] generating IKE_AUTH request 1 [ IDi N(INIT_CONTACT) CERTREQ CPRQ(ADDR ADDR
6 DNS DNS6) N(ESP_TFC_PAD_N) SA TSi TSr N(MOBIKE_SUP) N(NO_ADD_ADDR) N(MULT_AUTH) N(EAP_ONLY) N(MS
G_ID_SYN_SUP) ]
Aug 17 18:12:47 10[NET] sending packet: from 10.49.103.180[53573] to 103.254.155.147[4500] (560 by
tes)
Aug 17 18:12:48 11[NET] received packet: from 103.254.155.147[4500] to 10.49.103.180[53573] (532 b
ytes)
Aug 17 18:12:48 11[ENC] parsed IKE_AUTH response 1 [ EF(1/11) ]
Aug 17 18:12:48 11[ENC] received fragment #1 of 11, waiting for complete IKE message
Aug 17 18:12:48 12[NET] received packet: from 103.254.155.147[4500] to 10.49.103.180[53573] (532 b
ytes)
Aug 17 18:12:48 12[ENC] parsed IKE_AUTH response 1 [ EF(2/11) ]
Aug 17 18:12:48 12[ENC] received fragment #2 of 11, waiting for complete IKE message
Aug 17 18:12:48 13[NET] received packet: from 103.254.155.147[4500] to 10.49.103.180[53573] (532 b
ytes)
```

```
Aug 17 18:12:48 13[ENC] parsed IKE_AUTH response 1 [ EF(3/11) ]
Aug 17 18:12:48 13[ENC] received fragment #3 of 11, waiting for complete IKE message
Aug 17 18:12:48 14[NET] received packet: from 103.254.155.147[4500] to 10.49.103.180[53573] (532 b
ytes)
Aug 17 18:12:48 14[ENC] parsed IKE_AUTH response 1 [ EF(4/11) ]
Aug 17 18:12:48 14[ENC] received fragment #4 of 11, waiting for complete IKE message
Aug 17 18:12:48 16[NET] received packet: from 103.254.155.147[4500] to 10.49.103.180[53573] (532 b
ytes)
Aug 17 18:12:48 16[ENC] parsed IKE_AUTH response 1 [ EF(5/11) ]
Aug 17 18:12:48 16[ENC] received fragment #5 of 11, waiting for complete IKE message
Aug 17 18:12:48 08[NET] received packet: from 103.254.155.147[4500] to 10.49.103.180[53573] (532 b
ytes)
Aug 17 18:12:48 08[ENC] parsed IKE_AUTH response 1 [ EF(6/11) ]
Aug 17 18:12:48 08[ENC] received fragment #6 of 11, waiting for complete IKE message
Aug 17 18:12:48 07[NET] received packet: from 103.254.155.147[4500] to 10.49.103.180[53573] (532 b
ytes)
Aug 17 18:12:48 07[ENC] parsed IKE_AUTH response 1 [ EF(7/11) ]
Aug 17 18:12:48 07[ENC] received fragment #7 of 11, waiting for complete IKE message
Aug 17 18:12:48 15[NET] received packet: from 103.254.155.147[4500] to 10.49.103.180[53573] (532 b
ytes)
Aug 17 18:12:48 15[ENC] parsed IKE_AUTH response 1 [ EF(8/11) ]
Aug 17 18:12:48 15[ENC] received fragment #8 of 11, waiting for complete IKE message
Aug 17 18:12:48 09[NET] received packet: from 103.254.155.147[4500] to 10.49.103.180[53573] (532 b
ytes)
Aug 17 18:12:48 09[ENC] parsed IKE_AUTH response 1 [ EF(9/11) ]
Aug 17 18:12:48 09[ENC] received fragment #9 of 11, waiting for complete IKE message
Aug 17 18:12:48 10[NET] received packet: from 103.254.155.147[4500] to 10.49.103.180[53573] (532 b
ytes)
Aug 17 18:12:48 10[ENC] parsed IKE_AUTH response 1 [ EF(10/11) ]
Aug 17 18:12:48 10[ENC] received fragment #10 of 11, waiting for complete IKE message
Aug 17 18:12:48 11[NET] received packet: from 103.254.155.147[4500] to 10.49.103.180[53573] (116 b
ytes)
Aug 17 18:12:48 11[ENC] parsed IKE_AUTH response 1 [ EF(11/11) ]
Aug 17 18:12:48 11[ENC] received fragment #11 of 11, reassembling fragmented IKE message
Aug 17 18:12:48 11[ENC] parsed IKE_AUTH response 1 [ IDr CERT CERT AUTH EAP/REQ/ID ]
Aug 17 18:12:48 11[IKE] received end entity cert "C=MY, ST=Wilayah Persekutuan, L=Labuan, O=eVentu
re Limited, CN=*.hide.me"
Aug 17 18:12:48 11[IKE] received issuer cert "C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server
 CA"
Aug 17 18:12:48 11[CFG]   using certificate "C=MY, ST=Wilayah Persekutuan, L=Labuan, O=eVenture Li
mited, CN=*.hide.me"
Aug 17 18:12:48 11[CFG]   using untrusted intermediate certificate "C=US, O=DigiCert Inc, CN=DigiC
ert SHA2 Secure Server CA"
Aug 17 18:12:48 11[CFG] checking certificate status of "C=MY, ST=Wilayah Persekutuan, L=Labuan, O=
eVenture Limited, CN=*.hide.me"
Aug 17 18:12:48 11[LIB] building CRED_CERTIFICATE - OCSP_REQUEST failed, tried 0 builders
Aug 17 18:12:48 11[CFG] generating ocsp request failed
Aug 17 18:12:48 11[CFG] ocsp check failed, fallback to crl
Aug 17 18:12:48 11[CFG]   fetching crl from 'http://crl3.digicert.com/ssca-sha2-g5.crl' ...
Aug 17 18:12:48 11[CFG]   using certificate "C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server
CA"
Aug 17 18:12:48 11[CFG]   using trusted ca certificate "C=US, O=DigiCert Inc, OU=www.digicert.com,
 CN=DigiCert Global Root CA"
Aug 17 18:12:48 11[CFG]   reached self-signed root ca with a path length of 0
Aug 17 18:12:48 11[CFG]   crl correctly signed by "C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure S
erver CA"
Aug 17 18:12:49 11[CFG]   crl is valid: until Aug 24 01:00:00 2017
Aug 17 18:12:49 11[CFG] certificate status is good
Aug 17 18:12:49 11[CFG]   using trusted ca certificate "C=US, O=DigiCert Inc, OU=www.digicert.com,
 CN=DigiCert Global Root CA"
Aug 17 18:12:49 11[CFG] checking certificate status of "C=US, O=DigiCert Inc, CN=DigiCert SHA2 Sec
ure Server CA"
Aug 17 18:12:49 11[LIB] building CRED_CERTIFICATE - OCSP_REQUEST failed, tried 0 builders
Aug 17 18:12:49 11[CFG] generating ocsp request failed
Aug 17 18:12:49 11[CFG] ocsp check failed, fallback to crl
Aug 17 18:12:49 11[CFG]   fetching crl from 'http://crl3.digicert.com/DigiCertGlobalRootCA.crl' ..
.
```

```
Aug 17 18:12:49 11[CFG]   using trusted certificate "C=US, O=DigiCert Inc, OU=www.digicert.com, CN
=DigiCert Global Root CA"
Aug 17 18:12:49 11[CFG]   crl correctly signed by "C=US, O=DigiCert Inc, OU=www.digicert.com, CN=D
igiCert Global Root CA"
Aug 17 18:12:49 11[CFG]   crl is valid: until Sep 07 01:00:00 2017
Aug 17 18:12:49 11[CFG] certificate status is good
Aug 17 18:12:49 11[CFG]   reached self-signed root ca with a path length of 1
Aug 17 18:12:49 11[IKE] authentication of 'C=MY, ST=Wilayah Persekutuan, L=Labuan, O=eVenture Limi
ted, CN=*.hide.me' with RSA_EMSA_PKCS1_SHA2_512 successful
Aug 17 18:12:49 11[IKE] server requested EAP_IDENTITY (id 0x00), sending 's_lyh'
Aug 17 18:12:49 11[ENC] generating IKE_AUTH request 2 [ EAP/RES/ID ]
Aug 17 18:12:49 11[NET] sending packet: from 10.49.103.180[53573] to 103.254.155.147[4500] (96 byt
es)
Aug 17 18:12:49 12[NET] received packet: from 103.254.155.147[4500] to 10.49.103.180[53573] (128 b
ytes)
Aug 17 18:12:49 12[ENC] parsed IKE_AUTH response 2 [ EAP/REQ/MSCHAPV2 ]
Aug 17 18:12:49 12[IKE] server requested EAP_MSCHAPV2 authentication (id 0x01)
Aug 17 18:12:49 12[ENC] generating IKE_AUTH request 3 [ EAP/RES/MSCHAPV2 ]
Aug 17 18:12:49 12[NET] sending packet: from 10.49.103.180[53573] to 103.254.155.147[4500] (160 by
tes)
Aug 17 18:12:50 08[NET] received packet: from 103.254.155.147[4500] to 10.49.103.180[53573] (144 b
ytes)
Aug 17 18:12:50 08[ENC] parsed IKE_AUTH response 3 [ EAP/REQ/MSCHAPV2 ]
Aug 17 18:12:50 08[IKE] EAP-MS-CHAPv2 succeeded: '(null)'
Aug 17 18:12:50 08[ENC] generating IKE_AUTH request 4 [ EAP/RES/MSCHAPV2 ]
Aug 17 18:12:50 08[NET] sending packet: from 10.49.103.180[53573] to 103.254.155.147[4500] (96 byt
es)
Aug 17 18:12:50 07[NET] received packet: from 103.254.155.147[4500] to 10.49.103.180[53573] (96 by
tes)
Aug 17 18:12:50 07[ENC] parsed IKE_AUTH response 4 [ EAP/SUCC ]
Aug 17 18:12:50 07[IKE] EAP method EAP_MSCHAPV2 succeeded, MSK established
Aug 17 18:12:50 07[IKE] authentication of 's_lyh' (myself) with EAP
Aug 17 18:12:50 07[ENC] generating IKE_AUTH request 5 [ AUTH ]
Aug 17 18:12:50 07[NET] sending packet: from 10.49.103.180[53573] to 103.254.155.147[4500] (160 by
tes)
Aug 17 18:12:50 15[NET] received packet: from 103.254.155.147[4500] to 10.49.103.180[53573] (368 b
ytes)
Aug 17 18:12:50 15[ENC] parsed IKE_AUTH response 5 [ AUTH CPRP(ADDR DNS DNS) SA TSi TSr N(AUTH_LFT
) N(MOBIKE_SUP) N(ADD_4_ADDR) N(ADD_4_ADDR) ]
Aug 17 18:12:50 15[IKE] authentication of 'C=MY, ST=Wilayah Persekutuan, L=Labuan, O=eVenture Limi
ted, CN=*.hide.me' with EAP successful
Aug 17 18:12:50 15[IKE] IKE_SA android[1] established between 10.49.103.180[s_lyh]...103.254.155.1
47[C=MY, ST=Wilayah Persekutuan, L=Labuan, O=eVenture Limited, CN=*.hide.me]
Aug 17 18:12:50 15[IKE] scheduling rekeying in 35890s
Aug 17 18:12:50 15[IKE] maximum IKE_SA lifetime 36490s
Aug 17 18:12:50 15[IKE] installing DNS server 103.254.155.146
Aug 17 18:12:50 15[IKE] installing DNS server 103.254.155.148
Aug 17 18:12:50 15[IKE] installing new virtual IP 10.3.230.229
Aug 17 18:12:50 15[IKE] CHILD_SA android{1} established with SPIs b0f2ba8f_i ceb59649_o and TS 10.
3.230.229/32 === 0.0.0.0/0 ::/0
Aug 17 18:12:50 15[DMN] setting up TUN device for CHILD_SA android{1}
Aug 17 18:12:50 15[DMN] successfully created TUN device
Aug 17 18:12:50 15[IKE] received AUTH_LIFETIME of 86400s, scheduling reauthentication in 85800s
Aug 17 18:12:50 15[IKE] peer supports MOBIKE
Aug 17 18:12:50 10[IKE] sending address list update using MOBIKE
Aug 17 18:12:50 10[ENC] generating INFORMATIONAL request 6 [ N(NO_ADD_ADDR) ]
Aug 17 18:12:50 10[NET] sending packet: from 10.49.103.180[53573] to 103.254.155.147[4500] (96 byt
es)
Aug 17 18:12:51 12[NET] received packet: from 103.254.155.147[4500] to 10.49.103.180[53573] (96 by
tes)
Aug 17 18:12:51 12[ENC] parsed INFORMATIONAL response 6 [ ]
Aug 17 18:12:54 00[IKE] deleting IKE_SA android[1] between 10.49.103.180[s_lyh]...103.254.155.147[
C=MY, ST=Wilayah Persekutuan, L=Labuan, O=eVenture Limited, CN=*.hide.me]
Aug 17 18:12:54 00[IKE] sending DELETE for IKE_SA android[1]
Aug 17 18:12:54 00[ENC] generating INFORMATIONAL request 7 [ D ]
Aug 17 18:12:54 00[NET] sending packet: from 10.49.103.180[53573] to 103.254.155.147[4500] (96 byt
es)
```

And then I disconnect it and reconnect immediately.

```
Aug 17 18:13:44 00[DMN] Starting IKE charon daemon (strongSwan 5.5.3, Android 6.0.1 - MXB48T/2017-
06-01, LG-K220 - lge/mk6pn_global_com/LGE, Linux 3.18.19+, armv7l)
Aug 17 18:13:45 00[LIB] loaded plugins: androidbridge charon android-log openssl fips-prf random n
once pubkey chapoly curve25519 pkcs1 pkcs8 pem xcbc hmac socket-default revocation eap-identity ea
p-mschapv2 eap-md5 eap-gtc eap-tls
Aug 17 18:13:45 00[JOB] spawning 16 worker threads
Aug 17 18:13:46 07[IKE] initiating IKE_SA android[2] to 103.254.155.4
Aug 17 18:13:46 07[ENC] generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FR
AG_SUP) N(HASH_ALG) N(REDIR_SUP) ]
Aug 17 18:13:46 07[NET] sending packet: from 10.49.103.180[60849] to 103.254.155.4[500] (746 bytes
)
Aug 17 18:13:46 11[NET] received packet: from 103.254.155.4[500] to 10.49.103.180[60849] (38 bytes
)
Aug 17 18:13:46 11[ENC] parsed IKE_SA_INIT response 0 [ N(INVAL_KE) ]
Aug 17 18:13:46 11[IKE] peer didn't accept DH group ECP_256, it requested ECP_521
Aug 17 18:13:46 11[IKE] initiating IKE_SA android[2] to 103.254.155.4
Aug 17 18:13:46 11[ENC] generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FR
AG_SUP) N(HASH_ALG) N(REDIR_SUP) ]
Aug 17 18:13:46 11[NET] sending packet: from 10.49.103.180[60849] to 103.254.155.4[500] (814 bytes
)
Aug 17 18:13:46 12[NET] received packet: from 103.254.155.4[500] to 10.49.103.180[60849] (385 byte
s)
Aug 17 18:13:46 12[ENC] parsed IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) CERTREQ
 N(FRAG_SUP) N(HASH_ALG) N(MULT_AUTH) ]
Aug 17 18:13:46 12[IKE] local host is behind NAT, sending keep alives
Aug 17 18:13:46 12[IKE] received cert request for "C=US, O=DigiCert Inc, OU=www.digicert.com, CN=D
igiCert Global Root CA"
Aug 17 18:13:46 12[IKE] received 1 cert requests for an unknown ca
Aug 17 18:13:46 12[IKE] sending cert request for "C=US, O=DigiCert Inc, OU=www.digicert.com, CN=Di
giCert Global Root CA"
Aug 17 18:13:46 12[IKE] establishing CHILD_SA android
Aug 17 18:13:46 12[ENC] generating IKE_AUTH request 1 [ IDi N(INIT_CONTACT) CERTREQ CPRQ(ADDR ADDR
6 DNS DNS6) N(ESP_TFC_PAD_N) SA TSi TSr N(MOBIKE_SUP) N(NO_ADD_ADDR) N(MULT_AUTH) N(EAP_ONLY) N(MS
G_ID_SYN_SUP) ]
Aug 17 18:13:46 12[NET] sending packet: from 10.49.103.180[50250] to 103.254.155.4[4500] (560 byte
s)
Aug 17 18:13:46 13[NET] received packet: from 103.254.155.4[4500] to 10.49.103.180[50250] (532 byt
es)
Aug 17 18:13:46 13[ENC] parsed IKE_AUTH response 1 [ EF(1/11) ]
Aug 17 18:13:46 13[ENC] received fragment #1 of 11, waiting for complete IKE message
Aug 17 18:13:46 14[NET] received packet: from 103.254.155.4[4500] to 10.49.103.180[50250] (532 byt
es)
Aug 17 18:13:46 14[ENC] parsed IKE_AUTH response 1 [ EF(2/11) ]
Aug 17 18:13:46 14[ENC] received fragment #2 of 11, waiting for complete IKE message
Aug 17 18:13:46 09[NET] received packet: from 103.254.155.4[4500] to 10.49.103.180[50250] (532 byt
es)
Aug 17 18:13:46 09[ENC] parsed IKE_AUTH response 1 [ EF(3/11) ]
Aug 17 18:13:46 09[ENC] received fragment #3 of 11, waiting for complete IKE message
Aug 17 18:13:46 09[NET] received packet: from 103.254.155.4[4500] to 10.49.103.180[50250] (116 byt
es)
Aug 17 18:13:46 09[ENC] parsed IKE_AUTH response 1 [ EF(11/11) ]
Aug 17 18:13:46 09[ENC] received fragment #11 of 11, waiting for complete IKE message
Aug 17 18:13:46 07[NET] received packet: from 103.254.155.4[4500] to 10.49.103.180[50250] (532 byt
es)
Aug 17 18:13:46 07[ENC] parsed IKE_AUTH response 1 [ EF(5/11) ]
Aug 17 18:13:46 07[ENC] received fragment #5 of 11, waiting for complete IKE message
Aug 17 18:13:46 11[NET] received packet: from 103.254.155.4[4500] to 10.49.103.180[50250] (532 byt
es)
Aug 17 18:13:46 11[ENC] parsed IKE_AUTH response 1 [ EF(6/11) ]
Aug 17 18:13:46 11[ENC] received fragment #6 of 11, waiting for complete IKE message
Aug 17 18:13:46 17[NET] received packet: from 103.254.155.4[4500] to 10.49.103.180[50250] (532 byt
es)
Aug 17 18:13:46 17[ENC] parsed IKE_AUTH response 1 [ EF(7/11) ]
Aug 17 18:13:46 17[ENC] received fragment #7 of 11, waiting for complete IKE message
Aug 17 18:13:46 16[NET] received packet: from 103.254.155.4[4500] to 10.49.103.180[50250] (532 byt
```

```
es)
Aug 17 18:13:46 16[ENC] parsed IKE_AUTH response 1 [ EF(8/11) ]
Aug 17 18:13:46 16[ENC] received fragment #8 of 11, waiting for complete IKE message
Aug 17 18:13:46 15[NET] received packet: from 103.254.155.4[4500] to 10.49.103.180[50250] (532 byt
es)
Aug 17 18:13:46 15[ENC] parsed IKE_AUTH response 1 [ EF(9/11) ]
Aug 17 18:13:46 15[ENC] received fragment #9 of 11, waiting for complete IKE message
Aug 17 18:13:46 12[NET] received packet: from 103.254.155.4[4500] to 10.49.103.180[50250] (532 byt
es)
Aug 17 18:13:46 12[ENC] parsed IKE_AUTH response 1 [ EF(10/11) ]
Aug 17 18:13:46 12[ENC] received fragment #10 of 11, waiting for complete IKE message
Aug 17 18:13:46 08[NET] received packet: from 103.254.155.4[4500] to 10.49.103.180[50250] (532 byt
es)
Aug 17 18:13:46 08[ENC] parsed IKE_AUTH response 1 [ EF(4/11) ]
Aug 17 18:13:46 08[ENC] received fragment #4 of 11, reassembling fragmented IKE message
Aug 17 18:13:46 08[ENC] parsed IKE_AUTH response 1 [ IDr CERT CERT AUTH EAP/REQ/ID ]
Aug 17 18:13:46 08[IKE] received end entity cert "C=MY, ST=Wilayah Persekutuan, L=Labuan, O=eVentu
re Limited, CN=*.hide.me"
Aug 17 18:13:46 08[IKE] received issuer cert "C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server
 CA"
Aug 17 18:13:46 08[CFG]   using certificate "C=MY, ST=Wilayah Persekutuan, L=Labuan, O=eVenture Li
mited, CN=*.hide.me"
Aug 17 18:13:46 08[CFG]   using untrusted intermediate certificate "C=US, O=DigiCert Inc, CN=DigiC
ert SHA2 Secure Server CA"
Aug 17 18:13:46 08[CFG] checking certificate status of "C=MY, ST=Wilayah Persekutuan, L=Labuan, O=
eVenture Limited, CN=*.hide.me"
Aug 17 18:13:46 08[LIB] building CRED_CERTIFICATE - OCSP_REQUEST failed, tried 0 builders
Aug 17 18:13:46 08[CFG] generating ocsp request failed
Aug 17 18:13:46 08[CFG] ocsp check failed, fallback to crl
Aug 17 18:13:46 08[CFG]   fetching crl from 'http://crl3.digicert.com/ssca-sha2-g5.crl' ...
Aug 17 18:13:47 08[CFG]   using certificate "C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server
CA"
Aug 17 18:13:47 08[CFG]   using trusted ca certificate "C=US, O=DigiCert Inc, OU=www.digicert.com,
 CN=DigiCert Global Root CA"
Aug 17 18:13:47 08[CFG]   reached self-signed root ca with a path length of 0
Aug 17 18:13:47 08[CFG]   crl correctly signed by "C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure S
erver CA"
Aug 17 18:13:48 08[CFG]   crl is valid: until Aug 24 01:00:00 2017
Aug 17 18:13:48 08[CFG] certificate status is good
Aug 17 18:13:48 08[CFG]   using trusted ca certificate "C=US, O=DigiCert Inc, OU=www.digicert.com,
 CN=DigiCert Global Root CA"
Aug 17 18:13:48 08[CFG] checking certificate status of "C=US, O=DigiCert Inc, CN=DigiCert SHA2 Sec
ure Server CA"
Aug 17 18:13:48 08[LIB] building CRED_CERTIFICATE - OCSP_REQUEST failed, tried 0 builders
Aug 17 18:13:48 08[CFG] generating ocsp request failed
Aug 17 18:13:48 08[CFG] ocsp check failed, fallback to crl
Aug 17 18:13:48 08[CFG]   fetching crl from 'http://crl3.digicert.com/DigiCertGlobalRootCA.crl' ..
.
Aug 17 18:13:48 08[CFG]   using trusted certificate "C=US, O=DigiCert Inc, OU=www.digicert.com, CN
=DigiCert Global Root CA"
Aug 17 18:13:48 08[CFG]   crl correctly signed by "C=US, O=DigiCert Inc, OU=www.digicert.com, CN=D
igiCert Global Root CA"
Aug 17 18:13:48 08[CFG]   crl is valid: until Sep 07 01:00:00 2017
Aug 17 18:13:48 08[CFG] certificate status is good
Aug 17 18:13:48 08[CFG]   reached self-signed root ca with a path length of 1
Aug 17 18:13:48 08[IKE] authentication of 'C=MY, ST=Wilayah Persekutuan, L=Labuan, O=eVenture Limi
ted, CN=*.hide.me' with RSA_EMSA_PKCS1_SHA2_512 successful
Aug 17 18:13:48 08[IKE] server requested EAP_IDENTITY (id 0x00), sending 's_lyh'
Aug 17 18:13:48 08[ENC] generating IKE_AUTH request 2 [ EAP/RES/ID ]
Aug 17 18:13:48 08[NET] sending packet: from 10.49.103.180[50250] to 103.254.155.4[4500] (96 bytes
)
Aug 17 18:13:48 09[NET] received packet: from 103.254.155.4[4500] to 10.49.103.180[50250] (128 byt
es)
Aug 17 18:13:48 09[ENC] parsed IKE_AUTH response 2 [ EAP/REQ/MSCHAPV2 ]
Aug 17 18:13:48 09[IKE] server requested EAP_MSCHAPV2 authentication (id 0x01)
Aug 17 18:13:48 09[ENC] generating IKE_AUTH request 3 [ EAP/RES/MSCHAPV2 ]
Aug 17 18:13:48 09[NET] sending packet: from 10.49.103.180[50250] to 103.254.155.4[4500] (160 byte
```

```
s)
Aug 17 18:13:49 11[NET] received packet: from 103.254.155.4[4500] to 10.49.103.180[50250] (144 byt
es)
Aug 17 18:13:49 11[ENC] parsed IKE_AUTH response 3 [ EAP/REQ/MSCHAPV2 ]
Aug 17 18:13:49 11[IKE] EAP-MS-CHAPv2 succeeded: '(null)'
Aug 17 18:13:49 11[ENC] generating IKE_AUTH request 4 [ EAP/RES/MSCHAPV2 ]
Aug 17 18:13:49 11[NET] sending packet: from 10.49.103.180[50250] to 103.254.155.4[4500] (96 bytes
)
Aug 17 18:13:50 17[NET] received packet: from 103.254.155.4[4500] to 10.49.103.180[50250] (96 byte
s)
Aug 17 18:13:50 17[ENC] parsed IKE_AUTH response 4 [ EAP/SUCC ]
Aug 17 18:13:50 17[IKE] EAP method EAP_MSCHAPV2 succeeded, MSK established
Aug 17 18:13:50 17[IKE] authentication of 's_lyh' (myself) with EAP
Aug 17 18:13:50 17[ENC] generating IKE_AUTH request 5 [ AUTH ]
Aug 17 18:13:50 17[NET] sending packet: from 10.49.103.180[50250] to 103.254.155.4[4500] (160 byte
s)
Aug 17 18:13:50 16[NET] received packet: from 103.254.155.4[4500] to 10.49.103.180[50250] (368 byt
es)
Aug 17 18:13:50 16[ENC] parsed IKE_AUTH response 5 [ AUTH CPRP(ADDR DNS DNS) SA TSi TSr N(AUTH_LFT
) N(MOBIKE_SUP) N(ADD_4_ADDR) N(ADD_4_ADDR) ]
Aug 17 18:13:50 16[IKE] authentication of 'C=MY, ST=Wilayah Persekutuan, L=Labuan, O=eVenture Limi
ted, CN=*.hide.me' with EAP successful
Aug 17 18:13:50 16[IKE] IKE_SA android[2] established between 10.49.103.180[s_lyh]...103.254.155.4
[C=MY, ST=Wilayah Persekutuan, L=Labuan, O=eVenture Limited, CN=*.hide.me]
Aug 17 18:13:50 16[IKE] scheduling rekeying in 35581s
Aug 17 18:13:50 16[IKE] maximum IKE_SA lifetime 36181s
Aug 17 18:13:50 16[IKE] installing DNS server 103.254.155.3
Aug 17 18:13:50 16[IKE] installing DNS server 103.254.155.5
Aug 17 18:13:50 16[IKE] installing new virtual IP 10.3.208.96
Aug 17 18:13:50 16[IKE] CHILD_SA android{2} established with SPIs de78f9fe_i c325e6f8_o and TS 10.
3.208.96/32 === 0.0.0.0/0 ::/0
Aug 17 18:13:50 16[DMN] setting up TUN device for CHILD_SA android{2}
Aug 17 18:13:50 16[DMN] successfully created TUN device
Aug 17 18:13:50 16[IKE] received AUTH_LIFETIME of 86400s, scheduling reauthentication in 85800s
Aug 17 18:13:50 16[IKE] peer supports MOBIKE
Aug 17 18:13:50 08[IKE] sending address list update using MOBIKE
Aug 17 18:13:50 08[ENC] generating INFORMATIONAL request 6 [ N(NO_ADD_ADDR) ]
Aug 17 18:13:50 08[NET] sending packet: from 10.49.103.180[50250] to 103.254.155.4[4500] (96 bytes
)
Aug 17 18:13:50 13[NET] received packet: from 103.254.155.4[4500] to 10.49.103.180[50250] (96 byte
s)
Aug 17 18:13:50 13[ENC] parsed INFORMATIONAL response 6 [ ]
Aug 17 18:13:52 00[IKE] deleting IKE_SA android[2] between 10.49.103.180[s_lyh]...103.254.155.4[C=
MY, ST=Wilayah Persekutuan, L=Labuan, O=eVenture Limited, CN=*.hide.me]
Aug 17 18:13:52 00[IKE] sending DELETE for IKE_SA android[2]
Aug 17 18:13:52 00[ENC] generating INFORMATIONAL request 7 [ D ]
Aug 17 18:13:52 00[NET] sending packet: from 10.49.103.180[50250] to 103.254.155.4[4500] (96 bytes
)
```

The system builtin traffic counter shows that every time strongswan starts a connection, it consumes 0.7MB data. Which is matching the size of CRL file.

Associated revisions

Revision 0bebbae9 - 04.09.2017 10:41 - Tobias Brunner

android: Cache CRLs in app directory

Fixes #2405.

History

#1 - 17.08.2017 12:46 - Tobias Brunner

- Status changed from New to Feedback

- Assignee set to Tobias Brunner

Yes, that's a known issue. Will probably be fixed in the next update of the app.

#2 - 04.09.2017 11:30 - Tobias Brunner

- Status changed from Feedback to Closed

- Resolution set to Fixed